# A Comparison of Direct and Indirect Methods for Computing Selmer Groups of an Elliptic Curve

Z. Djabri*, Nigel P. Smart
Networked Systems Department
HP Laboratories Bristol
HPL-97-137
November, 1997

E-mail: zmd1@ukc.ac.uk
nsma@hplb.hpl.hp.com

elliptic curves,
Selmer groups

In this paper we examine differences between the two standard methods for computing the 2-Selmer group of an elliptic curve. In particular we focus on practical differences in the timings of the two methods. In addition we discuss how to proceed if one fails to determine the rank of the curve from the 2-Selmer group. Finally we mention briefly ongoing research into generalizing such methods to the case of computing the 3-Selmer group.

Internal Accession Date Only

*Institute of Mathematics and Statistics, University of Kent, Canterbury, Kent, United Kingdom
© Copyright Hewlett-Packard Company 1997

# A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve

Z. Djabri[1] and N.P. Smart[2]

[1] Institute of Maths and Statistics,
University of Kent at Canterbury,
Canterbury, Kent, CT2 7NF, U.K.
**e-mail : zmd1@ukc.ac.uk**
[2] Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford,
Bristol, BS12 6QZ, U.K.
**e-mail : nsma@hplb.hpl.hp.com**

**Abstract.** In this paper we examine differences between the two standard methods for computing the 2-Selmer group of an elliptic curve. In particular we focus on practical differences in the timings of the two methods. In addition we discuss how to proceed if one fails to determine the rank of the curve from the 2-Selmer group. Finally we mention briefly ongoing research into generalizing such methods to the case of computing the 3-Selmer group.

Computing the 2-Selmer group is a basic problem in the computational theory of elliptic curves over the rationals. It is, assuming the Tate-Shaferevich group, Ш, has no 2-primary part, the most efficient way known of computing the rank and generators of the Mordell-Weil group. That we do not have an algorithm to compute the Mordell-Weil group in general is one of the major open problems in the theory of elliptic curves. The computation of the Mordell-Weil group is basic to many Diophantine problems such as computing the set of integral points on a curve via elliptic logarithms, [11], [22], [21], or verifying the Birch-Swinnerton-Dyer conjecture, [2], [3].

Throughout this paper, by an elliptic curve we shall mean a curve of the form

$$E : Y^2 = X^3 - 3IX + J \tag{1}$$

where $I, J \in \mathbb{Z}$. We let $\Delta = 4I^3 - J^2$ denote the discriminant of the curve.

There are currently two methods used to compute the 2-Selmer group, $S_2$. The first method, which is essentially part of the standard proof of the Mordell-Weil theorem, uses number field arithmetic. This method works directly with the Selmer group and can therefore make explicit use of the underlying group structure of the elements. The second method, due to Birch and Swinnerton-Dyer, [2], computes $S_2$ in an indirect way by computing a set of binary quartic forms which indirectly represent the elements of $S_2$.

The indirect method of Birch and Swinnerton-Dyer has recently undergone major improvement due to the work of Cremona, [8]. The method has complexity

$O(\sqrt{|\Delta|})$, but is known to be very fast in practice. Cremona has implemented this method in his program, **mwrank**, which is now widely used.

On the other hand the direct method can be shown to have conjectured sub-exponential complexity in $|\Delta|$, see [20]. This sub-exponential behaviour is due to the conjectured sub-exponential complexity of determining the basic invariants of cubic number fields, such as generators of the unit and class groups.

We decided to compare the practical behaviour of the two methods. This paper describes our findings. For the indirect method we used the code in **mwrank** which we modified slightly so that it only output $S_2$ and did not try to determine which quartics had small rational points. It turned out that this modification made very little difference in practice.

After comparing the methods to compute $S_2$ we look at how one can overcome the obstruction to computing $E(\mathbb{Q})/2E(\mathbb{Q})$. The first way is by performing further descents on the elements in $S_2$. We shall see that the indirect method of computing $S_2$ is more suited to performing these second descents.

