London Mathematical Society ISSN 1461–1570

COMPUTING THE RANK OF ELLIPTIC CURVES OVER NUMBER FIELDS

DENIS SIMON

Abstract

This paper describes an algorithm of 2-descent for computing the rank of an elliptic curve without 2-torsion, defined over a general number field. This allows one, in practice, to deal with fields of degree from 1 to 5.

Introduction

Computing the rank of the Mordell–Weil group of an elliptic curve E defined over $\mathbb{Q}$ has now become a classical task. This is currently achieved by using 2-descent (see [7]). This method can provably compute only the 2-Selmer group of the curve. However, in many cases the Tate–Shafarevich group happens to have no 2-torsion, in which case $E(\mathbb{Q})/2E(\mathbb{Q})$ can be identified with the 2-Selmer group. From this, we can easily deduce the rank of $E(\mathbb{Q})$.

Two different strategies are currently used for computing such obects. The first one, called the *direct method*, uses the arithmetic of number fields, while the second one, called the *indirect method*, needs only arithmetic in $\mathbb{Q}$. A discussion of these different methods, and a comparison between them, can be found in [13] or [24].

Our goal is to describe completely a *direct* 2-descent method for elliptic curves defined over a number field K. A description has already been given for the *indirect* method over some specific real quadratic fields (see [11]). We dispense here with any assumption on the field K, and we give an example of an elliptic curve defined over an imaginary quadratic field with nontrivial class group. With the help of the package PARI/GP (see [5]), we have been able to treat a great number of curves defined over quadratic fields, and some over larger degree fields (up to degree 5). The complete gp-program is available at [23]. To make things easier, we shall restrict to elliptic curves without 2-torsion over K. The basis of our method can be found in [4], and in [24]. Elliptic curves with 2-torsion have already been dealt with by N. Bruin (see [2] and [3], or [25] for background information).

The present method is a direct consequence of the arithmetic of invariants of quartics as described by J. Cremona in [9]. The new ingredients introduced in the present work mainly comprise the solution of Legendre equations over number fields, a method for minimizing some quartics constructed over general number fields, and the implementation of the whole method.

We refer readers who are specifically interested in the Selmer group to [18], which describes a more general method for computing the Selmer group of the Jacobian of a hyperelliptic curve, or to [14], which performs p-descent over elliptic curves.

Received 29 March 2000, revised 27 February 2002*; published 17 April 2002*.
2000 Mathematics Subject Classification 11D25, 11R, 11Y50

1. *Description of the method*

1.1. *Definition of the morphism*

Let K be a number field, and let E be an elliptic curve defined over K, given by an equation of the form

$$y^2 = P(x),$$

where $P(x) = x^3 + Ax^2 + Bx + C$, with A, B and $C \in K$. The group of points of E with coordinates in K will be denoted by $E(K)$.

Without loss of generality, we can make the assumption that A, B and C are in the ring of algebraic integers $\mathbb{Z}_K$ of K. We make the further assumption that the polynomial P is irreducible over K. This is equivalent to saying that $E(K)$ has no 2-torsion.

Let θ be a root of P in $\mathbb{C}$. This algebraic integer generates a cubic extension $L = K(\theta)$ of K. It is not difficult to prove the following result (see [4]).

Proposition 1.1. *The map*

$$\begin{array}{rccc} \phi: & E(K) & \to & L^*/L^{*2} \\ & 0 & \mapsto & 1 \\ & (x, y) & \mapsto & x - \theta \end{array}$$

defines a group homomorphism with exact kernel $2E(K)$.

Thanks to this homomorphism, it is possible to obtain information about the rank of $E(K)$. Indeed, if we know the image of ϕ, we also know the group $E(K)/2E(K)$, whose cardinality is equal to 2^r, where r is precisely the rank of $E(K)$. Note also the following proposition.

Proposition 1.2. *The image of* ϕ *is a subgroup of the kernel of the norm map* $\mathcal{N}_{L/K}$ *from* L^*/L^{*2} *to* K^*/K^{*2}.

The proof is an immediate consequence of the relation $\mathcal{N}_{L/K}(x - \theta) = P(x) = y^2$. In [18], we find an identification of this kernel with the cohomology group $H^1(K, E(\bar{K})[2])$.

1.2. *Reduction to a finite set*

The next two propositions show that $\operatorname{Im}\phi$ is contained in some easily computable finite subgroup of the infinite group L^*/L^{*2}. We use the notation $\overline{\delta}$ for the projection of $\delta \in L^*$ in L^*/L^{*2}.

Let S be a finite set of places of L containing the infinite places. Let

$$L(S, 2) = \left\{ \overline{\delta} \in L^*/L^{*2},\ \forall \mathfrak{P} \notin S, v_{\mathfrak{P}}(\delta) \equiv 0 \pmod 2 \right\}.$$

In order to describe this group, we make use of the S-units of L, denoted by $\mathbb{U}_{L,S}$, and of the S-class group $\mathrm{Cl}_S(L)$. Recall that Dirichlet's S-unit theorem (see [15]) asserts that $\mathbb{U}_{L,S}$ is a finitely generated Abelian group, whose torsion part contains exactly the roots of unity in L, and whose free part has rank $|S| - 1$. The S-class group $\mathrm{Cl}_S(L)$ is isomorphic to the quotient of the ordinary class group $\mathrm{Cl}(L)$ by the subgroup generated by the classes of all prime ideals in S. In [21], we prove the following result (see also [17]).

