ON THE COMPLEXITY OF COMPUTING THE 2-SELMER GROUP OF AN ELLIPTIC CURVE

by S. SIKSEK and N. P. SMART

(Received 26 October, 1995)

Abstract. In this paper we give an algorithm for computing the 2-Selmer group of an elliptic curve

$$Y^2 = X^3 + AX + B$$

which has complexity $O(L_D(0\cdot5, c_1))$, where D is the absolute discriminant of the curve. Our algorithm is unconditional but the complexity estimate assumes the GRH and a standard conjecture on the distribution of smooth reduced ideals. This improves on the corresponding algorithm of Birch and Swinnerton-Dyer, which has complexity of $O(\sqrt{D})$.

When trying to compute the Mordell-Weil group of an elliptic curve one normally first computes the 2-Selmer group. This is a group which contains a subgroup isomorphic to $E(\mathbb{Q})/2E(\mathbb{Q})$. Whilst computing the 2-Selmer group is certainly an effective procedure there is no known effective procedure for computing the subgroup isomorphic to $E(\mathbb{Q})/2E(\mathbb{Q})$, and thus for computing $E(\mathbb{Q})$. However all is not lost as the 2-Selmer group gives one an upper bound on the rank of the elliptic curve, and this upper bound is often attained in practice. To measure the complexity of our algorithm we set

$$L_D(\alpha, \beta) = (e^{(\log D)^{\alpha}(\log\log D)^{1-\alpha}})^{\beta+o(1)}.$$

This is a function which interpolates between polynomial time, $\alpha = 0$, and exponential time, $\alpha = 1$. In this note we show the complexity of computing the 2-Selmer group is $O(L_D(0\cdot5, c_1))$, where D denotes the absolute discriminant of the elliptic curve, under the assumption of the GRH and a standard conjecture on the distribution of reduced smooth ideals.

Let E be our elliptic curve given by

$$E : Y^2 = X^3 + AX + B.$$

We shall assume that the elliptic curve has no points of order 2 defined over $\mathbb{Q}$. This is certainly the most difficult case for finding the 2-Selmer group. The modern method of computing the 2-Selmer group in this case goes back to the paper of Birch and Swinnerton-Dyer [**1**]. In their method a search is carried out for the quartics which represent the homogeneous spaces given their invariants. This method is certainly fast for small values of D; however it is not hard to see that its complexity is at least $O(\sqrt{D})$; see [**1, 11**]. In the present paper we shall show that the "old-fashioned" technique, which uses the arithmetic of number fields, combined with a method derived from a paper of Brumer and Kramer [**2**] will determine the 2-Selmer group in our stated time. Our complexity is therefore much better than the complexity of the algorithm of Birch and Swinnerton-Dyer. However due to numerous improvements to the method of Birch and Swinnerton-Dyer, most notably the ones due to Cremona [**8**], we expect that in practice the method of

Birch and Swinnerton-Dyer will be much faster than the asymptotically faster method of the current paper.

The authors would like to thank Ed. Schaefer for some helpful comments whilst this paper was in preparation. The first author would like to thank his Ph.D. supervisor John Cremona.

We let S denote the set of primes dividing $2D$; we note that this has cardinality $O(\log D)$. Let K denote the number field generated by θ where $\theta^3 + A\theta + B = 0$. We shall let R denote the set of primes of K lying above those in S as well as the infinite primes. As usual we let $K(R, 2)$ denote the group of all elements of K^*/K^{*2} such that by adjoining a square root of an element of $K(R, 2)$ to K one obtains an extension of K unramified outside R. Equivalently we have

$$K(R,2) \cong \{\alpha \in K^*/K^{*2} : \mathrm{ord}_{\wp}(\alpha) \equiv 0 \pmod 2 \quad \text{if } \wp \notin R\}. \tag{1}$$

One can show (see for example [**11**]) that $K(R, 2)$ contains the 2-Selmer group. We first find $K(R, 2)$ and then reduce it to the 2-Selmer group.

