HOW TO DO A p-DESCENT ON AN ELLIPTIC CURVE

EDWARD F. SCHAEFER AND MICHAEL STOLL

Abstract. In this paper, we describe an algorithm that reduces the computation of the (full) p-Selmer group of an elliptic curve E over a number field to standard number field computations like determining the (p-torsion of) the S-class group and a basis of the S-units modulo pth powers for a suitable set S of primes. In particular, we give a result reducing this set S of 'bad primes' to a very small set, which in many cases only contains the primes above p. As of today, this provides a feasible algorithm for performing a full 3-descent on an elliptic curve over $\mathbb{Q}$, but the range of our algorithm will certainly be enlarged by future improvements in computational algebraic number theory. When the Galois module structure of $E[p]$ is favorable, simplifications are possible and p-descents for larger p are accessible even today. To demonstrate how the method works, several worked examples are included.

1. Introduction

The art of performing 2-descents on elliptic curves has reached a considerable level of maturity. For curves over the rational numbers, John Cremona's `mwrank` program (see the description in [7]) has become the standard means of determining the 2-Selmer group and (if there is no obstruction) the Mordell-Weil rank; it performs very well on most 'real life' elliptic curves. Cremona's approach goes back to Birch and Swinnerton-Dyer; it uses the fairly concrete description of the 2-Selmer group as the set of equivalence classes of certain so-called 2-coverings, genus 1 curves over the base field that allow certain maps to the elliptic curve. Although this works very well for 2-descents over the rationals, it suffers from combinatorial explosion when the base field is enlarged, when higher p-descents are attempted, or even when the elliptic curve is 'large'.

There is an alternative method, going back to Mordell [19] and Weil [32]. It is based on the cohomological description of the Selmer group and represents it as a finite subgroup of $L^\times/(L^\times)^2$, where L is (usually) a degree 3 field extension of the base field. This method avoids the combinatorial problems of the first

Date: June 13, 2001.

1991 *Mathematics Subject Classification.* Primary 11G05; Secondary 14H25, 14H52, 14Q05.

Key words and phrases. elliptic curve over number field, p-descent, Selmer group, Mordell-Weil rank, Shafarevich-Tate group.

We are indebted to Claus Fieker for his invaluable help in getting KANT to produce a basis for the group $A(S,5)^{(1)}$ needed in the example in Section 11.2. We thank John Cremona, Zafer Djabri, Everett Howe, Hendrik W. Lenstra Jr., Karl Rubin, Nigel Smart and Don Zagier for useful and interesting discussions. The first author is supported by National Security Agency grant MDA904-99-1-0013.

approach, but it requires a thorough knowledge of the arithmetic of L. Thanks to the rapid progress in Algorithmic Algebraic Number Theory, these computations have become feasible for fields of larger and larger degree. This method already performs quite well for curves over the rationals, including fairly 'large' ones (see Djabri and Smart [10] for a comparison; they call the first method 'indirect' and the second, 'direct'). It also has been applied to determine the rank of several elliptic curves over number fields. Simon [28, 29] has a general description of the algorithm and worked examples, Bruin [3] and Flynn and Wetherell [14] use the method for the (somewhat simpler) descent via 2-isogeny. We will call this method the 'number field method' (as opposed to the 'homogeneous spaces method' used by Cremona).

Let E/K be an elliptic curve over a number field K and recall the usual exact sequence related to an m-descent,

$$0 \longrightarrow E(K)/mE(K) \longrightarrow \mathrm{Sel}^{(m)}(K,E) \longrightarrow Ш(K,E)[m] \longrightarrow 0\,.$$

We have seen that we are able to find the middle term for $m = 2$ in many cases, enabling us to bound the Mordell-Weil rank, and to determine it when $Ш(K,E)[2] = 0$. There are now several reasons why it is desirable to compute the m-Selmer group for values of m other than 2. The first is that we want to go around the obstruction $Ш(K,E)[2]$ for the determination of the rank. The second is that the knowledge of several Selmer groups for distinct values of m lets us deduce facts about the Shafarevich-Tate group $Ш(K,E)$. Selmer groups for arbitrary m are also of interest in Iwasawa theory as well as in the study of visible parts of Shafarevich-Tate groups (see Cremona and Mazur [8]).

There are two ways of doing such 'higher descents'. One possibility is to extend a given 2-descent computation to produce a 4-descent. This allows us to find the image of the 4-Selmer group inside the 2-Selmer group, or equivalently, to determine $Ш(K,E)[2]/2Ш(K,E)[4]$. For two different explicit descriptions of how to do a 4-descent, see Cassels [6] and Merriman, Siksek and Smart [18].

If we want to obtain information on p-primary parts of $Ш(K,E)$ with $p \neq 2$, we have to take the other direction, and that is to try and do a p-descent. In his paper [25], the first author has shown how to generalize the number field method to apply to a number of situations. (It should be noted that some special cases other than 2-descent for elliptic curves had been known before, see for example Faddeev [12], McCallum [17] or Top [31]. For recent work dealing with special cases of descent on elliptic curves, see also the theses of Dokchitser [11] and Fisher [13].) Djabri, Schaefer and Smart [9] have shown that the method should apply to perform a p-descent on an elliptic curve for an arbitrary odd prime p. To be precise, they show that there is an injective homomorphism

$$\bar{w} : H^1(K, E[p]) \quad\longrightarrow\quad A^\times/(A^\times)^p$$

(where A is an étale K-algebra depending functorially on K), which is the main condition that has to be satisfied to make the method work. In order to be able to compute the p-Selmer group, one needs in addition to know the image of $\bar{w}$. This image was not determined in [9], and therefore the authors could only describe how to compute a group Z containing the Selmer group.

The main purpose of this paper is to close this gap. We give a precise characterization of the image of H^1 in Section 7 and derive an algorithm that is guaranteed to compute the p-Selmer group. Our algorithm gives a feasible reduction of the p-descent on an elliptic curve to standard computations in number fields. Since we can expect progress on the latter, p-descent computations will become more and more feasible. Given the current state of the art in dealing with number fields, the only computations which are feasible at the moment are for the special case $p = 3$ over the base field $\mathbb{Q}$ (though this will certainly change). For this case we give a very explicit description of the algorithm in Section 10. This 3-descent algorithm has been implemented by the second author in MAGMA [16], and proved to work quite well on a number of (admittedly small) examples.

As a by-product of our results, we can deduce that the group Z in [9] is actually equal to the p-Selmer group, thereby providing a justification of the algorithm given there. (It should be noted, however, that the algorithm given here requires local computations only at a few bad primes, whereas the algorithm in [9] requires doing a lot of computations at a set of good primes that is often difficult to determine.)

Note also that we give a quite general result on the set of 'bad primes' that have to be considered in a p-descent. It says that it suffices to consider primes above p, together with primes such that the corresponding Tamagawa number of the elliptic curve (or one of the two curves involved in case of a descent by p-isogeny) is divisible by p, see Prop. 4.6. Since Tamagawa numbers are rarely large, this leads to a considerable improvement in the efficiency of the algorithm. We can simplify the computation of the p-Selmer group in the case that p splits in the endomorphism ring of E. In section 8 we give an algorithm for this special case. When the elliptic curve has a rational p-isogeny $h : E \to E'$, we can use Selmer groups related to h and the dual isogeny instead of the p-Selmer group. The computation is considerably simpler and is described in section 9.

We finish with four examples featuring computations of the various Selmer groups we describe. In the first, we use a 3-Selmer group to determine the Mordell-Weil rank of an elliptic curve which can not be determined from the analytic rank nor from the 2-Selmer group. In the second, we find the 5-Selmer group of an elliptic curve in which 5 splits in the endomorphism ring. In the third and fourth, we find h-Selmer groups of elliptic curves where the two h's are isogenies of degrees 3 and 13, respectively.

2. Notation

Throughout this paper, p will be a fixed odd prime number.

We let E be an elliptic curve over a number field K. The point at infinity on E (with respect to some Weierstrass model) is denoted O when it is considered as a point on the curve E; it is denoted 0 when it is considered as the identity in the group E. When we are dealing with explicit formulas, we will assume that E is given by an equation of the form

$$E : y^2 = x^3 + a\,x + b\,,$$

where a and b are in $\mathcal{O}_K$, the integers of K. This is done to keep explicit formulas simple. It is no problem to use more general Weierstrass equations in a practical implementation.

The groups $\mathrm{GL}(2, \mathbb{F}_p)$, $\mathrm{SL}(2, \mathbb{F}_p)$, $\mathrm{PSL}(2, \mathbb{F}_p)$ are the usual ones. The 2-by-2 identity matrix is denoted I.

The following notation will be used when we are working with the multiplication-by-p map. We let $K(E[p])$ be the field obtained from K by adjoining the coordinates of all p-torsion points on E. It is a Galois extension of K. When we choose a basis for the $\mathbb{F}_p$-vector space $E[p]$, the group $\mathrm{Gal}(K(E[p])/K)$ is identified with a subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$.

There is the Weil pairing $e_p : E[p] \times E[p] \longrightarrow \mu_p$, a perfect, alternating, Galois-equivariant pairing of $E[p]$ with itself into the pth roots of unity, μ_p. The fact that e_p is alternating implies that the action of $\mathrm{Gal}(K(E[p])/K)$ on μ_p is given by the determinant of the corresponding 2-by-2 matrix.

Any finite-dimensional $\mathbb{F}_p$-vector space M with (linear) $\mathrm{GL}(2, \mathbb{F}_p)$-action splits as a representation of the center $Z = \mathbb{F}_p^\times I$ of $\mathrm{GL}(2, \mathbb{F}_p)$ into a direct sum

$$M = M^{(0)} \oplus M^{(1)} \oplus \cdots \oplus M^{(p-2)}$$

of subspaces, where $M^{(\nu)}$ (for $\nu \in \mathbb{Z}/(p-1)\mathbb{Z}$) is the subspace of M on which a matrix αI (with $\alpha \in \mathbb{F}_p^\times$) acts as multiplication by α^ν. This direct sum decomposition is compatible with the GL(2)-action. In particular, the action on $E[p]$ is the standard one, so $E[p] = E[p]^{(1)}$. The action on μ_p is via the determinant, so $\mu_p = \mu_p^{(2)}$. Finally, $\mathbb{Z}/p\mathbb{Z}$ will denote a one-dimensional space with trivial action, so $\mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/p\mathbb{Z})^{(0)}$. We let $E[p]^\vee = \mathrm{Hom}(E[p], \mathbb{Z}/p\mathbb{Z})$, with the induced GL(2)-action. In particular, $E[p]^\vee = (E[p]^\vee)^{(-1)}$. Note also that it suffices to specify the action of gI, where g is a primitive root mod p, in order to define $M^{(\nu)}$.

Now assume E has a K-rational isogeny h of degree p onto E'. Let h' denote the dual isogeny, defined over K, from E' to E. There is the Weil pairing $e_h : E[h] \times E'[h'] \longrightarrow \mu_p$. When we choose a basis for the $\mathbb{F}_p$-vector space $E[h]$, the group $\mathrm{Gal}(K(E[h])/K)$ is identified with a subgroup of $\mathrm{GL}(1, \mathbb{F}_p) = \mathbb{F}_p^\times$. As before, any finite-dimensional $\mathbb{F}_p$-vector space M with (linear) $\mathrm{GL}(1, \mathbb{F}_p)$-action splits into a direct sum

$$M = M^{(0)} \oplus M^{(1)} \oplus \cdots \oplus M^{(p-2)}$$

of subspaces, where $M^{(\nu)}$ (for $\nu \in \mathbb{Z}/(p-1)\mathbb{Z}$) is the subspace of M on which $\alpha \in \mathbb{F}_p^\times$ acts as multiplication by α^ν.

We use the usual convention to denote Galois cohomology groups — $H^j(K, M)$ is an abbreviation for $H^j(G_K, M)$, where G_K is the absolute Galois group of K. When S is a finite set of places of K, then $H^j(K, M; S)$ denotes the subgroup of $H^j(K, M)$ of cocycle classes unramified at the finite places outside S (i.e., those classes that become trivial under restriction to $H^j(K_S, M)$, where K_S is the maximal extension of K that is unramified at the finite places outside S).

When X is a set with Galois action and M is a Galois module, $\mathrm{Map}(X, M)$ denotes the Galois module of maps from X into M.

3. Étale algebras

An *étale algebra* D over an infinite[1] field K is a K-algebra of the form $D = K[T]/(f(T))$, where $f(T) \in K[T]$ is a monic polynomial with non-zero discriminant. Such an algebra decomposes uniquely into a direct product of finite separable field extensions of K, i.e., $D \cong \prod_{i=1}^{m} D_i$. When K is a number field and S is a finite set of places of K, we define

$$D(S, p) = \{\alpha \in D^\times/(D^\times)^p \mid \alpha \text{ unramified outside } S\} = \prod_{i=1}^{m} D_i(S, p)\,.$$

Here α is called unramified outside S when all the extensions $D_j(\sqrt[p]{\alpha_j})$ are unramified at all primes of D_j lying above a place outside of S; $(\alpha_1, \dots, \alpha_m)$ is a representative of α, split into its components according to the splitting of D into number fields.

We write $\bar{D} = D \otimes_K \bar{K}$ with $\bar{K}$ a separable closure of K. A straightforward generalization of Hilbert's Theorem 90 shows that $H^1(K, \bar{D}^\times) = 0$. By the usual Kummer sequence, this implies $H^1(K, \mu_p(\bar{D})) \cong D^\times/(D^\times)^p$.

A more abstract definition of an étale algebra is that it is the affine algebra corresponding to a finite étale scheme X over K. When we look at it this way, $\bar{D}$ consists of functions from the points $X(\bar{K})$ into $\bar{K}$, and D is the subset of Galois-invariant functions (the Galois group acts both on the points and on the values). Similarly, $D^\times$ consists of Galois-invariant functions into $\bar{K}^\times$, and $\mu_p(\bar{D})$ consists of functions into μ_p. We will use this interpretation frequently in what follows.

In this setting, we get an anti-equivalence of categories between the category of finite G_K-sets and the category of étale algebras over K.

4. Computing a Selmer group. Theory

In this section, we give a general outline for the computation of a Selmer group. A good account of the theoretical background is given in Silverman's book [27, §X.4]. Let θ denote an isogeny from E to E' over K whose kernel has exponent p.

[1] In general, we can define an étale algebra over an arbitrary field K to be a finite product of finite separable field extensions of K. If K is finite, it is not always possible to find a polynomial f defining the algebra.

