Finding all elliptic curves with good reduction outside a given set of primes

J. E. Cremona and M. P. Lingham

Abstract

We describe an algorithm for determining elliptic curves defined over a given number field with a given set of primes of bad reduction. Examples are given over $\mathbb{Q}$ and over various quadratic fields.

1 Introduction

Let K be a number field with ring of integers $\mathcal{O}_K$, and $\mathcal{S}$ a finite set of (non-archimedean) primes of K. It is well known (Shafarevich's Theorem, see [25]) that the number of isomorphism classes of elliptic curves defined over K and having good reduction outside $\mathcal{S}$ is finite: see Silverman's text [28, pp.263–4] for a proof.

Here we describe a completely explicit algorithm for finding all the elliptic curves with good reduction outside a given set $\mathcal{S}$. The essential non-trivial algorithmic ingredients for this are as follows:

- Determining the finite groups $K(\mathcal{S}, p)$ (defined below);
- Determining the complete (finite) set of $\mathcal{S}$-integral points on a given elliptic curve E defined over K (needed for certain curves of the form $Y^2 = X^3 + k$ with $k \in \mathcal{O}_K$).

The first, which is trivial over $\mathbb{Q}$, involves computation of the class group and unit group of K, or at least the p-primary part of these. An efficient algorithm for this has been implemented in Magma (see [4]) by C. Fieker. We will also need to consider the groups $K(\mathcal{S}, m)$ for $m = 4$, $m = 6$ and $m = 12$, and in Section 2 below we show how to determine $K(\mathcal{S}, m)$ for composite m.

The second is far more problematical, especially over number fields. The methods of finding all integral points (and more generally, all $\mathcal{S}$-integral points) on an elliptic curve have advanced substantially in recent years, provided that generators for the full Mordell-Weil group $E(K)$ are known. For $K = \mathbb{Q}$, these methods are very well-developed, and Magma has a full implementation which allows one (in most cases) to easily determine the set of $\mathcal{S}$-integral points. The implementation of the $\mathcal{S}$-integral point finding algorithm in Magma is by E. Herrmann, whose thesis [14] contains several results concerning the explicit determination of $\mathcal{S}$-integral points over number fields; see also [15] and [24]. While the situation is less satisfactory over number fields, and we are still waiting for a general implementation, it is possible to settle certain specific cases.

The advantage of our algorithm, compared with much of the earlier work on cases of the problem, is that instead of relying on a collection of *ad hoc* techniques for solving a variety of Diophantine equations which arise, everything instead depends on solving one very specific type of equation, namely the Mordell elliptic equations $Y^2 = X^3 + k$. Any algorithmic advances on that specific problem would directly benefit the effectiveness of our algorithm.

The special case where $\mathcal{S} = \emptyset$ has been considered by several authors, notably in the case where K is a quadratic field. For example we cite the work of Setzer ([27], [26]), Kida and Kagawa ([19], [20], [21], [18], [17], [22]), Ishii [16], Comalada and Nart ([6], [7], [8]). That work concentrates on deriving conditions on a field for the existence or otherwise of curves with everywhere good reduction, in order to decide on the existence of such curves for whole families of fields. Our aim is rather different: given a specific field K and set of primes $\mathcal{S}$ we give an algorithmic method to find a potentially complete set of elliptic curves defined over K with good reduction outside $\mathcal{S}$.

In the examples below, we show that there are no elliptic curves defined over the field $K = \mathbb{Q}(\sqrt{-23})$ with everywhere good reduction, and we also exhibit an elliptic curve with everywhere good reduction defined over $\mathbb{Q}(\sqrt{38})$. These results are new. Other examples are given for $K = \mathbb{Q}(\sqrt{-23})$, and also for $K = \mathbb{Q}(\sqrt{-31})$, which arose in the second author's PhD thesis [23].

We give several other complete examples for small sets of rational primes below, indicating in some cases an application to the solution of certain Fermat-like Diophantine equations.

