Computing the *p*-Selmer Group of an Elliptic Curve

Z. Djabri[†], Edward Schaefer[‡], Nigel Smart
Extended Enterprise Laboratory
HP Laboratories Bristol
HPL-98-178(R.1)
26 May, 1999*

elliptic curves,
Selmer group,
Mordell-Weil rank

In this paper we explain how to bound the *p*-Selmer group of an elliptic curve over *K*, a number field. Our method is an algorithm which is relatively simple to implement, although it requires data such as units and class groups from number fields of degree at most $p^2 - 1$. Our method is practical for $p = 3$ but for larger values of *p* becomes impractical with current computing power. In the examples we have calculated, our method produces exactly the *p*-Selmer group of the curve, and so one can use the method to find the Mordell-Weil rank of the curve when the usual method of 2-descent fails.

[†]Institute of Maths and Statistics, University of Kent at Canterbury, Canterbury, Kent, UK
[‡]Department of Mathematics, Santa Clara University, Santa Clara, CA
*Internal Accession Date Only

COMPUTING THE p-SELMER GROUP OF AN ELLIPTIC CURVE

Z. DJABRI, EDWARD F. SCHAEFER AND N.P. SMART

ABSTRACT. In this paper we explain how to bound the p-Selmer group of an elliptic curve over K, a number field. Our method is an algorithm which is relatively simple to implement, although it requires data such as units and class groups from number fields of degree at most $p^2 - 1$. Our method is practical for $p = 3$ but for larger values of p becomes impractical with current computing power. In the examples we have calculated, our method produces exactly the p-Selmer group of the curve, and so one can use the method to find the Mordell-Weil rank of the curve when the usual method of 2-descent fails.

Let E denote an elliptic curve, defined over K, a number field, which we assume is given by an equation of the form

$$y^2 = x^3 + ax + b.$$

It is a fundamental question as to how to determine the Mordell-Weil rank of such curves. The standard method is to perform a descent type argument and to bound the size of $E(K)/mE(K)$ for some integer m. This is usually done by determining the mth Selmer group, $S_m(E/K)$ which contains $E(K)/mE(K)$. In the literature this method is only completely explained in the case $m = 2$, see [3] and [4], for which very efficient programs exist to carry out the computation, for example [7]. For other prime values of m the method, as it is described, requires one to extend the ground field to the minimal algebraic number field, L, which contains the m-division points, [18, VIII Lemma 1.1.1]. The Selmer group, $S_m(E/L)$, is then determined and not $S_m(E/K)$. The structure of $S_m(E/K)$, and hopefully generators of $E(K)$, can then be obtained using a Galois descent argument.

This is unsatisfactory for several reasons. If we rely on the use only of $m = 2$, then we lay ourselves open to the problem that we may not be able to determine the rank as the curve may have a non-trivial 2-part of the Tate-Shafarevich group, $Ш(E/K)$. Further descents, [10], can then be carried out but again this is only completely explicit for the case $m = 4$. Alternatively one can make use of the Cassels-Tate pairing on $Ш(E/K)$, [5].

Extending to a number field L also gives rise to problems. For example $Ш(E/L)$ could have a nontrivial m-part when $Ш(E/K)$ does not. So we could in fact make matters worse by extending the ground field. It is also somewhat against the spirit of the exercise to compute the generators of $E(K)$ given the generators of $E(L)$.

In this paper we hope to remedy the situation by giving an explicit method to compute an approximation to the m-Selmer group, $S_m(E/K)$, of an elliptic curve over K, for values of m which are prime. For the rest of the paper we shall take $m = p$, a prime number. We shall not need to extend the field of definition of the

1991 *Mathematics Subject Classification.* Primary: 11G05, 11Y99, Secondary: 14H52, 14Q05.
Key words and phrases. Elliptic Curves, Mordell-Weil rank, Selmer group.

elliptic curve, but we will need to perform arithmetic in the fields of definition of the points of order p.

Our method shall be based on that found in [15], to which we refer the reader for further details and proofs of some of the results. That paper gives a general algorithm for computing Selmer groups of Jacobians. The algorithm relies on two assumptions. The first requires there to be a rational divisor class of degree relatively prime to the exponent of the kernel of the isogeny. This is guaranteed in our case by the fact that an elliptic curve has a rational point. The second assumption is shown to hold for elliptic curves and multiplication by p maps in section 3.

Our method will be unconditional on any conjectures. For fixed p our method will have a conjectured sub-exponential complexity in the size of a and b. It will be exponential if we measure the complexity in terms of p. Throughout we shall illustrate the method with explicit equations for the familiar case of 2-descent and the perhaps unfamiliar case of 3-descent. We shall end with an example where we compute the 3-Selmer group of an elliptic curve over $\mathbb{Q}$. A preliminary report on our method in the case $p = 3$ appeared in [8], we now take the opportunity to include full proofs of the necessary results.

The method is practical for the case $p = 3$, but for $p = 5$ the number field data required approaches the limit of current computing power and techniques. Further advances in algorithms for computing class groups and unit groups of number fields should allow the range of applicability of our method to be extended.

We stress that our method is not to be used as the preferred choice for computing the rank of a curve. However it, hopefully, fills in a gap in the methods which require that the group $Ш(E/K)$ has no elements of order 2 or 4. We note that when $Ш(E/K)$ has elements of order 2 or 4 and E has a K-rational p-isogeny for a small prime p, then it is better to do a descent by p-isogeny than by the multiplication by p map described here. If $p = 2$ or $p = 3$ there are well developed techniques for descent via p-isogeny, see [18] and [20]. If $p > 3$, then use [21] to find the isogenous elliptic curve and [15] to do the descent. The second assumption of [15] holds since the sizes of the kernel of the p-isogeny and its automorphism group are relatively prime.

Throughout this paper we let K denote a field. For our applications K will be either a number field or the completion of a number field. We let $\overline{K}$ denote an algebraic closure. For a $\mathrm{Gal}(\overline{K}/K)$-module N we let $N(K)$ denote the $\mathrm{Gal}(\overline{K}/K)$-invariants. We use the point at infinity as the group identity of E and denote it $\mathcal{O}$. We denote by $E[p]$, the p-torsion subgroup of E, considered in some algebraic closure. We let $E(K)[p]$ denote the set of p-torsion points defined over the field K and let $L = K(E[p])$.

We thank Michael Stoll for his helpful comments on an earlier draft of this article and an anonymous referee for many useful comments.

1. The Selmer Group

In this and the next section, we let K be a number field and let $\mathfrak{r}$ denote a place of K, possibly infinite. We let S denote the set of places of K which lie above the prime p and the primes dividing the conductor of E. When $p = 2$, we also include in S the set of real places of K. Clearly the set S will depend on the number field K; to ease notation we will not make this dependence explicit but rely on the context to convey which number field we are referring to.

