MATHEMATICS OF COMPUTATION
Volume 68, Number 227, Pages 1187–1200
S 0025-5718(99)01055-8
Article electronically published on February 15, 1999

COMPUTING THE RANK OF ELLIPTIC CURVES OVER REAL QUADRATIC NUMBER FIELDS OF CLASS NUMBER 1

J. E. CREMONA AND P. SERF

Abstract. In this paper we describe an algorithm for computing the rank of an elliptic curve defined over a real quadratic field of class number one. This algorithm extends the one originally described by Birch and Swinnerton-Dyer for curves over $\mathbb{Q}$. Several examples are included.

1. Introduction

The method of 2-descent has been used for many years in the study of the arithmetic of elliptic curves, in both theoretical and computational investigations. For elliptic curves defined over the rational numbers $\mathbb{Q}$, an explicit algorithm for carrying out a general 2-descent was presented by Birch and Swinnerton-Dyer in [1]. A simpler algorithm, using 2-descent via 2-isogeny, can be applied when the curve has non-trivial 2-torsion; this is described in [11], [6], or [10]. Both algorithms have also been described in the book [2], and have been implemented by the first author. (His program `mwrank` may be obtained via anonymous ftp from //euclid.exeter.ac.uk/pub/cremona/progs.)

The aim of the present paper is to describe how to carry out general 2-descent over real quadratic number fields. For simplicity, we restrict to fields of class number 1. We also give several examples. The algorithms have been implemented by the second author; see [8], where more details and examples may be found. (The resulting program `rankrqnf1` can be obtained free via anonymous ftp from //ftp.math.uni-sb.de/pub/simath/pascale-serf.)

For the implementation of the algorithms, the computer algebra system SIMATH was used. This system is mainly designed for algebraic number theory, with an emphasis on elliptic curves and function fields over finite fields. It has been developed since 1985 in the research group of Prof. H. G. Zimmer in Saarbrücken. (For non-commercial applications, SIMATH is available free via anonymous ftp from //ftp.math.uni-sb.de/pub/simath.)

An independent implementation of 2-descent via 2-isogeny for number fields of arbitrary degree and class number is currently being developed by D. Simon in Bordeaux, as part of the PARI system.

Received by the editor June 7, 1996 and, in revised form, January 22, 1998.
1991 *Mathematics Subject Classification.* Primary 11G05, 11Y16, 11Y50, 14G25, 14H52, 14Q05.
Key words and phrases. Elliptic curves, Mordell-Weil, real quadratic fields.
The second author was supported in part by DFG grant 513 009 738 3.

Much of the work carried out here also applies to the case of imaginary quadratic fields; the main difference is that in order to obtain bounds for the search region (see subsections 2.1–2.3) it is necessary to do more work. This is currently in progress.

We would like to thank Prof. H. G. Zimmer for his support, and Prof. D. Zagier for some helpful suggestions.

2. 2-descent over real quadratic fields

If an elliptic curve E has a rational point of order 2 over a number field K, one can use 2-descent via 2-isogeny to determine $\mathrm{rk}(E/K)$. This algorithm goes back to Tate and is described in some detail in [11], [6], and [10]. See also [2] for a detailed description of the algorithm over $\mathbb{Q}$.

In order to implement 2-descent via 2-isogeny over a number field K, the following ingredients are needed in addition to basic arithmetic for the field and its ring of integers $\mathfrak{O}_K$:

1. For a given finite set S of prime ideals of K, determine representatives in K^* for the finite set $K(S,2)$ consisting of those $\alpha \in K^*$ modulo $(K^*)^2$ such that $\mathrm{ord}_{\mathcal{P}}(\alpha)$ is even for all primes $\mathcal{P} \in S$.
2. Given a quartic polynomial $g(X) \in K[X]$, determine whether $g(X)$ has any roots in K, and also whether the equation $Y^2 = g(X)$ is (a) soluble everywhere locally, i.e., in all completions $K_{\mathcal{P}}$ of K (including $\mathbb{R}$ if K has real embeddings); or (b) soluble globally, i.e., in K.

The first task is straightforward when K has class number one, since it amounts to listing all square-free divisors of a fixed element of K^*, modulo squares of units. The second is much harder and will be discussed in more detail below, as the same procedures are needed for the general 2-descent which we will describe. In practice it is not hard to determine the local solubility, but all we do to find global points on the quartics $Y^2 = g(X)$ is to carry out an efficient search for points with small height. Hence there are cases where we do not find a global point even when there is no local obstruction; in these cases, we cannot decide whether there are in fact no global points (in which case the curve we are studying has non-trivial Tate-Shafarevitch group), or such points exist but have large height. In such cases we will only be able to determine lower and upper bounds for the rank.

In our implementation, we handle separately curves which have a K-rational 2-torsion point, as descent via 2-isogeny is much simpler and faster than the general 2-descent. We have computed the rank r and found r independent points of infinite order for a large number of curves over the fields $\mathbb{Q}(\sqrt{D})$ for

$$D = 2, 3, 5, 6, 7, 11, 13, 14, 17, \text{ and } 19.$$

In particular, we have carried out the following investigations. We studied the curves defined over $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{6})$ considered by Graf in [5]. In several cases, we were able to show that the lower bounds for the ranks given in [5] are in fact too small, and we found explicit generators in all cases (which are not given in [5]). We also investigated the size of the 2-torsion subgroups of the Tate-Shafarevitch groups over $\mathbb{Q}(\sqrt{D})$ of a family of curves defined over $\mathbb{Q}$ studied by Kramer in [7], finding examples of order up to 2^{10}. See [8] for details of these investigations, which we have omitted here at the suggestion of the referee.

We now turn to general 2-descent, which (in principle) can be applied to an arbitrary elliptic curve E over a number field K, whether or not $E(K)$ has points of order 2. We follow the method described by Birch and Swinnerton-Dyer in [1] for the case $K = \mathbb{Q}$, with a few modifications. These are analogues in the real quadratic case of improvements made by the first author to the algorithm over $\mathbb{Q}$, implemented in his `mwrank` program; see [2] and [3].