In the next section we cover some preliminary algebraic matters concerning so-called "Selmer groups" $K(\mathcal{S}, m)$ associated to the multiplicative group K^*. In Section 3 we show how, given a set of primes $\mathcal{S}$, to find a finite set of j-invariants such that every elliptic curve defined over K with good reduction outside $\mathcal{S}$ has j-invariant in this set; and also how to find the curves with each possible j-invariant when this is neither 0 nor 1728. In Section 4 we consider the special cases $j = 0$ and $j = 1728$. In the final section we give several examples, both over $\mathbb{Q}$ and over various quadratic fields.

The algorithm over $\mathbb{Q}$ is simple to program; a MAGMA program is available from the first author. For general number fields, a proper implementation will be dependent on the further development of algorithms for finding the Mordell-Weil group and all $\mathcal{S}$-integral points on elliptic curves (of the form $Y^2 = X^3 + k$) defined over the field; a preliminary version, which produces lists of curves which are not necessarily complete, is also available.

Acknowledgements: The development of the algorithm has benefited greatly from discussions the first author has had with many people over several years. Certainly, the connection between the set of j-invariants of elliptic curves with everywhere good reduction and the set of integral points on certain elliptic curves has been observed previously in places too numerous to mention. In its present form, our algorithm was greatly influenced by the work of M. Kida, who first answered our query concerning elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{-23})$ with a sketched solution from which the present work developed.

2 m-Selmer groups for K^*

Let K be a number field with ring of integers $\mathcal{O}_K$, and let $\mathcal{S}$ be a finite set of (non-archimedean) primes of K (that is, prime ideals of $\mathcal{O}_K$). Recall that the ring of $\mathcal{S}$-integers $\mathcal{O}_{K,\mathcal{S}}$ and its group of units, the $\mathcal{S}$-units $\mathcal{O}^*_{K,\mathcal{S}}$, are defined as

$$\mathcal{O}_{K,\mathcal{S}} = \{x \in K \mid \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \quad \forall \mathfrak{p} \notin \mathcal{S}\}$$
$$\mathcal{O}^*_{K,\mathcal{S}} = \{x \in K \mid \mathrm{ord}_{\mathfrak{p}}(x) = 0 \quad \forall \mathfrak{p} \notin \mathcal{S}\}.$$

The $\mathcal{S}$-class-group of K is the finite group $\mathcal{C}_{K,\mathcal{S}}$ of $\mathcal{O}_{K,\mathcal{S}}$-ideals modulo principal $\mathcal{O}_{K,\mathcal{S}}$-ideals. This is (isomorphic to) the quotient of the usual class group $\mathcal{C}_K$ by the subgroup generated by the classes of the prime ideals in $\mathcal{S}$.

For each natural number $m > 1$, and each finite set $\mathcal{S}$ of primes of the number field K, we define the following (finite) subgroup of K^*/K^{*m}:

$$K(\mathcal{S}, m) = \{x \in K^*/K^{*m} \mid \mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \pmod{m} \quad \forall \mathfrak{p} \notin \mathcal{S}\}.$$

By abuse of notation we will say that an element x of K^* is in $K(\mathcal{S}, m)$ when $xK^{*m} \in K(\mathcal{S}, m)$, i.e. when $\mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \pmod{m} \quad \forall \mathfrak{p} \notin \mathcal{S}$. We observe that $x \in K^*$ is in $K(\mathcal{S}, m)$ if and only if the principal $\mathcal{O}_{K,\mathcal{S}}$-ideal $(x)\mathcal{O}_{K,\mathcal{S}}$ is an mth power, say $(x)\mathcal{O}_{K,\mathcal{S}} = J_S^m$ with $J_S \lhd \mathcal{O}_{K,\mathcal{S}}$. We now have the basic exact sequence[1], called the m-Kummer sequence for K^* (or for $\mathcal{O}^*_{K,\mathcal{S}}$):