Proposition 1.3. *There exists an isomorphism*

$$L(S, 2) \simeq \frac{\mathbb{U}_{L,S}}{\mathbb{U}_{L,S}^2} \times \mathrm{Cl}_S(L)[2].$$

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

If we denote by $h_2(S)$ the 2-rank of $\mathrm{Cl}_S(L)$, we have $|L(S,2)| = 2^{|S|+h_2(S)}$. Thus, if we adjoin to S a set of $h_2(S)$ prime ideals which generate exactly $\mathrm{Cl}_S(L)[2]$, we obtain a new set S' such that

$$L(S,2) \simeq L(S',2) \simeq \mathbb{U}_{L,S'}/\mathbb{U}_{L,S'}^2.$$

Proposition 1.4. *Let S be the set of all infinite places of L together with the prime ideals $\mathfrak{P}$ of L above $\mathfrak{p}$ in K such that $\mathfrak{P}|P'(\theta)$ and $\mathfrak{p}^2|\operatorname{Disc} P$. We have*

$$\operatorname{Im}\phi \subset L(S,2) \cap \operatorname{Ker} \mathcal{N}_{L/K}.$$

Remark 1.5. The norm in L/K of the number $P'(\theta)$ is precisely equal to the discriminant of the polynomial P. The discriminant of the elliptic curve is equal to 16 times that of the polynomial. As a consequence of this proposition, it will be enough to consider the prime ideals whose square divides Disc P. Thus, it is not necessary to consider all prime factors of 2 Disc P. See also [19] or [20] for a description of these primes in terms of Tamagawa numbers.

Proof. Let (x,y) be a nontrivial point on $E(K)$. We shall first prove that the valuation $v_{\mathfrak{P}}(x-\theta)$ is even at all primes not dividing $P'(\theta)$. Assume first that this valuation is negative. Since θ is integral, we have $v_{\mathfrak{P}}(x-\theta) = v_{\mathfrak{P}}(x)$. The relation $y^2 = x^3 + \ldots$ implies that $2v_{\mathfrak{P}}(y) = 3v_{\mathfrak{P}}(x)$, which proves our assertion in this case. Assume now that $v_{\mathfrak{P}}(x-\theta)$ is nonnegative and odd. In the relation

$$y^2 = P(x) = (x-\theta)\left(P'(\theta) + (x-\theta)\frac{P''(\theta)}{2} + (x-\theta)^2\right),$$

all the elements that occur are integral at $\mathfrak{P}$. If we compare the valuations of both sides of the equality, we see that $\mathfrak{P}$ divides the second factor and therefore divides $P'(\theta)$.

It now remains to prove that if $v_{\mathfrak{P}}(x-\theta)$ is odd, then $\mathfrak{p}^2$ divides Disc P. Since $\mathfrak{P}$ divides $P'(\theta)$, we know that $\mathfrak{p}$ divides Disc P. Assume that $\mathfrak{p}^2$ does not divide Disc P. Since we know that $v_{\mathfrak{p}}(\operatorname{Disc} P) \geqslant e(\mathfrak{P}/\mathfrak{p}) - 1$, where $e(\mathfrak{P}/\mathfrak{p})$ is the relative ramification index, it follows that $\mathfrak{p}$ factors as $\mathfrak{P}_1^2\mathfrak{P}_2$ in L/K, with $\mathfrak{P}_2$ not dividing $P'(\theta)$ (since $\mathfrak{p}^2$ does not divide Disc P). If we set $\alpha_i = v_{\mathfrak{P}_i}(x-\theta)$, we know that α_2 is even and that $2v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(\mathcal{N}_{L/K}(x-\theta)) = \alpha_1 + \alpha_2$ is also even. It follows that $\alpha_1 = v_{\mathfrak{P}}(x-\theta)$ is even, as claimed. □

1.3. *Legendre equations*

All the formulas of this section (1.3) and of the next (1.4) are byproducts of the theory developed in [9].

What we have just proved allows us to embed the group $\operatorname{Im}\phi$ into the finite computable group $L(S,2) \cap \operatorname{Ker} \mathcal{N}_{L/K}$ for an explicit finite set S. It now remains to decide whether a given element $\overline{\delta}$ of $L(S,2) \cap \operatorname{Ker} \mathcal{N}_{L/K}$ belongs to $\operatorname{Im}\phi$. Explicitly, such an element belongs to $\operatorname{Im}\phi$ if and only if it can be written in the form $\overline{x-\theta}$ with $x \in K$, or equivalently if we can find $z \in L^*$ such that $\delta z^2 = x - \theta$. After writing $\delta = a - b\theta + c\theta^2$ with $\mathcal{N}_{L/K}(\delta) = r^2$, and $z = u + v\theta + w\theta^2$, we get

$$\delta' = \delta z^2 = q_0(u,v,w) - q_1(u,v,w)\theta + q_2(u,v,w)\theta^2,$$

where q_0, q_1 and q_2 are three quadratic forms in the variables u, v and w. Their discriminants are respectively $\mathcal{N}_{L/K}((\theta^2 + A\theta + B)\delta) = C^2r^2$, $\mathcal{N}_{L/K}((\theta + A)\delta) = (AB - C)r^2$ and