Finally we report on problems that one encounters when trying to generalize the direct and indirect methods to compute the 3-Selmer group of an elliptic curve, $S_3$. If such a method could be made practical this would allow the computation of the Mordell-Weil group when there exists no 3-torsion in Ш. This clearly would be of importance when there elements of order 4 in Ш, as then the methods for constructing $S_2$ and performing further descents become useless.

The authors would like to thank P. Swinnerton-Dyer, E. Schaefer and J. Merriman for useful conversations and communications during which the work in this paper was carried out.

## 1 The Direct Method

If $F(X) = X^3 - 3IX + J$ is reducible then the curve has a point of order two so decent via two-isogeny should always be the preferred method. We therefore assume that $F(X)$ is irreducible.

We shall quickly recap on the direct method, so as to explain our implementation in more detail. Let $\theta$ denote a root of $F(X)$ and set $K = \mathbb{Q}(\theta)$. Let $S$ denote the set of places of $K$ which either divide $2\Delta$ or are infinite. We define $K(S,2)$ to be the set of elements of $K$, modulo squares, which give an unramified extension away from $S$ on addition of their square root to $K$.

Using the LiDIA, [14], and PARI, [1], libraries we wrote a C++ program to compute a set of generators for the group $K(S,2)$ in any given example. This is the "hard" part of the direct method which has conjectured sub-exponential complexity. The method used was the one described in [20].

We then restrict our attention to the subgroup, $H$, of $K(S,2)$ which is the kernel of the norm map:

$$N_{K/\mathbb{Q}} : K(S,2) \to \mathbb{Q}^*/\mathbb{Q}^{*2}.$$

Clearly determining the generators of $H$ is simply an application of linear algebra over $\mathbb{F}_2$. Then for every element $\alpha \in H$ we need to determine whether there

exists $X, Z \in \mathbb{Q}$ such that we can find a $\beta \in K$ with

$$X - \theta Z^2 = \alpha\beta^2.$$

Using a standard method, see [5][Page 70], this reduces the problem to determining a simultaneous solution to a system of quadratic forms

$$\begin{aligned} Q_1(x_1, x_2, x_3) &= 0, \\ Q_2(x_1, x_2, x_3) &= -x_4^2, \end{aligned}$$

where $Q_1$ and $Q_2$ are quadratic forms in three variables. The 2-Selmer group is those set of $\alpha$'s which give rise to a pair as above which have a solution everywhere locally. The first test is whether $Q_1 = 0$ has a solution everywhere locally. If it does we can find a global solution, by the Hasse Principle for curves of genus zero, and use this to express the general solution, $(x_1, x_2, x_3)$, as three quadratic forms in two variables. Substituting these into the second equation gives a "quartic" of the form

$$x_4^2 = G(m, n)$$

where $G(m, n)$ is a binary quartic form. We can then test whether this equation is locally soluble everywhere using the random polynomial time method described in [15]. This last method only works for $p \neq 2$ but for small $p$, in particular $p = 2$, we can use the standard method which is explained in [7].

If one naively carries out this method the two forms, $Q_1$ and $Q_2$, we obtain can have rather large coefficients. The global solution to $Q_1 = 0$ can be hard to determine as the standard solution method, due to Lagrange, requires square root extraction modulo composite moduli. The quartic form, $G(m, n)$, will in general also have prohibitively large coefficients. It should be noted that the indirect method does suffer from this problem as it computes "reduced" quartic forms.

To get around these problems we note that we need only check locally solubility at each stage for primes dividing $2\Delta$ and infinity. We could therefore carry the above computations out for each prime in turn and not work globally. Suppose we wish to test $\alpha$ for the prime $p$, it would be advantageous if we could decide what level of $p$-adic precision we would need before starting any computation. To see how to do this write the two quadratic forms as

$$\begin{aligned} Q_1(\mathbf{x}) &= \mathbf{x}^t A \mathbf{x} = 0, \\ -Q_2(\mathbf{x}) &= \mathbf{x}^t B \mathbf{x} = x_4^2, \end{aligned}$$

where $A$ and $B$ are symmetric integer matrices. Then by a unimodular change of variable we can diagonalize $A$. The matrices of the new equivalent quadratic forms we shall by abuse of notation also refer to as $A$ and $B$. We let $\partial(A, B)$ denote the discriminant of $\det(XA - B)$.