The main principle of general 2-descent is to consider 2-*coverings* (or *principal homogeneous spaces*) of the elliptic curve E. These are represented (provided that they are everywhere locally soluble, see the remark below) by quartic equations of the form

$$Y^2 = g(X) = aX^4 + bX^3 + cX^2 + dX + e \qquad \text{with } a, b, c, d, e \in K,$$

whose invariants

$$I(g) = 12ae - 3bd + c^2 \quad \text{and} \quad J(g) = 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3$$

differ from the invariants $c_4(E)$ and $2c_6(E)$ by a 4th and a 6th power, i.e.,

$$I(g) = \lambda^4 \, c_4(E) \quad \text{and} \quad J(g) = \lambda^6 \, 2c_6(E)$$

for some $\lambda \in K^*$. Two homogeneous spaces $Y^2 = g_1(X)$ and $Y^2 = g_2(X)$ are called *equivalent* if

$$g_2(X) = \mu^2(\gamma X + \delta)^4 g_1\left(\frac{\alpha X + \beta}{\gamma X + \delta}\right)$$

for some $\alpha, \beta, \gamma, \delta, \mu \in K$ with $(\alpha\delta - \beta\gamma)\mu \in K^*$. Then $I(g_2) = (\alpha\delta - \beta\gamma)^4\mu^4 I(g_1)$ and $J(g_2) = (\alpha\delta - \beta\gamma)^4\mu^4 J(g_1)$. By suitable scaling, each equivalence class contains integral quartics (with coefficients in the ring of integers $\mathfrak{O}_K$), and we will only consider integral quartics from now on.

Remark. Not all 2-coverings of E can be represented by quartics. However, this is certainly possible for those which have points everywhere locally (that is, in all completions of K) by [1, Lemma 1]. These are the only 2-coverings that will concern us here.

The set of all equivalence classes of 2-coverings forms an elementary abelian 2-group $\mathcal{G}$, isomorphic to the Galois cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})[2])$. The trivial class in $\mathcal{G}$ consists of those quartics $Y^2 = g(X)$ such that $g(X)$ has a root in K.

We are interested in the following two subgroups of $\mathcal{G}$ the subgroup G of all equivalence classes of 2-coverings which have a point everywhere locally (i.e., over all completions $K_{\mathcal{P}}$ of K); and the subgroup G' of all equivalence classes of 2-coverings which have a global point. These are both finite elementary abelian 2-groups: G is isomorphic to the Selmer group $S^{(2)}(E/K)$, while G' is isomorphic to $E(K)/2E(K)$. In fact, each global point on a quartic gives rise to a point in $E(K)$, whose coset modulo $2E(K)$ only depends on the equivalence class to which the quartic belongs; and all cosets of $2E(K)$ in $E(K)$ are covered by suitable quartics. Writing the orders of G and G' as 2^k and $2^{k'}$, respectively, by the Mordell-Weil Theorem the rank r of $E(K)$ is given by

$$r = k' - t,$$

where $2^t = \#E(K)[2]$. So in order to compute the rank r, all we have to do is determine the number 2^k of all everywhere locally soluble quartics (up to equivalence) and, among these, the number $2^{k'}$ of all globally soluble quartics.

Just as in the case of 2-descent via 2-isogeny, there is a major problem: How to decide whether a quartic with points everywhere locally has a global point? If we do not find such a point, it may be either because there is none, or because we have not searched long enough.

Quartics which are everywhere locally but not globally soluble come from elements of order 2 in the Tate-Shafarevitch group; more precisely, the exact sequence

$$0 \hookrightarrow E(K)/2E(K) \longrightarrow S^{(2)}(E/K) \longrightarrow Ш(E/K)[2] \longrightarrow 0$$

implies

$$\#Ш(E/K)[2] = \#(S^{(2)}(E/K)) \,/\, \#(E(K)/2E(K)) = \#(G/G') = 2^{k-k'}.$$

Thus $k' < k \iff Ш(E/K)[2]$ is non-trivial.

For a fixed pair of integral invariants (I, J), the number of equivalence classes of integral quartics is finite; we will show how to bound the coefficients (a, b, c) to a finite search region. We must also consider which pairs (I, J) are relevant for a given curve. We will return to the latter question in Section 3, and now confine ourselves to one fixed pair (I, J), explaining in detail how to find all quartics belonging to this pair.

Our approach is to determine suitable bounds on a triple loop for the coefficients (a, b, c), after which solving for the remaining coefficients (d, e) is easy. Thus we must determine the following:

(1) a search region for a,
(2) for each a, a search region for b,
(3) for each pair (a, b) in the search region, a search region for c,
(4) for each triple (a, b, c) in the search region, the coefficients d and e (if any) such that $I(a, b, c, d, e) = I$ and $J(a, b, c, d, e) = J$;

and then check whether each quartic $Y^2 = aX^4 + bX^3 + cX^2 + dX + e$ found is

(5) a trivial quartic,
(6) equivalent to a quartic obtained previously,
(7) everywhere locally soluble,
(8) globally soluble.

Finally we will derive

(9) points on the elliptic curve from the global points on the quartics.

The nine steps in this procedure are described in more detail in the following subsections 2.1–2.9.

2.0. The different types of quartics. Over $K = \mathbb{Q}$, Birch and Swinnerton-Dyer considered separately quartics with 0, 4, and 2 real roots, calling these quartics of type 1, 2, and 3, respectively. Note that $\Delta = 4I^3 - J^2 = 27 \cdot \mathrm{disc}(g)$, so that types 1 and 2 only arise when $\Delta > 0$, while only type 3 arises when $\Delta < 0$.

Moreover, when $\Delta > 0$, one can show that the classes of globally soluble quartics of type 2 form a subgroup of the group G', of index 1 or 2. This is because type 2 quartics in G' give points in $E(\mathbb{Q})$ which are on the identity component of $E(\mathbb{R})$, which has two connected components in this case: there will exist globally soluble quartics of type 1 if and only if there are rational points on the other component of $E(\mathbb{R})$. One can use this fact to speed up the algorithm, since it follows that if there are any globally soluble quartics of type 1, the number of them is equal to the number of type 2, so the search for type 1 quartics may be curtailed as soon as one is found.

Similarly, over a real quadratic field $K = \mathbb{Q}(\sqrt{D})$, there are nine types of quartics g, depending on the number of roots of g in each of the two real embeddings σ_1 and σ_2 of K. We say the type is (t_1, t_2) if $\sigma_i(g)$ has type t_i for $i = 1, 2$. Thus, depending on the pair of signs $\operatorname{sgn}(\Delta) = (\operatorname{sgn}\sigma_1(\Delta), \operatorname{sgn}\sigma_2(\Delta)) = (\pm, \pm)$, there are 1, 2 or 4 types to be considered separately:

$$\begin{aligned} \{(1,1),(1,2),(2,1),(2,2)\} &\quad \text{if} \quad \operatorname{sgn}(\Delta) = (+,+);\\ \{(1,3),(2,3)\} &\quad \text{if} \quad \operatorname{sgn}(\Delta) = (+,-);\\ \{(3,1),(3,2)\} &\quad \text{if} \quad \operatorname{sgn}(\Delta) = (-,+);\\ \{(3,3)\} &\quad \text{if} \quad \operatorname{sgn}(\Delta) = (-,-). \end{aligned}$$

As over $\mathbb{Q}$, we may use the group structure to reduce the running time of the algorithm, since (for example) the number of globally soluble quartics of type $(3, 1)$ is either 0 or equal to the number of type $(3, 2)$; similarly in other cases.