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

$\mathcal{N}_{L/K}(\delta) = r^2$, where A, B and C are the coefficients of the polynomial P defining E. Since we have assumed that the polynomial P is irreducible, the quantities C and $AB - C$ cannot vanish. We have to solve simultaneously $q_2 = 0$ and $q_1 = 1$. We first look for a particular solution of $q_2 = 0$. We have:

$$\begin{aligned} q_2(u, v, w) = \; & cu^2 + (A^2c + Ab - Bc + a)v^2 \\ & + (A^4c + A^3b - 3A^2Bc + A^2a - 2ABb + 2ACc + B^2c - Ba + Cb)w^2 \\ & - 2(b + Ac)uv + 2(A^2c + Ab - Bc + a)uw \\ & + 2(-A^3c - A^2b + 2ABc - Aa + Bb - Cc)vw. \end{aligned}$$

Using the auxiliary variables $\alpha = Abc + Bc^2 - ac + b^2$ and $\beta = A^2bc + ABc^2 + Ab^2 - Cc^2 + ab$, we make the linear change of variables:

$$\begin{aligned} U &= cu - (b + Ac)v + (a + Ab + A^2c - Bc)w, \\ V &= \alpha v - \beta w, \\ W &= rw, \end{aligned}$$

so that we obtain $-\alpha c q_2(u, v, w) = Q_2(U, V, W)$ with

$$Q_2(U, V, W) = V^2 - \alpha U^2 - cW^2. \tag{1}$$

Thus, we are reduced to solving the Legendre equation $Q_2 = 0$. The above is valid only if αc does not vanish. However, if $c = 0$, there is a trivial solution (there is essentially nothing to do), and if $\alpha = 0$, we observe that $\mathcal{N}_{L/K}(\delta)/\delta = (r/\delta)^2\delta$ is equivalent to δ and has no term in θ^2, since this term is precisely given by α.

When $\alpha c \neq 0$, equation (1) defines a conic. For such a curve, we know that the Hasse principle applies: the existence of a solution in K is equivalent to the existence of a local solution at every place of K. In fact, it is only necessary to test the infinite places and the places dividing $2\alpha c$. This local solubility is given by the Hilbert symbol.

In the classical situation where we look for rational points on elliptic curves defined over $\mathbb{Q}$, this leads to Legendre equations with coefficients in $\mathbb{Z}$. In this case, we have at our disposal an efficient algorithm to solve this equation (see [**10**]). This algorithm makes a crucial use of Euclidean division in $\mathbb{Z}$. For this reason, it is difficult to write down a direct generalization that is valid over general number fields; in fact, it is seldom even possible (see [**21**]). We must proceed in another way.

Let us consider the quadratic extension $K(\sqrt{\alpha})/K = F/K$. Equation (1) is equivalent to

$$\mathcal{N}_{F/K}\left(\frac{V + \sqrt{\alpha}U}{W}\right) = c. \tag{2}$$

Note that the two numbers α and c play a symmetrical role. The question is whether or not c is a norm for the extension F/K, and, if this is the case, to find an explicit element of norm c.

Before giving an answer to this question, we need some notation. The extension F/K is quadratic, and hence cyclic. Denote by G its Galois group. Let S_K be a finite set of primes of K, and let S_F be the set of primes of F above those in S_K. By an abuse of notation, we shall write S for both. As before, we denote by $\mathbb{U}_{K,S}$ the S-units of K, and by $\mathbb{U}_{F,S}$ the S-units of F. If $\mathrm{Cl}_S(F)$ is the S-class group of F, $\mathrm{Cl}_S(F)^G$ is the subgroup of invariant classes under the action of G, and $\mathrm{Cl}_S(\mathfrak{I}^G)$ the subgroup of classes of invariant ideals under this action. We have $\mathrm{Cl}_S(\mathfrak{I}^G) \subset \mathrm{Cl}_S(F)^G \subset \mathrm{Cl}_S(F)$.

With this notation, we have the following proposition.

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

Proposition 1.6. *Let F/K be a cyclic extension of number fields with Galois group G. There exists an isomorphism*

$$\frac{\mathrm{Cl}_S(F)^G}{\mathrm{Cl}_S(\mathfrak{I}^G)} \simeq \frac{\mathcal{N}_{F/K}(F^*) \cap \mathbb{U}_{K,S}}{\mathcal{N}_{F/K}(\mathbb{U}_{F,S})}.$$

In particular, if S generates the class group $\mathrm{Cl}(F)$, we have

$$\mathcal{N}_{F/K}(F^*) \cap \mathbb{U}_{K,S} = \mathcal{N}_{F/K}(\mathbb{U}_{F,S}).$$

This is essentially Chevalley's ambiguous classes theorem; a proof of the statement as given above, and more complete results about norm equations in non-Galois extensions, can be found in [22].