**Lemma 1.** *There is an algorithm to detect the local solubility of the pair of quadratic forms at an odd prime $p$ which runs in random polynomial time and which requires working to a $p$-adic accuracy of $p^e$ where $e = \mathrm{ord}_p(2^{12}\partial(A, B)\det(A)^2)$.*

*Proof.* We first check whether $\mathbf{x}^t A\mathbf{x} = 0$ has a solution modulo $p$. If it does then we find a $p$-adic solution $(x_1, x_2, x_3) \equiv (\chi_1, \chi_2, \chi_3) \pmod{p^e}$ such that, after a possible reordering of the variables, we have $\chi_i \in \mathbb{Z}$ and $\chi_1 \not\equiv 0 \pmod{p}$. This last step can be done in polynomial time using Hensel's Lemma. As $A = \mathrm{diag}(a_1, a_2, a_3)$ we set

$$r = -\left(\frac{a_2 m^2 + a_3 n^2}{2a_2 m\chi_2 + 2a_3 n\chi_3}\right),$$

for two new variables $m$ and $n$. Then all solutions to $Q_1 \equiv 0 \pmod{p^e}$ are parameterized by $m$ and $n$ where

$$\begin{aligned} x_1 &= r\chi_1, \\ x_2 &= r\chi_2 + m, \\ x_3 &= r\chi_3 + n. \end{aligned}$$

Substituting these into $x_4^2 = \mathbf{x}^t B\mathbf{x}$ and clearing the denominator of $4(a_2 m\chi_2 + a_3 n\chi_3)^2$ we obtain a binary quartic form, $G(m, n) \pmod{p^e}$. The discriminant of $G(m, n)$ is equal to

$$\Lambda = 2^{12}\partial(A, B)a_1^2 a_2^2 a_3^2 \chi_1^6,$$

as can be verified by a computer algebra system. To check the local solubility of $x_4^2 = G(m, n)$ at $p$ we need only have computed $G(m, n)$ to an accuracy of at most $p^{\mathrm{ord}_p(\Lambda)} = p^e$. That we can determine the local solubility of $x_4^2 = G(m, n)$, when $p$ is odd, in random polynomial time follows from Section 7 of [15], as has already been mentioned.

A similar method to the one above can be applied when one wishes to check the pair of forms for local solubility over $\mathbb{R}$ or over $\mathbb{Q}_2$. Care of course needs to be taken that one works to a sufficient number of decimal or 2-adic digits.

One does not actually have to perform the above for all values of $\alpha \in H$, which we recall was the kernel of the norm map from $K(S, 2)$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$. This is because we can make use of the underlying group structure. We adopted the method in [20] for this purpose which greatly sped up the overall computation.

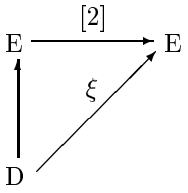
The entire method was programmed in C++ using the LiDIA library and using the program for $K(S, 2)$ which we mentioned previously.

## 2 The Indirect Method

The indirect method proceeds by computing the binary quartic forms directly. This is done by application of what is essentially $19^{th}$ century invariant theory. This idea is due to Birch and Swinnerton-Dyer, [2], and in recent years the method has been greatly improved and simplified by work of Cremona, [8]. We note that the map, $\xi$, from the curve

$$D : z^2 = G(m, 1)$$

to the elliptic curve, $E$, in the "descent diagram"




is given by the covariant syzygy of the binary quartic $G$. This map, $\xi$, can be used to map rational points on $D$ to representatives of the cosets of $E(\mathbb{Q})$ in $E(\mathbb{Q})$. Classical invariant theory, see [10] or [12], tells us that $G(m,n)$ has two fundemental invariants denoted by $I$ and $J$. These are the values of $I$ and $J$ used to define our elliptic curve in equation (1). By appealing to [2][Lemmata 3, 4 and 5] we can assume that $G(m,n)$ has integral coefficients at the expense of increasing the possible values of $(I,J)$ from a single pair to a couple of pairs. It is then possible to construct all the possible binary quartic forms, $G(m,n)$, upto equivalence, using a standard reduction theory, [13]. As this method is explained well elsewhere we shall be content with just giving the following references, [2], [7] and [8].