1. The method of Brumer and Kramer. We define G to be the kernel of the map $K(R, 2) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, given by $\alpha \mapsto \mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$. For each prime $p \in S \cup \{\infty\}$ we define

$$K_p = \mathbb{Q}_p[T]/(f(T)) = \mathbb{Q}_p[t],$$

where $(f(T))$ is the ideal in $\mathbb{Q}_p[T]$ generated by $f(T) = T^3 + AT + B$, and $t = T + (f(T))$. K_p is an algebra over $\mathbb{Q}_p$ and we can define a *norm* map $K_p \to \mathbb{Q}_p$ as in [**5**, p. 66]. We can now let G_p be the kernel of the analogous map from K_p^*/K_p^{*2} to $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Just as in the classical case of 2-descent over $\mathbb{Q}$ we have an embedding

$$E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) \to G_p. \tag{2}$$

Here, for each prime p we have the following diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \xrightarrow{X-t} & G \\ & & \downarrow & & \downarrow{\scriptstyle \sigma_p} \\ 0 & \longrightarrow & E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) & \xrightarrow{X-t} & G_p \end{array} \tag{3}$$

where we have denoted the natural map from G to G_p by σ_p.

For each prime $p \in S \cup \{\infty\}$ we let U_p be the image of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ in G_p under the mapping (2). In [**2**] Brumer and Kramer showed that the Selmer group is the maximal subgroup of $K(R, 2)$, whose image under the natural map σ_p is contained in U_p for all primes $p \in S \cup \{\infty\}$. Ostensibly, to use this method, one must first calculate $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ for each prime $p \in S \cup \{\infty\}$. However, we have found this mildly troublesome, and indeed what is really needed is to compute the images U_p. We note that the size of G_p is bounded for all primes p and all (cubic) polynomials f.

To determine U_p it is sufficient to take each element of G_p and determine whether or not it is in U_p. As in the classical case (see, for example [**5**, p. 70]) this leads to a homogeneous space as the intersection of 2 quadric surfaces, and here all that is required is to check their solubility over the local field $\mathbb{Q}_p$. Again just as in the classical case we can reduce, in polynomial time, to considering whether a curve of the form $Y^2 = G(X)$ has a point in $\mathbb{Q}_p$, where $G(X)$ is a degree four polynomial but which has coefficients in $\mathbb{Z}_p$. This can be done by the polynomial time algorithm given in **[9]**; this algorithm is non-constructive (it does not give points on the homogeneous space but simply determines whether or not it has a point over $\mathbb{Q}_p$, which is all that is needed here). The usual method for this problem is constructive (see **[7]**), but has an exponential complexity. The non-constructive method of **[9]** reduces the problem to extracting roots of polynomials over finite fields. This problem is soluble in probabilistic polynomial time, or alternatively in deterministic polynomial time assuming the GRH; see **[6**, pp. 31–37].

One should note that the above method of Brumer and Kramer has also been applied to computing the Mordell-Weil group of Jacobians of hyperelliptic curves of higher genus by Schaefer **[10]**. Our method for determining $K(R,2)$ given below could also be used for Schaefer's algorithm for higher genus curves.

2. Finding $K(R,2)$. In this section we give an algorithm for computing $K(R,2)$ in time $O(L_D(0{\cdot}5, c_1))$, where D is the absolute discriminant of the K; the complexity estimate assumes the conjectures mentioned previously. Nowhere do we assume that K is a cubic field, and hence the algorithm in this section can be used for any number field K.

We shall assume that we are given an integral basis for the maximal order of K and generators for the unit and class groups. To determine this information will take time $O(L_D(0{\cdot}5, c_2))$ as computing a basis for the maximal order can be done in time $O(L_D(\frac{1}{3}, c_3))$, **[4]** (using the Number Field Sieve), and computing the unit and class groups can be done in time $O(L_D(0{\cdot}5, c_2))$, **[3]**, assuming the GRH and a certain conjecture about the number of reduced smooth ideals of a number field. The class group Cl_K is then presented as a set of ideals $\mathfrak{c}_1, \dots, \mathfrak{c}_g$ and integers s_i with $s_{i-1} \mid s_i$, such that, if for an ideal $\mathfrak{a}$ we denote by $\bar{\mathfrak{a}}$ the image of $\mathfrak{a}$ in the class group, we have

$$Cl_K \cong \langle \overline{\mathfrak{c}_1} \rangle \times \dots \times \langle \overline{\mathfrak{c}_g} \rangle,$$

with $\langle \overline{\mathfrak{c}_i} \rangle \cong \mathbb{Z}/s_i\mathbb{Z}$. We denote by $\eta_1, \dots, \eta_r$ a set of r fundamental units for K. Given an ideal of K then using the basis of the relation lattice which was used in computing the class group one can determine whether the ideal is principal and if so compute a generator in time $O(L_D(0{\cdot}5, c_4))$; (see **[3]** or **[6**, Algorithm 6.5.10]). We note that in general one can not write down the elements we require in polynomial time when we express them in standard representation and so throughout we assume all elements are in a compact representation; see **[12]**. We now give the algorithm to compute $K(R,2)$ as a product of cyclic groups of order 2. Let the finite prime ideals in R be denoted $\wp_1, \dots, \wp_t$.