Thanks to this result, we know in which cases the S-units that are norms for a cyclic extension are simply norms of S-units (this is not always the case!). Thus, a solution of equation (2) will be given by an S-unit of F, where S contains all prime factors of c, and generators of the 2-part of $\mathrm{Cl}(F)$. Since there is only a finite number of S-units modulo squares, there is only a finite number of potential solutions. If this construction does not give a solution, then there is no solution at all.

The above discussion either gives one solution to $q_2 = 0$, or proves that it is impossible. Using this solution, we can construct an element $z \in L^*$ such that $\delta' = \delta z^2 = a - b\theta$.

1.4. *Construction of the quartic*

Assume now that δ is of the form $\delta = a - b\theta$, with a and b algebraic integers in $\mathbb{Z}_K$. We have $\mathcal{N}_{L/K}(\delta) = r^2$. We want to find δ' with $\overline{\delta'} = \overline{\delta}$ and of the form $\delta' = x - \theta$. This is equivalent to looking for $z = u + v\theta + w\theta^2 \in L^*$ such that $\delta' = \delta \cdot z^2$ satisfies both $q_2 = 0$ and $q_1 = 1$. The previous discussion is no longer applicable, since we are precisely in the case $c = 0$. These equations can be written as follows:

$$\begin{aligned} q_2(u,v,w) &= (Ab+a)v^2 + (A^3b + A^2a - 2ABb - Ba + Cb)w^2 \\ &\quad -2buv + 2(Ab+a)uw + 2(-A^2b - Aa + Bb)vw; \\ q_1(u,v,w) &= bu^2 - Bbv^2 + (-ABa - A^2Bb + ACb + B^2b + Ca)w^2 \\ &\quad +2(ABb + Ba - Cb)vw - 2Bbuw - 2auv. \end{aligned}$$

Here, it is important to note that $b \neq 0$ if $\overline{\delta} \neq 1$. Indeed, otherwise we would have $\delta = a$ and $a^3 = \mathcal{N}_{L/K}(\delta) = r^2$, and therefore $a = \delta$ would be a square, which can only occur for the trivial case $\overline{\delta} = 1$, a contradiction. The case $\overline{\delta} = 1$ is, of course, of no interest. We can thus make the linear change of variables

$$\begin{aligned} U &= -2b^2u + (Ab^2 + ab)v + (a^2 + 2Bb^2 - A^2b^2)w, \\ V &= -bv + (a + Ab)w, \\ W &= rw, \end{aligned}$$

and we get the identity $b^2 q_2(u,v,w) = W^2 - UV$. The solutions of $q_2 = 0$ are given by $(U,V,W) = (\lambda^2/y, \mu^2/y, \lambda\mu/y)$, where (λ, μ, y) belongs to $K \times K \times K^*$. We can express u, v and w in terms of y, λ and μ. The equation $q_1 = 1$ becomes:

$$\begin{aligned} 4b^3y^2 &= \lambda^4 - 2(Ab + 3a)\lambda^2\mu^2 + 8r\lambda\mu^3 + (A^2b^2 - 2Aab - 4Bb^2 - 3a^2)\mu^4 \\ &= Q(\lambda, \mu). \end{aligned}$$

The discriminant of this fourth-degree polynomial in λ and μ is equal to $2^{12}b^6 \,\mathrm{Disc}\, P$.

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

Now recall that a quartic has two polynomial invariants I and J, of total degree 2 and 3 and weight 4 and 6 respectively, in the coefficients of the quartic, such that the ring of invariants of the quartic is the free polynomial algebra generated by I and J. For example, the usual discriminant of the quartic is equal to $(4I^3 - J^2)/27$. It is easy to check that the I and J invariants of Q are related to the I and J invariants of P (considered as a degree-4 polynomial with zero leading term) by the relations $I(Q) = 2^4 b^2 I(P)$ and $J(Q) = 2^6 b^3 J(P)$. They are also related to the c_4 and c_6 invariants of the elliptic curve by $I(Q) = b^2 c_4$ and $J(Q) = 2b^3 c_6$.

1.5. *Minimization of the quartic*

In classical 2-descent over $\mathbb{Q}$, we get only quartics with discriminant Disc P or 2^{12} Disc P (see, for example, [7]). This comparison suggests that the factor b^6 can be removed and the quartic minimized. Such a minimization can be achieved as follows, using the fact that the factorization of $Q \mod b$ is formally given by $a^4 Q = (a\lambda - r\mu)^3(a\lambda + 3r\mu)$.

(An algorithm for finding such u and v, valid over general number fields, is given in [6]).