## 3 Numerical Results

We ran both **mwrank** and our own program for the direct method on a list of over 2900 curves, made up of a subset of the list of curves of conductor less than one thousand plus some randomly chosen curves with large coefficients or ranks of the order of 4 and 5. The results we summarize in the table below.

The indirect method in the range of $\Delta$ we considered often had much shorter running times on average. However there was wild variation in the running times for the indirect method.

The direct method on the other hand exhibited remarkably small variation in running times. Clearly, the direct method is as fast as the underlying programs one is using to compute field invariants, in our case PARI. There were some curves of "small" discrmininant which took mwrank a couple of hours to perform the computation but which took the direct method under twenty seconds. John Cremona has informed us that later versions of **mwrank** will overcome these problems using new improvements he has been developing. However, for curves of large discriminant, the direct method can fail because PARI does. Sometimes for these curves **mwrank** succeeded and other times not.

We divided the curves up into twenty equal groups ranked according to the size of $|\Delta|$. In Table 1 we give the average and worst case running times for each of these twenty groupings. The timings are given in seconds and represent processor time and not user time.

An obvious course of future investigation would be to investigate the indirect method more closely. Perhaps there is an automatic decision which can be performed which would select the best method from the two available.

**Table 1.** Comparison of the Direct and Indirect Methods

| | Indirect Method | | Direct Method | |
|---|---|---|---|---|
| $\log \lvert\Delta\rvert$ | Mean | Worst | Mean | Worst |
| 4.88-7.03 | 0.29 | 14.25 | 14.17 | 17.56 |
| 7.06-8.03 | 1.02 | 116.98 | 13.79 | 30.05 |
| 8.04-8.52 | 0.32 | 6.42 | 13.79 | 18.04 |
| 8.52-8.83 | 50.40 | 7205.7 | 14.56 | 42.39 |
| 8.83-9.05 | 0.27 | 2.27 | 14.81 | 27.82 |
| 9.05-9.24 | 0.28 | 4.15 | 14.66 | 29.64 |
| 9.24-9.39 | 6.49 | 448.18 | 14.95 | 24.21 |
| 9.39-9.66 | 1.24 | 149.04 | 14.91 | 30.03 |
| 9.66-9.91 | 0.44 | 7.95 | 15.84 | 81.91 |
| 9.91-10.11 | 23.48 | 3351.45 | 15.38 | 75.47 |
| 10.11-10.35 | 18.68 | 2650.16 | 15.02 | 29.94 |
| 10.35-10.55 | 7.51 | 747.76 | 16.45 | 102.15 |
| 10.55-10.74 | 0.34 | 7.96 | 15.50 | 37.96 |
| 10.74-10.91 | 0.29 | 2.08 | 16.14 | 47.86 |
| 10.91-11.17 | 3.15 | 386.26 | 16.77 | 111.06 |
| 11.18-12.02 | 47.15 | 2629.17 | 15.99 | 32.95 |
| 12.02-12.49 | 35.88 | 3025.83 | 18.36 | 51.35 |
| 12.49-12.90 | 1.46 | 76.62 | 19.50 | 152.16 |
| 12.90-15.34 | 2052.7 | 141682 | 18.56 | 55.99 |
| 15.34-21.55 | 3133.9 | 95520 | 19.91 | 215.52 |

## 4 Further descents and the Mordell-Weil group

We now discuss how one can perform further descents with both the direct and the indirect methods and in addition determine elements in the Mordell-Weil group and not just $S_2$. As will be seen the indirect method is more efficient than the direct method in this case as well.