Recall the definition of the θ-Selmer group. There is the standard diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & E'(K)/\theta E(K) \arrow[r, "\delta_\theta"] \arrow[d] & H^1(K,E[\theta]) \arrow[r] \arrow[d, "\prod_v \mathrm{res}_v"] \arrow[dr, "\alpha"] & H^1(K,E)[\theta] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v E'(K_v)/\theta E(K_v) \arrow[r, "\prod_v \delta_{\theta,v}"] & \prod_v H^1(K_v,E[\theta]) \arrow[r] & \prod_v H^1(K_v,E)[\theta] \arrow[r] & 0
\end{tikzcd}$$

(the products in the bottom row are over all places v of K). Then $\mathrm{Sel}^{(\theta)}(K,E)$ is defined to be the kernel of α, or equivalently, the subgroup of $H^1(K,E[\theta])$ of elements mapping under every restriction map res_v into the image of $E'(K_v)/\theta E(K_v)$ in $H^1(K_v,E[\theta])$.

There is a finite description of $\mathrm{Sel}^{(\theta)}(K,E)$. Let I_v denote the inertia subgroup of G_{K_v}. The unramified subgroup of $H^1(K_v,E[\theta])$ is the kernel of the restriction map to $H^1(I_v,E[\theta])$.

Lemma 4.1. *If v is infinite then $E'(K_v)/\theta E(K_v)$ and the unramified subgroup of $H^1(K_v,E'[\theta])$ are both trivial.*

Proof: Trivial. (Recall that the degree of θ is odd.) □

Lemma 4.2. *The size of the unramified subgroup of $H^1(K_v,E[\theta])$ is the same as the size of $E(K_v)[\theta]$.*

Proof: The kernel of the restriction map $H^1(G_{K_v},E[\theta]) \to H^1(I_v,E[\theta])$ is isomorphic to $H^1(\mathrm{Gal}(K_v^{\mathrm{unr}}/K_v),E(K_v^{\mathrm{unr}})[\theta])$, where K_v^{unr} is the maximal unramified extension of K_v. Let Fr_v denote the Frobenius element of $\mathrm{Gal}(K_v^{\mathrm{unr}}/K_v)$. The latter cohomology group is isomorphic to the cokernel of $\mathrm{Fr}_v - 1$ on $E(K_v^{\mathrm{unr}})[\theta]$ and therefore has the same size as the kernel $E(K_v)[\theta]$ of $\mathrm{Fr}_v - 1$. □

Let E be defined by a minimal Weierstrass equation over K_v, and let $E_0(K_v)$ denote the points with non-singular reduction. Equivalently, $E_0(K_v)$ is isomorphic to the group of sections from $\mathcal{O}_{K_v}$ to the open subgroup scheme of the Néron model of $E/\mathcal{O}_{K_v}$ gotten by removing the non-identity components of the special fiber.

Lemma 4.3. *Assume v does not lie over p. Let $R \in E_0'(K_v)$. Then the image of R in $H^1(K_v,E[\theta])$ is unramified.*

Proof: Let k_v denote the residue class field of K_v, and denote by E_1 and E_1' the kernels of reduction. Note that $E_0'(K_v)$ is contained in $E_0'(K_v^{\mathrm{unr}})$. We show that $E_0'(K_v^{\mathrm{unr}})/\theta E_0(K_v^{\mathrm{unr}})$ is trivial. To see this, consider the following diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & E_1(K_v^{\mathrm{unr}}) \arrow[r] \arrow[d, "\theta"] & E_0(K_v^{\mathrm{unr}}) \arrow[r] \arrow[d, "\theta"] & E(\bar{k}_v)^{\mathrm{ns}} \arrow[r] \arrow[d, "\theta"] & 0 \\
0 \arrow[r] & E_1'(K_v^{\mathrm{unr}}) \arrow[r] & E_0'(K_v^{\mathrm{unr}}) \arrow[r] & E'(\bar{k}_v)^{\mathrm{ns}} \arrow[r] & 0
\end{tikzcd}$$

Here the superscript ns denotes the smooth part of the reduction. The rightmost vertical map is surjective since $\bar{k}_v$ is algebraically closed. The leftmost vertical map is surjective since the kernels of reduction are pro-q groups with $q \neq p$. Hence the middle vertical map is also surjective.

The following diagram commutes.

$$\begin{tikzcd}
E_0'(K_v)/\theta E_0(K_v) \arrow[r, "\delta_v"] \arrow[d] & H^1(K_v, E[\theta]) \arrow[d, "\mathrm{res}"] \\
E_0'(K_v^{\mathrm{unr}})/\theta E_0(K_v^{\mathrm{unr}}) \arrow[r, "\delta_v"] & H^1(K_v^{\mathrm{unr}}, E[\theta])
\end{tikzcd}$$

Since the lower left group is trivial, the image of the upper left group in the lower right group must be trivial. By definition, this means that its image in the upper right group is unramified. □

We remark that one can extend this proof to show that the image of $E'(K_v)$ in $H^1(I_v, E[\theta])$ is isomorphic to the image of $\Phi'(k_v)$ in $\Phi'/\theta\Phi$. Here we use Φ' to denote $E'(K_v^{\mathrm{unr}})/E_0'(K_v^{\mathrm{unr}})$, the component group of the Néron model, and $\Phi'(k_v)$ denotes the subgroup fixed under the action of Frobenius. (Similarly for E and Φ.) This provides an alternative way to prove Lemma 4.5 below.

Let $c_{E,v} = \#E(K_v)/E_0(K_v) = \#\Phi(k_v)$. This is often called the Tamagawa number. The only possible primes at which the Tamagawa number is not 1 are those dividing the conductor of E.

Lemma 4.4. *Assume v does not lie over p. Then the size of $E'(K_v)/\theta E(K_v)$ is*

$$\frac{\#E(K_v)[\theta] \cdot c_{E',v}}{c_{E,v}}.$$

Proof: See [24, Lemma 3.8]. □

Lemma 4.5. *Assume that v does not lie over p and that $c_{E,v}$ and $c_{E',v}$ are not divisible by p. Then the image of $E'(K_v)/\theta E(K_v)$ in $H^1(K_v, E[\theta])$ is equal to the unramified subgroup.*

Proof: Since $c_{E,v}$ and $c_{E',v}$ are not divisible by p and the exponent of $E[\theta]$ is p, they must be the same. From Lemmas 4.2 and 4.4, the image and the unramified subgroup have the same size. So it suffices to prove that the image is contained in the unramified subgroup. Since $c_{E,v}$ and $c_{E',v}$ are not divisible by p, the map from $E_0'(K_v)/\theta E_0(K_v)$ to $E'(K_v)/\theta E(K_v)$ is an isomorphism. So from Lemma 4.3, the image of $E'(K_v)/\theta E(K_v)$ is unramified. □

Proposition 4.6. Let S be any finite set of places containing the places above p and the places v such that at least one of $c_{E,v}$ and $c_{E',v}$ is divisible by p. Then

$$\mathrm{Sel}^{(\theta)}(K, E) = \{\xi \in H^1(K, E[\theta]; S) \mid \mathrm{res}_v(\xi) \in \delta_{\theta,v}(E'(K_v)/\theta E(K_v)) \text{ for all } v \in S\}.$$

Proof: This follows from Lemmas 4.1 and 4.5. □

5. Computing a Selmer group. Practice

In order to implement this description, we need a practical representation of the a priori rather abstractly defined group $H^1(K, E[\theta]; S)$ and the maps δ_v. Our approach (based on [25]) is to identify the cohomology group with a subgroup of $D(S, p)$ for a suitable étale algebra D over K. It will turn out that the coboundary maps δ_v can then be realized as polynomial (or rational) functions on E with values in D_v.

This leaves the task of determining a basis of $D(S, p)$. Thanks to the advances in the computational theory of number fields, this is now feasible in many cases. In practical terms we have to find a basis of the group U_S of S-units of D (or of a subgroup of finite index prime to p) and of the S-class group $\mathrm{Cl}_S(D)$. (Both of these groups are defined component-wise in terms of the splitting of D as a product of number fields.) We then obtain a basis for $D(S, p)$ from the exact sequence

$$0 \longrightarrow U_S/U_S^p \longrightarrow D(S,p) \longrightarrow \mathrm{Cl}_S(D)[p] \longrightarrow 0\,,$$

compare [21, Prop. 12.6].

Now let us proceed to find a suitable algebra D. Let θ' denote the dual isogeny over K from E' to E. Let X be a Galois-invariant subset of $E'[\theta'] \setminus \{0\}$ spanning $E'[\theta']$, and let D be the étale K-algebra corresponding to X, considered as a finite étale subscheme of E'. Recall that we interpret elements of D as functions on X.

Let w_θ denote the map from $E[\theta]$ to $\mu_p(\bar{D})$ which sends R to the function $P \mapsto e_\theta(R, P)$. Since X is a spanning set of $E'[\theta']$, the map w_θ is injective. Let $\bar{w}_\theta$ denote the induced map from $H^1(K, E[\theta])$ to $H^1(K, \mu_p(\bar{D}))$. Let k denote the Kummer isomorphism from $H^1(K, \mu_p(\bar{D}))$ to $D^\times/(D^\times)^p$. The image of $H^1(K, E[\theta]; S)$ under $k \circ \bar{w}_\theta$ is contained in $D(S, p)$.

For the method to work, the following two conditions on X have to be satisfied.

(i) The map $\bar{w}_\theta$ must be injective both globally and locally (i.e., over K_v).
(ii) We must be able to find the image of $H^1(K, E[\theta]; S)$ in $D(S, p)$.

In the cases we present, we will verify both conditions. For the following general discussion, we simply assume them.

We now find a nice description of the composition $k \circ \bar{w}_\theta \circ \delta_\theta$. For each $P \in X$, choose a function f_P in $K(P)(E')$ with the property that $\mathrm{div}(f_P) = p\,P - p\,O$ and such that for $\sigma \in G_K$ we have $\sigma f_P = f_{\sigma P}$. Let F be the rational function from E' to $\bar{D}$ which sends a point R to the function $P \mapsto f_P(R)$. Put differently, we choose $F \in D(E')$ such that $\mathrm{div}(F)$ corresponds to the function $X \to \mathrm{Div}_{E'}(\bar{K})$ given by $P \mapsto p\,P - p\,O$.

We call a degree-0 divisor on E' *good* if it is defined over K and its support avoids $X \cup \{O\}$. Since E' has a K-rational point, every element of $E'(K)$ can be represented by a good divisor. We can evaluate F on a good K-rational divisor $\sum_j n_j Q_j$ to get $\prod_j F(Q_j)^{n_j} \in D^\times$. By evaluating on good divisors, the function F induces a well-defined map from $E'(K)/\theta E(K)$ to $D^\times/(D^\times)^p$, which is the same as $k \circ \bar{w}_\theta \circ \delta_\theta$ (see [25, Thm. 2.3]).

For a place v of K, define $D_v = D \otimes_K K_v$. The map F then induces a map F_v from $E'(K_v)/\theta E(K_v)$ to $D_v^\times/(D_v^\times)^p$. The maps F and F_v are injective by our assumptions.

We can now reformulate how we compute the Selmer group. Consider the following diagram.

$$\begin{tikzcd}
E'(K)/\theta E(K) \arrow[r, "F"] \arrow[d] & D(S,p) \arrow[d, "\prod_v \mathrm{res}_v"] \\
\prod_{v\in S} E'(K_v)/\theta E(K_v) \arrow[r, "\prod_v F_v"] & \prod_{v\in S} D_v^\times/(D_v^\times)^p
\end{tikzcd}$$

We have

$$\begin{aligned}\mathrm{Sel}^{(\theta)}(K,E) = \{\alpha \in (&\text{image of } H^1(K,E[\theta];S) \text{ in } D(S,p)) \mid \\ &\mathrm{res}_v(\alpha) \in F_v(E'(K_v)/\theta E(K_v)) \text{ for all } v \in S\}\,.\end{aligned} \tag{5.1}$$

Let us outline an algorithm. Assume $D \cong \prod_{i=1}^m D_i$ where the D_i's are number fields, corresponding to the G_K-orbits in X. For $1 \le i \le m$, choose some $P_i \in X$ in the orbit corresponding to D_i (so that $D_i = K(P_i)$) and let $f_i = f_{P_i}$.

1. Determine S, the (finite) set of places of K consisting of the places above p and the places for which at least one of $c_{E,v}$ and $c_{E',v}$ is divisible by p.
2. Choose a K-defined function ϕ on E' that is defined on all of X and such that it does not take the same value on any two points in X (in most cases, the y-coordinate will do). We can then use $\varphi(T) = \prod_{P\in X}(T - \phi(P))$ as the polynomial defining D. Each factor of $\varphi(T)$ over K will define one of the D_i's.
3. Find the S-unit and S-class groups of each D_i and construct $D_i(S,p)$ (see [21, pp. 171–172]). We have $D(S,p) = \prod_{i=1}^m D_i(S,p)$.
4. Determine the subgroup of $D(S,p)$ that is the image of $H^1(K,E[\theta];S)$ and denote it T_1 (see Sections 7 through 9).
5. Determine the function F, as described below.
6. For each $v \in S$, compute the local image $F_v(E'(K_v)) \subset D_v^\times/(D_v^\times)^p$, as described below.
7. Let $T \subset T_1$ be the subgroup of elements mapping into $F_v(E'(K_v))$ under the map $\mathrm{res}_v : D^\times/(D^\times)^p \longrightarrow D_v^\times/(D_v^\times)^p$ for all $v \in S$.
8. Finally, the Selmer group $\mathrm{Sel}^{(\theta)}(K,E)$ is isomorphic to T.

Let us expand on steps 5 and 6. By abuse of notation, we can take $F = \prod_{i=1}^m f_i$ as the map from $E'(K)/\theta E(K)$ to $\prod_{i=1}^m D_i^\times/(D_i^\times)^p$ and also $F_v = \prod_{i=1}^m f_{i,v}$ from $E'(K_v)/\theta E(K_v)$ to $\prod_{i=1}^m D_{i,v}^\times/(D_{i,v}^\times)^p$, where $D_{i,v} = D_i \otimes_K K_v$. For an algorithm to construct the f_i's see [9, §2]. The particular representation of an f_i in that article can vanish or be undefined at points outside $X \cup \{O\}$. Those other points (which are always in $E'[p]$) must also be avoided in the supports of the divisors representing $E'(K_v)/\theta E(K_v)$ on which F will be evaluated. In other words, we may have to restrict the notion of good divisors over K_v.