Suppose $\alpha \in K(R,2)$. Then by the definition (1) above $(\alpha) = \mathfrak{a}\mathfrak{b}^2$, where $\mathfrak{a} \mid (2D)$. Let $\mathcal{F}$ be the group of fractional ideals. We have a homomorphism

$$\phi : K(R,2) \to \mathcal{F}/\mathcal{F}^2$$

given by $\alpha \to (\alpha)\mathcal{F}^2$. Clearly the image of ϕ is contained in the group

$$H_1 = \langle \wp_1 \mathcal{F}^2 \rangle \times \dots \times \langle \wp_n \mathcal{F}^2 \rangle.$$

Let

$$H_2 = \{\mathfrak{b}\mathcal{F}^2 \in H_1 : \mathfrak{b}\mathcal{F}^2 = (\gamma)\mathcal{F}^2 \text{ for some } \gamma \in K^*\}.$$

Clearly $\mathrm{Im}(\phi) = H_2$. We want to show how to calculate H_2 and then how to refine it to obtain $K(R,2)$ as a product of cyclic groups of order 2. We assume that for each $\wp_i$ that we can write

$$\overline{\wp_j} = \prod_{i=1}^{g} \bar{\mathfrak{c}}_i^{b_{ij}}.$$

This can be done by the method in [3] in time $O(L_D(0{\cdot}5, c_4))$. Suppose $\mathfrak{b}\mathcal{F}^2 \in H_2$; then we can take $\mathfrak{b} = \prod_{j=1}^{n} \wp_j^{a_j}$. Hence

$$\bar{\mathfrak{b}} = \prod_{i=1}^{g} \bar{\mathfrak{c}}_i^{e_i},$$

where $e_i = \sum_{j=1}^{n} a_j b_{ij}$. Suppose that $s_1, \ldots, s_k$ are odd, and $s_{k+1}, \ldots, s_g$ are even. Then $\mathfrak{b}\mathcal{F}^2$ lies in H_2 if and only if $\sum_{j=1}^{n} a_j b_{ij} \equiv 0 \pmod 2$ for $i = k+1, \ldots, g$.

By computing an $\mathbb{F}_2$-basis for the subspace of the vectors $(a_1, \ldots, a_n)$ in $\mathbb{F}_2^n$ which satisfy the congruences above, we get a basis for H_2. Further we may replace the representative of each element of this basis by one which is a principal ideal as follows. Suppose $\mathfrak{b}$ is such a representative which we want to replace by a principal ideal. By construction of this basis we know $\mathfrak{b}$ as a product of the $\wp_i$ and hence we can write $\bar{\mathfrak{b}} = \prod \bar{\mathfrak{c}}_i^{u_i}$, where $u_{k+1}, \ldots, u_g$ are even. Now since $s_1, \ldots, s_k$ are odd we can find $t_1, \ldots, t_k$ such that $u_i + 2t_i \equiv 0 \pmod{s_i}$, for $i = 1, \ldots, k$. We take $t_j = -u_j/2$ for $j = k+1, \ldots, g$. Hence we have that

$$\mathfrak{b} \prod_{i=1}^{g} \mathfrak{c}_i^{2t_i} = (\alpha),$$

for some $\alpha \in K^*$. This α can be computed in time $O(L_D(0{\cdot}5, c_4))$ as we stated above. Hence we can write

$$H_2 = \langle (\alpha_1)\mathcal{F}^2 \rangle \times \ldots \times \langle (\alpha_n)\mathcal{F}^2 \rangle,$$

for some $\alpha_1, \ldots, \alpha_n \in K^*$.

LEMMA 1. *Let $\mathfrak{b}_1, \ldots, \mathfrak{b}_l$ be an $\mathbb{F}_2$-basis for* $\mathrm{Cl}[2]$. *Write $\mathfrak{b}_i^2 = (\beta_i)$. Then*

$$\alpha_1 K^{*2}, \ldots, \alpha_n K^{*2}, \qquad \beta_1 K^{*2}, \ldots, \beta_l K^{*2}, \qquad \eta_1 K^{*2}, \ldots, \eta_r K^{*2}, \qquad \eta_{r+1} K^{*2}$$

is a basis for $K(R,2)$, where $\eta_1, \ldots, \eta_r$ is a system of fundamental units for K, and we take η_{r+1} a generator for the roots of unity.