We now let $r$ denote the rank of the Mordell-Weil group of $E$. The above two methods as described compute $S_2$ which, assuming there is no two torsion on $E$, has order $2^r$. If one can find $r$ independent rational points on $E$ then we then know that the rank is $r$. We hence have a sublattice of finite index which we can pass to a procedure for enlargement to the whole of $E(\mathbb{Q})$, see [19] for such a procedure.

If we cannot find enough points we could be in one of two positions:

1. The points exist but the smallest ones are far too large to be spotted by a simple search procedure.
2. There exists a non-trivial element in Ш of order two.

We would clearly like to be able to cope with both occurances. In the first situation it is better to work with the representation that the indirect method

gives us for elements of $S_2$, namely the global quartics;

$$z^2 = G(m,1) = am^4 + bm^3 + cm^2 + dm + e.$$

In the second situation it is better to represent elements in $S_2$ by means of an algebraic integer $\alpha \in K(S,2)$.

If we let $p = 3b^2 - 8ac$ denote the seminvariant of $G(m,n)$ of degree two and weight two then we can pass from the representation used in the indirect method to that used in the direct method using the formula

$$\alpha = \frac{4a\theta + p}{3},$$

see [8]. To go the other way is a little more tricky, which is a major drawback of the direct method as we shall now see.

In the indirect method we can, given an element of $S_2$

$$D : z^2 = G(m,1),$$

determine whether it has any small solutions and then map these to $E$ using the covariant syzygy. Any element of $E(\mathbb{Q})$ we find in this way we would expect to have much larger height than the corresponding point on $D$. Hence this is a way of finding points of large height on the curve. As the image of a point on each $D \in S_2$ gives a representative of a coset of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$, this hopefully allows us to determine $r$ independent points on $E$.

Now suppose that we cannot find any small solutions on the curve $D$. We first test whether the curve $D$ could arise as an image of an element of the 4-Selmer group, $S_4$, if not then $D$ must be an element of order two in Ш. To test whether $D$ is an image of an element in $S_4$ we map the curve, $D$, to the corresponding element $\alpha \in K(S,2)$ and then use the method of [6], which makes use of the Cassels-Tate pairing on Ш. Finally, if $D$ does arise as an image of an element of $S_4$, we can apply the method of [15] to perform a further descent on the curve $D$ and actually determine the element of $S_4$. Searching for points on this further descent gives us a way of finding points on $D$ of large height, which in turn gives us a way of finding points on $E$ of very large height.

In the direct method such a variety of techniques are not available to us. Given $\alpha \in K(S,2)$ we cannot determine a corresponding curve $D$ with ease, which is why we only worked locally in the algorithm of Section 1. We only have available the Cassels-Tate pairing to detect whether $\alpha$ corresponds to the image of an element of $S_4$. In practice this may be all that is required but we do fail to obtain a method of searching for points of large height.

## 5 The 3-Selmer group

Clearly the problem that remains is; what should we do when we have a curve which has an element of 4-torsion in Ш ? If we could construct $S_3$ we would have at least solved our problem in the cases where Ш has no elements of order three.

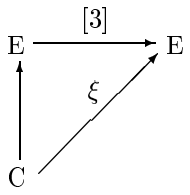
However there is a problem, although the algorithms to construct the $m$-Selmer group in the standard literature are constructive they are not exactly practical methods. For example they often involve determining the $m$-Selmer group of the curve over a large degree number field and then constructing the $m$-Selmer group over $\mathbb{Q}$ using Galois theory.

We shall assume that our curve does not possess a 3-isogeny. If a 3-isogeny does exist one can attempt to determine the rank of the curve using descent via 3-isogeny. This has been explained in the literature in many places, see [24] for a very accessable account.