Proposition 1.7. *Let l, a_1, r_1, u, and v be five integers in $\mathbb{Z}_K$, such that*

$$f = (la + ba_1)u - (lr + br_1)v \neq 0.$$

The quartic $4b^3y^2 = Q(\lambda, \mu)$ can be minimized to $4y^2 = Q'(\lambda', \mu')$ such that

- *Q' has integral coefficients;*
- Disc $Q' = 2^{12} f^{12}$ Disc P*;*
- *$I(Q') = 2^4 f^4 I(P)$ and $J(Q') = 2^6 f^6 J(P)$.*

Proof. Consider the linear change of variables

$$\lambda = bu\lambda' + (lr + br_1)\mu';$$
$$\mu = bv\lambda' + (la + ba_1)\mu'.$$

Its determinant is bf. Applied to Q, this linear change of variables defines a new polynomial which is formally divisible by b^3. Letting $Q(\lambda, \mu) = b^3 Q'(\lambda', \mu')$, we see that our quartic becomes

$$4y^2 = Q'(\lambda', \mu').$$

The discriminant of Q' is now equal to $2^{12} f^{12}$ Disc P, and we obtain the conclusion of the proposition. Note that the I and J invariants are also reduced in the same way. □

Remark 1.8. It is quite common that a and b are coprime. In this case, we can find l and a_1 such that $la + ba_1 = 1$ (an algorithm for finding such l and a_1, valid over general number fields, is given in [6]). A suitable change of variables is then

$$\lambda = b\lambda' + (lr + br_1)\mu',$$
$$\mu = \mu',$$

since it gives $u = 1$, $v = 0$, and hence $f = 1$.

I do not claim that these choices will always lead to a Q' with small coefficients, and a better choice should be sought. In [8], J. Cremona describes a very efficient reduction algorithm for the coefficients of a real quartic; in some sense, it gives the smallest possible reduction.

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

1.6. *Solubility of the quartic*

Before looking for a solution of the quartic over K, we can look at its local solubility. Since the quartic defines a curve of genus 1, we know that there exist local solutions at all places not dividing $2\,\mathrm{Disc}\,Q = 2^{13}b^3\,\mathrm{Disc}\,P$ (see, for example, [11]).

The local solubility at the bad primes is tested by using a classical Hensel lift (see [11]). For the Archimedean real places, this is equivalent to knowing whether the polynomial bQ or Q' can assume non-negative values.

As soon as we know that the quartic is everywhere locally soluble, we can hope to find a global point. For this, we can test all values of x up to a given height, using more or less powerful methods. If we are lucky, we find a point on the quartic, from which it is not difficult to recover a point on the elliptic curve by using the formulas of this paper. If we do not know where the quartic comes from (for example, if it has been constructed by another method; see [8]), it is still possible to recover the point on the elliptic curve by using a syzygy (see [9]). But since we do not have any bound for the height of a point on the quartic, it may happen that the smallest one is too large to be found by such a naive search, and hence we might miss it. In fact it is not always true that such a point will exist at all.

The set of all $\overline{\delta}$ which lead to everywhere locally soluble quartics forms a subgroup of $L(S,2)\cap\mathrm{Ker}\,\mathcal{N}_{L/K}$: this is the Selmer group $S^2(E/K)$ (see [18]). Recall the exact sequence

$$1 \to E(K)/2E(K) \to S^2(E/K) \to Ш(E/K)[2] \to 1.$$

Since the group $Ш(E/K)[2]$ of elements of order 2 in the Tate–Shafarevich group is not always trivial, this implies the well-known fact that the local-global Hasse principle does not hold for genus 1 curves; in other words, the existence of local solutions does not imply the existence of a global one (over K).

Remark 1.9. As has been pointed out to me by J. Cremona and M. Stoll, it is not necessary to have the explicit equation of the quartic in order to know its local solubility. Indeed, we can use a criterion of Siksek (given in [16]) to test the local solubility directly on the system $q_2 = 0$, $q_1 = 1$. Using the notation of [16], it is necessary only to test the local solubility at the primes dividing 2 or $\partial(q_2, q_1 - 1) = r^{12}\,\mathrm{Disc}\,P$. The main advantage of this idea is that it allows one to compute the Selmer group directly, and we save the time needed for solving all the Legendre equations that lead to non-soluble quartics.

2. *Examples*

Using the PARI/GP package (see [5]), we have implemented this algorithm and computed the Mordell–Weil groups of various elliptic curves for several number fields with degrees ranging from 1 to 5, and having *a priori* any class number. However, this requires a large amount of work for large degrees (we have to compute class groups and units in degree-15 fields), and for such degrees, the computation was possible only for a few well-chosen examples. The complete gp-program is available at [23].

2.1. *A complete example*

For the quadratic case, the computations are quite fast (less than one second for the easy cases). The following example consists of an elliptic curve defined over an imaginary quadratic field with nontrivial class number (as opposed to the situation in [11]).

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

Let $K = \mathbb{Q}(\varepsilon)$, with $\varepsilon^2 - \varepsilon + 4 = 0$. This is the imaginary quadratic field of discriminant -15. Its class group is of order 2.