For an arbitrary field F and $\mathrm{Gal}(\bar{F}/F)$-module N, we use $H^1(F,N)$ to denote $H^1(\mathrm{Gal}(\bar{F}/F),N)$. We denote by $H^1(K,E[p];S)$, the subgroup of $H^1(K,E[p])$ consisting of the cocycle classes that are unramified away from S. We let δ denote the coboundary map from $E(K)$ to $H^1(K,E[p])$; it has kernel $pE(K)$. Its image is contained in $H^1(K,E[p];S)$. For any place $\mathfrak{r}$ we let $K_{\mathfrak{r}}$ denote the completion of K at $\mathfrak{r}$ and let $\delta_{\mathfrak{r}}$ denote the coboundary map from $E(K_{\mathfrak{r}})$ to $H^1(K_{\mathfrak{r}},E[p])$, this map has kernel $pE(K_{\mathfrak{r}})$. We let $\alpha_{\mathfrak{r}}$ denote the restriction map from $H^1(K,E[p])$ to $H^1(K_{\mathfrak{r}},E[p])$.

We obtain the following commutative diagram.

$$\begin{array}{ccc} E(K)/pE(K) & \stackrel{\delta}{\hookrightarrow} & H^1(K,E[p];S) \\ \downarrow & & \downarrow \prod \alpha_{\mathfrak{s}} \\ \prod_{\mathfrak{s}\in S} E(K_{\mathfrak{s}})/pE(K_{\mathfrak{s}}) & \stackrel{\prod \delta_{\mathfrak{s}}}{\hookrightarrow} & \prod_{\mathfrak{s}\in S} H^1(K_{\mathfrak{s}},E[p]) \end{array}$$

The p-Selmer group is defined to be

$$S_p(E/K) = \bigcap_{\mathfrak{s}\in S} \alpha_{\mathfrak{s}}^{-1}(\delta_{\mathfrak{s}}(E(K_{\mathfrak{s}})/pE(K_{\mathfrak{s}}))).$$

Clearly the image of $E(K)/pE(K)$ in $H^1(K,E[p];S)$ is contained in $S_p(E/K)$. However we will require the consideration of the equivalent, but on first sight weaker, commutative diagram

$$\begin{array}{ccc} E(K)/pE(K) & \stackrel{\delta}{\hookrightarrow} & H^1(K,E[p];S) \\ \downarrow & & \downarrow \prod \alpha_{\mathfrak{r}} \\ \prod E(K_{\mathfrak{r}})/pE(K_{\mathfrak{r}}) & \stackrel{\prod \delta_{\mathfrak{r}}}{\hookrightarrow} & \prod H^1(K_{\mathfrak{r}},E[p]) \end{array}$$

where the products are now over all places, $\mathfrak{r}$, of K.

As it is difficult to work in the group $H^1(K,E[p];S)$, we will instead work in a group containing its isomorphic image, in which it is easier to do computations. This group will be the quotient of the multiplicative groups of a product of number fields. Let us define this group. When $p \neq 2$ we let $\psi_p(\sigma)$ denote the pth division polynomial and then let $g(\sigma,\tau) = \tau^2 - \sigma^3 - a\sigma - b$. We can then define the algebra

$$A = K[\sigma,\tau]/(\psi_p(\sigma), g(\sigma,\tau)).$$

In other words we let (σ,τ) denote a generic point of order p. When $p = 2$ we define the algebra A by

$$A = K[\sigma]/(\sigma^3 + a\sigma + b),$$

since the generic point of order 2 is given by $(\sigma, 0)$.

Here we establish a map from the cohomology group to a quotient of the units in A. Let $A' = A \otimes_K \overline{K}$. Let w denote the map

$$w : E[p] \to \mu_p(A') \quad \text{by} \quad R \mapsto e_p(R,(\sigma,\tau))$$

where e_p denotes the p Weil pairing. Since A' is isomorphic to a product of p^2-1 copies of $\overline{K}$, this is essentially the Weil pairing of R with all p^2-1 points of order p (see [15]). The map w is defined over K. Let *coker* denote the group which makes the following an exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules,

$$0 \to E[p] \stackrel{w}{\to} \mu_p(A') \to coker \to 0.$$

Let $\overline{w}$ denote the induced map from $H^1(K, E[p])$ to $H^1(K, \mu_p(A'))$. We shall also make use of the Kummer map, which defines the following isomorphism,

$$k : H^1(K, \mu_p(A')) \to A^*/A^{*p}.$$

Now we have a map from $E(K)/pE(K)$ to A^*/A^{*p}. Though the group A^*/A^{*p} is easier to work in, the map $k \circ \overline{w} \circ \delta$ is not straightforward. So we would like to replace that map also.

We let $f \in K(\sigma, \tau)(E)$ denote a function on E whose divisor is $p(\sigma, \tau) - p\mathcal{O}$. This can be computed via the method in [9, Chapter 5], which we describe in section 2. There is an isomorphism of E with its degree 0 divisor classes by $R \mapsto [R - \mathcal{O}]$, where brackets denote a divisor class. This map induces an isomorphism of $E(K)$ and the K-rational divisor classes. Every K-rational divisor class of degree 0 contains a K-rational divisor of the form

$$\sum_{i=1}^{n} P_i - \sum_{i=1}^{n} Q_i,$$

where $P_i, Q_i \in E(\overline{K})$ can be chosen to avoid any given finite set. We use f to define a map on the K-rational degree 0 divisor classes instead of on $E(K)$. Let $R \in E(K)$. Let D be a K-defined divisor of degree 0 whose support is disjoint from the support of f with the property that D is linearly equivalent to $R - \mathcal{O}$. We let $F(R) = f(D)$. As is shown in [15], this is a well-defined group homomorphism from $E(K)/pE(K)$ to A^*/A^{*p}. In addition, F is equal to the composition $k \circ \overline{w} \circ \delta$. For $\mathfrak{r}$ a prime of K, let $A_{\mathfrak{r}} = A \otimes_K K_{\mathfrak{r}}$. We can similarly define maps $w_{\mathfrak{r}}$, $\overline{w}_{\mathfrak{r}}$, $k_{\mathfrak{r}}$ and $F_{\mathfrak{r}}$. We also have $F_{\mathfrak{r}} = k_{\mathfrak{r}} \circ \overline{w}_{\mathfrak{r}} \circ \delta_{\mathfrak{r}}$.

At this point, we can write down a similar commutative diagram to the one we traditionally think of for computing a Selmer group. We have

$$\begin{array}{ccc} E(K)/pE(K) & \stackrel{F}{\to} & A^*/A^{*p} \\ \downarrow & & \downarrow \prod \beta_{\mathfrak{r}} \\ \prod E(K_{\mathfrak{r}})/pE(K_{\mathfrak{r}}) & \stackrel{\prod F_{\mathfrak{r}}}{\to} & \prod A_{\mathfrak{r}}^*/A_{\mathfrak{r}}^{*p} \end{array}$$

where the products are over all primes $\mathfrak{r}$ of K. We can improve on this. We can write A as a product of number fields $\prod L_i$. For each i, let $L_i(S, p)$ denote the subgroup of elements of L_i^*, modulo pth powers, with the property that if we adjoin the pth root of such an element to L_i, we get an extension unramified outside of primes in S. These groups can be computed in conjectured sub-exponential time (with p fixed) using an obvious generalization of the method in [17]. Let $A(S, p)$ denote $\prod L_i(S, p)$; it is a finite group. We have the following commutative diagram.