Firstly we look at the generalization of the indirect method. As was noted by Swinnerton-Dyer, [4][Page 269], an element of $S_3$ can be represented as a ternary cubic form

$$C : \begin{array}{l} a_{300}x^3 + 3a_{210}x^2y + 3a_{201}x^2z + 3a_{120}xy^2 + 3a_{102}xz^2 \\ +6a_{111}xyz + a_{030}y^3 + 3a_{021}y^2z + 3a_{012}yz^2 + a_{003}z^3 = 0 \end{array}$$

and the map, $\xi$, in the "descent diagram"




is given by the covariant syzygy, [16][Page 203], of the ternary form, $C$, just as it was in the indirect method for computing $S_2$. Hence if we can determine all possible curves $C$ upto the necessary equivalence then we can test them for local solubility and determine $S_3$. In addition, using the covariant syzygy, we can map any rational points on $C$ to representatives of cosets of $3E(\mathbb{Q})$ in $E(\mathbb{Q})$.

The curve $C$ has two classical fundamental invariants, usually denoted $S$ and $T$, these play the exactly the same role as the invariants $I$ and $J$ before. The curve is non-degenerate if $T^2 + 64S^3 \neq 0$. Using the covariant syzygy one can relate the pair $(S, T)$ to the pair $(I, J)$ which define the elliptic curve (1).

Swinnerton-Dyer has pointed out to us, [23], that if the curve $C$ has integral coefficients, by which we mean the $a_{ijk}$ above are integral, then one can construct representatives of equivalence classes of all such curves with given invariants. A simplification of the method of Swinnerton-Dyer is given in the following result;

**Theorem 2.** *Let $S$ and $T$ be two given integers such that $T^2+64S^3 \neq 0$. There is an algorithm which computes a complete set of representatives from the $GL_3(\mathbb{Z})$-equivalence classes of ternary cubic forms with integral coefficients and invariants given by $S$ and $T$.*

*Proof.* We first determine a finite set of $SL_3(\mathbb{R})$-equivalence classes. Let $F(x, y, z)$ be a ternary cubic form with invariants $S$ and $T$. By [9] there is a real unimodular transformation which sends $F$ to the form

$$G = \alpha(X^3 + Y^3 + Z^3) + 6\beta XYZ,$$

where $\alpha, \beta \in \mathbb{R}$. The invariants of $G$, and hence of $F$, are given by

$$\begin{aligned} S &= \alpha^3\beta - \beta^4, \\ T &= 8\beta^6 - \alpha^6 + 20\alpha^3\beta^3. \end{aligned}$$

Hence, by solving these two equations for $\alpha$ and $\beta$, we can determine a finite set of possible pairs $(\alpha, \beta) \in \mathbb{R}^2$. Now

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

where $A = (\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \boldsymbol{\lambda}_3) \in SL_3(\mathbb{R})$. We then apply a $GL_3(\mathbb{Z})$ transformation to $F(x, y, z)$ to obtain a form, which we also denote by $F(x, y, z)$, for which the columns of $A$ form a Minkowski reduced basis. Hence

$$|\boldsymbol{\lambda}_1| \leq |\boldsymbol{\lambda}_2| \leq |\boldsymbol{\lambda}_3| \text{ and } |\boldsymbol{\lambda}_1\boldsymbol{\lambda}_2\boldsymbol{\lambda}_3| \leq 2.$$

Now if

$$F(x, y, z) = \sum_{i_1+i_2+i_3=3} \frac{3!}{i_1!i_2!i_3!} a_{i_1 i_2 i_3} x^{i_1} y^{i_2} z^{i_3}$$

then it is easy to see that

$$|a_{ijk}| \leq c_1 |\boldsymbol{\lambda}_1|^i |\boldsymbol{\lambda}_2|^j |\boldsymbol{\lambda}_3|^k, \tag{2}$$

where $c_1 = |3|\alpha| + 6|\beta||$.