In order to find the image $F_v(E'(K_v))$ in $D_v^\times/(D_v^\times)^p$, we need to know the size of $E'(K_v)/\theta E(K_v)$. If v does not lie over p, then this is given in Lemma 4.4. If v

does lie over p and $\theta = p$, then

$$\#E(K_v)/pE(K_v) = p^{[K_v:\mathbb{Q}_p]} \cdot \#E(K_v)[p]$$

(see [25, Prop. 2.4]). If v lies over p and θ is a p-isogeny, then

$$\#E'(K_v)/\theta E(K_v) = \frac{\gamma \cdot \#E(K_v)[\theta] \cdot c_{E',v}}{c_{E,v}}$$

where γ is the norm of the leading coefficient of the power series representation of θ on formal groups (see [24, p. 92]). This computation with formal groups can sometimes be avoided by combining the result for $\#E(K_v)/pE(K_v)$ and the exact sequence (9.1).

Once we know the size of $E'(K_v)/\theta E(K_v)$, we search for good divisors (here defined over K_v) whose classes span the group. Since F_v is injective by assumption, it is typically easier to determine the independence of such divisors by looking at their images in $D_v^\times/(D_v^\times)^p$. Though in practice, finding good divisors that span $E'(K_v)/\theta E(K_v)$ is usually not difficult, a deterministic algorithm could be modeled on that found in [30].

6. Full p-descent. Condition (i)

In this and the following two sections, we consider the situation where θ is the multiplication-by-p map on E. We begin with deriving a sufficient condition on X for condition (i) in Section 5 to hold.

Some standard references for the group cohomology needed are [1] and [2].

Lemma 6.1. *Let $M_1 \longrightarrow M_2$ be a monomorphism of finite-dimensional $\mathbb{F}_p$-vector spaces with linear action by a subgroup $G \subset \mathrm{GL}(2, \mathbb{F}_p)$. We assume that a scalar matrix $\alpha I \in G$ acts as multiplication by α on M_1. Then the induced map*

$$H^1(\Gamma, M_1) \longrightarrow H^1(\Gamma, M_2)$$

is injective for all subgroups $\Gamma \subset G$, if either $p \nmid \#G$ or $H^1(W, M_1) \longrightarrow H^1(W, M_2)$ is injective, where W is a p-Sylow subgroup of G.

Proof: (See also [9].) We divide the set of subgroups Γ of $\mathrm{GL}(2, \mathbb{F}_p)$ into three classes.

1. The order of Γ is prime to p. Then $H^1(\Gamma, M_1) = 0$, and the assertion holds trivially.
2. Γ contains a p-Sylow subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ as a normal subgroup. Conjugating if necessary, we may assume that Γ contains W as a normal subgroup. Since the order of Γ/W is prime to p, the usual inflation-restriction sequence tells us that $H^1(\Gamma, M_j) = H^1(W, M_j)^{\Gamma/W}$. By assumption, $H^1(W, M_1) \longrightarrow H^1(W, M_2)$ is injective, and this is not affected when we restrict to Γ/W-invariants.
3. In the remaining case, Γ contains $\mathrm{SL}(2, \mathbb{F}_p)$ (see [26, Prop. 15]), which must then be normal in Γ. In this case, Γ contains $-I$, which acts as

multiplication by -1 on M_1. Hence $M_1^{\langle -I\rangle} = 0$, and we get from the inflation-restriction sequence

$$0 = H^1(\mathrm{PSL}(2,\mathbb{F}_p), M_1^{\langle -I\rangle}) \longrightarrow H^1(\mathrm{SL}(2,\mathbb{F}_p), M_1) \longrightarrow H^1(\langle -I\rangle, M_1) = 0$$

that $H^1(\mathrm{SL}(2,\mathbb{F}_p), M_1) = 0$. As in case 2, we then also have $H^1(\Gamma, M_1) = 0$, and the injectivity holds trivially.

□

Corollary 6.2. Let $M_1 \to M_2$ be a monomorphism of K-Galois modules with Galois action factoring through a linear action of $G \subset \mathrm{GL}(2,\mathbb{F}_p)$. We assume that $\alpha I \in G$ acts as multiplication by α on M_1. If either $p \nmid \#G$ or the map $H^1(W, M_1) \to H^1(W, M_2)$ is injective, where $W \subset G$ is a p-Sylow subgroup, then the map on Galois cohomology, $H^1(L, M_1) \to H^1(L, M_2)$, is also injective for all field extensions L/K.

Proof: Let K' be the smallest Galois extension of K such that M_2 is a trivial K'-Galois module, and let $G_1 = \mathrm{Gal}(K'/K)$ be its Galois group; then G_1 injects into G. We can assume $G = G_1$. For all field extensions L/K, we then have $\mathrm{Gal}(LK'/L) = \Gamma_L \subset G$. Define M_3 to make the following sequence exact.

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0\,.$$

The long exact sequences of group cohomology with respect to Γ_L and of Galois cohomology over L then show that

$$\begin{aligned} & H^1(L, M_1) \longrightarrow H^1(L, M_2) \text{ is injective}\\ \iff\quad & H^0(L, M_2) \longrightarrow H^0(L, M_3) \text{ is surjective}\\ \iff\quad & H^0(\Gamma_L, M_2) \longrightarrow H^0(\Gamma_L, M_3) \text{ is surjective}\\ \iff\quad & H^1(\Gamma_L, M_1) \longrightarrow H^1(\Gamma_L, M_2) \text{ is injective.}\end{aligned}$$

(Note that $H^0(L, -) = H^0(\Gamma_L, -)$ for the modules considered.) By Lemma 6.1, the last statement is true under the assumptions made. □

Corollary 6.3. Let X be a Galois-invariant spanning set of $E[p]$ and let G be the image of the absolute Galois group of K in $\mathrm{GL}(E[p]) = \mathrm{GL}(2,\mathbb{F}_p)$. Then condition (i) is satisfied if either p does not divide the order of G, or if the induced map

$$\bar{w}_p : H^1(W, E[p]) \longrightarrow H^1(W, \mu_p(\bar{D}))$$

is injective, where W is a p-Sylow subgroup of G and D is the étale K-algebra corresponding to X.

Proof: We apply Cor. 6.2 to the map $E[p] \to \mu_p(D)$. The Galois action on $E[p]$ and on $\mu_p(D) = \mathrm{Map}(X, \mu_p)$ factors through $G = \mathrm{Gal}(K(E[p])/K) \subset \mathrm{GL}(2,\mathbb{F}_p)$, and the action of scalar matrices $\alpha I \in G$ on $E[p]$ is multiplication by α. Hence the assumptions are satisfied and the result follows. □

The upshot of this result is that (apart from fairly trivial cases) condition (i) is satisfied for a Galois-invariant spanning set X for $E[p]$ if

$$\bar{w}_p : H^1(W, E[p]) \longrightarrow H^1(W, \mu_p(\bar{D}))$$

is injective. Let us see what properties of X guarantee this to be the case. By changing the basis of $E[p]$ if necessary, we can assume that $W = \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\}$.

The set X is the union of W-orbits of size p, which we denote S_i, and singleton W-orbits, which we denote Q_j. As W-modules, we have the direct sum decomposition

$$\begin{aligned} \mu_p(\bar{D}) = \operatorname{Map}(X, \mu_p) &= \bigoplus_i \operatorname{Map}(S_i, \mu_p) \oplus \bigoplus_j \operatorname{Map}(Q_j, \mu_p) \\ &\cong \bigoplus_i \operatorname{Map}(W, \mathbb{Z}/p\mathbb{Z}) \oplus \bigoplus_j \mathbb{Z}/p\mathbb{Z}\,. \end{aligned}$$

(Note that W acts trivially on μ_p.) Hence

$$H^1(W, \mu_p(\bar{D})) \cong \bigoplus_i H^1(W, \operatorname{Map}(W, \mathbb{Z}/p\mathbb{Z})) \oplus \bigoplus_j H^1(W, \mathbb{Z}/p\mathbb{Z}) \cong \bigoplus_j \mathbb{Z}/p\mathbb{Z}$$

by Shapiro's lemma and the explicit description of the cohomology of cyclic groups. On the other hand,

$$H^1(W, E[p]) \cong E[p]/(\sigma - 1)E[p] = E[p]/E[p]^W$$

(where σ is a generator of W) is one-dimensional, so $\bar{w}_p$ cannot be injective when X has no singleton W-orbits. We thank Hendrik W. Lenstra Jr. for pointing this out to us.

If X contains a point Q fixed by W, then we see that $\bar{w}_p$ is injective as follows. A generator of $H^1(W, E[p])$ is represented by a point $P \in E[p] \setminus E[p]^W$, so P and Q are independent and their Weil pairing $e_p(Q, P)$ is non-trivial. Hence the image of P is non-zero in the component of $H^1(W, \mu_p(\bar{D}))$ corresponding to Q.

Proposition 6.4. *Let X be a Galois-invariant subset of $E[p] \setminus \{0\}$ spanning $E[p]$, and let $G = \operatorname{Gal}(K(E[p])/K)$. Then X satisfies condition (i) of Section 5 if $p \nmid \#G$ or $p \nmid \#X$.*

PROOF: We have seen earlier that it is sufficient to have $p \nmid \#G$.

Now suppose that $p \mid \#G$ and $p \nmid \#X$. Then X must contain a point fixed by W (in fact, since $\#(E[p]^W \setminus \{0\}) = p - 1$, we have $X \cap E[p]^W \neq \emptyset \iff p \nmid \#X$). In the discussion preceding the proposition, we have seen that $\bar{w}_p$ is injective on $H^1(W, E[p])$ in this case. By Corollary 6.3, the result follows. □

As a kind of converse to this result, we can state that if the sufficient conditions are not satisfied, $\bar{w}_p$ will fail to be injective on $H^1(L, E[p])$ for any field extension L of K such that $G = \operatorname{Gal}(L(E[p])/L)$ satisfies $H^1(G, E[p]) \neq 0$ and contains W as a normal subgroup.

Dokchitser independently proved that if G acts irreducibly on $E[p]$, then $\bar{w}_p$ is injective (see [11, §6.1]). Note that in this case, D corresponds to all of $E[p] \setminus \{0\}$ and is a field.

7. Full p-descent. The generic case

For the rest of this paper, A will be the étale algebra corresponding to the finite étale subscheme $E[p] \setminus \{0\}$ of E.

Our goal in this section is to prove that the conditions (i) and (ii) of section 5 are satisfied when θ is the multiplication-by-p map and $X = E[p] \setminus \{0\}$ (so $D = A$). This is the generic case, since usually the action of the absolute Galois group G_K is transitive on $E[p] \setminus \{0\}$.

Since $X = E[p] \setminus \{0\}$, $\mathrm{GL}(2, \mathbb{F}_p)$ acts on X and acts linearly on all modules derived from it, and the Galois action on them factors through a subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$. We will call modules of this type *Galois modules with* $\mathrm{GL}(2)$*-action.* Similarly, a G_K-set Y with Galois action factoring through an action of $\mathrm{GL}(2, \mathbb{F}_p)$ on Y is called a *G_K-set with* $\mathrm{GL}(2)$*-action.*

Recall the notation $\bar{A} = A \otimes_K \bar{K}$ and that elements of $\bar{A}^\times$ can be regarded as functions $E[p] \setminus \{0\} \longrightarrow \bar{K}^\times$. In order to simplify some statements below, we will extend these functions to all of $E[p]$ by defining their value at 0 to be 1. So with this convention, we have

$$\bar{A}^\times = \{\varphi : E[p] \to \bar{K}^\times \mid \varphi(0) = 1\}\,.$$

Corollary 7.1. The cohomology group $H^1(K, E[p])$ embeds into $A^\times/(A^\times)^p$. (See Section 5 for an explicit description of the embedding map.) In the same way, the local cohomology group $H^1(K_v, E[p])$ embeds into $A_v^\times/(A_v^\times)^p$. In other words, condition (i) holds.

When S is a finite set of places of K, then $H^1(K, E[p]; S)$ embeds into $A(S, p)$.

Proof: The first statements follow from Prop. 6.4, since $\#(E[p] \setminus \{0\}) = p^2 - 1$ is not divisible by p.

The statement $H^1(K, E[p]; S) \hookrightarrow A(S, p)$ then follows from the definitions of $H^1(K, E[p]; S)$ and $A(S, p)$; more precisely, we have that $H^1(K, E[p]; S) = H^1(K, E[p]) \cap A(S, p)$, where we identify $H^1(K, E[p])$ with its image in $A^\times/(A^\times)^p$. □

We now have exhibited $H^1(K, E[p])$ as a subgroup of $A^\times/(A^\times)^p$. It remains to determine precisely which subgroup it is. The following lemma provides a first step towards this goal.

Lemma 7.2. *Let D be an étale algebra over K corresponding to a G_K-set X with* $\mathrm{GL}(2)$*-action. Assume that the stabilizers in* $\mathrm{GL}(2, \mathbb{F}_p)$ *of points in X meet the center Z of* $\mathrm{GL}(2, \mathbb{F}_p)$ *trivially.*

Then there is an étale subalgebra D_+ of D corresponding to the orbits in X of $Z = \mathbb{F}_p^\times I$; D is an extension of degree $p-1$ of D_+, and the automorphism group of D/D_+ is cyclic of order $p-1$.

Let $\mu_p(\bar{D})^{(1)}$ be the Galois submodule of $\mu_p(\bar{D})$ consisting of the elements on which the action of a central element αI is multiplication by α. Then

$$H^1(K, \mu_p(\bar{D})^{(1)}) \cong \ker(g - \sigma_g : D^\times/(D^\times)^p \to D^\times/(D^\times)^p)\,,$$

where g is a primitive root mod p, and σ_g is the automorphism of D/D_+ corresponding to the action of gI on the set X.

If $p = 3$, this simply means

$$H^1(K, \mu_3(\bar{D})^{(1)}) \cong \ker(N_{D/D_+} : D^\times/(D^\times)^3 \to D_+^\times/(D_+^\times)^3)\,.$$

Proof: The assumption implies that the canonical map $X \longrightarrow X/Z$ has fibers of size $p-1$. Hence the corresponding injection $D_+ \longrightarrow D$ of étale algebras has degree $p-1$. Since Z acts transitively and faithfully on each fiber, the covering $X \longrightarrow X/Z$ is Galois with cyclic Galois group Z, and this carries over to the extension D/D_+.