$$\begin{array}{ccc} E(K)/pE(K) & \stackrel{F}{\to} & A(S,p) \\ \downarrow & & \downarrow \prod \beta_{\mathfrak{r}} \\ \prod E(K_{\mathfrak{r}})/pE(K_{\mathfrak{r}}) & \stackrel{\prod F_{\mathfrak{r}}}{\to} & A_{\mathfrak{r}}^*/A_{\mathfrak{r}}^{*p} \end{array}$$

The group

$$\bigcap_{\mathfrak{r} \text{ of } K} \beta_{\mathfrak{r}}^{-1}(F_{\mathfrak{r}}(E(K_{\mathfrak{r}})/pE(K_{\mathfrak{r}})))$$

contains a quotient of the p-Selmer group. This is not satisfactory for three reasons: the quotient, the containment and the fact that there are infinitely many primes to check. We will address all three of these problems but only satisfactorily resolve the first and to some extent, the third. In section 3, we will show that the maps F and

$F_{\mathfrak{r}}$ are always injective. Thus that intersection will, in fact, contain the p-Selmer group, not another quotient. In section 4, we will replace $A(S,p)$ by a somewhat smaller group and the new intersection will still contain the p-Selmer group. Then we will show that we can compute the same intersection by using a finite subset of the primes of K.

2. The map F

In this section, we compare the two kinds of functions that have been traditionally used to do descents and describe a practical algorithm for computing one of them. Recall f is a function, defined over K, with divisor $p(\sigma,\tau) - p\mathcal{O}$. We notice that f is only defined up to a constant multiple. Since F is defined on degree zero divisors, that constant does not matter. We can fix this multiple of f so that $f \circ [p] = g^p$, where $g \in K(\sigma,\tau)(E)$. When f has this property, we denote it by $\overline{f}$. Then, when $R \in E(K)$ is not in the support of $\overline{f}$, we have $F([R-\mathcal{O}]) = \overline{f}(R)$. (see [18, pp. 278, 320]). The advantage of using such an $\overline{f}$ is the following. When R is not in the support of the divisor of $\overline{f}$, then we can simply compute $\overline{f}(R)$ instead of finding a K-defined divisor linearly equivalent to $R-\mathcal{O}$ on which $\overline{f}$ is well-defined. The disadvantage is the necessity of determining the correct constant multiple. If found, one still needs to find linearly equivalent divisors when R is in the support of the divisor of $\overline{f}$. Thus, in practice, finding such an $\overline{f}$ may not be so useful.

Here are two examples.

$\underline{p=2}$

When $p=2$ we have, as mentioned before,

$$A = K[\sigma]/(\sigma^3 + a\sigma + b).$$

Let P denote a generic 2-torsion point, i.e. $P = (\sigma, 0)$. Then the divisor of the function $x - \sigma$ is $2P - 2\mathcal{O}$, so we take $\overline{f} = x - \sigma$. We note that $\overline{f} \circ [2]$ is, indeed, a square in $K(\sigma)(E)$ (see [18, p. 280]). Thus we can use $\overline{f}$ directly on points of $E(K)$ outside of $E[2]$. We have

$$F : \begin{cases} E(K)/2E(K) & \longrightarrow & A^*/A^{*2} \\ (x,y) & \longmapsto & x - \sigma \ \text{ when } y \neq 0. \end{cases}$$

Let x_1, x_2, x_3 be the roots of $x^3 + ax + b$ and assume that $x_1 \in K$. From [13] we also have

$$F : \ (x_1, 0) \ \longmapsto \ (x_1 - \sigma) + (x_2 - \sigma)(x_3 - \sigma).$$

We hence recover the classical method of 2-descent which is explained in [4] and [18].

$\underline{p=3}$

When $p=3$ we have

$$A = K[\sigma,\tau]/(\psi(\sigma), g(\sigma,\tau))$$

where

$$\begin{aligned} \psi(\sigma) &= 3\sigma^4 + 6a\sigma^2 + 12b\sigma - a^2, \\ g(\sigma,\tau) &= \tau^2 - \sigma^3 - a\sigma - b. \end{aligned}$$

The algebra A decomposes into a sum of number fields, $A = \sum_{i=1}^{n} L_i$, and if we assume that E possesses no rational 3-isogeny we have $n = 1$ or 2. We then define

$$f(x,y) = -2\tau(\tau - y) + (3\sigma^2 + a)(\sigma - x) \pmod{A^{*3}},$$

which is a function such that $\mathrm{div}(f(x,y)) = 3(\sigma,\tau) - 3\mathcal{O}$, as the line $-2\tau(\tau - y) + (3\sigma^2 + a)(\sigma - x) = 0$ is the tangent line to E at an affine inflection point (σ,τ) (i.e. a non-trivial 3-torsion point). The map $F : E(K)/3E(K) \to A^*/A^{*3}$ is given by

$$F : \begin{cases} E(K)/3E(K) & \longrightarrow & A^*/A^{*3} \\ \sum_{i=1}^n P_i - \sum_{i=1}^n Q_i & \longmapsto & \prod_{i=1}^n f(P_i)/f(Q_i) \end{cases}$$

where $\sum_{i=1}^n P_i - \sum_{i=1}^n Q_i$ is a K-defined divisor, whose support is disjoint from points in $E[3]$ and which is linearly equivalent to $R - \mathcal{O}$ where $R \in E(K)$ is the point whose image we want.

At this point let us discuss algorithms for finding linearly equivalent divisors avoiding certain points. Suppose we are given a point $R \in E(K)$. We will need a method to find a divisor linearly equivalent to the divisor $R - \mathcal{O}$ that avoids all points in the support of f.

If R is not a p-torsion point or a 2-torsion point then we proceed as follows. Setting $P_1 = [2]R$ we obtain

$$[R - \mathcal{O}] = [P_1 - R]\,,$$

as required. We now assume that R is a p-torsion point or a 2-torsion point. We find a line through $-R$ and some K-rational point S (which does not need to lie on the curve). This line should not pass through any (other) p-torsion point. We then let P_1 and P_2 denote the two other points of intersection of this line with the curve. Let c denote an element in the field, K, which is not the x-coordinate of a p-torsion point. We then define two points $Q_1 = (c,d)$ and $Q_2 = (c,-d)$ of E; it does not matter whether d is in K as the set $\{Q_1, Q_2\}$ is K-rational. We have

$$[R - \mathcal{O}] = [P_1 + P_2 - Q_1 - Q_2]\,,$$

and f can be evaluated on the divisor on the right.

$\underline{p > 3}$

For larger values of p, while it is possible to compute an explicit function such as those above, this is probably not a good idea. Instead we can use the following adaption of an algorithm of Miller, [11] and [9].

Let $Q = (\sigma,\tau) \in E(A)$ denote the generic point of order p considered above. We wish to carry around another piece of information with points in $E(A)[p]$, which we shall represent as a third coordinate (we stress that this is not a projective representation). We set $(P_1, f_1) = (P_2, f_2) = (Q, 1)$. We can then compute $[p](Q,1)$ using an addition chain (or binary) method using the following function *Add*.