Suppose $|\boldsymbol{\lambda}_2| < c_1^{-1/3}$ then we obtain $|a_{300}||, |a_{210}|, |a_{120}|, |a_{030}| < 1$. As these are all integers we have $a_{300} = a_{210} = a_{120} = a_{030} = 0$, which implies that $T^2 + 64S^3 = 0$, a contradiction. So we can assume that $|\boldsymbol{\lambda}_2| \geq c_1^{-1/3}$.

Now suppose that $|\boldsymbol{\lambda}_1| < c_1^{-4/3}/2$. Then as $|\boldsymbol{\lambda}_1|^2|\boldsymbol{\lambda}_3| \leq 2||\boldsymbol{\lambda}_1|/|\boldsymbol{\lambda}_2| < c_1^{-1}$ we have that $a_{300} = a_{210} = a_{201} = 0$ which again implies that $T^2 + 64S^3 = 0$. So we must have $|\boldsymbol{\lambda}_1| \geq c_1^{-4/3}/2$.

All that remains is to bound the values of $a_{ijk}$ which we can now do using the three inequalities

$$|\boldsymbol{\lambda}_1| \geq c_1^{-4/3}/2, \quad |\boldsymbol{\lambda}_2| \geq c_1^{-1/3}, \quad |\boldsymbol{\lambda}_3| \leq 4c_1^{5/3}$$

and inequality (2). We obtain

$$\begin{aligned} |a_{300}|, |a_{210}|, |a_{120}|, |a_{201}|, |a_{111}| &\leq 2c_1, \\ |a_{102}| &\leq 8c_1^3, \\ |a_{030}|, |a_{021}|, |a_{012} &\leq 16c_1^4, \\ |a_{003}| &\leq 64c_1^6. \end{aligned}$$

So to find all forms $F(x, y, z)$ up to $GL_3(\mathbb{Z})$-equivalence we loop through all coefficients which are bounded by the inequalities above and determine which forms have invariants given by $S$ and $T$. Such a set will contain a representative

from each $GL_3(\mathbb{Z})$-equivalence class. To determine a unique representative from each class we need to determine which forms in the list are $GL_3(\mathbb{Z})$-equivalent. But this is just a matter of solving a set of eleven non-linear equations in nine integer unknowns.

However there is a problem; before we can apply this result we need to reduce to the consideration of forms with integral coefficients. As mentioned earlier this was done in the case of computing $S_2$ by applying to Lemmata 3, 4 and 5 of [2]. The standard method for doing this for binary quartic forms, which is explained in detail in [18], appears to suffer from combinatorial explosion when applied to ternary cubic forms. We have therefore been unable to fully work out the details of how this can be done for $S_3$.

We now turn our attention to the direct method. We apply the procedure which is explained in [17]. Let $L$ denote the algebra

$$L = \mathbb{Q}[\sigma,\tau]/(f(\sigma), g(\sigma,\tau)) \cong \mathbb{Q}[\tau]/(h(\tau))$$

where

$$\begin{aligned} f(\sigma) &= \sigma^4 + 2A\sigma^2 + 4B\sigma - A^2/3, \\ g(\sigma,\tau) &= \tau^2 - \sigma^3 - A\sigma - B, \\ h(\tau) &= \tau^8 + 8B\tau^6 + (8A^3/3 + 18B^2)\tau^4 - 16A^6/27 - 8B^2A^3 - 27B^4, \end{aligned}$$

where $A = -3I$ and $B = J$. Then $(\sigma,\tau)$ represents a generic point of order 3 on our elliptic curve. The algebra $L$ decomposes into a sum of number fields, $L = \sum_{i=1}^{a} K_i$, and as we are assuming that $E$ possesses no rational 3-isogeny we have $a = 1$ or 2. Every element of $E(\mathbb{Q})$ can be represented by a rational divisor class of degree zero,