2.1. A search region for a. In order to bound the leading coefficient a for $K = \mathbb{Q}$, Birch and Swinnerton-Dyer introduced the notion of a *reduced quartic*. They associate to each quartic a positive definite quadratic form, covariant under real transformations, and they call a real quartic reduced if the quadratic form is reduced. Since every positive definite quadratic form is $\mathrm{SL}(2,\mathbb{Z})$-equivalent to a reduced quadratic form, every quartic is $\mathrm{SL}(2,\mathbb{Z})$-equivalent to a reduced quartic. For a reduced quadratic form, the root with positive imaginary part lies in the usual fundamental domain for the action of $\mathrm{SL}(2,\mathbb{Z})$ on the complex upper half plane $\mathcal{H}$, which implies that its imaginary part is at least $\sqrt{3}/2$. From this lower bound Birch and Swinnerton-Dyer derived bounds for the leading coefficient a of reduced quartics. The relevant a are the integers between the lower and the upper bound.

Let us now come to a real quadratic number field $K = \mathbb{Q}(\sqrt{D})$, $D > 0$. For each quartic over $\mathfrak{O}_K$, we consider its two real embeddings. The action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathcal{H}$ is replaced by the action of $\mathrm{SL}(2,\mathfrak{O}_K)$ on $\mathcal{H}\times\mathcal{H}$:

$$M(z_1,z_2) \;=\; (\sigma_1(M)(z_1), \sigma_2(M)(z_2)) \qquad \forall M \in \mathrm{SL}(2,\mathfrak{O}_K),\ (z_1,z_2)\in\mathcal{H}\times\mathcal{H}.$$

The product of the two imaginary parts can be bounded below as follows.

Theorem 1. *Let $K = \mathbb{Q}(\sqrt{D})$, $D > 0$, with $h(K) = 1$. For all $(z_1, z_2) \in \mathcal{H}^2$ there exists $M \in \mathrm{SL}(2,\mathfrak{O}_K)$ such that*

$$\operatorname{Im}(\sigma_1(M)(z_1)) \cdot \operatorname{Im}(\sigma_2(M)(z_2)) \geq \frac{\pi^2}{16\operatorname{disc}(K/\mathbb{Q})}.$$

Proof. The first part of the proof is a simplification of a similar proof in [4] for arbitrary totally real number fields. For some fixed $z = (z_1, z_2) \in \mathcal{H}^2$ we set

$$\Lambda \;=\; \mathfrak{O}_K\cdot z + \mathfrak{O}_K \;=\{(\sigma_1(a)\cdot z_1 + \sigma_1(b), \sigma_2(a)\cdot z_2 + \sigma_2(b)) \mid a, b \in \mathfrak{O}_K\} \;\subset\; \mathbb{C}^2$$

and for arbitrary $L \in \mathbb{R}_{>0}$ we define

$$V_L \;=\; \{u = (u_1,u_2)\in\mathbb{C}^2;\ |u_j|^2 \leq L\cdot \operatorname{Im}(z_j) \text{ for } j = 1,2\}.$$

A well-known lemma by Minkowski says that if the volume of V_L is greater than or equal to 2^4 times the volume of a fundamental parallelogram for Λ, which is the case for $L \geq \frac{2^2}{\pi}\sqrt{\mathrm{disc}(K/\mathbb{Q})}$, then there exists a non-zero element of Λ lying in V_L, i.e., there are $c, d \in \mathfrak{O}_K$, not both zero, satisfying

$$|\sigma_j(c)\cdot z_j + \sigma_j(d)|^2 \ \leq\ L\cdot \mathrm{Im}(z_j) \qquad \text{for } j = 1, 2.$$

Let $e = \gcd(c, d)$, hence $1 = \gcd(c', d')$ for $c' = \frac{c}{e}$ and $d' = \frac{d}{e}$, so that there exist $a', b' \in \mathfrak{O}_K$ with $1 = a'd' - b'c'$. Then we have, for the matrix $M = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$,

$$\mathrm{Im}(\sigma_j(M)(z_j)) \ \geq\ L^{-1}\cdot|\sigma_j(e)|^2.$$

If we now try to bound the imaginary parts simultaneously, which is done in [4], some power of $\sigma_1(\varepsilon_0)$ comes in, where ε_0 is the fundamental unit of K. But this can be avoided by bounding the product of the imaginary parts:

$$\mathrm{Im}(\sigma_1(M)(z_1))\cdot\mathrm{Im}(\sigma_2(M)(z_2)) \ \geq\ L^{-2}\cdot|\,\mathrm{norm}_{K/\mathbb{Q}}(e)|^2 \ \geq\ L^{-2}.$$

For $L = \frac{2^2}{\pi}\sqrt{\mathrm{disc}(K/\mathbb{Q})}$ we obtain the desired result. $\square$

Applying this result leads to bounds on the norm of a, so that we only have to determine all $a \in \mathfrak{O}_K$ whose norm lies between these bounds. For each unit ε of K, the integral quartic with coefficients (a, b, c, d, e) is equivalent to $(\varepsilon^2 a, \varepsilon b, c, \varepsilon^{-1}d, \varepsilon^{-2}e)$, which is also integral and has the same invariants. Since the number of elements $a \in \mathfrak{O}_K$ with bounded norm is finite modulo multiplication by squares of units, we obtain a finite set of candidate first coefficients a. We omit the details of the bounds, in which the various types must be treated separately; see [8] for details.

2.2. For each a, a search region for b. For all $\beta \in \mathfrak{O}_K$, the quartic $g^*(X) = g(X+\beta)$ has integral coefficients and the same invariants as g. Its first two coefficients are $a^* = a$ and $b^* = b + 4\beta a$. Hence we may assume b lies in a fixed complete set of representatives modulo $4a$. We choose this set to be (almost) symmetric about 0, which makes it possible to consider b and $-b$ simultaneously.

2.3. For each pair (a, b), a search region for c. When determining bounds on a in Subsection 2.1, we may also obtain lower and upper bounds on $\sigma_1(c)$ and $\sigma_2(c)$ with very little extra work. These bounds are similar to the corresponding bounds over $\mathbb{Q}$ (see [2]), except that they also involve both the discriminant $\mathrm{disc}(K/\mathbb{Q})$ and the fundamental unit (see [8] for details).

2.4. For each triple (a, b, c), the coefficients d and e. Given a triple (a, b, c), we define $H = 8ac - 3b^2$. If there is a quartic with invariants (I, J) and coefficients (a, b, c, d, e) for some d, e, then the following syzygy is satisfied, where $R = b^3 + 8a^2d - 4abc$:

$$H^3 - 48a^2HI + 64a^3J = -27R^2.$$

We now compute $S(a, b, c) = H^3 - 48a^2HI + 64a^3J$, and test if it is of the form $-27R^2$ with R in $\mathfrak{O}_K$. If not, we discard the triple (a, b, c); if so, we set $d = (R - b^3 + 4abc)/(8a^2)$ and $e = (I + 3bd - c^2)/(12a)$. (Note that $a \neq 0$ for a nontrivial quartic.) Provided that d and e are integral, we have found a suitable quartic.