Add

`DESCRIPTION:Modified addition algorithm`
`INPUT:` `Two pairs` (P_1, f_1), (P_2, f_2) `with` $P_i \in E[p]$ `and` $f_i \in K(\sigma,\tau)(E)$.
`OUTPUT:` `The sum` (P_3, f_3)

1. `Set` $P_3 = P_1 + P_2$ `using the usual addition formulae on the curve.`
2. `Let` $l(X,Y) \in K(\sigma,\tau)[X,Y]$ `be such that` $l(X,Y) = 0$ `is an equation of the line through` P_1 `and` P_2. `Let` x `and` y `denote the coordinate functions on` E `then` $l(x,y) \in K(\sigma,\tau)(E)$.
3. `Let` $v(x) = x - x(P_3)$ `if` $P_3 \neq \mathcal{O}$ `and` $v(x) = 1$ `if` $P_3 = \mathcal{O}$.
4. `Put` $f_3 = f_1 f_2 l(x,y)/v(x)$.

The divisor of the function $l(x,y)/v(x)$ is $P_1+P_2-P_3-\mathcal{O}$. At the end of a given iteration, let $P_3=[n]Q$, with $2\leq n\leq p$. Then, by induction, the divisor of f_3 is $nQ-[n]Q-(n-1)\mathcal{O}$. When $P_3=[p]Q=\mathcal{O}$, then $f=f_3$ is the required element in $K(\sigma,\tau)(E)$. We note that the divisor of f is indeed $pQ-p\mathcal{O}$. In practice, it is not necessary to simplify f in the function field. Here we present a good way to evaluate f. We can store the l's and v's from the above algorithm with their appropriate exponents. To evaluate f on a divisor class, we must find a K-rational divisor in that class whose support is disjoint from the supports of the divisors of all of the l's and v's (which contain only p-torsion points). Then we can evaluate each l and v on that divisor and get numbers which we multiply together with the appropriate exponents. This requires little storage and avoids the difficult symbolic manipulations required to find a representation of f in the function field which can be evaluated on any point other than $\mathcal{O}$ and Q.

3. The map $H^1(K,E[p])\stackrel{\overline{w}}{\to}H^1(K,\mu_p(A'))$

In this section we let K be a number field or the completion of a number field. The map F is equivalent to $k\circ\overline{w}\circ\delta$. The maps δ and k are injections. So if $\overline{w}$ is an injection then F is also. We show that in the case under consideration, that of elliptic curves and the multiplication by p map, that $\overline{w}$ is always an injection. This is the second assumption of [15]. Those readers who are prepared to take this fact on trust can skip this section if they wish. See [1] as a reference on the results from group cohomology that we will use. This result has been shown for $p=2$ in [13], so we will assume that p is odd.

The following two sequences are exact. Recall $L=K(E[p])$.

$$0\to E[p](K)\stackrel{w}{\to}\mu_p(A')(K)\to coker(K)\to$$

$$H^1(\mathrm{Gal}(L/K),E[p])\to H^1(\mathrm{Gal}(L/K),\mu_p(A'))$$

and

$$0\to E[p](K)\stackrel{w}{\to}\mu_p(A')(K)\to coker(K)\to H^1(K,E[p])\stackrel{\overline{w}}{\to}H^1(K,\mu_p(A')).$$

We will show that $H^1(\mathrm{Gal}(L/K),E[p])$ maps injectively into $H^1(\mathrm{Gal}(L/K),\mu_p(A'))$. Therefore $\mu_p(A')(K)$ maps surjectively onto $coker(K)$ and so the map $H^1(K,E[p])\stackrel{\overline{w}}{\to}H^1(K,\mu_p(A'))$ is injective.

Lemma 1. *If p does not divide $\#\mathrm{Gal}(L/K)$ then $\overline{w}$ is injective.*

Proof. Since the orders of $\mathrm{Gal}(L/K)$ and $E[p]$ are co-prime, $H^1(\mathrm{Gal}(L/K),E[p])=0$. □

From now on we assume that p divides the order of $\mathrm{Gal}(L/K)$. We know $\mathrm{Aut}(E[p])\cong\mathrm{GL}(2,\mathbb{F}_p)$ and $\#\mathrm{Aut}(E[p])=p(p-1)^2(p+1)$. Let Sy be a p-Sylow subgroup of $\mathrm{Gal}(L/K)$.

Lemma 2. *If Sy is not normal in $\mathrm{Gal}(L/K)$ then $\mathrm{Gal}(L/K)$ contains $SL(2,\mathbb{F}_p)$.*

Proof. [16, Proposition 15] □

Lemma 3. $H^1(\mathrm{SL}(2,\mathbb{F}_p),E[p])=0$.

Proof. Let $\langle -1 \rangle$ denote the group generated by the negative of the identity matrix. Let J denote the quotient of $\mathrm{SL}(2, \mathbb{F}_p)$ by $\langle -1 \rangle$. The inflation-restriction sequence then is

$$0 \to H^1(J, E[p]^{\langle -1 \rangle}) \to H^1(\mathrm{SL}(2, \mathbb{F}_p), E[p]) \to H^1(\langle -1 \rangle, E[p]).$$

Since $E[p]^{\langle -1 \rangle}$ is trivial and the orders of $E[p]$ and $\langle -1 \rangle$ are co-prime, the first and third cohomology groups are trivial. Thus the second one is also. □

Lemma 4. *If Sy is not normal in $\mathrm{Gal}(L/K)$, then $\overline{w}$ is injective.*

Proof. From Lemma 2, if Sy is not normal in $\mathrm{Gal}(L/K)$ then $\mathrm{SL}(2, \mathbb{F}_p)$ is normal in $\mathrm{Gal}(L/K)$ since it is the kernel of the determinant on $\mathrm{Gal}(L/K)$. Let J denote the quotient of $\mathrm{Gal}(L/K)$ by $\mathrm{SL}(2, \mathbb{F}_p)$. We have the following inflation-restriction sequence

$$0 \to H^1(J, E[p]^{\mathrm{SL}(2,\mathbb{F}_p)}) \to H^1(\mathrm{Gal}(L/K), E[p]) \to H^1(\mathrm{SL}(2, \mathbb{F}_p), E[p]).$$

Since $E[p]^{\mathrm{SL}(2,\mathbb{F}_p)}$ is trivial, the first cohomology group is trivial. From Lemma 3, the third cohomology group is trivial. Thus the second one is also. □

Lemma 5. *If $Sy = \mathrm{Gal}(L/K)$, then $\overline{w}$ is injective.*

Proof. Let Sy be generated by σ. Let N be a Sy-module. Since Sy is cyclic, the group $H^1(Sy, N)$ is isomorphic to $\hat{H}^{-1}(Sy, N)$. The latter group is the quotient of the kernel of Norm_σ on N by the image of $\sigma - 1$ on N. When $N = E[p]$, the kernel of Norm_σ is all of $E[p]$ and the image of $\sigma - 1$ is $E[p]^{Sy}$. It is then a straightforward verification that the image of a non-trivial element in $\hat{H}^{-1}(Sy, E[p])$ is not in the image of $\sigma - 1$ on $\mu_p(A')$. □

Lemma 6. *If Sy is normal in $\mathrm{Gal}(L/K)$, then $\overline{w}$ is injective.*