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

where $P_i, Q_i \in E(\overline{\mathbb{Q}})$ are not points of order 3. Let $S_i$ denote the set of primes ideals of $K_i$ lying above $3, \infty$ and the primes of bad reduction of the curve $E$. There is then an injective group homomorphism given by

$$\phi : \begin{cases} E(\mathbb{Q})/3E(\mathbb{Q}) & \to Ker\{N_{L/\mathbb{Q}} : \sum_{i=1}^{a} K_i(S_i,3) \to \mathbb{Q}^*/\mathbb{Q}^{*3}\} \\ \sum_{i=1}^{n} P_i - \sum_{i=1}^{n} Q_i & \to \prod_{i=1}^{n} \Theta(P_i)/\Theta(Q_i) \end{cases}$$

where

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

Using a minor adaption of the program mentioned earlier we can compute $K(S,3)$. However the problem is that one needs the equivalent local maps, $\phi_p$, at all the "bad" primes to also be injections. A little group cohomology reveals that this means that for all "bad" primes, $p$, the galois group $G_p = Gal(\mathbb{Q}_p(E[3]), \mathbb{Q}_p)$ must not be equal to either the cyclic or symmetric group on three elements. Unluckily such groups occur quite often and the method fails.

In a future paper we intend to show how one can remove such an obstruction and compute explicitly $S_3$ for any given elliptic curve using the direct method outlined above.

## 6 Summary

We have shown that for the case of computing the 2-Selmer group that the indirect method of Birch and Swinnerton-Dyer appears to be more suitable. This is even though it has a much worse complexity than the direct method using number field arithmetic. On the other hand our early investigation of the case of computing the 3-Selmer group seems to point in the direction that the direct method via number fields is to be the preferred one.

## References


1. C. Batut, D. Bernardi, H. Cohen, and M. Olivier. GP/PARI version 1.39.03. *Université Bordeaux I*, 1994.
2. B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.
3. B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.
4. J.W.S. Cassels. Diophantine equations with special reference to elliptic curves. *J. of LMS*, 41:193–291, 1966.
5. J.W.S. Cassels. *Lectures on Elliptic Curves.* LMS Student Texts, Cambridge University Press, 1991.
6. J.W.S. Cassels. Second descents for elliptic curves. *Preprint*, 1997.
7. J.E. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1992.
8. J.E. Cremona. Classical invariants and 2-descent on elliptic curves. *Preprint*, 1996.
9. H. Davenport. On the minimum of a ternary cubic form. *J. London Math. Soc.*, 19:13–18, 1944.
10. E.B. Elliott. *An Introduction to the Algebra of Quantics.* Oxford University Press, 1895.
11. J. Gebel, A. Pethő, and H.G. Zimmer. Computing integral points on elliptic curves. *Acta. Arith.*, 68:171–192, 1994.
12. D. Hilbert. *Theory of Algebraic Invariants.* Cambridge University Press, 1993.
13. G. Julia. Étude sur les formes binaires non quadratiques. *Mem. Acad. Sci. l'Inst. France*, 55:1–293, 1917.
14. LiDIA Group. LiDIA v1.3 - a library for computational number theory. *TH Darmstadt*, 1997.
15. J.R. Merriman, S. Siksek, and N.P. Smart. Explicit 4-descents on an elliptic curve. *Acta. Arith.*, 77:385–404, 1996.
16. G. Salmon. *Higher Plane Curves.* Hodges, Foster and Figgis, 1879.
17. E.F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Preprint*, 1997.
18. P. Serf. *The rank of elliptic curves over real quadratic number fields of class number 1.* PhD thesis, Universität des Saarlandes, 1995.

19. S. Siksek. Infinite descent on elliptic curves. *Rocky Mountain Journal of Maths*, 25:1501–1538, 1995.
20. S. Siksek and N.P. Smart. On the complexity of computing the 2-Selmer group of an elliptic curve. *To appear Glasgow Math. Journal.*, 1997.
21. N.P. Smart. $S$-integral points on elliptic curves. *Proc. Camb. Phil. Soc.*, 116:391–399, 1994.
22. R.J. Stroeker and N. Tzanakis. Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. *Acta. Arith.*, 67:177–196, 1994.
23. P. Swinnerton-Dyer. Private communication. 1996.
24. 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.

This article was processed using the LaTeX macro package with LLNCS style