We can save much time in practice by using a quadratic sieve: we only wish to consider a triple (a, b, c) which lies in our search region if $S(a, b, c)$ is -27 times a square in $\mathfrak{O}_K$. We can use a number of auxiliary sieving moduli $\mathcal{P}$, and restrict the search to triples (a, b, c) for which $-3S(a, b, c)$ is a square modulo $\mathcal{P}$. This can be done efficiently by initializing a suitable array of binary flags: a 2-dimensional array suffices, as (for fixed I and J) $S(a, b, c)$ is a function only of a and H.

To give an idea of the time saved by using this quadratic sieve based on the syzygy, in the program `mwrank` (over $\mathbb{Q}$) sieving modulo the five rational primes $5, 7, 11, 13, 17$ saves up to 90% of cpu time; for a real quadratic number field, sieving modulo the smallest 11 degree one primes still saves between 30% and 70%.

2.5. Checking triviality. Testing whether a quartic $Y^2 = g(X)$ is trivial, i.e., whether $g(X)$ has a root in K, is straightforward, assuming that one is using a computer algebra system containing a routine for factorizing polynomials over K.

2.6. Testing equivalence. A simple method of testing equivalence of quartics over an arbitrary field K was derived in [3], based on invariant theory. We present this test here; see [3] for details and proofs. Even over $\mathbb{Q}$, this test is much simpler to implement than the equivalence test presented in [1].

It suffices to test equivalence of quartics with the same invariants I, J, since if $g_2(X)$ has invariants $\lambda^4 I$, $\lambda^6 J$ we may initially replace $g_1(X)$ by $\lambda^2 g_1(X)$ (or $g_1(\lambda X)$).

Proposition 2. *Let $g_j(X)$ for $j = 1, 2$ be quartics over $\mathfrak{O}_K$ with coefficients a_j, b_j, c_j, d_j, e_j, both having the same invariants I, J. For $j = 1, 2$, set $H_j = 8a_jc_j - 3b_j^2$ and $R_j = b_j^3 + 8a_j^2 d_j - 4a_jb_jc_j$. Define*

$$T = -\frac{2}{3}(H_1H_2 + 32a_1a_2I); \qquad R = R_1R_2;$$
$$S = \frac{1}{27}(64I(H_1^2a_2^2 + H_1H_2a_1a_2 + H_2^2a_1^2) + 256Ja_1a_2(H_1a_2 + H_2a_1) - H_1^2H_2^2).$$

Then g_1 and g_2 are equivalent if and only if the quartic $X^4 + TX^2 - 8Rx + S$ has a root in K.

Remark. The quartic $X^4 + TX^2 - 8Rx + S$ does not (in general) have invariants I, J, though its cubic resolvent field is the same as that of g_1 and g_2.

2.7. Local solubility. Testing local solubility of $Y^2 = g(X)$ at the infinite primes of a real quadratic number field K (or, more generally, an arbitrary number field with real embeddings) is easy. One simply has to find out whether the corresponding embedding has a solution over $\mathbb{R}$, i.e., whether $g(X)$ can take non-negative values.

Now let K be an arbitrary number field, $\mathcal{P}$ a finite prime of K, and $g(X)$ a polynomial over $\mathbb{Z}_{\mathcal{P}}$, the ring of $\mathcal{P}$-adic integers in the completion $K_{\mathcal{P}}$. Local solubility of $Y^2 = g(X)$ is guaranteed for all odd primes not dividing the discriminant $4I(g)^3 - J(g)^2$, since the curve is then nonsingular modulo $\mathcal{P}$. Thus we can restrict to testing local solubility modulo finitely many "bad primes". Also, it is clear that $Y^2 = g(X)$ has a solution over $K_{\mathcal{P}}$ if and only if $Y^2 = g(X)$ has a solution over $\mathbb{Z}_{\mathcal{P}}$ or $Y^2 = g^*(X)$ has a solution over $\mathbb{Z}_{\mathcal{P}}$ with $X \equiv 0 \pmod{\mathcal{P}}$, where $g^*(X) = X^4 g(1/X) = eX^4 + dX^3 + cX^2 + bX + a$ for $g(X) = aX^4 + bX^3 + cX^2 + dX + e$.

Following [1], we use a modified form of Hensel's Lemma to determine whether for each residue class $x_0 \bmod \mathcal{P}^\nu$ there is a solution of $Y^2 = g(X)$ with $X \equiv x_0 \pmod{\mathcal{P}^\nu}$. (See [9] for an explicit statement over an arbitrary number field.) The lemma gives three possible answers: either "definitely yes" or "definitely no" or "maybe". If the lemma certainly gives a solution, we have no more to do. If it certainly gives none, we reject this class. If the lemma gives us no definite information (in the "maybe" case), we recursively consider the corresponding classes modulo $\mathcal{P}^{\nu+1}$. This procedure is guaranteed to come to an end, as the "maybe" case cannot occur for sufficiently large ν.

If $Y^2 = g(X)$ is insoluble over $\mathbb{Z}_{\mathcal{P}}$, we go on to consider $Y^2 = g^*(X)$, starting now with the one class 0 mod $\mathcal{P}$. If this too does not give a solution over $\mathbb{Z}_{\mathcal{P}}$, the equation $Y^2 = g(X)$ is insoluble over $K_{\mathcal{P}}$.

This procedure works adequately provided that none of the "bad primes" under consideration has large norm. For large primes, one should instead use the method of Siksek (see [9]), but we have not yet implemented this for real quadratic fields, as in all our examples the bad primes were small.

2.8. Global solubility. To test for global solubility of $Y^2 = g(X)$, we simply search for a point over K. This is realized by loops on the numerator and the denominator of X and testing whether $g(X)$ is a square. Here one can save much time by sieving, i.e., by checking first whether $g(X)$ is a square modulo some appropriate moduli. The number of moduli should not be too large, because we then need more time for initializing arrays for local squares/non-squares than we save; and too few moduli do not reject enough global non-squares. It is often preferable to use composite moduli (e.g., containing small powers of 2 and 3) instead of primes. We found that $72 = 2^3 \cdot 3^2$, $77 = 7 \cdot 11$, $65 = 5 \cdot 13$ was the best choice in our case.