Proof. Let J denote the quotient of $\mathrm{Gal}(L/K)$ by Sy and let m be a $\mathrm{Gal}(L/K)$-module of exponent p. We have the following extended inflation-restriction sequence

$$0 \to H^1(J, m^{Sy}) \to H^1(\mathrm{Gal}(L/K), m) \to H^1(Sy, m)^J \to H^2(J, m^{Sy}).$$

Since p does not divide the size of J, we have $H^i(J, m^{Sy}) = 0$ for all i. Thus $H^1(\mathrm{Gal}(L/K), m) \cong H^1(Sy, m)^J$. From Lemma 5, $H^1(Sy, E[p])$ maps injectively to $H^1(Sy, \mu_p(A'))$. This still holds when we compute J-invariants. Thus $H^1(\mathrm{Gal}(L/K), E[p])$ maps injectively to $H^1(\mathrm{Gal}(L/K), \mu_p(A'))$. □

Proposition 7. *Let K be a number field or the completion of a number field. The map F from $E(K)/pE(K)$ to A^*/A^{*p} is injective.*

Proof. The map $\overline{w}$ has been shown to be injective in all possible cases in Lemmas 1,4 and 6. □

4. The image of $H^1(K, E[p]; S)$ in $A(S, p)$

In this and the next section, we again let K be a number field. Since the map $\overline{w}$ is injective (see section 3), we can embed $H^1(K, E[p]; S)$ in $A(S, p) \subset A^*/A^{*p}$. The image of $H^1(K, E[p]; S)$ in $A(S, p)$ is equal to

$$U = Ker\{A(S, p) \to H^1(K, coker)\}.$$

Here we run into a (possible) obstruction to computing the Selmer group. We need to find U. Let us first assume that we want to find U before doing local

computations. The only algorithm that the authors are aware of would be tedious for $p > 2$. Note $A(S,p)$ is a finite group contained in $H^1(K, \mu_p(A'))$. We can find an explicit description of the map w from $E[p]$ to $\mu_p(A')$ and hence an explicit description of the map from $\mu_p(A')$ to *coker*. Now we want to determine if an element of $A(S,p)$ maps trivially to $H^1(K, coker)$. We can pick a cocycle representing the element of $A(S,p)$. We know that it factors through the finite group $\mathrm{Gal}(M/K)$ where M is the maximal abelian p-extension of $L = K(E[p])$ that is unramified outside of primes in S. We can then check to see if this cocycle is a coboundary going from the finite group $\mathrm{Gal}(M/K)$ to the finite group *coker*. If we do the above, then we will not create an obstruction to computing the Selmer group. We have the following commutative diagram.

$$\begin{array}{ccc} E(K)/pE(K) & \overset{F}{\hookrightarrow} & U \\ \downarrow & & \downarrow \prod \beta_{\mathfrak{s}} \\ \prod_{\mathfrak{s} \in S} E(K_{\mathfrak{s}})/pE(K_{\mathfrak{s}}) & \overset{\prod F_{\mathfrak{s}}}{\hookrightarrow} & \prod_{\mathfrak{s} \in S} A^*_{\mathfrak{s}}/A^{*p}_{\mathfrak{s}} \end{array}$$

We note that

$$S_p(E/K) \cong \bigcap_{\mathfrak{s} \in S} \beta_{\mathfrak{s}}^{-1}(F_{\mathfrak{s}}(E(K_{\mathfrak{s}})/pE(K_{\mathfrak{s}}))).$$

The main problem here seems how to efficiently write down all the cocycles from $\mathrm{Gal}(M/K)$ to $\mu_p(A')$ and then test which ones are coboundaries. The only technique known to us is effective but akin to exhaustive search and therefore totally impractical.

If we want to avoid the above computation, then we can at least replace $A(S,p)$ by a smaller group as we see in the following proposition.

Proposition 8. *We have*

$$U \subseteq G = Ker\{N_{A/K} : A(S,p) \to K^*/K^{*p}\}.$$

Proof. We identify $A(S,p)$ with a subgroup of $H^1(K, \mu_p(A'))$, and K^*/K^{*p} with $H^1(K, \mu_p(\bar{K}))$. Recall that $coker = \mu_p(A')/w(E[p])$. The norm map is trivial on the image of $E[p]$ since the Weil pairing is additive and we are pairing with all non-trivial elements of $E[p]$. Thus we can restrict the norm map

$$N : \mu_p(A') \to \mu_p(\bar{K})$$

to *coker* in an obvious way. Hence there is an induced norm map

$$N' : H^1(K, coker) \longrightarrow H^1(K, \mu_p(\bar{K})),$$

and the composition of N' and the map $A(S,p) \to H^1(K, coker)$ commutes with $N_{A/K}$. Thus any element of U is contained in G. □

For $p = 2$, we note that $U = G$ (see [13, p. 220]).

4.1. **Using G instead of U.** Let us assume that we will start our computations by finding G and not U. So we can assume that p is odd. We have the following commutative diagram

$$\begin{array}{ccc} E(K)/pE(K) & \overset{F}{\hookrightarrow} & G \\ \downarrow & & \downarrow \prod \beta_{\mathfrak{r}} \\ \prod E(K_{\mathfrak{r}})/pE(K_{\mathfrak{r}}) & \overset{\prod F_{\mathfrak{r}}}{\hookrightarrow} & \prod A^*_{\mathfrak{r}}/A^{*p}_{\mathfrak{r}} \end{array}$$

where the products are over all primes $\mathfrak{r}$ of K. Let

$$Z_p(E/K) = \bigcap \beta_{\mathfrak{r}}^{-1}(F_{\mathfrak{r}}(E(K_{\mathfrak{r}})/pE(K_{\mathfrak{r}}))).$$

We note $S_p(E/K)$ is contained in $Z_p(E/K)$. We will present an example in section 6 where they are equal. In Corollary 12 we show that we can intersect over a finite set of primes of K and still get $Z_p(E/K)$. Readers who are only interested in implementing the algorithm can skip the rest of this section and just read Corollary 12, since in practice we will only compute $Z_p(E/K)$.

For a prime $\mathfrak{t}$ of K, let $M_{\mathfrak{t}}$ denote the completion of M at a prime over $\mathfrak{t}$.