Proof. It is clear that the elements of the list above generate $K(R,2)$. What remains is to show that these are independent. Suppose that

$$\prod_{i=1}^{n} \alpha_i^{a_i} \prod_{i=1}^{l} \beta_i^{b_i} \prod_{i=1}^{r+1} \eta_i^{c_i} \in K^{*2},$$

where the a's, b's, c's, are in $\{0, 1\}$. Then $\prod ((\alpha_i)\mathcal{F}^2)^{a_i} = (1)\mathcal{F}^2$, which implies that $a_i = 0$ for $i = 1, \ldots, n$. Hence we can now assume that

$$\prod_{i=1}^{l} \beta_i^{b_i} \prod_{i=1}^{r+1} \eta_i^{c_i} \in K^{*2}.$$

Hence $\prod \mathfrak{b}_i^{2b_i} = (\epsilon)^2$, where $\epsilon \in K^*$; i.e. $\prod \mathfrak{b}_i^{b_i} = (\epsilon)$, and so $b_i = 0$. The result now follows. □

LEMMA 2. *The complexity of finding $K(R, 2)$ as a product of cyclic groups of order 2 is given by $O(L_D(0{\cdot}5, c_1))$.*

Proof. We note that the number of ideals $\wp_i$ dividing $(2D)$ is $O(\log D)$. The number of elements in a basis of $\mathrm{Cl}[2]$ is $O(\log(h_K)) = O(\log(D))$. Hence the number of ideals that we need to check to be principal is a polynomial function in $\log D$. As we stated earlier for each ideal this can be done in time $O(L_D(0{\cdot}5, c_4))$ by an algorithm which will also produce a generator of any principal ideal found. The desired complexity then follows. □

3. Computing the 2-Selmer group. Having determined $K(R, 2)$ we then need to determine a basis of the $\mathbb{F}_2$ vector subspace G; recall that G is the kernel of the homomorphism $K(R, 2) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ given by $\alpha \mapsto \mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$. Clearly determining a basis for G is elementary linear algebra over $\mathbb{F}_2$, and so can certainly be accomplished in polynomial time.

We wish to eliminate from the group G every element whose image under σ_p does not lie in U_p for any $p \in S \cup \{\infty\}$. Suppose we know that the Selmer group is a subgroup of some group

$$\langle k_1 \rangle \times \ldots \times \langle k_v \rangle \leq G \leq K(R, 2),$$

where the $\langle k_i \rangle$ are cyclic groups of order 2; (it is understood that the k_i are in fact $k_i K^{*2}$). Consider any prime $p \in S \cup \{\infty\}$. Recall that we denoted the image of the map

$$E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) \to G_p$$

by U_p. To determine the Selmer group we want to determine the maximal subgroup of $\langle k_1 \rangle \times \ldots \times \langle k_v \rangle$ whose image under σ is in U_p for all primes p; obviously we need only consider those primes which divide $2D$ and the infinite prime. This idea we find explained in **[2]** or **[10]** as we stated above.

LEMMA 3. *The image of an element of $K(R, 2)$ under σ_p can be checked to lie in U_p in polynomial time.*

Proof. Suppose $X^3 + AX + B$ has three roots in $\mathbb{Q}_p$ and $p > 2$; then

$$U_p \leq \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \times \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \times \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}.$$

There are at most four elements of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ and $|U_p|$ has order $O(1)$ as $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$

also has order $O(1)$. We therefore have $O(1)$ tests to perform as to whether an element of $\mathbb{Q}_p$ is a p-adic square. This can certainly be done in polynomial time. The other cases are similar. □

For $i = 1, \ldots, v$, we define the subgroup S_i of $\langle k_1\rangle \times \ldots \times \langle k_i\rangle$ to be the maximal subgroup of $\langle k_1\rangle \times \ldots \times \langle k_i\rangle$ whose image under σ_p is in U_p. To simplify the notation, we will for now write σ for σ_p. We let

$$b_1, \ldots, b_{j_i} \in \langle k_1\rangle \times \ldots \times \langle k_i\rangle$$

be such that

$$H_i := \langle b_1 S_i\rangle \times \ldots \times \langle b_{j_i} S_i\rangle = (\langle k_1\rangle \times \ldots \times \langle k_i\rangle)/S_i.$$

Notice that $|H_i| < O(1)$. This is because $|E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)| = O(1)$. Hence if there were too many b_j then there would exist a relation of the form

$$\sigma(b_1^{s_1}) \ldots \sigma(b_{j_i}^{s_{j_i}}) = \text{identity of } G_p,$$

where the $s_j \in \{0, 1\}$ and not all $s_j = 0$. But certainly the identity is in the image of the map (2). Hence $b_1^{s_1} \ldots b_{j_i}^{s_{j_i}}$ is in S_i, giving a contradiction. Hence, as we claimed, $|H_i| = O(1)$.