For a Galois module M with GL(2)-action, recall the notation $M^{(\nu)}$ for the submodule on which gI acts as multiplication by g^ν. By the elementary representation theory of finite abelian groups, we have a splitting $M = \bigoplus_{\nu \bmod (p-1)} M^{(\nu)}$ as Galois modules, and $M^{(1)} = \ker(g \cdot I - 1 \cdot (gI) : M \to M)$ (the element $g \cdot I - 1 \cdot (gI)$ is in the group ring $\mathbb{F}_p[Z]$). Since H^1 is an additive functor, this implies the claim. □

Since $X = E[p] \setminus \{0\}$ satisfies the assumptions in the preceding lemma, we can apply it to A. In particular, A_+ denotes the subalgebra corresponding to $\mathbb{P}(E[p])$, the set of lines through the origin in the $\mathbb{F}_p$-vector space $E[p]$. If $p = 3$, this is simply the étale algebra corresponding to the 3-division polynomial of E (since the x-coordinate takes the same value on P and on $-P = 2P$, but distinct values on distinct pairs of inverse points). In general, A_+ can be defined by a polynomial of degree $p+1$.

Corollary 7.3. $H^1(K, E[p])$ embeds into $\ker(g - \sigma_g : A^\times/(A^\times)^p \to A^\times/(A^\times)^p)$, where g is a primitive root mod p and σ_g is the corresponding automorphism of A/A_+.

Proof: Since $E[p] = E[p]^{(1)}$, the image of $E[p]$ under w_p must be contained in $\mu_p(\bar{A})^{(1)}$. Hence the claim follows from Cor. 7.1 and Lemma 7.2. □

Note that in the interpretation of the elements of $A^\times$ as functions on $E[p]$, the automorphism σ_g is given by $(\sigma_g\varphi)(P) = \varphi(g \cdot P)$.

Dokchitser independently proved that when A is a field, the image of $E(K)$ in $A^\times/(A^\times)^p$ is contained in the kernel of the norm to $M^\times/(M^\times)^p$ for any proper subfield M of A (see [11, Cor. 6.5.2]).

The following lemma is an analogue of Cor. 6.2, but for a longer exact sequence.

Lemma 7.4. *Let*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow M_4 \longrightarrow 0$$

be an exact sequence of K-Galois modules with GL(2)*-action. Assume further that $M_2 = M_2^{(1)}$. Let W be a p-Sylow subgroup of* GL$(2, \mathbb{F}_p)$ *and suppose that*

(i) $H^1(W, M_1) \longrightarrow H^1(W, M_2)$ *is injective, and*
(ii) $H^0(W, M_3) \longrightarrow H^0(W, M_4)$ *is surjective.*

Then the following sequence of Galois cohomology groups is exact.

$$(7.1) \qquad 0 \longrightarrow H^1(K, M_1) \longrightarrow H^1(K, M_2) \longrightarrow H^1(K, M_3)\,.$$

PROOF: By Cor. 6.2, assumption (i) implies that the sequence (7.1) is exact at $H^1(K, M_1)$.

Now let M be the image of M_2 in M_3; then we have two short exact sequences

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M \longrightarrow 0 \text{ and } 0 \longrightarrow M \longrightarrow M_3 \longrightarrow M_4 \longrightarrow 0\,.$$

The long exact sequence of group cohomology with respect to W then shows that assumption (ii) implies that $H^1(W, M) \longrightarrow H^1(W, M_3)$ is injective. Cor. 6.2 again then tells us that $H^1(K, M) \longrightarrow H^1(K, M_3)$ is injective, too. Hence the map $H^1(K, M_2) \longrightarrow H^1(K, M) \longrightarrow H^1(K, M_3)$ is injective on the cokernel of $H^1(K, M_1) \longrightarrow H^1(K, M_2)$, and this means that the sequence (7.1) is also exact at $H^1(K, M_2)$. □

It is now clear what we have to do. We have to find a suitable Galois module M that makes the sequence

$$0 \longrightarrow E[p] \xrightarrow{w_p} \mu_p(\bar{A})^{(1)} \longrightarrow M$$

exact (and then we have to check that the sequence stays exact when we apply $H^1(K, -)$). Now $\mu_p(\bar{A})$ is the same as the module of μ_p-valued functions on $E[p]$ taking the value 1 at 0, whereas the image of w_p consists exactly of those functions that are homomorphisms. The submodule $\mu_p(\bar{A})^{(1)}$ contains the functions φ that satisfy $\varphi(\alpha P) = \varphi(P)^\alpha$, but in order to be a homomorphism, φ has to satisfy more relations, namely that $\varphi(P + Q) = \varphi(P)\varphi(Q)$ for all points $P, Q \in E[p]$ such that $P, Q, P + Q$ are non-zero. We can write this more symmetrically in the form

$$\varphi(P_1)\,\varphi(P_2)\,\varphi(P_3) = 1$$

for all $P_1, P_2, P_3 \in E[p] \setminus \{0\}$ with $P_1 + P_2 + P_3 = 0$.

To carry through this approach would require considering the étale algebra corresponding to the set of all the unordered triples as above. This algebra splits into a direct product of the algebra corresponding to triples lying on a line through the origin in $E[p]$ and the algebra corresponding to triples spanning $E[p]$. The first part is not really needed, since we have already restricted to $\mu_p(\bar{A})^{(1)}$. Since to each basis v, w of $E[p]$, we can associate the triple $\{v, w, -v - w\}$, and each triple is associated to six bases, the other factor of the algebra would have degree $\frac{1}{6}\#\,\mathrm{GL}(2, \mathbb{F}_p) = \frac{1}{6}(p-1)^2 p(p+1)$; this is too large to be useful in practice, when $p > 3$.

But we can do better. In any $\mathbb{F}_p$-vector space (with p odd), the points on an affine line sum to zero. Hence every $\varphi \in \mu_p(\bar{A})^{(1)}$ that is in the image of w_p must satisfy the conditions

$$\prod_{P \in \ell} \varphi(P) = 1$$

for all affine lines ℓ in $E[p] \cong \mathbb{F}_p^2$ missing the origin. We will see below that this is indeed sufficient.

Lemma 7.5. *The set of affine lines in $E[p]$ missing the origin is in natural correspondence with the points in $E[p]^\vee \setminus \{0\}$, where $E[p]^\vee = \operatorname{Hom}(E[p], \mathbb{Z}/p\mathbb{Z})$. The bijection is given by*

$$\ell \longleftrightarrow \phi \iff \ell = \{P \in E[p] \mid \phi(P) = 1\}\,.$$

Proof: Easy. □

So let us take the étale algebra B over K that corresponds to the G_K-set with GL(2)-action consisting of the lines as above, or equivalently, of the points in $E[p]^\vee \setminus \{0\}$. Note that B has the same degree as A, namely $p^2 - 1$. Note also that $E[p]^\vee = (E[p]^\vee)^{(-1)}$. We will use the same convention for B as we use for A, i. e., we identify

$$\bar{B}^\times = \{\phi : E[p]^\vee \to \bar{K}^\times \mid \phi(0) = 1\}\,.$$

Lemma 7.6. *The following is an exact sequence of Galois modules with* GL(2)*-action.*

$$0 \longrightarrow E[p] \xrightarrow{w_p} \mu_p(\bar{A})^{(1)} \xrightarrow{u} \mu_p(\bar{B})^{(1)} \xrightarrow{w_p^\vee} E[p]^\vee \otimes \mu_p \longrightarrow 0$$

The map u is given by

$$\varphi \longmapsto (\ell \mapsto \prod_{P \in \ell} \varphi(P))\,,$$

and the map $w_p^\vee$ is given by

$$\phi \longmapsto \sum_{\ell : \phi(\ell) = \zeta} \ell \otimes \zeta = \sum_{\langle \ell \rangle \in \mathbb{P}(E[p]^\vee)} \ell \otimes \phi(\ell)\,,$$

where $\zeta \in \mu_p$ is some generator. In the second sum, ℓ runs through a set of representatives of the lines through the origin in $E[p]^\vee$.

Note that since $E[p]^\vee = (E[p]^\vee)^{(-1)}$ and $\phi \in \mu_p(\bar{B})^{(1)}$, the element $\ell \otimes \phi(\ell)$ does not depend on the representative chosen. The image $w_p^\vee(\phi)$ can also be written as an element of $\operatorname{Hom}(E[p], \mu_p)$ as follows.

$$P \longmapsto \prod_{\ell : P \in \ell} \phi(\ell)\,.$$

Note also that $\operatorname{Hom}(E[p], \mu_p) \cong E[p]$ by the Weil pairing.

Proof: We know that w_p is injective and that $u \circ w_p = 0$. It is easy to see that $w_p^\vee \circ u = 0$, too, as follows. Let $\varphi \in \mu_p(\bar{A})^{(1)}$. Then $w_p^\vee(u(\varphi)) \in \operatorname{Hom}(E[p], \mu_p)$ maps a point P to $\prod_{\ell : P \in \ell} \prod_{Q \in \ell} \varphi(Q)$. In this product, the value $\varphi(P)$ occurs p times (once for every line ℓ through P that misses the origin), and no other multiple of P shows up. On the other hand, for each $Q \in E[p] \setminus \langle P \rangle$, we get $\varphi(Q)$ exactly once. In total, we have $w_p^\vee(u(\varphi))(P) = \prod_{Q \in E[p] \setminus \langle P \rangle} \varphi(Q) = 1$, since $\prod_{R \in \langle Q \rangle \setminus \{0\}} \varphi(R) = 1$ for all Q.

Furthermore, $w_p^\vee$ is surjective. In order to get $\ell \otimes \zeta$ in the image, we take ℓ as the representative of $\langle \ell \rangle$ and choose ϕ to map ℓ to ζ and to map all elements in $E[p]^\vee \setminus \langle \ell \rangle$ to 1.

So we only have to show that the kernel of u is contained in the image of w_p. Abstractly, this means that any map $\varphi : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p$ that satisfies the following two conditions is a homomorphism.

(i) $\varphi(\alpha v) = \alpha\varphi(v)$ for all $v \in \mathbb{F}_p^2$, $\alpha \in \mathbb{F}_p$.
(ii) $\sum_{v\in\ell} \varphi(v) = 0$ for all affine lines ℓ contained in $\mathbb{F}_p^2 \setminus \{0\}$. (For the lines containing the origin, this follows already from (i).)

This is shown in Lemma 7.7 below. □

Our first proof of the following result was fairly involved. During a conference in Oberwolfach in July 1999, we asked for a better one. The proof given below has evolved from ideas that emerged from discussions between Bjorn Poonen, Harold Stark, Don Zagier and the second author.

Lemma 7.7. *Let p be an odd prime, and let $\varphi : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p$ be a map. Then φ is linear if and only if it satisfies the following two conditions.*

(i) *φ is homogeneous of degree 1;*
(ii) *$\sum_{v\in\ell} \varphi(v) = 0$ for all affine lines $\ell \subset \mathbb{F}_p^2 \setminus \{0\}$.*

Proof: Note first that φ can be written in a unique way as a polynomial in two variables of degree at most $p-1$ in each of the variables,

$$\varphi(x,y) = \sum_{j,k=0}^{p-1} a_{jk}\, x^j y^k\,.$$

Our first claim is that φ satisfies condition (i) if and only if $a_{jk} = 0$ for all (j,k) with $j + k \not\equiv 1 \bmod (p-1)$. This is easily seen by comparing coefficients in $\varphi(\alpha x, \alpha y) = \alpha\varphi(x,y)$ and by noting that $\alpha^m = \alpha^n$ for all $\alpha \in \mathbb{F}_p^\times$ if and only if $n \equiv m \bmod (p-1)$.

Our second claim is that φ satisfies condition (ii) if and only if $a_{jk} = 0$ for all (j,k) with $j+k \geq p-1$. Obviously, the two claims together prove the lemma. Let us prove the second claim. Take any line ℓ as in condition (ii). It can be defined by an equation $ax + by = 1$ with $(a,b) \in \mathbb{F}_p^2 \setminus \{0\}$. Let $\phi_\varphi(a,b) = \sum_{v\in\ell} \varphi(v)$ and set $\phi_\varphi(0,0) = 0$. Then the map $\varphi \mapsto \phi_\varphi$ is an endomorphism of the space of maps from $\mathbb{F}_p^2$ to $\mathbb{F}_p$. Let us see what a monomial $x^j y^k$ maps to. Assume that $b \neq 0$, so

$y = b^{-1}(1-ax)$ on ℓ. Unless we have $j = k = p-1$, we get

$$\begin{aligned}\sum_{(x,y)\in\ell} x^j y^k &= \sum_{x\in\mathbb{F}_p} x^j (b^{-1}(1-ax))^k \\ &= b^{-k}\sum_x \sum_{h=0}^{k} \binom{k}{h}(-a)^h x^{j+h} \\ &= b^{-k}\sum_{h=0}^{p-1}\binom{k}{h}(-a)^h \sum_x x^{j+h} \\ &= -b^{-k}\binom{k}{p-1-j}(-a)^{p-1-j} \\ &= (-1)^{j+1}\binom{k}{p-1-j} a^{p-1-j} b^{p-1-k}\,.\end{aligned}$$

This is because $\sum_x x^m$ is nonzero if and only if m is a positive multiple of $(p-1)$, when the sum equals -1. When $b = 0$, then we must have $a \neq 0$, and we get the same result. (Note that $(-1)^{j+1}\binom{k}{p-1-j} = (-1)^{k+1}\binom{j}{p-1-k}$ in $\mathbb{F}_p$.) When $j = k = p-1$, the result is $1 - 2a^{p-1} - 2b^{p-1} + (ab)^{p-1}$ by direct calculation. Since the binomial coefficient vanishes precisely when $j + k < p - 1$, the kernel of the map $\varphi \mapsto \phi_\varphi$ contains the monomials $x^j y^k$ with $j + k < p - 1$. Since the images of the other monomials are linearly independent, the claim follows. □

Now we know that we have an exact sequence

$$0 \longrightarrow E[p] \longrightarrow \mu_p(\bar{A})^{(1)} \longrightarrow \mu_p(\bar{B})^{(1)}$$

as required. It remains to show that the induced sequence on H^1 is also exact.

Proposition 7.8. The sequence

$$0 \longrightarrow H^1(K, E[p]) \xrightarrow{\bar{w}_p} H^1(K, \mu_p(\bar{A})^{(1)}) \xrightarrow{\bar{u}} H^1(K, \mu_p(\bar{B})^{(1)})$$

is exact.

Proof: By Lemmas 7.6 and 7.4, it suffices to show that

$$H^1(W, E[p]) \xrightarrow{\bar{w}_p} H^1(W, \mu_p(\bar{A})^{(1)})$$

is injective and that

$$H^0(W, \mu_p(\bar{B})^{(1)}) \xrightarrow{\bar{w}_p^\vee} H^0(W, E[p]^\vee \otimes \mu_p)$$

is surjective. The first condition was already dealt with in Cor. 7.1. The second condition is also easily checked. □

Now we have found the description of $H^1(K, E[p])$.