Lemma 9. *Let m be one of the $\mathrm{Gal}(\overline{K}/K)$-modules $E[p]$, $\mu_p(A')$ or coker. We have $H^1(K, m; S) \cong H^1(\mathrm{Gal}(M/K), m)$. For any prime $\mathfrak{t} \in S$ we have $H^1(K_{\mathfrak{t}}, m) \cong H^1(\mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}}), m)$ and for $\mathfrak{t} \notin S$ we have $H^1(\mathrm{Gal}(K_{\mathfrak{t}}^{\mathrm{unr}}/K_{\mathfrak{t}}), m)$ $\cong H^1(\mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}}), m)$.*

Proof. Note $L = K(E[p]) = K(\mu_p(A')) \supseteq K(coker)$. We have the following inflation-restriction sequence

$$0 \to H^1(\mathrm{Gal}(L/K), m) \to H^1(\mathrm{Gal}(\overline{K}/K), m; S) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/L), m).$$

Consider the restriction of a cocycle in $H^1(\mathrm{Gal}(\overline{K}/K), m; S)$ to $\mathrm{Hom}(\mathrm{Gal}(\overline{K}/L), m)$. Since m has exponent p, this restricted map is trivial on $\mathrm{Gal}(\overline{K}/M)$. The proofs for the local cases are similar. □

For the remainder of this section, we will replace the cohomology groups on $\mathrm{Gal}(\overline{K}/K)$ by $\mathrm{Gal}(M/K)$, and on $\mathrm{Gal}(\overline{K}_{\mathfrak{t}}/K_{\mathfrak{t}})$ by $\mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}})$. Note that for $\mathfrak{t} \notin S$, this is in order since the images of both $E(K_{\mathfrak{t}})/pE(K_{\mathfrak{t}})$ and $H^1(K, E[p]; S)$ in $H^1(K_{\mathfrak{t}}, E[p])$ are contained in the subgroup $H^1(\mathrm{Gal}(K_{\mathfrak{t}}^{\mathrm{unr}}/K_{\mathfrak{t}}), E[p])$. By abuse of notation, let $\beta_{\mathfrak{t}}$ also denote the map

$$\beta_{\mathfrak{t}} : H^1(\mathrm{Gal}(M/K), \mu_p(A')) \longrightarrow H^1(\mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}}), \mu_p(A')).$$

Assume that $\mathfrak{t}$ and $\mathfrak{v}$ are primes of K, outside of S, with the same splitting behaviour in M. This means that the conjugacy classes of decomposition subgroups of primes over $\mathfrak{t}$ and of primes over $\mathfrak{v}$ are the same. Choose an isomorphism $\iota : \mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}}) \to \mathrm{Gal}(M_{\mathfrak{v}}/K_{\mathfrak{v}})$ such that if $\sigma \in \mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}})$ and $P \in E[p]$, then $\sigma(P) = (\iota\sigma)(P)$. Note, by the definition of $\mu_p(A')$, that if $\sigma \in \mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}})$ and $\zeta \in \mu_p(A')$, then $\sigma(\zeta) = (\iota\sigma)(\zeta)$. The map ι induces isomorphisms on cohomology groups and the following is a commutative diagram.

$$\begin{array}{ccc} E(K_{\mathfrak{t}})/pE(K_{\mathfrak{t}}) & & E(K_{\mathfrak{v}})/pE(K_{\mathfrak{v}}) \\ \downarrow & & \downarrow \\ H^1(\mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}}), E[p]) & \xrightarrow{\iota} & H^1(\mathrm{Gal}(M_{\mathfrak{v}}/K_{\mathfrak{v}}), E[p]) \\ \downarrow \overline{w}_{\mathfrak{t}} & & \downarrow \overline{w}_{\mathfrak{v}} \\ H^1(\mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}}), \mu_p(A')) & \xrightarrow{\iota} & H^1(\mathrm{Gal}(M_{\mathfrak{v}}/K_{\mathfrak{v}}), \mu_p(A')) \\ \uparrow \beta_{\mathfrak{t}} & \nearrow \beta_{\mathfrak{v}} & \\ H^1(\mathrm{Gal}(M/K), \mu_p(A')) & & \end{array} \tag{1}$$

Lemma 10. *Let $\mathfrak{t}$ be a prime of K outside of S. The map from $E(K_{\mathfrak{t}})/pE(K_{\mathfrak{t}})$ to $H^1(\mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}}), E[p])$ is an isomorphism.*

Proof. Since $E(K_{\mathfrak{t}})/pE(K_{\mathfrak{t}})$ maps injectively into $H^1(\mathrm{Gal}(M_{\mathfrak{t}}/K_{\mathfrak{t}}), E[p])$, it suffices to show that they have the same size. Since $\mathfrak{t}$ does not lie over p, the sizes of $E(K_{\mathfrak{t}})/pE(K_{\mathfrak{t}})$ and $E(K_{\mathfrak{t}})[p]$ are the same (see Lemma 14). The group

$\mathrm{Gal}(M_\mathfrak{t}/K_\mathfrak{t})$ is cyclic of order pn and generated by some σ, where n is some positive integer. Therefore, the group $H^1(\mathrm{Gal}(M_\mathfrak{t}/K_\mathfrak{t}), E[p])$ has the same size as $\hat{H}^0(\mathrm{Gal}(M_\mathfrak{t}/K_\mathfrak{t}), E[p])$. The latter group is the quotient of the kernel of $\sigma - 1$ on $E[p]$ by the image of Norm_σ. The kernel of $\sigma - 1$ is $E(K_\mathfrak{t})[p]$ and the image of Norm_σ is trivial. □

Proposition 11. *Assume that $\mathfrak{t}$ and $\mathfrak{v}$ are primes of K, outside of S, with the same splitting behaviour in M. Let g denote a cocycle class in $H^1(K, \mu_p(A'); S)$. Then $\beta_\mathfrak{t}(g)$ is in the image of $E(K_\mathfrak{t})/pE(K_\mathfrak{t})$ if and only if $\beta_\mathfrak{v}(g)$ is in the image of $E(K_\mathfrak{v})/pE(K_\mathfrak{v})$*

Proof. This follows from Lemma 10 and a diagram chase in diagram (1). □

Let T be a set of primes of K that contains S and one prime outside S with each possible splitting behaviour in M.

Corollary 12. *We have*

$$Z_p(E/K) = \bigcap_{\mathfrak{r} \in T} \beta_\mathfrak{r}^{-1}(F_\mathfrak{r}(E(K_\mathfrak{r})/pE(K_\mathfrak{r}))).$$

Proof. This follows immediately from Proposition 11. □

The previous corollary makes the computation of $Z_p(E/K)$ a finite task. The group $Z_p(E/K)$ contains the desired group $S_p(E/K)$.

5. The p-Descent Algorithm

Our first task is to find a basis for $A(S,p)$, considered as a vector space over $\mathbb{F}_p$. As noted earlier, this can be done, assuming fixed p, in conjectured sub-exponential time using a simple adaptation of the method in [17]. However, we note that since the algebra A is created using relative extensions, the relevant number field data could be created using relative algorithms such as those in [6]. This last paper is particularly relevant since the algebra, A, is a relative quadratic extension of the algebra $K[\sigma]/(\psi_p(\sigma))$, when p is odd.

Earlier we defined S as the set of primes of K lying above p, those dividing the conductor of E, and if $p = 2$, the real primes also. However, we note that we can remove from S finite primes $\mathfrak{s}$, not lying over p, for which p does not divide the Tamagawa number $E(K_\mathfrak{s})/E^0(K_\mathfrak{s})$ (see [14, §3]).

Then we make a decision and compute U or G, as described in section 4. In practice the group G is easier to find, even though this may add an obstruction to our method for computing the Selmer group.

If we are using the group U, then we can take $T = S$. If we are using G, we determine, if possible, the set of primes T, which will consist of the primes in S plus one prime outside S for each possible splitting behaviour in the field M. This may be a difficult task due to the possibly large degree of the field M. We shall note below that it is possible to take random primes in turn until one obtains no further reduction in the size of the group. This is particularly effective if after a few such primes we already find a group whose size is equal to a known lower bound on the size of the Selmer group.