Now we determine the S_i and H_i recursively. To determine S_1 simply check if the image of k_1 is in U_p. If it is, then $S_1 \cong \langle k_1\rangle$ and $H_1 \cong \{S_1\}$. If it is not, then $S_1 \cong$ identity and $H_1 \cong \langle k_1 S_1\rangle$.

Suppose we have determined S_i and the H_i. To determine S_{i+1} and H_{i+1} we check if

$$\sigma(b_1^{s_1}) \ldots \sigma(b_{j_i}^{s_{j_i}})\sigma(k_{i+1}) \tag{4}$$

is in U_p for any $s_j = 0$ or 1. If none of these are in U_p, then $S_{i+1} = S_i$, and

$$H_{i+1} = \langle b_1 S_{i+1}\rangle \times \ldots \times \langle b_{j_i} S_{i+1}\rangle \times \langle k_{i+1} S_{i+1}\rangle.$$

If, on the other hand, the expression (4) is in U_p for some choice of $s_j = 0$ or 1 (there can be at most one such choice), then

$$S_{i+1} \cong S_i \times \langle b_1^{s_1} \ldots b_{j_i}^{s_{j_i}} k_{i+1}\rangle$$

and

$$H_{i+1} \cong \langle b_1 S_{i+1}\rangle \times \ldots \times \langle b_{j_i} S_{i+1}\rangle.$$

The number of choices of b_j that we have is $O(1)$ as $|H_i| = O(1)$. Hence we can determine S_k as a product of cyclic groups all of order 2. The time to do this is then polynomial in $\log D$ via Lemma 3.

Now to determine the Selmer group, we start with G expressed as a product of cyclic groups. For our bad primes $p_1, \ldots, p_r$ we start with p_1 and we determine as above the maximal subgroup $V_{p_1} \leq G$, whose image under $\sigma = \sigma_{p_1}$ is contained in U_{p_1}. Our construction will give us V_{p_1} as a product of cyclic groups of order 2. This will certainly contain the Selmer group. We now discard G and find the maximal subgroup of V_{p_1} whose image under σ_{p_2} is contained in U_{p_2}. Doing this recursively we arrive at the Selmer group as soon as we have carried out the construction above for all the bad primes $p_1, \ldots, p_r$ and also the infinite prime.

If we have $K(R,2)$ as a product of cyclic groups of order 2 then we will find the Selmer group in polynomial time. Hence the total complexity is given by the complexity of finding $K(R,2)$.

REFERENCES

1. B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves I, *J. Reine Angew. Math.* **212** (1963), 7–25.

2. A. Brumer and K. Kramer, The rank of elliptic curves, *Duke Math. J.*, **44** (1977), 715–743.

3. J. Buchmann, A subexponential algorithm for the determination of class groups and regulators of algebraic number fields, in *Séminaire de théorie des nombres, Paris (1988–1989)*, 28–41.

4. J. Buchmann and H. W. Lenstra Jnr, Approximating rings of integers in number fields *Journal de Theorie des Nombres de Bordeaux*, **6** (1994), 221–260.

5. J. W. S. Cassels, *Lectures on elliptic curves*, LMS Student text 24 (1991).

6. H. Cohen, *A course in computational algebraic number theory* (Springer-Verlag, 1993).

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, *J. Symbolic Computation*, *1997*, to appear.

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

10. E. F. Schaefer, 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory*, **51** (1995), 219–232.

11. J. H. Silverman, *The arithmetic of elliptic curves* (Springer-Verlag, 1986).

12. C. Thiel, Under the assumption of the Generalized Riemann Hypothesis verifying the class number belongs to $\mathcal{NP} \cap \text{co} - \mathcal{NP}$, in *ANTS-1: Algorithmic Number Theory*, Eds L. M. Adelman and M-D. Huang, Lecture Notes In Computer Science No. 877, (Springer-Verlag, 1994), 234–247.

Institute of Mathematics and Statistics
University of Kent at Canterbury
Canterbury
Kent CT2 7NF
England
E-mail address: S.Siksek@ukc.ac.uk

Hewlett-Packard Laboratories
Filton Road
Stoke Gifford
Bristol BS12 6QZ
England
E-mail address: nsmaehplb.hpl.hp.com

https://doi.org/10.1017/S0017089500032183 Published online by Cambridge University Press