$$1 \to \mathcal{O}^*_{K,\mathcal{S}}/\mathcal{O}^{*m}_{K,\mathcal{S}} \to K(\mathcal{S}, m) \xrightarrow{\alpha_m} \mathcal{C}_{K,\mathcal{S}}[m] \to 1$$

where $\mathcal{C}_{K,\mathcal{S}}[m]$ is the m-torsion subgroup of $\mathcal{C}_{K,\mathcal{S}}$, and the map $\alpha_m \colon K(\mathcal{S}, m) \to \mathcal{C}_{K,\mathcal{S}}[m]$ is given by $x \mapsto [J_S]$ where $(x)\mathcal{O}_{K,\mathcal{S}} = J_S^m$.

For many applications, one only needs to consider $K(\mathcal{S}, p)$ for primes p: this is a finite elementary abelian p-group which may be computed efficiently and explicitly given explicit knowledge of the class group $\mathcal{C}_K$ and unit group of K. In fact, we can see from the Kummer sequence that we need only the p-part of the $\mathcal{S}$-class group and the $\mathcal{S}$-units modulo p'th powers. However, below we will also need to consider $K(\mathcal{S}, m)$ for $m = 4$, $m = 6$ and $m = 12$, and so (lacking any suitable reference) we now explain how to achieve this.

When $\gcd(m, n) = 1$, the determination of $K(\mathcal{S}, mn)$ reduces easily to that of $K(\mathcal{S}, m)$ and $K(\mathcal{S}, n)$:

Proposition 2.1. *Let m, n be coprime. Then*

$$K(\mathcal{S}, mn) \cong K(\mathcal{S}, m) \times K(\mathcal{S}, n)$$

via the map $w \mapsto (w, w)$, with inverse map $(u, v) \mapsto v^{am}u^{bn}$, where $am+bn = 1$.

Proof. It is easy to check that the given maps are both well-defined and mutual inverses. □

For example, $K(\mathcal{S}, 6) \cong K(\mathcal{S}, 2) \times K(\mathcal{S}, 3)$ via $w \mapsto (w, w)$, with inverse map $(u, v) \mapsto v^{-2}u^3$.

For the general case, we have the following[2]:

[1] Note the close analogy with the m-descent Kummer sequence for elliptic curves, $0 \to E(K)/mE(K) \to \mathrm{Sel}^{(m)}(K, E) \to Ш[m] \to 0$.

[2] The corresponding diagram for higher descents on elliptic curves appears in `http://www.maths.nott.ac.uk/personal/jec/papers/d2.ps`

Proposition 2.2. *Let m, n be positive integers. The Kummer sequences for m, mn and n fit together to form the following commutative diagram with exact rows and columns:*

$$\begin{array}{ccccccccc}
 & & 1 & 1 & 1 & 1 & & & \\
 & & \downarrow & \downarrow & \downarrow & \downarrow & & & \\
1 & \to & \mu_{m,n} & \to & \mathcal{O}_{K,\mathcal{S}}^*/\mathcal{O}_{K,\mathcal{S}}^{*n} & \xrightarrow{m} & \mathcal{O}_{K,\mathcal{S}}^*/\mathcal{O}_{K,\mathcal{S}}^{*mn} & \to \mathcal{O}_{K,\mathcal{S}}^*/\mathcal{O}_{K,\mathcal{S}}^{*m} & \longrightarrow 1 \\
 & & \| & & \downarrow & & \downarrow & \downarrow & \downarrow \\
1 & \to & \mu_{m,n} & \longrightarrow & K(\mathcal{S},n) & \xrightarrow{m} & K(\mathcal{S},mn) & \longrightarrow K(\mathcal{S},m) & \xrightarrow{\alpha_{m,n}} \frac{\mathcal{C}_{K,\mathcal{S}}[m]}{n\mathcal{C}_{K,\mathcal{S}}[mn]} \to 1 \\
 & & \downarrow & & \downarrow & & \downarrow & \downarrow & \| \\
 & & 1 & \longrightarrow & \mathcal{C}_{K,\mathcal{S}}[n] & \longrightarrow & \mathcal{C}_{K,\mathcal{S}}[mn] & \xrightarrow{n} \mathcal{C}_{K,\mathcal{S}}[m] & \longrightarrow \frac{\mathcal{C}_{K,\mathcal{S}}[m]}{n\mathcal{C}_{K,\mathcal{S}}[mn]} \to 1 \\
 & & & & \downarrow & & \downarrow & \downarrow & \downarrow \\
 & & & & 1 & & 1 & 1 & 1
\end{array}$$