2.9. Points on the elliptic curve from the global points on the quartics. Let

$$\begin{aligned} g_4(X,Y) = {} & (3b^2 - 8ac)X^4 + 4(bc - 6ad)X^3Y + 2(2c^2 - 24ae - 3bd)X^2Y^2 \\ & + 4(cd - 6be)XY^3 + (3d^2 - 8ce)Y^4 \end{aligned}$$

and

$$\begin{aligned} g_6(X,Y) = {} & (b^3 + 8a^2d - 4abc)X^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)X^5Y \\ & + 5(8abe + b^2d - 4acd)X^4Y^2 + 20(b^2e - ad^2)X^3Y^3 \\ & - 5(8ade + bd^2 - 4bce)X^2Y^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)XY^5 \\ & - (d^3 + 8be^2 - 4cde)Y^6 \end{aligned}$$

be the classical quartic and sextic covariants of the quartic $g(X) = aX^4 + bX^3 + cX^2 + dX + e$. Note that the leading coefficients of $g_4(X)$ and $g_6(X)$ are $-H$ and R, respectively. The syzygy aleady used in Subsection 2.7 extends to a syzygy between the covariants

$$g_4(X)^3 - 48Ig(X)^2g_4(X) - 64Jg(X)^3 = 27g_6(X)^2.$$

It follows easily that for each K-rational point (x_0, y_0) on the quartic $Y^2 = g(X)$, the point

$$(x, y) = \left(\frac{3g_4(x_0)}{4y_0^2}, \frac{27g_6(x_0)}{8y_0^3}\right)$$

lies on the elliptic curve $Y^2 = X^3 - 27IX - 27J$, which is isomorphic to the original curve E.

The theoretical basis for the general 2-descent method is the fact that the points we thus obtain on $E(K)$ are in the same coset of $2E(K)$ in $E(K)$ if and only if they come from equivalent quartics; see [3] for details.

3. The relevant (I, J) pairs

We have described in Section 2 how to determine all reduced quartics for one fixed pair (I, J). We will now explain how to find all relevant (I, J) pairs.

We start with the case $K = \mathbb{Q}$. We may assume that the elliptic curve E over $\mathbb{Q}$ is given in the form

$$E: \ Y^2 = X^3 - 27IX - 27J \qquad \text{with } I, J \in \mathbb{Z}.$$

As noted above, I and J differ from $c_4(E) = 2^4 3^4 I$ and $2c_6(E) = 2^6 3^6 J$ by a 4th and a 6th power, respectively. The question is whether we can divide out further 4th and 6th prime powers from I and J. This can be done (for a prime p satisfying $p^4 \mid I$ and $p^6 \mid J$) if *every* quartic over $\mathbb{Z}$ with invariants I and J which is p-adically soluble is equivalent to a quartic over $\mathbb{Z}$ with invariants $p^{-4}I$ and $p^{-6}J$. In this case we say that I and J can be *p-reduced*. In addition, we might conceivably have to multiply I and J by 4th and 6th prime powers. This must be done if we cannot prove that $p^4 I$ and $p^6 J$ can be p-reduced. In [1], the following criteria for p-reducibility are stated in three lemmas:

Lemma 3:	$p \neq 2, 3$:	$p^4 \mid I,\ p^6 \mid J$	$\Longleftrightarrow I, J$ can be p-reduced.
Lemma 4:	$p = 3$:	$3^5 \mid I,\ 3^9 \mid J$ or	
		$3^4 \parallel I,\ 3^6 \parallel J,\ 3^{15} \mid 4I^3 - J^2$	$\Longleftrightarrow I, J$ can be 3-reduced.
Lemma 5:	$p = 2$:	$2^6 \mid I,\ 2^9 \mid J,\ 2^{10} \mid 8I + J$	$\Longrightarrow I, J$ can be 2-reduced.

Note that for $p = 2$, we only have sufficient conditions for reducibility, while for all odd primes we have necessary and sufficient conditions.

This shows that for primes $p \neq 2, 3$, we can always make I and J free of 4th and 6th powers. For $p = 3$ and $p = 2$, the situation is more complicated: in both cases $p^4 \mid I$ and $p^6 \mid J$ may occur, but we can always avoid $p^8 \mid I$ and $p^{12} \mid J$. To find the relevant (I, J) pairs over $\mathbb{Q}$ we therefore proceed as follows.

- For all primes $p \neq 2, 3$, we may assume that $p^4 \nmid I$ or $p^6 \nmid J$.
- $p = 3$: We may assume that $3^8 \nmid I$ or $3^{12} \nmid J$. If $3^5 \mid I$, $3^9 \mid J$ or $3^4 \parallel I$, $3^6 \parallel J$, $3^{15} \mid 4I^3 - J^2$ hold, we replace (I, J) by $(3^{-4}I, 3^{-6}J)$.
- $p = 2$: We may assume that $2^8 \nmid I$ or $2^{12} \nmid J$. If $2^4 \mid I$, $2^6 \mid J$, we replace (I, J) by $(2^{-4}I, 2^{-6}J)$. Then as well as the basic pair (I, J), we also consider the pair $(I', J') = (2^4 I, 2^6 J)$, unless $2^2 \mid I$, $2^3 \mid J$, and $2^4 \mid 2I + J$.

Hence we have either one or two relevant pairs of invariants over $\mathbb{Q}$.

Remark. If c_4 and c_6 are the invariants of a global minimal model for E over $\mathbb{Q}$, then the invariant values $I = c_4$, $J = 2c_6$ are automatically p-reduced for all odd primes p (including $p = 3$). The pairs to be considered are thus $(c_4, 2c_6)$ in all cases, and also $(2^4 c_4, 2^7 c_6)$ unless $2^2 \mid c_4$, $2^2 \mid c_6$, and $2^3 \mid c_4 + c_6$.

Now we come to the case $K = \mathbb{Q}(\sqrt{D})$, $D > 0$. As before, we may assume that we have an elliptic curve of the form

$$E: \ Y^2 = X^3 - 27IX - 27J \qquad \text{with } I, J \in \mathfrak{O}_K,$$

and try to divide out 4th and 6th powers from I and J. Therefore we need analogous versions of Lemmas 3, 4, and 5 over K. In order to generalize these, we first had to write down in detail the proofs of Lemma 3, 4, and 5 in [1] (over $\mathbb{Q}$), since [1] only contains a sketch of the proof of Lemma 3; the proofs of Lemma 4 and 5 were omitted, because they are "similar to that of Lemma 3, but far more tedious ...". We were then able to obtain versions of these lemmas valid over (quadratic) number fields. In [8] we have given in detail all proofs over (quadratic) number fields. They did require an enormous amount of time and patience, but not a very high theoretical level. Here we will confine ourselves to listing the results. We will restrict our consideration to prime ideals which are principal, as we will only apply the algorithm over quadratic number fields of class number 1. Lemma 3 holds for arbitrary number fields; Lemma 4 too, but with an additional condition for ramification index 2. Lemma 5 only holds for quadratic number fields, but it should be considered as a great success to have such a lemma for real and imaginary quadratic number fields of arbitrary discriminant.