Consider the elliptic curve E given by the equation

$$y^2 = P(x) = x^3 + \varepsilon x - 1.$$

The discriminant of P is equal to $12\varepsilon - 11$, and is not divisible by the square of a nontrivial ideal in K. The field L is generated by θ such that $P(\theta) = 0$ or, equivalently, such that $0 = 1 - \theta + 4\theta^2 - 2\theta^3 + \theta^4 + \theta^6$. The class group of L is of order 2, and is generated by the prime ideal $\mathfrak{P}_2$ above 2 such that $\mathfrak{P}_2^2 = (1-\theta)\mathbb{Z}_L$, and $\mathcal{N}_{L/K}(1-\theta) = \varepsilon$. The units of L are generated by -1, θ and $-2 + \varepsilon\theta + \theta^2$, with respective relative norms -1, 1 and 1.

Following Proposition 1.4, we set $S = \{\infty_1, \infty_2, \infty_3\} \cup \{\mathfrak{P}_2\}$. For this choice, the group $L(S, 2)$ is generated by -1, θ, $-2+\varepsilon\theta+\theta^2$, and $1-\theta$. Since we have computed the norms of these elements, linear algebra over $\mathbb{Z}/2\mathbb{Z}$ tells us that the group $L(S, 2) \cap \mathrm{Ker}\ \mathcal{N}_{L/K}$ is of order 4, and is generated by the classes of θ and $-2 + \varepsilon\theta + \theta^2$. From this, we already know that the rank of $E(K)$ is at most equal to 2. We have

$$L(S, 2) \cap \mathrm{Ker}\ \mathcal{N}_{L/K} = \left\{1, \theta, -2 + \varepsilon\theta + \theta^2, 1 - (\varepsilon + 2)\theta + \varepsilon\theta^2\right\}.$$

Let $\delta = \delta_1 = \theta$. Since δ has no coefficient in θ^2, we are already at the final step of the method, and we have to find a K-rational point on the quartic

$$-4y^2 = \lambda^4 + 8\lambda\mu^3 - 4\varepsilon\mu^4.$$

We check that this quartic has no local solution at $\mathfrak{p}_2$ (below $\mathfrak{P}_2$), and hence no global solution.

Let $\delta = \delta_2 = -2 + \varepsilon\theta + \theta^2$. Here, we have $c = 1$, and hence the Legendre equation $V^2 - \alpha U^2 = cW^2$ is satisfied by $(U, V, W) = (0, 1, 1)$. From this, we find the solution $(u, v, w) = (\varepsilon, 2-\theta, 2)$ for $q_2 = 0$, which gives $\delta' = \delta(u + v\theta + w\theta^2)^2 = \varepsilon(1-\theta)$, with $\mathcal{N}_{L/K}(\delta') = \varepsilon^4$. We then have to find a K-rational point on the quartic

$$4\varepsilon^3 y^2 = \lambda^4 - 6\varepsilon\lambda^2\mu^2 + 8(\varepsilon - 4)\lambda\mu^3 + (9\varepsilon + 28)\mu^4.$$

Once again, we check that this quartic has no local solution at $\mathfrak{p}_2$, and hence no global solution.

Let $\delta = \delta_3 = 1 - (\varepsilon + 2)\theta + \varepsilon\theta^2$. Here, we have $\alpha = \varepsilon^2$, and thus the Legendre equation $V^2 - \alpha U^2 = cW^2$ has the solution $(U, V, W) = (1, \varepsilon, 0)$. From this, we find the solution $(u, v, w) = (-5 + \varepsilon, -2, 0)$ for $q_2 = 0$, which gives $\delta' = \delta(u + v\theta + w\theta^2)^2 = (29 + 3\varepsilon) - (10 + 14\varepsilon)\theta$, with $\mathcal{N}_{L/K}(\delta') = (93 - 41\varepsilon)^2$. We then have to find a K-rational point on the quartic

$$4(10 + 14\varepsilon)^3 y^2 = \lambda^4 - 6(29 + 3\varepsilon)\lambda^2\mu^2 + 8(93 - 41\varepsilon)\lambda\mu^3 + (5201 + 283\varepsilon)\mu^4.$$

This quartic is minimized by the linear change of variables $\lambda = b\lambda' + (lr + br_1)\mu'$ and $\mu' = \mu$ with $l = (29/4)\varepsilon + 4$ and $r_1 = -48 + 19\varepsilon$. Thus, the quartic is equivalent to

$$4y^2 = (14\varepsilon + 10)\lambda'^4 + (-12\varepsilon + 68)\lambda'^3\mu' - 24\varepsilon\lambda'^2\mu'^2 + (2\varepsilon - 16)\lambda'\mu'^3 + \varepsilon\mu'^4.$$

By a naive search, we find the solution $\lambda = \varepsilon$, $\mu = 2$ and $y = 4 - 2\varepsilon$, which gives the point

$$\left(-\frac{\varepsilon}{3} + 1, \frac{\varepsilon}{9} + \frac{4}{9}\right) \in E(K).$$

We have therefore proved that $E(K)$ has rank 1, and that the group $Ш(E/K)[2]$ is trivial.