Corollary 7.9. We have

$$H^1(K, E[p]) \cong \ker\bigl(g - \sigma_g : A^\times/(A^\times)^p \longrightarrow A^\times/(A^\times)^p\bigr) \cap \ker \bar{u}\,,$$

where $\bar{u}$ is the map induced by u on H^1,

$$A^\times/(A^\times)^p = H^1(K, \mu_p(\bar{A})) \longrightarrow H^1(K, \mu_p(\bar{B})) = B^\times/(B^\times)^p\,.$$

With this identification, we have $H^1(K, E[p]; S) = H^1(K, E[p]) \cap A(S, p)$.

In order to make this completely explicit, we still need a good description of $\bar{u} : A^\times/(A^\times)^p \longrightarrow B^\times/(B^\times)^p$. This can be obtained in the following way. Let Y denote the G_K-set consisting of all pairs $(P, \ell) \in (E[p] \setminus \{0\}) \times (E[p]^\vee \setminus \{0\})$ such that $P \in \ell$, and let D be the étale algebra corresponding to Y. The two projections give us canonical maps $\pi_1 : Y \longrightarrow E[p]\setminus\{0\}$ and $\pi_2 : Y \longrightarrow E[p]^\vee\setminus\{0\}$ and corresponding inclusions $i_{D/A} : A \longrightarrow D$ and $B \longrightarrow D$. The effect of u is to take a function φ on $E[p] \setminus \{0\}$, pull it back to a function $\varphi \circ \pi_1$ on Y, and to produce a function on $E[p]^\vee \setminus \{0\}$ by multiplying over the fibers of π_2. This last step corresponds exactly to taking the norm $N_{D/B}$. Hence we have proved the following result.

Proposition 7.10. The map $\bar{u} : A^\times/(A^\times)^p \longrightarrow B^\times/(B^\times)^p$ is induced by the composition $N_{D/B} \circ i_{D/A} : A \longrightarrow B$.

In practice, we choose a basis of D over B and express the multiplication-by-α map of D as a p-by-p matrix M_α over B, where α is (the image in D of) a generator of A. Any given element of A can be written as a polynomial $h(\alpha)$, and then we have $\bar{u}(h(\alpha)) = \det(h(M_\alpha))$. See Section 10 for an example. In any case, we can now claim condition (ii) of Section 5 to hold.

In [9], the authors were not able to determine the image of $H^1(K, E[p])$ in $A^\times/(A^\times)^p$ explicitly. Therefore their algorithm was only able to find the following group Z,[2] which was shown to contain the Selmer group.

$$Z = \{\xi \in A^\times/(A^\times)^p \mid \operatorname{res}_v(\xi) \in F_v(E(K_v)/pE(K_v)) \text{ for all } v\}$$

Our characterization of the image of $H^1(K, E[p])$ in $A^\times/(A^\times)^p$ now implies the following result, which gives some justification for the algorithm in [9].

Proposition 7.11. We have $Z = \operatorname{Sel}^{(p)}(K, E)$.

Proof: By the definitions of Z and of the Selmer group, we certainly must have that $Z \cap H^1(K, E[p]) = \operatorname{Sel}^{(p)}(K, E)$ (considering $H^1(K, E[p])$ as a subgroup of $A^\times/(A^\times)^p$). We therefore have to show that Z is contained in $H^1(K, E[p]) = \ker(g - \sigma_g) \cap \ker \bar{u}$. Now we certainly have that this holds locally, i.e., if $\xi \in Z$, then $(g - \sigma_g)(\xi) \in (A_v^\times)^p$ and $\bar{u}(\xi) \in (B_v^\times)^p$ for all places v of K. But an element that is a pth power everywhere locally must be a global pth power, hence $\xi \in \ker(g - \sigma_g) \cap \ker \bar{u}$, proving the claim. □

[2] Actually, they also require $N_{A/K}(\xi)$ to be a pth power, but this leads to the same group, as Prop. 7.11 shows.

8. Full p-descent. A special case

When E is a generic elliptic curve, all of $E[p] \setminus \{0\}$ will form a single Galois orbit, and we are forced to work with the algebra A (a number field of degree p^2-1 over K) as described in the preceding section. But in some cases we are lucky and the set of points of exact order p splits into several orbits. This has two advantages. The first advantage is that the algebra A splits into a product of several number fields (one for each orbit), which are of lower degree and therefore easier to handle. The second advantage is that we can perhaps throw away some of the factors and thus reduce the amount of computation further.

One of these special cases occurs when E has a Galois-stable (unordered) pair of cyclic subgroups of order p. In this case, the two subgroups together generate $E[p]$ and thus form a Galois-invariant spanning set. We can use the corresponding étale algebra, a factor of degree $2(p-1)$ of A, to perform the p-descent. The other part of A is redundant in this case. This situation occurs in particular when E has complex multiplication and the prime p splits in the endomorphism ring. We will focus on this case in the description given here.

Let E/K have complex multiplication by the ring $\mathcal{O}$. Assume that the ideal generated by p splits in $\mathcal{O}$ as $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$. Let $E[\mathfrak{p}]$ and $E[\mathfrak{p}']$ denote the subgroups of E killed by the elements of $\mathfrak{p}$ and $\mathfrak{p}'$, respectively. Let A_1 be the étale K-algebra corresponding to $(E[\mathfrak{p}] \cup E[\mathfrak{p}']) \setminus \{0\}$. The set $(E[\mathfrak{p}] \cup E[\mathfrak{p}']) \setminus \{0\}$ comes with a $\mathrm{GL}(1, \mathbb{F}_p)$-action. Note A_1 has degree $2(p-1)$ over K and the dimension of $\mu_p(\bar{A}_1)^{(1)}$ is 2. We define w_p with respect to this spanning set; it gives an isomorphism $E[p] \xrightarrow{\cong} \mu_p(\bar{A}_1)^{(1)}$. The composition of $\bar{w}_p$ and the Kummer map induces an isomorphism of $H^1(K, E[p])$ and $\ker(g - \sigma_g : A_1^\times/(A_1^\times)^p \to A_1^\times/(A_1^\times)^p)$, where g is a primitive root mod p and σ_g is the corresponding automorphism of $A_1/A_{1,+}$. Note that the algebra $A_{1,+}$ is isomorphic to $\mathcal{O} \otimes_{\mathbb{Z}} K$.

Recall that a CM elliptic curve has everywhere potential good reduction, and so the Tamagawa numbers are at most 4. In particular, if $p > 3$, then the places of K above p are the only bad places we have to consider in the computation of the p-Selmer group. For an example with $p = 5$, see Section 11.2.

A more careful analysis provides the following result, which is essentially the first part of Theorem 1 in [22] in the split case. (But note that we do not require E to have good reduction at p.)

Theorem 8.1. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by an order $\mathcal{O}$ in the imaginary quadratic field K, and let p be an odd prime such that p is split in $\mathcal{O}$ and does not divide any of the Tamagawa numbers $c_{E,q}$ for $q \neq p$ (this last condition is automatic for $p \geq 5$).*

Let $A_1 = K(E[\mathfrak{p}]) = \mathbb{Q}(E[\mathfrak{p}] \cup E[\mathfrak{p}'])$, where $\mathfrak{p}$ is a prime in $\mathcal{O}$ above p. Then $A_{1,+} = K$. Let $r = \dim_{\mathbb{F}_p} \mathrm{Cl}(A_1)[p]^{(1)}$ and $t = \dim_{\mathbb{F}_p} E(\mathbb{Q}_p)[p] \in \{0,1\}$. Then we have

$$r - t \leq \dim_{\mathbb{F}_p} \mathrm{Sel}^{(p)}(\mathbb{Q}, E) \leq r + t + 1\,.$$

Proof: We use the description given in (5.1). By Prop. 4.6, we can take $S = \{p\}$, given our assumptions.

Let U be the unit group of A_1. Let I_p be the group of ideals of A_1 supported in primes above p, and define s by

$$s = \dim \ker(I_p/p\, I_p \to \mathrm{Cl}(A_1)/p\ \mathrm{Cl}(A_1))^{(1)}\,.$$

We then have

$$\dim A_1(\{p\}, p)^{(1)} = \dim(U/U^p)^{(1)} + r + s\,.$$

From the Dirichlet unit theorem, we find $\dim(U/U^p)^{(1)} = 1$. The action of $\mathbb{F}_p^\times \cong \mathrm{Gal}(A_1/A_{1,+})$ on $X = (E[\mathfrak{p}]\setminus\{0\})\cup(E[\mathfrak{p}']\setminus\{0\})$ is by cyclic permutation on the two parts. This is easily seen to imply that $I_p^{(1)}$ has rank $\dim E(\mathbb{Q}_p)[\mathfrak{p}] + \dim E(\mathbb{Q}_p)[\mathfrak{p}']$. Since $\mu_p \not\subset \mathbb{Q}_p$, we have $t \le 1$, and since the endomorphisms of E are defined over $\mathbb{Q}_p$, we then have $E(\mathbb{Q}_p)[p] = E(\mathbb{Q}_p)[\mathfrak{p}] \cup E(\mathbb{Q}_p)[\mathfrak{p}']$. Hence $I_p^{(1)}$ has rank t. Therefore $s \le t$ and

$$r + 1 \le \dim A_1(\{p\}, p)^{(1)} \le r + t + 1\,.$$

Now the Selmer group is the subgroup consisting of elements of $A_1(\{p\}, p)^{(1)}$ that map into the image of $E(\mathbb{Q}_p)/p\,E(\mathbb{Q}_p)$ in $\big(A_{1,p}^\times/(A_{1,p}^\times)^p\big)^{(1)} \cong H^1(\mathbb{Q}_p, E[p])$. This image has dimension $t+1$, and by Tate local duality, its codimension in $H^1(\mathbb{Q}_p, E[p])$ is also $t+1$. The claim follows. □

A similar analysis should be possible for inert primes.

9. p-descent by isogeny

When the elliptic curve has a K-rational cyclic subgroup of order p, we can perform a descent via p-isogeny. This can be done by essentially the same method as for a full p-descent, but is considerably simpler, both in theory and in practical computation. In this section, we describe this type of descent and relate it to the full p-descent discussed in the preceding sections.

Let E be an elliptic curve over K, with a K-defined isogeny h of degree p onto the elliptic curve E' over K. Let h' be the dual isogeny, defined over K, from E' to E. Let C_2 and C_1 be the étale K-algebras corresponding to $E[h] \setminus \{0\}$ and $E'[h'] \setminus \{0\}$, respectively. Note C_1 has degree $p-1$ over K and the dimension of $\mu_p(\bar{C}_1)$ is $p-1$. The map w_h gives an isomorphism $E[h] \xrightarrow{\cong} \mu_p(\bar{C}_1)^{(1)}$. The composition of $\bar{w}_h$ and the Kummer map induces an isomorphism of $H^1(K, E[h])$ and $\ker(g - \sigma_g : C_1^\times/(C_1^\times)^p \to C_1^\times/(C_1^\times)^p)$, where g is a primitive root mod p and σ_g is the corresponding automorphism of C_1/K.

If C_1 splits over K, then we can replace it by one of its factors. This amounts to replacing the set $E'[h]\setminus\{0\}$ by a smaller Galois-invariant subset X. Let $\mathcal{C}_1$ be this factor (all the factors are isomorphic since they are permuted by the automorphism σ_g of C_1/K). Similarly, we let $\mathcal{C}_2$ be one of the factors of C_2. Note that both $\mathcal{C}_1$ and $\mathcal{C}_2$ are cyclic Galois extensions of K. This fact can sometimes be exploited if one wants to find the dimension of $\mathcal{C}_1(S,p)^{(1)}$ or $\mathcal{C}_2(S,p)^{(1)}$; compare example 11.3.

If $Ш(K,E)[h]=0$ and $Ш(K,E')[h']=0$ then $\mathrm{Sel}^{(h)}(K,E)$ and $\mathrm{Sel}^{(h')}(K,E')$ are isomorphic to $E'(K)/hE(K)$ and $E(K)/h'E'(K)$, respectively. We can get $E(K)/pE(K)$ from $E'(K)/hE(K)$ and $E(K)/h'E'(K)$ using the exact sequence

$$(9.1)\qquad 0 \longrightarrow \frac{E'(K)[h']}{h(E(K)[p])} \longrightarrow \frac{E'(K)}{hE(K)} \xrightarrow{h'} \frac{E(K)}{pE(K)} \longrightarrow \frac{E(K)}{h'E'(K)} \longrightarrow 0$$

(see [27, p. 301]; a proof can be found in [25, Prop. 2.6]). Computing $\mathrm{Sel}^{(h)}(K,E)$ and $\mathrm{Sel}^{(h')}(K,E')$ typically involves working in two extensions of K of degree $p-1$. Whereas computing $\mathrm{Sel}^{(p)}(K,E)$ directly typically involves working in extensions of degrees $p-1$ and p^2-p, which in this case would clearly be disadvantageous. However, in the case that $Ш(K,E)[p]=0$ and $Ш(K,E')[h']\neq 0$, it may be necessary to compute $\mathrm{Sel}^{(p)}(K,E)$ in order to find $E(K)/pE(K)$.

We can compute the size of $\mathrm{Sel}^{(h')}(K,E')$ from the size of $\mathrm{Sel}^{(h)}(K,E)$ using a result of Cassels' in [5]. When $K=\mathbb{Q}$, this result is as follows. Let

$$y'^2 + a_1\,x'y' + a_3\,y' = x'^3 + a_2\,x'^2 + a_4\,x' + a_6$$

be a minimal Weierstrass equation for E, and let Ω_E denote the integral over $E(\mathbb{R})$ of $|dx'/(2y'+a_1x'+a_3)|$. This is the real period if $E(\mathbb{R})$ has one component and twice the real period otherwise. Recall that $c_{E,q}$ denotes the Tamagawa number of E at the prime q (see Section 4). Then we have

$$(9.2)\qquad \frac{\#\,\mathrm{Sel}^{(h)}(\mathbb{Q},E)}{\#\,\mathrm{Sel}^{(h')}(\mathbb{Q},E')} = \frac{\#E(\mathbb{Q})[h]\cdot\Omega_{E'}\cdot\prod_q c_{E',q}}{\#E'(\mathbb{Q})[h']\cdot\Omega_E\cdot\prod_q c_{E,q}}\,.$$

Systems like PARI [20] or Magma [16] can compute all terms on the right hand side. Using this to compute the size of the second Selmer group will probably be easier than a direct computation of it. For examples, see Sections 11.3 and 11.4.