As before, we say that the pair I, J can be *$\mathcal{P}$-reduced* for a principal prime ideal $\mathcal{P} = (\pi)$ of K, if every quartic over $\mathfrak{O}_K$ with invariants I, J which is $\mathcal{P}$-adically soluble is equivalent to a quartic over $\mathfrak{O}_K$ with invariants $\pi^{-4}I$, $\pi^{-6}J$.

Lemma 3 (Generalization of Lemma 3 of [1])**.** *Let K be an arbitrary number field and $\mathcal{P} = (\pi)$ a principal prime ideal of K dividing the rational prime $p \neq 2, 3$. If*

$$\pi^4 \mid I,\ \pi^6 \mid J,$$

then I, J can be $\mathcal{P}$-reduced.

Lemma 4 (Generalization of Lemma 4 of [1])**.** *Let K be an arbitrary number field and $\mathcal{P} = (\pi)$ a principal prime ideal of K dividing the rational prime 3, with ramification index ε. If*

$$\begin{aligned}
&\pi^{\varepsilon+4} \mid I,\ \pi^{3\varepsilon+6} \mid J \ \textit{or}\\
&\pi^6 \mid I,\ \pi^9 \parallel J,\ \pi^{21} \mid 4I^3 - J^2 \ \textit{and}\ \varepsilon = 2 \ \textit{or}\\
&\pi^4 \parallel I,\ \pi^6 \parallel J,\ \pi^{3\varepsilon+12} \mid 4I^3 - J^2,
\end{aligned}$$

then I, J can be $\mathcal{P}$-reduced.

Lemma 5 (Generalization of Lemma 5 of [1])**.** *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field and $\mathcal{P} = (\pi)$ a principal prime ideal of K dividing the rational prime 2. Then we have*

(a) *for $(2) = \mathcal{P}$, i.e., $D \equiv 5 \pmod 8$ and $\pi = 2$:*

$$2^7 \mid I,\ 2^{10} \mid J \implies I, J \ \textit{can be}\ \mathcal{P}\textit{-reduced};$$

(b) *for $(2) = \mathcal{P}_1\mathcal{P}_2$ with $\mathcal{P}_1 \neq \mathcal{P}_2$, i.e., $D \equiv 1 \pmod 8$ and $\mathcal{P} = \mathcal{P}_1$ or $\mathcal{P}_2$:*

$$\pi^6 \mid I,\ \pi^9 \mid J,\ \pi^{10} \mid \pi^3 I + J \implies I, J \ \textit{can be}\ \mathcal{P}\textit{-reduced};$$

(c) *for $(2) = \mathcal{P}^2$, i.e., $D \equiv 2, 3 \pmod 4$:*

$$\begin{aligned}
&\pi^8 \mid I,\ \pi^{11} \parallel J \ \textit{or}\\
&\pi^9 \parallel I,\ \pi^{13} \parallel J \ \textit{or}\\
&\pi^{10} \mid I,\ \pi^{15} \mid J,\ \pi^{16} \mid \pi^5 I + J \implies I, J \ \textit{can be}\ \mathcal{P}\textit{-reduced.}
\end{aligned}$$

Remark. Just as in the case $K = \mathbb{Q}$, the conditions in Lemma 3 are necessary and sufficient for $\mathcal{P}$-reducibility, and those in Lemma 5 are only sufficient. The situation in Lemma 4 is more complicated. In the case $\varepsilon = 1$, the conditions are the same as over $\mathbb{Q}$; they are necessary and sufficient. For $\varepsilon \geq 2$, however, they are only sufficient.

We now derive from these lemmas the relevant (I, J) pairs over a quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Lemma 5 shows that they depend on the decomposition of the rational prime 2 in K, and we may need to consider up to four pairs.

- Just as over $\mathbb{Q}$, we may assume I and J to be free of 4th and 6th powers of prime elements belonging to primes not dividing 2 and 3.
- Let $\mathcal{P} = (\pi)$ be a prime ideal dividing 3, with ramification index ε (= 1 or 2). We may exclude the case $\pi^8 \mid I,\ \pi^{12} \mid J$. If either

$$\varepsilon = 1 \quad \text{and} \quad \begin{array}{l} \pi^5 \mid I,\ \pi^9 \mid J \text{ or} \\ \pi^4 \parallel I,\ \pi^6 \parallel J,\ \pi^{15} \mid 4I^3 - J^2, \end{array}$$

or

$$\varepsilon = 2 \quad \text{and} \quad \begin{array}{l} \pi^6 \mid I,\ \pi^{12} \mid J \text{ or} \\ \pi^6 \mid I,\ \pi^9 \parallel J,\ \pi^{21} \mid 4I^3 - J^2 \text{ or} \\ \pi^4 \parallel I,\ \pi^6 \parallel J,\ \pi^{18} \mid 4I^3 - J^2, \end{array}$$

we replace (I, J) by $(\pi^{-4}I, \pi^{-4}J)$.
- For prime ideals dividing 2, we must consider three cases:
  (a) $D \equiv 5 \pmod 8$, i.e., $(2) = \mathcal{P}$ and $\pi = 2$:
  We may exclude that $2^8 \mid I,\ 2^{12} \mid J$. If $2^4 \mid I,\ 2^6 \mid J$, we replace (I, J) by $(2^{-4}I, 2^{-6}J)$. As well as the basic pair (I, J), we also consider the pair $(I', J') = (2^4I, 2^6J)$, unless $2^3 \mid I$ and $2^4 \mid J$.
  (b) $D \equiv 1 \pmod 8$, i.e., $(2) = \mathcal{P}_1\mathcal{P}_2$ with $\mathcal{P}_1 \neq \mathcal{P}_2$ and $\mathcal{P}_1 = (\pi_1)$, $\mathcal{P}_2 = (\pi_2)$:
  Let π be π_1 or π_2. As in case (a) we may exclude $\pi^8 \mid I,\ \pi^{12} \mid J$. If $\pi^4 \mid I,\ \pi^6 \mid J$, we replace (I, J) by $(\pi^{-4}I, \pi^{-6}J)$. But we also take into consideration the pair $(I', J') = (\pi^4 I, \pi^6 J)$. We have

$$\pi^6 \mid I',\ \pi^9 \mid J',\ \pi^{10} \mid \pi^3 I' + J' \iff \pi^2 \mid I,\ \pi^3 \mid J,\ \pi^4 \mid \pi I + J.$$