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

Table 1: Quadratic examples

N	a_1	a_2	a_3	a_4	a_5	$\#S^2$	r	$\#Ш[2]$	P
				$K=\mathbb{Q}(\sqrt{-3})$; $\varepsilon^2-\varepsilon+1=0$					
19	0	$-\varepsilon$	1	$-1+\varepsilon$	0	2	1	1	$(1,0)$
19	0	$-\varepsilon$	1	$9-9\varepsilon$	-15	2	1	1	$(2\varepsilon,-1+\varepsilon)$
19	0	$-\varepsilon$	14	$769-769\varepsilon$	-8470	2	1	1	$(\frac{801}{49}\varepsilon,-\frac{171+\varepsilon}{343})$
19	0	$-\varepsilon$	1	$-31-99\varepsilon$	$74-498\varepsilon$	2	1	1	$(-4-3\varepsilon,2-\varepsilon)$
19	0	$-\varepsilon$	1	$99+31\varepsilon$	$-424+498\varepsilon$	2	1	1	$(3-3\varepsilon,5+10\varepsilon)$
				$K=\mathbb{Q}(\sqrt{-4})$; $\varepsilon^2+1=0$					
$13+8\varepsilon$	0	$1-\varepsilon$	ε	$-\varepsilon$	0	2	1	1	$(0,0)$
				$K=\mathbb{Q}(\sqrt{-8})$; $\varepsilon^2+2=0$					
$13+8\varepsilon$	0	$-1+\varepsilon$	1	$1-\varepsilon$	ε	1	0	1	
$13+8\varepsilon$	0	$-1+\varepsilon$	1	$11-11\varepsilon$	$-27+3\varepsilon$	1	0	1	
$13+8\varepsilon$	0	$-1+\varepsilon$	1	$-9+39\varepsilon$	$-210-39\varepsilon$	1	0	1	
$13+8\varepsilon$	0	$1-\varepsilon$	1	$2-2\varepsilon$	1	1	0	1	
				$K=\mathbb{Q}(\sqrt{-19})$; $\varepsilon^2-\varepsilon+5=0$					
2ε	ε	$1-\varepsilon$	1	-1	0	1	0	1	
2ε	ε	$1-\varepsilon$	1	$9-5\varepsilon$	$-24-2\varepsilon$	1	0	1	
2ε	ε	$1-\varepsilon$	1	$-31-15\varepsilon$	$-60-54\varepsilon$	1	0	1	
$-3+6\varepsilon$	0	1	1	20	-32	4	0	4	
$-3+6\varepsilon$	0	1	1	-4390	-113432	4	0	4	
$-3+6\varepsilon$	0	-1	1	-2	2	4	2	1	$(2,1)$
									$(1+4\varepsilon,15-12\varepsilon)$
				$K=\mathbb{Q}(\sqrt{-43})$; $d\varepsilon^2-\varepsilon+11=0$					
$13+\varepsilon$	0	$-\varepsilon$	$1+\varepsilon$	-2	$1-\varepsilon$	2	1	1	$(-1,-2)$
				$K=\mathbb{Q}(\sqrt{-67})$; $\varepsilon^2-\varepsilon+17=0$					
3ε	ε	$1+\varepsilon$	ε	$-1-3\varepsilon$	$16-5\varepsilon$	2	1	1	$(-\varepsilon,-4)$

2.2. *A collection of quadratic examples*

In [12], we find a collection of elliptic curves defined over imaginary quadratic fields with class number 1. Using the theory of L functions, J. Cremona and E. Whitley computed the analytic rank and some other data associated with these elliptic curves. In each case, our 2-descent method is able to prove the observations that they made from their computations. We present the results in Table 1.

The number field K is given by the square root of its discriminant, and by the minimal polynomial of its generator ε. We use here the standard notation for elliptic curves: its Weierstrass model is given by $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$, and its conductor is N. The result of the 2-descent is given by the quantities $\#S^2$ (the order of the Selmer group), r (the rank), $\#Ш[2]$ (the order of the 2-part of the Tate–Shafarevich group) and a set of independent points on the curve.

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

Remark 2.1. A word has to be said about the two curves with nontrivial Tate–Shafarevich group. These curves are in fact defined over $\mathbb{Q}$. It is well known that

$$\operatorname{rank}\left(E\left(\mathbb{Q}\left(\sqrt{-19}\right)\right)\right) = \operatorname{rank}(E(\mathbb{Q})) + \operatorname{rank}\left(E^{(-19)}(\mathbb{Q})\right),$$

where $E^{(-19)}$ is the twist of E by -19. From this, it is not difficult to prove that the rank must be equal to 0 over $\mathbb{Q}(\sqrt{-19})$. On the other hand, our 2-descent produces three nontrivial everywhere locally soluble quartics, which certainly represent nontrivial elements in the Tate–Shafarevich group. To be more precise, we give these three quartics for the first curve:

$$\begin{aligned} y^2 &= -103x^4 - 160x^3 - 134x^2 - 56x + 5 \\ y^2 &= (27\varepsilon - 56)x^4 + (20\varepsilon - 36)x^3 + (-48\varepsilon + 22)x^2 + (-4\varepsilon + 32)x + (\varepsilon + 7) \\ y^2 &= (50\varepsilon - 229)x^4 + (76\varepsilon + 612)x^3 + (-306\varepsilon - 782)x^2 \\ &\quad +(236\varepsilon + 520)x + (-53\varepsilon - 134). \end{aligned}$$