The kernels $\mu_{m,n} = \mu_m(K)/\mu_{mn}(K)^n$ are finite, and trivial when $\gcd(m,n) = 1$. *The cokernels $\mathcal{C}_{K,\mathcal{S}}[m]/n\mathcal{C}_{K,\mathcal{S}}[mn]$ are finite, and trivial when* $\gcd(m,n) = 1$ *or when $\mathcal{C}_{K,\mathcal{S}}$ has order coprime to m.*

Proof. Exercise. □

To compute $K(\mathcal{S},4)$ specifically, we may proceed as follows. First we find $K(\mathcal{S},2)$ using the standard algorithm. Then we determine the homomorphism $\alpha_{2,2}\colon K(\mathcal{S},2) \to \mathcal{C}_{K,\mathcal{S}}[2]/2\mathcal{C}_{K,\mathcal{S}}[4]$: for each $u \in K(\mathcal{S},2)$ we may write $(u)\mathcal{O}_{K,\mathcal{S}} = J_S^2$ and set $\alpha(u)$ to be the class of J_S modulo $2\mathcal{C}_{K,\mathcal{S}}[4]$. If $[J_S] = [I_S]^2$ for some $\mathcal{S}$-ideal I_S, then writing $(v)J_S = I_S^2$ with $v \in K^*$ we can replace u by uv^2 which represents the same element of $K(\mathcal{S},2)$ as x but which also lies in $K(\mathcal{S},4)$ since $(uv^2)\mathcal{O}_{K,\mathcal{S}} = I_S^4$.

Thus for each generator of the kernel of $\alpha_{2,2}$ we can lift to a representative element $u \in K^*$ such that u modulo K^{*4} lies in $K(S,4)$. Then $K(\mathcal{S},4)$ is generated by these elements, together with the v^2 for v in a set of generators of $K(\mathcal{S},2)$ modulo $\langle -1\rangle$. If required we may determine the precise structure of $K(\mathcal{S},4)$ (as an abelian group of exponent 4) using standard techniques: see [5, Algorithm 4.1.8].

Our Magma implementation includes functions to determine $K(\mathcal{S},4)$ and $K(\mathcal{S},6)$, using the Magma function `pSelmerGroup()` to compute $K(\mathcal{S},2)$ and $K(\mathcal{S},3)$.

Denote by $K(\mathcal{S},m)_{mn}$ the image of the natural map $K(\mathcal{S},mn) \to K(\mathcal{S},m)$ determined as above as $\ker(\alpha_{m,n})$. In our algorithm, as well as needing to determine $K(\mathcal{S},4)$ (via $K(\mathcal{S},2)_4$), we will also need to consider $K(\mathcal{S},6)_{12}$; but this is clearly isomorphic to $K(\mathcal{S},3) \times K(\mathcal{S},2)_4$.