  This means:
  If $(\pi_1^2 \mid I,\ \pi_1^3 \mid J,\ \pi_1^4 \mid \pi_1 I + J)$ and $(\pi_2^2 \mid I,\ \pi_2^3 \mid J,\ \pi_2^4 \mid \pi_2 I + J)$, then only (I, J) is relevant;
  if $(\pi_1^2 \mid I,\ \pi_1^3 \mid J,\ \pi_1^4 \mid \pi_1 I + J)$ and $(\pi_2^2 \nmid I$ or $\pi_2^3 \nmid J$ or $\pi_2^4 \nmid \pi_2 I + J)$, then (I, J) and $(\pi_2^4 I, \pi_2^6 J)$ are relevant;
  if $(\pi_1^2 \nmid I$ or $\pi_1^3 \nmid J$ or $\pi_1^4 \nmid \pi_1 I + J)$ and $(\pi_2^2 \mid I,\ \pi_2^3 \mid J,\ \pi_2^4 \mid \pi_2 I + J)$, then (I, J) and $(\pi_1^4 I, \pi_1^6 J)$ are relevant;
  if $(\pi_1^2 \nmid I$ or $\pi_1^3 \nmid J$ or $\pi_1^4 \nmid \pi_1 I + J)$ and $(\pi_2^2 \nmid I$ or $\pi_2^3 \nmid J$ or $\pi_2^4 \nmid \pi_2 I + J)$, then (I, J), $(\pi_1^4 I, \pi_1^6 J)$, $(\pi_2^4 I, \pi_2^6 J)$, and $(\pi_1^4\pi_2^4 I, \pi_1^6\pi_2^6 J) = (2^4 I, 2^6 J)$ are relevant.
  So in this case we have to consider one, two, or four pairs of invariants.
  (c) $D \equiv 2, 3 \pmod 4$, i.e., $(2) = \mathcal{P}^2$ with $\mathcal{P} = (\pi)$:
  Here we can only exclude that $\pi^{12} \mid I,\ \pi^{18} \mid J$. If $\pi^8 \mid I,\ \pi^{12} \mid J$, we replace (I, J) by $(\pi^{-8}I, \pi^{-12}J)$; if $\pi^4 \mid I,\ \pi^6 \mid J$, we replace (I, J) by $(\pi^{-4}I, \pi^{-6}J)$. But we also take into consideration the two pairs $(I', J') = (\pi^4 I, \pi^6 J) = (4I, \pm 8J)$ and $(I'', J'') = (\pi^8 I, \pi^{12} J) = (16I, 64J)$. Lemma 5 gives the following three cases:
  If $\pi^4 \mid I,\ \pi^5 \parallel J$, then only (I, J) is relevant; otherwise,
  if $\pi \parallel I,\ \pi \parallel J$ or $\pi^2 \mid I,\ \pi^3 \mid J,\ \pi^4 \mid \pi I + J$, then the two pairs (I, J) and (I', J') are relevant;
  otherwise, all three pairs (I, J), (I', J'), and (I'', J'') are relevant.
  Hence there are one, two, or three relevant (I, J) pairs in this case.

4. Examples

When we implemented general 2-descent over real quadratic number fields of class number 1, we saw that the search region on the first three coefficients a, b, c of the quartics often becomes very large. Using the syzygy to apply a quadratic sieve to the search is thus essential. We are also in the process of obtaining improved bounds for the coefficients of real reduced quartics, better than the ones obtained in [1] for quartics with negative discriminant, by using a new definition of "reduced" in that case. We expect that these improvements, when implemented, will improve the running time of the algorithm considerably. Using the old bounds, even for the four number fields with the smallest discriminant, namely $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{13})$, we had to test many curves in order to find examples with "reasonable" cpu times. We have listed below two examples over each of the four fields. All examples have trivial 2-torsion. In $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{13})$, the rational prime 2 is inert, i.e., we have either one or two relevant (I, J) pairs. We include one example for each case. In $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$, the rational prime 2 is ramified, i.e., there are one, two, or three pairs of invariants. For both D we have given one example with one pair and one example with three pairs.

We ran these examples on an SGI Challenge.

The curves are defined as $E = [a_1, a_2, a_3, a_4, a_6]$, where the a_i are the standard Weierstrass coefficients, and each coefficient a_i is denoted by an ordered pair of integers which are its coefficients with respect to the standard integral basis of $\mathfrak{O}_K$.

Example 1: $K = \mathbb{Q}(\sqrt{5})$**,** $E = [(2,0), (-2,0), (-1,-1), (0,1), (0,-1)]$**.**
One (I, J) pair: $((64,0), (-160,432))$.
Three inequivalent nontrivial globally soluble quartics:
#1: $(a,b,c,d,e) = ((1,0),(0,0),(2,0),(4,-4),(5,0))$
$\mapsto P_1 = ((0,0),(1,0))$.
#2: $(a,b,c,d,e) = ((1,0),(0,0),(-46,30),(-204,124),(-246,155))$
$\mapsto P_2 = ((8,-5),(-33,21))$.
#3: $(a,b,c,d,e) = ((1,0),(0,0),(-4,-6),(-4,-12),(1,-7))$
$\mapsto P_3 = ((1,1),(-1,-2)) = P_1 + P_2$.
Rank $= 2$.
Total cpu time: $19m,\ 49s$.

Example 2: $K = \mathbb{Q}(\sqrt{5})$**,** $E = [(-2,0), (-2,-1), (2,-2), (-2,1), (0,0)]$**.**
Two (I, J) pairs: $((14,-6),(-35,25))$ and $((224,-96),(-2240,1600))$.
Seven inequivalent nontrivial globally soluble quartics:
$(I,J) = ((14,-6),(-35,25))$ (cpu time $19s$):
#1: $(a,b,c,d,e) = ((1,0),(1,-1),(2,-1),(3,-2),(2,-1))$
$\mapsto P_1 = (\frac{1}{4}(-2,3), \frac{1}{8}(3,4))$.
$(I,J) = ((224,-96),(-2240,1600))$ (cpu time $8m,\ 1s$):
#2: $(a,b,c,d,e) = ((1,0),(0,0),(8,-4),(-16,8),(12,-4))$
$\mapsto P_2 = ((-1,1),(-4,3))$.
#3: $(a,b,c,d,e) = ((1,0),(0,0),(-220,140),(-2112,1304),(-5648,3492))$
$\mapsto P_3 = ((37,-23),(-228,141))$.
#4: $(a,b,c,d,e) = ((1,0),(0,0),(-16,14),(-40,24),(-19,13))$
$\mapsto P_4 = ((3,-2),(-3,2)) = P_1 - P_2 - P_3$.
#5: $(a,b,c,d,e) = ((1,0),(0,0),(-28,-52),(-192,-280),(-272,-476))$
$\mapsto P_5 = ((5,9),(-20,-25)) = P_1 - 4P_2 - P_3$.
#6: $(a,b,c,d,e) = ((1,0),(0,0),(-16,-34),(-104,-136),(-99,-195))$
$\mapsto P_6 = ((3,6),(-11,-10)) = -2P_1 + 7P_2 + 3P_3$.
#7: $(a,b,c,d,e) = ((1,0),(0,0),(-304,164),(-3248,1928),(-9924,6060))$
$\mapsto P_7 = ((51,-27),(-356,215)) = P_1 + P_2$.