Then we find bases for the groups $A_\mathfrak{t}^*/A_\mathfrak{t}^{*p}$ for each prime $\mathfrak{t}$ in T. We then describe the maps $\beta_\mathfrak{t}$ from $A(S,p)$ to $A_\mathfrak{t}^*/A_\mathfrak{t}^{*p}$ in terms of bases of each. In order to do this, we must decide which elements of $A_\mathfrak{t}^*$ are pth powers. We know that $A_\mathfrak{t}$

is a product of completions of number fields; let $L_\mathfrak{t}$ be one of those factors of $A_\mathfrak{t}$. Given an element $\alpha \in L_\mathfrak{t}$, we need to determine if α is a pth power in $L_\mathfrak{t}$. If $\mathfrak{t}$ is an infinite place then the solution is trivial, so we assume that $\mathfrak{t}$ is finite. Clearly we can reduce the problem to the case where $v_\mathfrak{t}(\alpha) = 0$. We assume that $\mathfrak{t}$ lies above the rational prime t. The problem is resolved using the following lemma.

Lemma 13. *Let $\alpha \in L_\mathfrak{t}^*$ with $v_\mathfrak{t}(\alpha) = 0$ and let*

$$r = \begin{cases} 1 & v_\mathfrak{t}(p) = 0, \\ \lfloor e_\mathfrak{t}/(t-1) \rfloor + e_\mathfrak{t} + 1 & v_\mathfrak{t}(p) \neq 0. \end{cases}$$

Then α is a pth power in $L_\mathfrak{t}^*$ if and only if α is a pth power modulo $\mathfrak{t}^r$.

Proof. The case where $v_\mathfrak{t}(p) = 0$ follows from Hensel's Lemma. Applying Hensel's Lemma in the case $v_\mathfrak{t}(p) \neq 0$ would lead us to $r = 2e_\mathfrak{t} + 1$. The improved bound given in the Lemma we deduce using the following argument.

If α is a pth power in $L_\mathfrak{t}^*$, then, since reduction modulo $\mathfrak{t}^r$ is a homomorphism, α is a pth power modulo $\mathfrak{t}^r$.

Conversely, suppose that α is a pth power modulo $\mathfrak{t}^r$, and let π denote a uniformizing parameter for $L_\mathfrak{t}^*$. We have $\alpha = b^p + b'\pi^r$ where b is a unit and b' is an integer in $L_\mathfrak{t}$. So if we set $\gamma = \alpha/b^p$, we obtain $\gamma = 1 + c'\pi^r$ with c' an integer in $L_\mathfrak{t}$. Clearly it suffices to show that γ is a pth power in $L_\mathfrak{t}^*$.

Recall that $\log(1+z)$ is convergent in $L_\mathfrak{t}^*$ when $v_\mathfrak{t}(z) > 0$, so we find that $\log\gamma = \log(1+c'\pi^r)$ is well defined. Further $\exp(z)$ converges in $L_\mathfrak{t}^*$ when $v_\mathfrak{t}(z) > e_\mathfrak{t}/(t-1)$, and in such a situation we have $v_\mathfrak{t}(\log(1+z)) = v_\mathfrak{t}(z)$. Therefore

$$\begin{aligned} v_\mathfrak{t}\left(\frac{\log\gamma}{p}\right) &= v_\mathfrak{t}\left(\frac{\log(1+c'\pi^r)}{p}\right) \\ &= v_\mathfrak{t}(c'\pi^r) - v_\mathfrak{t}(p) \geq r - v_\mathfrak{t}(p) \\ &> e_\mathfrak{t}/(t-1), \end{aligned}$$

since $v_\mathfrak{t}(p) = e_\mathfrak{t}$. So $\exp(\frac{1}{p}\log\gamma)$ converges in $L_\mathfrak{t}^*$, and hence $\gamma^{1/p} \in L_\mathfrak{t}^*$, as required. □

If the value of r from this theorem is equal to 1, then the problem can be solved by polynomial factorization techniques over finite fields. However if $r > 1$, then we need to lift the solution modulo $\mathfrak{t}$ to a solution modulo $\mathfrak{t}^2, \ldots, \mathfrak{t}^r$. However there may not be unique lifts as Hensel's Lemma does not apply in the range of r under consideration. This means we need to apply a technique like that in [12].

Let us return to the larger algorithm. We then find a representation for F as described in section 2. At this point we require the enumeration of groups of the form $E(K_\mathfrak{t})/pE(K_\mathfrak{t})$. We can compute the order of such groups using the following result.

Lemma 14.

- *If $\mathfrak{p}|p$ then $\#E(K_\mathfrak{p})/pE(K_\mathfrak{p}) = p^{[K_\mathfrak{p}:\mathbb{Q}_p]}\#E(K_\mathfrak{p})[p]$.*
- *$\#E(\mathbb{R})/2E(\mathbb{R}) = \#E(\mathbb{R})[2]/2$.*
- *If $\mathfrak{t}$ does not divide p or ∞ then $\#E(K_\mathfrak{t})/pE(K_\mathfrak{t}) = \#E(K_\mathfrak{t})[p]$.*

Proof. See [15]. □

Given we know the order of $\#E(K_\mathfrak{t})/pE(K_\mathfrak{t})$ for some prime $\mathfrak{t}$ of K, to enumerate such a group we need to select random elements in $E(K_\mathfrak{t})$. We use the injective maps $F_\mathfrak{t} : E(K_\mathfrak{t})/pE(K_\mathfrak{t}) \hookrightarrow A_\mathfrak{t}^*/A_\mathfrak{t}^{*p}$ to determine the size of the group generated by the

chosen elements of $E(K_\mathfrak{t})$. A deterministic algorithm for finding the generators can also be created along the lines of that in [19], which for fixed p and K will not affect any overall complexity estimate depending only on the coefficients of E. In practice, when $K = \mathbb{Q}$, generators are not difficult to find. This part is also simplified by the fact that the required groups are usually cyclic.

Now we have found the groups $E(K_\mathfrak{t})/pE(K_\mathfrak{t})$ and have mapped them, via $F_\mathfrak{t}$, to $A_\mathfrak{t}^*/A_\mathfrak{t}^{*p}$. We then intersect their inverse images through $\beta_\mathfrak{t}^{-1}$ and get $S_p(E/K)$ or $Z_p(E/K)$.

If our primary goal is in finding $E(K)/pE(K)$, and we started with G instead of U, then we may not need to use all primes of T or even find a full set of primes making T. We can find one prime at a time in T (starting, perhaps, with primes in S). Then we find the inverse image of $F_\mathfrak{t}(E(K_\mathfrak{t})/pE(K_\mathfrak{t}))$, for each prime, and intersect each with the previous ones. After using only a non-trivial subset of T, the intersection may have the same size as the subgroup of $E(K)/pE(K)$ generated by known points of $E(K)$. Of course the image of $E(K)/pE(K)$ in $A(S,p)$ is contained in this intersection. Thus at this point we could quit as we would have found $E(K)/pE(K)$.