There are maps between the three Selmer groups we are describing.

Lemma 9.1. *The following sequence is exact.*

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{E'(K)[h']}{h(E(K)[p])} \arrow[r, "\delta_h"] & \mathrm{Sel}^{(h)}(K,E) \arrow[r] & \mathrm{Sel}^{(p)}(K,E) \\
\arrow[r, "h"] & \mathrm{Sel}^{(h')}(K,E') \arrow[r] & \dfrac{Ш(K,E')[h']}{h(Ш(K,E)[p])} \arrow[r] & 0
\end{tikzcd}$$

Proof: Let v be a prime of K. The following diagram is commutative, where the products are over the places of K.

$$\begin{tikzcd}
 & H^1(K,E[h]) \arrow[r] \arrow[d] & H^1(K,E[p]) \arrow[r, "h"] \arrow[d] & H^1(K,E'[h']) \arrow[d] \\
0 \arrow[r] & \prod_v H^1(K_v,E)[h] \arrow[r] & \prod_v H^1(K_v,E)[p] \arrow[r, "h"] & \prod_v H^1(K_v,E')[h']
\end{tikzcd}$$

A straightforward diagram chase, which is part of the proof of the Snake Lemma, shows that the maps between the kernels of the vertical arrows are exact at the second kernel. Those kernels are the Selmer groups.

The following diagram is commutative and all sequences are exact.

$$\begin{tikzcd}
0 \arrow[r] & E'(K)/hE(K) \arrow[r, "\delta_h"] \arrow[d, "h'"] & \mathrm{Sel}^{(h)}(K,E) \arrow[r] \arrow[d] & \text{Ш}(K,E)[h] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K)/pE(K) \arrow[r, "\delta_p"] \arrow[d] & \mathrm{Sel}^{(p)}(K,E) \arrow[r] \arrow[d, "h"] & \text{Ш}(K,E)[p] \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & E(K)/h'E'(K) \arrow[r, "\delta_{h'}"] & \mathrm{Sel}^{(h')}(K,E) \arrow[r] & \text{Ш}(K,E')[h'] \arrow[r] & 0
\end{tikzcd}$$

The kernel from $\text{Ш}(K,E)[h]$ to $\text{Ш}(K,E)[p]$ is trivial. So the kernel of the map between $\mathrm{Sel}^{(h)}(K,E)$ and $\mathrm{Sel}^{(p)}(K,E)$ is the image of $E'(K)[h']/h(E[p])$. The map from $E(K)/pE(K)$ to $E(K)/h'E'(K)$ is surjective. So the co-kernel of the map h on the Selmer groups is isomorphic to the co-kernel of h on the Shafarevich-Tate groups. □

Now let us see what these maps between Selmer groups look like in the étale algebra interpretation. Let D be the étale K-algebra corresponding to $E[p]\setminus E[h]$. We have $A \cong D \times C_2$. Since there is the map $h : E[p]\setminus E[h] \longrightarrow E[h']\setminus\{0\}$, we can embed C_1 in D. Let us describe the desired embedding and denote it ι. For $(x,y) \in E$, let $h(x,y) = (h_x(x,y), h_y(x,y))$. Let $\Psi(x)$ and $\psi(x)$ be the polynomials whose roots are the x-coordinates of the points in $E[p]\setminus E[h]$ and $E'[h']\setminus\{0\}$, respectively. Let $g_E(x,y)$ and $g_{E'}(x,y)$ denote the polynomials of the form $x^3+ax+b-y^2$ defining E and E', respectively. We have $D \cong K[U,V]/(\Psi(U), g_E(U,V))$ and $C_1 \cong K[u,v]/(\psi(u), g_{E'}(u,v))$. The embedding ι from C_1 to D maps a polynomial $r(u,v)$ to $r(h_x(U,V), h_y(U,V))$.

We prefer to define these algebras in terms of a single variable. We have $D \cong K[T]/(f_D(T))$ where $f_D(T) = \prod_{P\in E[p]\setminus E[h]}(T-\phi(P))$ and ϕ is the K-defined function on E used to define A. The isomorphism of $K[T]/(f_D(T))$ and $K[U,V]/(\Psi(U), g_E(U,V))$ should be chosen so that $T \mapsto \phi(U,V)$. We can similarly use a K-defined function ϕ' on E' to note that $C_1 \cong K[t]/(f_{C_1}(t))$ where $f_{C_1}(t) = \prod_{P\in E'[h']\setminus\{0\}}(t-\phi'(P))$. Then the isomorphism of $K[t]/(f_{C_1}(t))$ and $K[u,v]/(\psi(u), g_{E'}(u,v))$ should be chosen so that $t \mapsto \phi'(u,v)$. To describe ι from C_1 to D, defined in terms of single variables, it suffices to find the image of t by letting $r(u,v) = \phi'(u,v)$. This maps to $\phi'(h_x(U,V), h_y(U,V))$. Thus it is necessary to find the images of U and V in $K[T]/(f_D(T))$.

By abuse of notation, let ι also denote the map $C_1^\times/(C_1^\times)^p \longrightarrow A^\times/(A^\times)^p \cong D^\times/(D^\times)^p \times C_2^\times/(C_2^\times)^p$ given by $c \mapsto (\iota(c), 1)$. Let π denote the projection map from $A \cong D \times C_2$ to C_2. A straightforward diagram chase shows that the following is commutative.

$$\begin{tikzcd}
\dfrac{E'(K)[h']}{h(E(K)[p])} \arrow[r, "\delta_h"] \arrow[dr, "F"] & \mathrm{Sel}^{(h)}(K,E) \arrow[r] \arrow[d] & \mathrm{Sel}^{(p)}(K,E) \arrow[r, "h"] \arrow[d] & \mathrm{Sel}^{(h')}(K,E') \arrow[d] \\
 & C_1^\times/(C_1^\times)^p \arrow[r, "\iota"] & A^\times/(A^\times)^p \arrow[r, "\pi"] & C_2^\times/(C_2^\times)^p
\end{tikzcd}$$

Note that the lower sequence is not exact unless we restrict to the images of the H^1's.

10. Explicit 3-descent

In this section, we describe an explicit algorithm that computes the 3-Selmer group of an elliptic curve

$$E : y^2 = x^3 + a\,x + b$$

over $\mathbb{Q}$. We use the notations of Section 7.

10.1. **The algorithm for $a \neq 0$.** Let us first assume that $a \neq 0$. Then the polynomial that has as its roots the y-coordinates of the 3-torsion points on E is a separable polynomial of degree eight and therefore defines the étale algebra A. We let $\Delta = -4\,a^3 - 27\,b^2$ be the discriminant of the right hand side in the equation for E. Then the defining polynomial of A is given by

$$f(y) = y^8 + 8b\,y^6 - \tfrac{2}{3}\Delta\,y^4 - \tfrac{1}{27}\Delta^2\,.$$

The algebra A_+ is defined by the 3-division polynomial

$$\phi(x) = x^4 + 2a\,x^2 + 4b\,x - \tfrac{1}{3}a^2\,,$$

and y is related to x by the equation of E.

The algebra B corresponds to all lines in $E[3] \setminus \{0\}$; by the geometric description of the group law on E, they correspond to all lines in the projective plane containing E that intersect E in three distinct 3-torsion points. There are 8 such lines. If (as we still assume) $a \neq 0$, then the slopes of these lines are all distinct, and so we can use them to get a defining polynomial for B. The polynomial we get is as follows.

$$s(m) = m^8 + 2a\,m^4 - 4b\,m^2 - \tfrac{1}{3}a^2\,.$$

From this it is obvious that $B_+ \cong A_+$ as abstract algebras and that the relation is simply $m^2 = -x$. The reason behind this is the fact that when we have a line of slope m joining three distinct 3-torsion points on E with coordinates (x_j, y_j) $(j = 1, 2, 3)$, then

$$\phi(x) = (x - x_1)(x - x_2)(x - x_3)(x + m^2)\,. \tag{10.1}$$

The algebra D can be described as $A[m] = B[y]$, and we have to bear in mind that $-m^2$ is a zero of ϕ different from the x-coordinate of the generic 3-torsion point (x, y). (This means that A_+ and B_+ are not the same as subalgebras of D.) We take y to be the generator of A and want to find the characteristic polynomial of $y \in D$ over B. This means that we have to take a line of slope m. It contains the three 3-torsion points (x_j, y_j) $(j = 1, 2, 3)$, and the characteristic polynomial of y has coefficients given by the elementary symmetric polynomials in the y_j.

From relation (10.1), we can extract expressions for the elementary symmetric polynomials in the x_j, namely,

$$\begin{aligned} x_1 + x_2 + x_3 &= m^2 \\ x_1x_2 + x_2x_3 + x_3x_1 &= m^4 + 2a \\ x_1x_2x_3 &= m^6 + 2a\,m^2 - 4b = a^2/(3m^2)\,. \end{aligned} \tag{10.2}$$

Let $y = mx + t$ be the equation of the line. We can express t in terms of m if we first square this equation to get $x_j^3 + a\,x_j + b = m^2\,x_j^2 + 2mt\,x_j + t^2$ for all j; then we take differences and divide by $x_i - x_j$; finally, we sum the three equations obtained in this way. This results in

$$t = -\frac{3\,m^7 + 7a\,m^3 - 12b\,m}{2a} = -\frac{m^4 + a}{2m}\,.$$

Using $y_j = mx_j + t$ and equations (10.2), we obtain

$$\begin{aligned} y_1 + y_2 + y_3 &= m^3 + 3t\,, \\ y_1y_2 + y_2y_3 + y_3y_1 &= m^2(m^4 + 2a) + 2m^3t + 3t^2\,, \\ y_1y_2y_3 &= \tfrac{1}{3}a^2m + m^2(m^4 + 2a)t + m^3t^2 + t^3\,. \end{aligned}$$

This gives us the characteristic polynomial of y over B and then also the matrix M_y.

We get the following algorithm for the computation of the 3-Selmer group of an elliptic curve $E : y^2 = x^3 + a\,x + b$ over $\mathbb{Q}$, where a and b are integers with $a \neq 0$. Note that the ordering of the steps differs slightly from the general outline in Section 5 in that we use the second condition (being in the kernel of $\bar{u}$) for the image of $H^1(\mathbb{Q}, E[3]; S)$ at the end rather than at the beginning. This is done for reasons of efficiency. The test can be time-consuming, and the fewer elements we have to check, the better. We recall the notations $A_q = A \otimes_{\mathbb{Q}} \mathbb{Q}_q$ and $F_q : E(\mathbb{Q}_q) \to A_q^\times/(A_q^\times)^3$.

1. Let S be the (finite) set of prime numbers q such that the Tamagawa number $c_{E,q}$ is divisible by 3, together with $q = 3$.
2. Let $\phi(x) = x^4 + 2a\,x^2 + 4b\,x - \frac{1}{3}a^2$, and let $A_+ = \mathbb{Q}[x]/(\phi(x))$ be the corresponding étale algebra.
3. Let $f(y) = y^8 + 8b\,y^6 + (\frac{8}{3}a^3 + 18b^2)\,y^4 - \frac{16}{27}a^6 - 8a^3b^2 - 27b^4$, and let A be the étale algebra defined by f. Find its S-unit and S-class groups and construct the $\mathbb{F}_3$-vector space $A(S, 3)$.
4. Let $T_1 \subset A(S, 3)$ be the subspace of elements τ such that $N_{A/A_+}(\tau)$ is a third power in A_+ (or, equivalently, in A).
5. For each $q \in S$, compute the local image $F_q(E(\mathbb{Q}_q)) \subset A_q^\times/(A_q^\times)^3$ as described below.
6. Let $T_2 \subset T_1$ be the subspace of elements mapping into $F_q(E(\mathbb{Q}_q))$ under the 'restriction map' $A^\times/(A^\times)^3 \longrightarrow A_q^\times/(A_q^\times)^3$ for all $q \in S$.
7. Let $s(m) = \phi(-m^2)$, and let B be the étale algebra defined by s. Find its unit and class groups and construct $B(\emptyset, 3)$ if this is feasible.

8. Let $T \subset T_2$ be the subspace of elements τ such that $\bar{u}(\tau)$ (as defined above) is a third power in B. (Note that $\bar{u}(\tau)$ will be in $B(\emptyset, 3)$.)
9. Finally, the Selmer group $\mathrm{Sel}^{(3)}(\mathbb{Q}, E)$ is isomorphic to T.

The reason behind the parenthesized remark in step 8 is the following. Since $\bar{u}$ commutes with the restriction map $H^1(\mathbb{Q}, -) \to H^1(I_q, -)$ (where $I_q \subset G_{\mathbb{Q}}$ is an inertia subgroup at q of the absolute Galois group of $\mathbb{Q}$), it follows that elements unramified at some prime q are mapped to elements that are again unramified at q. Hence the image lies in $B(S, 3)$. But at a prime $q \in S$, we know that the elements considered map into the local image at q. Since in the cohomology sequence, this lands in $H^1(\mathbb{Q}_q, E[3])$, it must be in the kernel of $\bar{u}_q : A_q^\times/(A_q^\times)^3 \longrightarrow B_q^\times/(B_q^\times)^3$. This means that the image is even trivial at q, and unramified in particular.

We remark that it is not strictly necessary to find the class and unit groups of B in step 7. It is possible to find the kernel of $\bar{u}$ in step 8 by checking directly whether $\bar{u}(\tau)$ is a cube in B or not. The advantage of having the class and unit group information is that we can construct $B(\emptyset, 3)$ and reduce step 8 to linear algebra over $\mathbb{F}_3$.