Rank $= 3$.
Total cpu time: $8m,\ 20s$.

Example 3: $K = \mathbb{Q}(\sqrt{2})$**,** $E = [(2,-2),(-2,2),(-2,0),(1,2),(-2,0)]$**.**
One (I,J) pair: $((4,-12),(16,36))$.
No nontrivial globally soluble quartics.
Rank $= 0$.
Total cpu time: $31m,\ 16s$.

Example 4: $K = \mathbb{Q}(\sqrt{2})$**,** $E = [(0,0),(2,1),(0,0),(1,0),(-1,-1)]$**.**
Three (I,J) pairs: $((3,4),(5,8))$, $((12,16),(40,64))$, and $((48,64),(320,512))$.
One nontrivial globally soluble quartic.
$(I,J) = ((3,4),(5,8))$ (cpu time $1m,\ 47s$):
No nontrivial globally soluble quartics.
$(I,J) = ((12,16),(40,64))$ (cpu time $7m,\ 56s$):
#1: $(a,b,c,d,e) = ((1,0),(0,0),(-2,2),(-4,2),(0,2))$
$\mapsto P_1 = ((0,-1),(1,-1))$.
$(I,J) = ((48,64),(320,512))$ (cpu time $1h,\ 42m,\ 31s$):
No nontrivial globally soluble quartics.
Rank $= 1$.
Total cpu time: $1h,\ 52m,\ 14s$.

Example 5: $K = \mathbb{Q}(\sqrt{13})$**,** $E = [(0,2),(0,-1),(1,2),(0,1),(0,1)]$**.**
One (I,J) pair: $((16,-16),(-112,64))$.
One nontrivial globally soluble quartic:
#1: $(a,b,c,d,e) = ((1,-2),(10,2),(-4,-8),(6,4),(-1,-1))$
$\mapsto P_1 = (\frac{1}{4}(-3,0),\frac{1}{8}(-3,-2))$.
Rank $= 1$.
Total cpu time: $17h,\ 59m,\ 10s$.

Example 6: $K = \mathbb{Q}(\sqrt{13})$**,** $E = [(0,0),(1,2),(0,0),(2,3),(1,1)]$**.**
Two (I,J) pairs: $((7,-1),(31,-10))$ and $((112,-16),(1984,-640))$.
No nontrivial globally soluble quartics.
$(I,J) = ((7,-1),(31,-10))$ (cpu time $10m,\ 43s$):
No nontrivial globally soluble quartics.
$(I,J) = ((112,-16),(1984,-640))$ (cpu time $5h,\ 35m,\ 12s$):
No nontrivial globally soluble quartics.
Rank $= 0$.
Total cpu time: $5h,\ 44m,\ 4s$.

Example 7: $K = \mathbb{Q}(\sqrt{3})$**,** $E = [(2,2),(1,1),(0,0),(0,2),(-2,-2)]$**.**
One (I,J) pair: $((52,24),(-844,-468))$.
Three inequivalent nontrivial globally soluble quartics.
#1: $(a,b,c,d,e) = ((2,1),(0,2),(8,-6),(-26,14),(31,-17))$
$\mapsto P_1 = ((-2,-1),(10,5))$.
#2: $(a,b,c,d,e) = ((2,1),(2,0),(2,0),(-8,2),(-9,6))$
$\mapsto P_2 = (\frac{1}{121}(1756,-1405),\frac{1}{1331}(169325,-77612))$.
#3: $(a,b,c,d,e) = ((2,1),(1,-1),(2,-6),(14,-10),(18,-10))$
$\mapsto P_3 = (\frac{1}{2}(32,19),\frac{1}{4}(-599,-349)) = -3P_1 - P_2$.
Rank $= 2$.
Total cpu time: $10h,\ 56m,\ 11s$.

Example 8: $K = \mathbb{Q}(\sqrt{3})$**,** $E = [(-2,2),(1,-1),(0,0),(0,-2),(2,-2)]$**.**

Three (I,J) pairs: $((163,-94),(-6334,3657))$, $((52,-24),(-952,576))$, and $((304,160),(9344,5568))$.

No nontrivial globally soluble quartics.

$(I,J) = ((163,-94),(-6334,3657))$ (cpu time $2h,\ 12m,\ 13s$):

No nontrivial globally soluble quartics.

$(I,J) = ((52,-24),(-952,576))$ (cpu time $8h,\ 9m,\ 58s$):

No nontrivial globally soluble quartics.

$(I,J) = ((304,160),(9344,5568))$ (cpu time $20h,\ 17m,\ 47s$):

No nontrivial globally soluble quartics.

Rank $= 0$.

Total cpu time: $30h,\ 39m,\ 58s$.

References

1. B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on Elliptic Curves I*, J. Reine Angew. Math. **212** (1963), 7–25. MR **26:**3669
2. J. E. Cremona, *Algorithms for Modular Elliptic Curves (Second Edition)*, Cambridge University Press, 1997.
3. J. E. Cremona, *Classical invariants and elliptic curves*, preprint, 1996.
4. P. B. Garrett, *Holomorphic Hilbert modular forms*, Wadsworth, 1990. MR **90k:**11058
5. H. Graf, *Konstruktion elliptischer Kurven hohen Ranges über quadratischen Zahlkörpern der Klassenzahl eins*, Diploma thesis, Universität des Saarlandes, Saarbrücken, 1995.
6. D. Husemöller, *Elliptic curves*, Springer-Verlag, 1987. MR **88h:**11039
7. K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. Amer. Math. Soc. **89** (1983), No. 3, 379–386. MR **85d:**14059
8. P. Serf, *The rank of elliptic curves over real quadratic number fields of class number* 1, PhD thesis, Universität des Saarlandes, Saarbrücken, 1995.
9. S. Siksek, *Infinite Descent on Elliptic Curves*, Rocky Mountain J. Math. **25**, (1995) No. 4, 1501–1538. MR **97g:**11053
10. J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer-Verlag, 1992. MR **93g:**11003
11. J. Tate, *Rational points on elliptic curves*, Lectures held at Haverford College, 1961.

Department of Mathematics, University of Exeter, Laver Building, North Park Road, Exeter EX4 4QE, U.K.

E-mail address: `cremona@maths.exeter.ac.uk`

Fachbereich 9 Mathematik, Universität des Saarlandes, Postfach 151150, D-66041 Saarbrücken, Germany

E-mail address: `pascale@math.uni-sb.de`