6. Example

We present an example to illustrate the methods of the previous sections. We show that the 3-Selmer group of the elliptic curve

$$E : y^2 = x^3 + 12x - 35$$

over $\mathbb{Q}$ has dimension 0 as an $\mathbb{F}_3$-vector space. This example is interesting because the 2-Selmer group has dimension 2 as an $\mathbb{F}_2$-vector space which shows (as $E(\mathbb{Q})_{\mathrm{tors}} = 0$) that the 2-part of the Tate-Shafarevich group has dimension 2.

We first carried out a 2-descent using **mwrank**, [7]. This proved ineffective, for although we found that the 2-Selmer group has dimension 2 as an $\mathbb{F}_2$-vector space, the program was unable to determine whether the associated homogeneous spaces actually had a rational point, even after a couple of hours of computing time. Thus we were unable to determine the rank.

We are able to resolve this using our descent algorithm for $p = 3$. Let us find the algebra A. The third division polynomial for E is $3(x^4 + 24x^2 - 140x - 48)$. The roots are the x-coordinates of the 3-torsion points. Denote a root by α. Then $\tau^2 = \alpha^3 + 12\alpha - 35$ is the square of the corresponding y-coordinates. We find $\tau^8 - 280\tau^6 + 26658\tau^4 - 59220747 = 0$. Since $x^8 - 280x^6 + 26658x^4 - 59220747$ is irreducible over $\mathbb{Q}$, we see $\mathbb{Q}(\tau)$ is isomorphic to the algebra A. Note, for other elliptic curves, the octic polynomial produced by this method can be non-separable over K and other techniques must be used to describe the algebra A as a product of number fields.

To simplify the computations, we note that the field $\mathbb{Q}(\tau)$ is isomorphic to the field obtained by adjoining to $\mathbb{Q}$ a root θ of

$$z^8 - 4z^7 + 7z^6 - 7z^5 - 68z^4 + 143z^3 - 288z^2 + 216z - 486,$$

the isomorphism being given by

$$\tau \mapsto 1/5211(\theta^7 - 644\theta^6 + 580\theta^5 + 160\theta^4 - 13976\theta^3 + 20482\theta^2 + 288\theta - 3537).$$

The generic point of order 3 has coordinates (σ, τ), where τ is as above and

$$\sigma = 1/27(\theta^6 - 3\theta^5 + 4\theta^4 - 3\theta^3 - 71\theta^2 + 72\theta - 162).$$

The function $f(x,y)$, as described in section 2, is given by

$$(2316\theta^6 - 6948\theta^5 - 1158\theta^4 + 13896\theta^3 - 185280\theta^2 + 177174\theta + 125064)x$$
$$+(368\theta^7 - 1288\theta^6 + 1160\theta^5 + 320\theta^4 - 27952\theta^3 + 40964\theta^2 + 576\theta - 7074)y$$
$$-6176\theta^6 + 18528\theta^5 - 31652\theta^4 + 32424\theta^3 + 487132\theta^2 - 500256\theta + 2178198.$$

Using **PARI/GP**, [2], we note that the class group of A is trivial and the unit group has rank 4 and torsion $\{\pm 1\}$. The primes dividing the conductor of E are 2, 3 and 1481. However, the Tamagawa numbers at 2 and 1481 are both 1. So as the set S, we simply take $S = \{3\}$. The ideal (3) splits in the following manner in A,

$$(3) = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_4\mathfrak{p}_5,$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_5$ all have norm 3. We see that $A(S,3)$ has dimension 9 as an $\mathbb{F}_3$-vector space, and the group

$$G = Ker\{N_{A/\mathbb{Q}} : A(S,3) \to \mathbb{Q}^*/\mathbb{Q}^{*3}\}$$

has dimension 8.

We can demonstrate that $Z_3(E/\mathbb{Q}) = 0$ by finding a set of primes P for which the largest subgroup of G that maps to the image of F_p for all $p \in P$ is trivial. We find that the set of primes

$$P = \{5, 7, 11, 17, 23, 29, 31\}$$

has this property. These primes simplify the computation since at each of these primes, the group $E(\mathbb{Q}_p)/3E(\mathbb{Q}_p)$ is trivial. We can conclude that $S_3(E/\mathbb{Q}) = 0$, and that the rank of the curve is 0. Thus we deduce that the dimension of $Ш(E/\mathbb{Q})[2]$ is indeed 2.

Notice that in this example we have used primes outside of S to determine the Selmer group. This does not occur in the better-known case of computing 2-Selmer groups for elliptic curves.

References

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

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. GP/PARI version 2.0.6 *Université Bordeaux I*, 1998.

[3] B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[4] J.W.S. Cassels. *Lectures on Elliptic Curves*. LMS Student Texts, Cambridge University Press, 1991.

[5] J.W.S. Cassels. Second descents for elliptic curves. *J. Reine Angew. Math.*, 494:101–127, 1998.

[6] H. Cohen. Computation of relative quadratic class groups. In *ANTS-3 : Algorithmic Number Theory*, J. Buhler, editor. Springer-Verlag, LNCS 1423, pp 433–440, 1998.

[7] J. Cremona. *mwrank*. Available from **ftp://euclid.ex.ac.uk/pub/cremona/progs/**

[8] Z. Djabri and N.P. Smart. A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve. In *ANTS-3 : Algorithmic Number Theory*, J. Buhler, editor. Springer-Verlag, LNCS 1423, pp 502–513, 1998.

[9] A.J. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Press, 1993.

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

[11] V. Miller. Short programs for functions on curves. Unpublished Manuscript, 1986.

[12] M. Pohst. A note on index divisors. In *Computational Number Theory*, Eds A. Pethő, M. Pohst, H.C. Williams and H.G. Zimmer, Walter de Gruyter, 1991, pp 173–182.

[13] E.F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Th.*, 51:219–232, 1995.
[14] E.F. Schaefer. Class groups and Selmer groups. *J. Number Th.*, 56:79–114, 1996.
[15] E.F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310:447-471, 1998.
[16] J.-P. Serre. Points d'ordre fini des courbes elliptiques. *Inv. Math.* 15:259-331, 1972.
[17] S. Siksek and N.P. Smart. On the complexity of computing the 2-Selmer group of an elliptic curve. *Glasgow Math. Journal.*, 39:251–258, 1997.
[18] J.H. Silverman. *The arithmetic of elliptic curves.* Springer Verlag, GTM 106, 1985.
[19] M. Stoll. Implementing 2-descent in genus 2. Preprint.
[20] J. Top. Descent by 3-isogeny and the 3-rank of quadratic fields. In F.Q. Gouvea and N. Yui, editors, *Advances in Number Theory*, pages 303–317. Clarendon Press, Oxford, 1993.
[21] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A*, 243:238-241, 1971.

Institute of Maths and Statistics,University of Kent at Canterbury, Canterbury, Kent, CT2 7NF, U.K.
E-mail address: zmd1@ukc.ac.uk

Department of Mathematics, Santa Clara University, Santa Clara, CA 95053, U.S.A.
E-mail address: eschaefe@math.scu.edu

Hewlett-Packard Laboratories,Filton Road, Stoke Gifford, Bristol, BS12 6QZ, U.K.
E-mail address: nsma@hplb.hpl.hp.com