2.3. *A degree-5 example*

Consider the number field $K = \mathbb{Q}(\varepsilon)$, with $\varepsilon^5 - \varepsilon^3 - \varepsilon^2 + \varepsilon + 1 = 0$. This field has a single real embedding, and its discriminant is equal to 1609. Using 2-descent, we have computed that the curve

$$E:\ y^2 = x^3 + \varepsilon$$

has rank 1, and that the group $Ш(E/K)[2]$ is trivial. The point $(\varepsilon^4 - \varepsilon, \varepsilon + 1)$ has infinite order in $E(K)$. We do not go into the cumbersome details here; the interested reader should run the `gp`-program available at [**23**].

References

1. B. J. Birch and H. P. F. Swinnerton–Dyer, 'Notes on elliptic curves', *J. Reine Angew. Math.* 212 (1963) 7–25.
2. N. Bruin, 'Algae, a program for computing 2-Selmer groups of elliptic curves over number fields', `http://www.cecm.sfu.ca/~bruin/ell.shar`. 7
3. N. Bruin, 'Visualizing Sha[2] in abelian surfaces', preprint, 2002. 7
4. J. W. S. Cassels, *Lectures on elliptic curves*, London Math. Soc. Stud. Texts 24 (Cambridge University Press, 1991). 7, 8
5. H. Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math. 138, 3rd corrected printing (Springer, 1996). 7, 13
6. H. Cohen, *Advanced topics in computational algebraic number theory*, Grad. Texts in Math. 193 (Springer, 2000). 12, 12
7. J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edn (Cambridge University Press, 1997). 7, 12
8. J. E. Cremona, 'Reduction of binary cubic and quartic forms', *LMS J. Comput. Math.* 2 (1999) 62–92; `http://www.lms.ac.uk/jcm/2/lms1998-007/`. 12, 13
9. J. E. Cremona, 'Classical invariants and 2-descent on elliptic curves', *J. Symb. Comput.* 31 (2001) 71–87. 7, 9, 13
10. J. E. Cremona and D. Rusin, 'Efficient solution of rational conics', *Math. Comp.* (2002), to appear. 10

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press

11. J. E. Cremona and P. Serf, 'Computing the rank of elliptic curves over real quadratic fields of class number 1', *Math. Comp.* 68 (1999) 1187–1200. 7, 13, 13, 13

12. J. E. Cremona and E. Whitley, 'Periods of cusp forms and elliptic curves over imaginary quadratic fields', *Math. Comp.* 62 (1994) 407–429. 15

13. Z. Djabri and N. P. Smart, 'A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve', *ANTS-III*, Lecture Notes in Comput. Sci. 1423 (ed. J. Buhler, Springer, 1998) 502–513. 7

14. Z. Djabri, E. F. Schaefer and N. P. Smart, 'Computing the p-Selmer group of an elliptic curve', *Trans. Amer. Math. Soc.* 352 (2000) 5583–5597. 7

15. S. Lang, *Algebraic number theory*, Grad. Texts in Math. 110, 2nd edn (Springer, 1994). 8

16. J. R. Merriman, S. Siksek and N. P. Smart, 'Explicit 4-descent on an elliptic curve', *Acta Arith.* 77 (1996) 385–404. 13, 13

17. B. Poonen and E. F. Schaefer, 'Explicit descent for Jacobians of cyclic covers of the projective line', *J. Reine Angew. Math.* 488 (1997) 141–188. 8

18. E. F. Schaefer, '2-descent on the Jacobians of hyperelliptic curves', *J. Number Theory* 51 (1995) 219–232. 7, 8, 13

19. E. F. Schaefer, 'Class groups and Selmer groups', *J. Number Theory* 56 (1996) 79–114. 9

20. E. F. Schaefer and M. Stoll, 'How to do a p-descent on an elliptic curve', preprint, 2001. 9

21. D. Simon, 'Equations dans les corps de nombres et discriminants minimaux', Doctoral Thesis, Université Bordeaux I, France (1998). 8, 10

22. D. Simon, 'Solving norm equations using S-units', *Math. Comp.* (2002), to appear. 11

23. D. Simon, 'The gp-program', `http://www.math.unicaen.fr/~simon/ell.gp`. 7, 13, 16

24. N. P. Smart, *The algorithmic resolution of diophantine equations*, London Math. Soc. Stud. Texts 41 (Cambridge University Press, 1998). 7, 7

25. M. Stoll, 'Implementing 2-descent for Jacobians of elliptic curves', *Acta Arith.* 98 (2001) 245–277. 7

Denis Simon `Denis.Simon@math.unicaen.fr`

Université de Caen – France

Campus II – Boulevard Maréchal Juin

BP 5186

14032 Caen cedex

France

https://doi.org/10.1112/S1461157000000668 Published online by Cambridge University Press