We now give a more detailed description of how one can perform step 5. By [9], the map F_q is given by evaluating the function

$$F = 2\tau(y - \tau) - (3\sigma^2 + a)(x - \sigma) = 2\tau\, y - (3\sigma^2 + a)x + \sigma^3 - a\sigma - 2b \in A(E)$$

(where $(\sigma, \tau) \in E(A)$ is a generic 3-torsion point) on a degree zero divisor D representing the given point $P \in E(\mathbb{Q}_q)$ such that the support of D does not meet $E[3]$. In this way, we get a well-defined map

$$F_q : \mathrm{Pic}(E)(\mathbb{Q}_q) \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \longrightarrow A_q^\times/(A_q^\times)^3 .$$

Let $O \in E$ be the origin. We want to find the image of the class of $-O$. This is the same as the image of the class of $2O$, and since $2O \sim D$, where $D = (0, \sqrt{b}) + (0, -\sqrt{b})$, it suffices to find the image of D. Now

$$\begin{aligned} F(D) &= (2\tau\sqrt{b} + \sigma^3 - a\sigma - 2b)(-2\tau\sqrt{b} + \sigma^3 - a\sigma - 2b) \\ &= (\sigma^3 - a\sigma - 2b)^2 - 4b\tau^2 \\ &= -12b\sigma^3 + \tfrac{28}{3}a^2\sigma^2 + 16ab\sigma - \tfrac{4}{3}a^3 \in A_+ \end{aligned}$$

Let $c = F(D) \in A_+$. If $P \in E(\mathbb{Q}_q)$ is not a 3-torsion point, then

$$F_q(P) = F(P - O) = c \cdot F(x(P), y(P)) \pmod{(A_q^\times)^3} .$$

On the other hand, if $P \in E(\mathbb{Q}_q)[3]$, then $A_q = \mathbb{Q}_q \times \mathbb{Q}_q \times A'_q$ splits, and the first two factors correspond to P and to $-P$. The image in the first factor is not defined if we just evaluate F on P, but we can use the condition that the product of the first two components must be a cube in $\mathbb{Q}_q$. Hence the image is

$$F_q(P) = ((c')^2 F'(x(P), y(P))^2, c'F'(x(P), y(P)), c''F''(x(P), y(P)) ,$$

where F' is F with $(\sigma, \tau) = (x(P), -y(P))$ and F'' is F with $(\sigma, \tau) =$ its image in A'_q (and analogously with c' and c'').

Since we can determine the dimension of $F_q(E(\mathbb{Q}_q))$ beforehand—we have

$$\dim_{\mathbb{F}_3} F_q(E(\mathbb{Q}_q)) = \begin{cases} \dim_{\mathbb{F}_3} E(\mathbb{Q}_q)[3] & \text{if } q \neq 3, \\ \dim_{\mathbb{F}_3} E(\mathbb{Q}_q)[3] + 1 & \text{if } q = 3, \end{cases}$$

we now simply find points in $E(\mathbb{Q}_q)$ (in a random or systematic way, compare [30] for a description in the case of a 2-descent) until their images under F_q generate a space of the correct size.

10.2. **The algorithm for $a = 0$.** For an algorithm that is applicable when ζ_3 is contained in the basefield, see Cassels [4].

When $a = 0$, we have $\phi(x) = x(x^3 + 4b)$, hence

$$A_+ = A_{+,1} \times A_{+,2} = \mathbb{Q} \times \mathbb{Q}(\sqrt[3]{4b}) .$$

The eight 3-torsion points are $(0, \pm\sqrt{b})$ and $(-\omega^\nu \sqrt[3]{4b}, \pm\sqrt{-3b})$, where ω is a primitive cube root of unity and $\nu \in \{0, 1, 2\}$. This means that

$$A = A_1 \times A_2 = \mathbb{Q}(\sqrt{b}) \times \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) .$$

Similarly,

$$B = B_1 \times B_2 = \mathbb{Q}(\sqrt{-3b}) \times \mathbb{Q}(\sqrt{b}, \sqrt[3]{4b}) .$$

(Here, $\mathbb{Q}(\sqrt{b})$ is to be read as the étale algebra $\mathbb{Q}[T]/(T^2-b)$, and hence $A_1 \cong \mathbb{Q}\times\mathbb{Q}$ if b is a square. Similarly for the other terms.)

Note that we cannot throw away the first component A_1 of A, even though the subset X_2 of $E[3]$ corresponding to A_2 is a Galois-invariant spanning set. This is because $\#X_2 = 6$ is a multiple of 3, compare Prop. 6.4.

The definition of $\bar{u}$ has to be adapted accordingly. We fix a basis $P = (0, \sqrt{b})$, $Q = (-\sqrt[3]{4b}, \sqrt{-3b})$ of $E[3]$. This serves to fix the elements $\sqrt{b}, \sqrt{-3b}, \sqrt[3]{4b} \in L$, where $L = \mathbb{Q}(\sqrt{b}, \sqrt{-3b}, \sqrt[3]{4b})$. We then define $\sqrt{-3} = \sqrt{-3b}/\sqrt{b}$ and the cube root of unity $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. We have $D = D_1 \times D_2 \times D_3$ with

$$\begin{aligned} D_1 &= \mathbb{Q}(\sqrt{b}, \sqrt[3]{4b}) = B_2 , \\ D_2 &= \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) = A_2 , \\ D_3 &= \mathbb{Q}(\sqrt{b}, \sqrt{-3b}, \sqrt[3]{4b}) = L . \end{aligned}$$

The inclusion of A in D is given by $A_1 \longrightarrow D_1$ and $A_2 \longrightarrow D_2 \times D_3$ (diagonally), and the inclusion of B in D is given by $B_1 \longrightarrow D_2$ and $B_2 \longrightarrow D_1 \times D_3$, where the map $B_2 \longrightarrow D_3$ is inclusion followed by the automorphism ρ of order 3 of D_3 sending $\sqrt[3]{4b}$ to $\omega^{-1}\sqrt[3]{4b}$. Hence we have for an element $\alpha = (\alpha_1, \alpha_2) \in A_1 \times A_2 = A$ that

$$\bar{u}(\alpha) = N_{D/B}(\alpha_1, \alpha_2, \alpha_2) = (N_{A_2/B_1}(\alpha_2), \alpha_1 \, N_{D_3/B_2}(\alpha_2^\rho)) \in B_1 \times B_2 = B .$$

This implies the following description (taking an arbitrary field K instead of $\mathbb{Q}$ as the base).

$$\begin{aligned} H^1(K, E[3]) \cong \{(\alpha_1, \alpha_2) \in A_1^\times/(A_1^\times)^3 \times A_2^\times/(A_2^\times)^3 \mid \\ N_{A_1/K}(\alpha_1) \in (K^\times)^3, N_{A_2/A_{+,2}}(\alpha_2) \in (A_{+,2}^\times)^3, \\ i_{B_2/A_1}(\alpha_1) N_{D_3/B_2}(\alpha_2^\rho) \in (B_2^\times)^3, N_{A_2/B_1}(\alpha_2) \in (B_1^\times)^3\} \end{aligned}$$

From this, the algorithm for $y^2 = x^3 + b$ can easily be derived.

Note that such a curve has complex multiplication, and hence has good or additive reduction everywhere. Therefore the Tamagawa number can only be divisible by 3 when the reduction type is IV or IV*. A more careful analysis using Tate's algorithm shows that we can take

$$S = \{3\} \cup \{q \mid 4b \in (\mathbb{Q}_q^\times)^2, 6 \nmid v_q(4b)\}\,.$$

It is also fairly easy to determine the image of F_q for $q \in S \setminus \{3\}$.

Lemma 10.1. *Let $q \in S \setminus \{3\}$, and let ω be the primitive cube root of unity defined above. The image of F_q is a one-dimensional $\mathbb{F}_3$-vector space, and a generator is represented by*

$$(4b, 2b^2, \omega^2) \in \mathbb{Q}_q \times \mathbb{Q}_q \times \mathbb{Q}_q(\sqrt{-3}, \sqrt[3]{4b}) = A_q$$

if $q \equiv 2 \bmod 3$, and by

$$(4b, 2b^2, \omega^2, \omega) \in \mathbb{Q}_q \times \mathbb{Q}_q \times \mathbb{Q}_q(\sqrt[3]{4b}) \times \mathbb{Q}_q(\sqrt[3]{4b}) = A_q$$

if $q \equiv 1 \bmod 3$. The first factor of A_q here corresponds to the point $P = (0, \sqrt{b})$. In the second case, the third factor corresponds to the orbit of the point $Q = (-\sqrt[3]{4b}, \sqrt{-3b})$.

Proof: We have already seen that $A_+ = \mathbb{Q} \times \mathbb{Q}(\sqrt[3]{4b})$ splits and that $\sigma = 0$ in the first factor. Hence we have to modify the calculation of $c = F(-O)$ for this first component. Instead of the two points with $x = 0$, we take the two points with $x = 1$ and get (modulo cubes)

$$c = (-4b, 3(1 + \sqrt[3]{4b})^3) \sim (4b, 3) \in \mathbb{Q} \times \mathbb{Q}(\sqrt[3]{4b})\,.$$

Now for $q \in S \setminus \{3\}$, we have that b is a square in $\mathbb{Q}_q$, but $4b$ is not a cube in $\mathbb{Q}_q$. Hence $E(\mathbb{Q}_q)[3]$ has order 3 and is generated by $(0, \sqrt{b})$. This already implies that the image of F_q also has order 3.

We now proceed to find the image under F_q of $(0, \sqrt{b}) \in E(\mathbb{Q}_q)[3]$. The relevant components of F are

$$F' = -2\sqrt{b}\,y - 2b \qquad \text{and} \qquad F'' = 2\sqrt{-3b}\,y - 3\sqrt[3]{4b}^2 x - 6b\,,$$

hence

$$\begin{aligned} F_q(0, \sqrt{b}) &= ((4b \cdot (-4b))^2, 4b \cdot (-4b), 3 \cdot (2\sqrt{-3} - 6)b) \\ &\sim (4b, 2b^2, \frac{-1 - \sqrt{-3}}{2}) \in \mathbb{Q}_q \times \mathbb{Q}_q \times A'_q \end{aligned}$$

(note that $b \sim 2$ and that $3(\sqrt{-3}-3) \sim -1-\sqrt{-3}$ in A'_q). Since $4b$ is not a cube in $\mathbb{Q}_q$, this image is non-trivial and therefore generates the image of F_q, proving the claim. □

11. Examples

In this section we present four worked examples covering the various cases discussed in this paper. The first example shows a full 3-descent in the generic case where one has to deal with an octic number field. The second example shows a full 5-descent in the special case where the curve has CM by $\mathbb{Z}[i]$ and so 5 splits in the endomorphism ring. This also leads to an octic number field. The other two examples show a descent by isogeny. One uses a 13-isogeny to show that Ш[13] is trivial for two isogenous curves of rank one; the other uses a 3-isogeny to show that #Ш[3] = 81 for a certain elliptic curve.

When dealing with concrete examples, it is often possible to exploit bounds like

$$\dim E(\mathbb{Q})[p] + \operatorname{rank} E(\mathbb{Q}) \le \dim \operatorname{Sel}^{(p)}(\mathbb{Q}, E) \le \dim A(S,p)^{(1)}\,.$$

If upper and lower bounds coincide, the dimension of the Selmer group is determined, and some of the computations (like finding local images or determining the kernel of $\bar{u}$) can be avoided. This is demonstrated in some of the examples below.

11.1. **An example of a generic full 3-descent.** Let E be the elliptic curve over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 - 22\,x^2 + 21\,x + 1\,.$$

One easily finds the two independent points $P = (0,1)$ and $Q = (1,1)$, so E has Mordell-Weil rank at least 2.

A 2-descent gives 4 as the 2-Selmer rank. The analytic rank is 2, and (assuming P, Q to be a basis of the Mordell-Weil group) the analytic size of the Shafarevich-Tate group is 4 (to many decimal digits; thanks to John Cremona for his help with the computation). So we conjecture that the rank is 2 and that $\#Ш(\mathbb{Q}, E) = 4$.

We will show (assuming GRH) that the rank is indeed 2 and that $\#Ш(\mathbb{Q}, E)[2] = 4$. One could try to use a 4-descent to prove this, but we will use a 3-descent. The curve has no rational isogenies and is not CM, therefore we have to do a generic full 3-descent.

The conductor is $1685192 = 2^3 \cdot 313 \cdot 673$; the Tamagawa numbers are $c_2 = 2$, $c_{313} = c_{673} = 1$. This means that we can take $S = \{3\}$.

The algebra A_+ is a quartic number field, generated by a zero of the 3-division polynomial

$$3\,x^4 - 88\,x^3 + 126\,x^2 + 12\,x - 529\,.$$

The algebra A is an octic number field and can be generated by a zero of the polynomial

$$T^8 - 2526\,T^4 - 68444\,T^2 - 531723\,.$$

We find that A_+ has signature $(2,1)$, whereas A has signature $(2,3)$. (This is always the case for elliptic curves over $\mathbb{Q}$.) Furthermore, all the primes above 3 in A are in A/A_+ either ramified or inert. From this, we conclude for the S-units U_S of A that

$$\dim(U_S/U_S^3)^{(1)} = 2\,.$$

(This comes from the 'new units' in A/A_+; the primes above S do not contribute, since they 'come from A_+'.)

Using KANT/KASH [15] or MAGMA [16], we find that the class group of A is cyclic of order 24, whereas the class group of A_+ has order 2 (this part of the computation is not strictly proven to be correct, since it assumes GRH). This implies that $\mathrm{Cl}_S(A)^{(1)}$ is one-dimensional, and so

$$\dim A(S,3)^{(1)} = 3\,.$$

We can find explicit generators b_1, b_2, b_3 by using KASH again. We do not give them here, since the coefficients get fairly big (around 125 digits for b_3 on the integral basis chosen by KASH). The first two are units, the third is a generator of $\mathfrak{p}_{47}^3$, where $\mathfrak{p}_{47}$ is a prime ideal of norm 47 in A (this is the smallest norm of an integral ideal whose ideal class has order 3).

We have $E(\mathbb{Q}_3)[3] = 0$, so the image of $E(\mathbb{Q}_3)$ in $H^1(\mathbb{Q}_3, E[3])$ is one-dimensional. We find that the restriction map

$$\mathrm{res}_3 : A(S,3)^{(1)} \quad\longrightarrow\quad A_3^\times/(A_3^\times)^3$$

has one-dimensional kernel generated by $b_1 b_3^2$. We now have

$$2 \le \operatorname{rank} E(\mathbb{Q}) \le \dim \mathrm{Sel}^{(3)}(\mathbb{Q}, E) \le \dim\ker(\mathrm{res}_3) + \dim\mathrm{image}(\delta_3) = 1 + 1 = 2\,.$$

So we can conclude that the rank is indeed 2. Together with the result of the 2-descent, this then also shows that $\#\text{Ш}(\mathbb{Q}, E)[2] = 4$ (and $\text{Ш}(\mathbb{Q}, E)[3] = 0$).

11.2. **An example of a full 5-descent in a special case.** Let E be the elliptic curve given by

$$y^2 = x^3 - 1483\,x$$

over $\mathbb{Q}$. The endomorphism ring is isomorphic to $\mathbb{Z}[i]$. The prime 5 splits as $5 = (2+i)(2-i)$ in the endomorphism ring. A descent via 2-isogeny shows that the Mordell-Weil rank of E over $\mathbb{Q}$ is 0. The only rational, non-trivial torsion point is $(0,0)$ (of order 2). Therefore, the two groups $\mathrm{Sel}^{(5)}(\mathbb{Q}, E)$ and $\text{Ш}(\mathbb{Q}, E)[5]$ are isomorphic. We will show that they have dimension 2 over $\mathbb{F}_5$. Note that this is in accordance with the analytic size of $\text{Ш}(\mathbb{Q}, E)$ predicted by the Birch and Swinnerton-Dyer conjecture, which is 25.

Since E has complex multiplication, our result (and much more) also follows from work of Coates and Wiles and of Rubin (see for example [23] and the references given there). We thank Karl Rubin for pointing this out to us. The reason for including this example here is to demonstrate the technique. Our approach is also applicable when the rank is at least two or when there is a Galois-conjugate pair of cyclic subgroups and the curve does not have CM.

The x-coordinates of the points in $(E[2+i] \cup E[2-i]) \setminus \{0\}$ are roots of the polynomial

$$5\,x^4 - 3446\,x^2 + 2968729\,.$$

The resultant of that and the equation defining the elliptic curve is

$$y^8 - 2262538514230\,y^4 + 1323479838749136590028125\,.$$

This is an irreducible polynomial over $\mathbb{Q}$. For computations in KASH and PARI, we need as simple an octic as possible, defining the same field. We use

$$f(T) = T^8 + 32626\,T^4 + 274911125\,,$$

where $y = 9/370750\,T^7 + 73/250\,T^3$. Let A_1 be the étale algebra corresponding to $f(T)$. Following the discussion in Section 8, we can take $S = \{5\}$ and the group $H^1(\mathbb{Q}, E[5]; S)$ is then isomorphic to $A_1(S, 5)^{(1)}$.

Assuming GRH (as is usually done in practical computations like this), KANT [15] computes the class group of A_1 to be isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/60\mathbb{Z}$. Since the quartic subfield of A_1 (generated by T^2) has class number prime to 5, we have

$$\mathrm{Cl}(A_1)[5] \cong \mathrm{Cl}(A_1)[5]^{(1)} \oplus \mathrm{Cl}(A_1)[5]^{(3)}\,,$$

and we find that both summands are one-dimensional. Since $E(\mathbb{Q}_5)[5] = 0$, we get from Theorem 8.1 that $\dim_{\mathbb{F}_5} A_1(\{5\}, 5)^{(1)} = 2$ and that the dimension of the Selmer group is either 1 or 2. With the help of Claus Fieker, we were able to use KASH to find explicit generators of $A_1(\{5\}, 5)^{(1)}$.

We now proceed to find the image of F_5. The group $E(\mathbb{Q}_5)/5E(\mathbb{Q}_5)$ is generated by the divisor class $[(50, y_1) - (1/25, y_2)]$ where $y_1 \equiv 10 \bmod 25$ and $y_2 \equiv 1/125 \bmod 5$. Let $B = A_1 \otimes_{\mathbb{Q}} \mathbb{Q}_5$. We have $B \cong B_1 \times B_2 \times B_3$ where B_1 is a quartic, totally ramified extension of $\mathbb{Q}_5$ and the other two are each the quadratic unramified extension of $\mathbb{Q}_5$.

We have the point

$$P = (-2/37075\,T^6 - 19/25\,T^2, 9/370750\,T^7 + 73/250\,T^3)$$

in $(E[2+i] \cup E[2-i]) \setminus \{0\}$. Following the algorithm in [9], we find a function F, over B, with divisor $5\,P - 5\,O$. The image in $\prod_i B_i^\times/(B_i^\times)^5$ of the divisor class generating $E(\mathbb{Q}_5)/5E(\mathbb{Q}_5)$ is $(1, (1+5T)^3, (1+5T)^3)$. The dimensions of $\big(B_1^\times/(B_1^\times)^5\big)^{(1)}$ and $\big((B_2 \times B_3)^\times/((B_2 \times B_3)^\times)^5\big)^{(1)}$ are each 1. Therefore, to show that an element of $A_1(S, 5)^{(1)}$ maps to the image of $E(\mathbb{Q}_5)/5E(\mathbb{Q}_5)$, it suffices to show that it maps to a fifth power in B_1. Both generators do. Thus, the groups $A_1(S, 5)^{(1)}$, $\mathrm{Sel}^{(5)}(\mathbb{Q}, E)$ and $\text{Ш}(\mathbb{Q}, E)[5]$ are all isomorphic, and each has $\mathbb{F}_5$-dimension 2.

11.3. **An example of a 13-isogeny descent.** Let E and E' be the following elliptic curves over $\mathbb{Q}$ (curves 441F1 and 441F2 in Cremona's list, see [7]).

$$E : y^2 + y = x^3 - 21\,x + 40$$
$$E' : y^2 + y = x^3 - 8211\,x - 286610$$

From the list, we see that they are related by a 13-isogeny and that they both have Mordell-Weil rank 1. In fact it is easy to spot the point $P = (1, 4)$ on E of infinite order. The analytic sizes of $\text{Ш}(\mathbb{Q}, E)$ and of $\text{Ш}(\mathbb{Q}, E')$ are both 1. We will show by a 13-isogeny descent that

$$\text{Ш}(\mathbb{Q}, E)[13] = \text{Ш}(\mathbb{Q}, E')[13] = 0\,.$$

All the Tamagawa numbers are prime to 13, so we take $S = \{13\}$ for both Selmer group computations. Let us first consider $\mathrm{Sel}^{(h')}(\mathbb{Q}, E')$. The factor of the 13-division polynomial of E corresponding to the kernel of h is

$$(x^3 - 21\,x - 7)(x^3 - 21\,x^2 + 84\,x - 91)\,.$$

We see that the algebra C_2 will split into two copies of a sextic field $\mathcal{C}_2$. A short computation using Magma or PARI shows that $\mathcal{C}_2$ is generated by a root of the polynomial

$$T^6 + T^5 - 6\,T^4 - 6\,T^3 + 8\,T^2 + 8\,T + 1\,.$$

The Minkowski constant for this field is only 10, so we can compute all the relevant arithmetic data unconditionally. It turns out that the class group is trivial. The field is a totally real cyclic extension of $\mathbb{Q}$, hence the (1)-eigenspace on the units mod 13th powers is one-dimensional. The primes above 13 in $\mathcal{C}_2$ are all inert in the quadratic subextension, hence there is no contribution from them to the (1)-eigenspace of the S-units. Together, we have

$$\dim \mathcal{C}_2(S, 13)^{(1)} = 1$$

and therefore

$$\dim \mathrm{Sel}^{(h')}(\mathbb{Q}, E') \le 1\,.$$

Now since $\Omega_E = 13\,\Omega_{E'}$ (as computed by PARI), Cassels' formula (9.2) tells us that

$$0 \le \dim \mathrm{Sel}^{(h)}(\mathbb{Q}, E) = \dim \mathrm{Sel}^{(h')}(\mathbb{Q}, E') - 1 \le 0\,,$$

so we must have equality throughout.

By Lemma 9.1, we now get the following inequalities (note that neither E nor E' have non-trivial rational torsion).

$$1 \le \dim \mathrm{Sel}^{(13)}(\mathbb{Q}, E) \le \dim \mathrm{Sel}^{(h)}(\mathbb{Q}, E) + \dim \mathrm{Sel}^{(h')}(\mathbb{Q}, E') = 1$$

$$1 \le \dim \mathrm{Sel}^{(13)}(\mathbb{Q}, E') \le \dim \mathrm{Sel}^{(h')}(\mathbb{Q}, E') + \dim \mathrm{Sel}^{(h)}(\mathbb{Q}, E) = 1$$

Hence $\dim \mathrm{Sel}^{(13)}(\mathbb{Q}, E) = \dim \mathrm{Sel}^{(13)}(\mathbb{Q}, E') = 1$, and since this equals the Mordell-Weil rank, we get

$$Ш(\mathbb{Q}, E)[13] = Ш(\mathbb{Q}, E')[13] = 0\,.$$

11.4. **An example of a 3-isogeny descent.** Let E be the elliptic curve over $\mathbb{Q}$ defined by

$$y^2 - 41\,xy + 2310\,y = x^3 + 94710\,x\,.$$

The point $(0, 0)$ has order 3. Let E' be the elliptic curve over $\mathbb{Q}$ defined by

$$y^2 + xy = x^3 - 485065\,x - 130065985\,.$$

There is an isogeny h over $\mathbb{Q}$ from E to E' whose kernel is generated by $(0, 0)$. The analytic rank of both curves is 0 so their Mordell-Weil ranks are also. The analytic sizes of their Shafarevich-Tate groups are 1 and 81 respectively; of course this is only conjectural. Let us verify $Ш(\mathbb{Q}, E')[3]$. First we compute $\mathrm{Sel}^{(h')}(\mathbb{Q}, E')$. From the discussion in Section 9, the group $H^1(\mathbb{Q}, E'[h'])$ is isomorphic to $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$. The primes dividing the conductor of E are $2, 3, 5, 7, 11$ and 6551. We have $c_{E,q} = 3$ for $q = 2, 3, 5, 7$ and 11 and $c_{E,6551} = 1$. We have $c_{E',q} = 1$ for all primes.

So $\mathrm{Sel}^{(h')}(\mathbb{Q},E')$ is contained in the subgroup $\langle 2,3,5,7,11\rangle$ of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$. The tangent line at $(0,0)$ on E is $y=41\,x$. So we take $F=y-41\,x$ as the function from $E(\mathbb{Q})/h'E'(\mathbb{Q})$ to $\langle 2,3,5,7,11\rangle$. Evaluating F on a good divisor linearly equivalent to $(0,0)-O$, we compute

$$F((0,0))=2^2\cdot 3^2\cdot 5^2\cdot 7^2\cdot 11^2 \bmod (\mathbb{Q}^\times)^3\,.$$

For the primes $q=2,3,5,7$ and 11, the groups $E(\mathbb{Q}_q)/h'E'(\mathbb{Q}_q)$ are $\langle(0,0)\rangle$, $\langle(0,0),(9,\alpha)\rangle$, $\langle(0,0)\rangle$, $\langle(0,0),(\beta,2)\rangle$, and $\langle(0,0)\rangle$ respectively (where α is either possible y-coordinate and $\beta\equiv 2 \bmod 7$). The function F maps these onto $\mathbb{Q}_q^\times/(\mathbb{Q}_q^\times)^3$ for all five primes (F is injective and the dimensions match). Thus $\mathrm{Sel}^{(h')}(\mathbb{Q},E')$ is all of $\langle 2,3,5,7,11\rangle$. Since the image of $E(\mathbb{Q})$ is a 1-dimensional subspace of $\mathrm{Sel}^{(h')}(\mathbb{Q},E')$, the dimension of $\text{Ш}(\mathbb{Q},E')[h']$ is 4. Using Cassels' formula (9.2) we find that $\mathrm{Sel}^{(h)}(\mathbb{Q},E)$ is trivial and hence $\text{Ш}(\mathbb{Q},E)[h]$ is trivial. Since

$$0 \longrightarrow \text{Ш}(\mathbb{Q},E')[h'] \longrightarrow \text{Ш}(\mathbb{Q},E')[3] \longrightarrow \text{Ш}(\mathbb{Q},E)[h]$$

is exact, we see that $\text{Ш}(\mathbb{Q},E')[3]$ has dimension 4.

References

[1] M.F. Atiyah and C.T.C. Wall, *Cohomology of groups*, in: *Algebraic Number Theory*, Ed. J.W.S. Cassels and A. Fröhlich, Academic Press, London, 1967, pp. 94–115.

[2] K.S. Brown, *Cohomology of groups*, Springer, GTM vol. 87, 1982.

[3] N. Bruin, *Chabauty methods and covering techniques applied to generalised Fermat equations*, Ph.D. dissertation, Leiden, 1999.

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

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

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

[7] J.E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997.

[8] J.E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), 13–28.

[9] 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.

[10] Z. Djabri and N.P. Smart, *A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve*, in: *Algorithmic number theory. 3rd international symposium, ANTS-III, 1998*, Ed. J.P. Buhler, Springer LNCS vol. 1423, 1998, pp. 502–513.

[11] T. Dokchitser, *Deformations on p-divisible groups and p-descent on elliptic curves*, Ph.D. dissertation, Universiteit Utrecht, 2000.

[12] D.K. Faddeev: *Invariants of divisor classes for the curves $x^k(1-x)=y^l$ in an l-adic cyclotomic field* (Russian), Tr. Mat. Inst. Steklova **64** (1961), 284–293.

[13] T. Fisher, *On 5 and 7 descents for elliptic curves*, Ph.D. thesis, Cambridge, UK, 2000.

[14] E.V. Flynn and J.L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscr. Math. **100** (1999), 519–533.

[15] KANT/KASH is described in M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, *KANT V4*, J. Symbolic Comp. **24** (1997), 267–283.

[16] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), 235–265. (Also see the Magma home page at `http://www.maths.usyd.edu.au:8000/u/magma/`.)

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

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

[19] L.J. Mordell, *On the rational solutions of the indeterminate equations of the 3rd and 4th degrees*, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

[20] PARI homepage: `http://www.parigp-home.de/`

[21] B. Poonen and E.F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188.

[22] K. Rubin, *Descents on elliptic curves with complex multiplication*, in: *Théorie des nombres, Séminaire Paris 1985/86*, Ed. C. Goldstein, Progress in Mathematics, vol. 71, Birkhäuser, 1987, pp. 165–173.

[23] K. Rubin, *The one-variable main conjecture for elliptic curves with complex multiplication*, in: *L-functions and arithmetic*, Ed. J. Coates and M.J. Taylor, LMS Lecture Notes Series, vol. 153, Cambridge University Press, Cambridge, 1991, pp. 353–371.

[24] E.F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), 79–114.

[25] E.F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), 447–471.

[26] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[27] J.H. Silverman, *The arithmetic of elliptic curves*, Springer GTM 106, 1986.

[28] D. Simon, *Équations dans les corps de nombres et discriminants minimaux*, Thèse, Bordeaux, 1998.

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

[30] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.

[31] J. Top, *Descent by 3-isogeny and 3-rank of quadratic fields*, in: *Advances in number theory*, Ed. F. Gouvea and N. Yui, Clarendon Press, Oxford, 1993, pp. 303–317

[32] A. Weil, *Sur un théorème de Mordell*, Bull. Sci. Math. (2) **54** (1930), 182–191.

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053, USA.

E-mail address: `eschaefe@math.scu.edu`

School of Engineering and Science, International University Bremen, P.O.Box 750 561, 28 725 Bremen, Germany.

E-mail address: `m.stoll@iu-bremen.de`