3 Curves with j-invariants $j \neq 0, 1728$

We use the standard notation for the Weierstrass coefficients a_i of an elliptic curve E given by a Weierstrass equation or model, together with the associated weighted invariants c_4 and c_6, the discriminant $\Delta = (c_4^3 - c_6^2)/1728$ and the j-invariant $j = c_4^3/\Delta = 1728 + c_6^2/\Delta$. Recall that the elliptic curve E is said to have *good reduction at* $\mathfrak{p}$ if there exists a $\mathfrak{p}$-integral model (*i.e.*, $\mathrm{ord}_{\mathfrak{p}}(a_i) \geq 0$ for all i) with Δ a $\mathfrak{p}$-unit (*i.e.*, $\mathrm{ord}_{\mathfrak{p}}(\Delta) = 0$).

Different Weierstrass models for E will have invariants which are scaled according to their weight, say $(c_4', c_6', \Delta', j') = (u^4c_4, u^6c_6, u^{12}\Delta, j)$ with $u \in K^*$ arbitrary. So we see that associated to E we have well-defined classes $c_4 \in K^*/K^{*4}$, $c_6 \in K^*/K^{*6}$, $\Delta \in K^*/K^{*12}$, as well as the j-invariant j.

The following elementary observation will be used repeatedly below.

Lemma 3.1. *Let E be an elliptic curve defined over K with good reduction at the prime $\mathfrak{p}$. Then for any Weierstrass model for E, with invariants c_4, c_6, Δ, there exists an integer e such that*

$$\mathrm{ord}_{\mathfrak{p}}(\Delta) = 12e, \qquad \mathrm{ord}_{\mathfrak{p}}(c_4) \geq 4e, \qquad \mathrm{ord}_{\mathfrak{p}}(c_6) \geq 6e.$$

Moreover if $\mathrm{ord}_{\mathfrak{p}}(6) = 0$ then this condition is sufficient for E to have good reduction at $\mathfrak{p}$.

Proof. Necessity is obvious, since a local minimal model with good reduction satisfies the conditions with $e = 0$, and the conditions are invariant under scaling. For the converse, let π be a uniformizer at $\mathfrak{p}$; then the short Weierstrass model for E with $a_4 = -27\pi^{-4e}c_4$ and $a_6 = -54\pi^{-6e}c_6$ is integral, and has good reduction at $\mathfrak{p}$ since it has discriminant $6^{12}\pi^{-12e}\Delta$. □

For the rest of this section we exclude the exceptional cases $j = 0$ and $j = 1728$ which will be treated separately later. Hence c_4 and c_6 are nonzero for any model. We also define the possibly enlarged set $\mathcal{S}^{(6)}$ by

$$\mathcal{S}^{(6)} = \mathcal{S} \cup \{\mathfrak{p} \mid \mathrm{ord}_{\mathfrak{p}}(6) > 0\}.$$

Proposition 3.2. *Let E be an elliptic curve defined over K with good reduction at all primes $\mathfrak{p} \notin \mathcal{S}$. Set $w = j^2(j-1728)^3$. Then*

$$\Delta \in K(\mathcal{S}, 12); \qquad j \in \mathcal{O}_{K,\mathcal{S}}; \qquad w \in K(\mathcal{S}, 6)_{12}.$$

Conversely, if $j \in \mathcal{O}_{K,\mathcal{S}}$ with $j^2(j-1728)^3 \in K(\mathcal{S}, 6)_{12}$ then there exist elliptic curves E with $j(E) = j$ and good reduction outside $\mathcal{S}^{(6)}$.

Proof. For all $\mathfrak{p} \notin \mathcal{S}$, since E has good reduction at $\mathfrak{p}$, Lemma 3.1 shows that $\mathrm{ord}_{\mathfrak{p}}(\Delta) \equiv 0 \pmod{12}$, so we have $\Delta \in K(\mathcal{S}, 12)$. Writing $\mathrm{ord}_{\mathfrak{p}}(\Delta) = 12e$ where $\mathrm{ord}_{\mathfrak{p}}(c_4) \geq 4e$ and $\mathrm{ord}_{\mathfrak{p}}(c_6) \geq 6e$ we also have $\mathrm{ord}_{\mathfrak{p}}(j) = \mathrm{ord}_{\mathfrak{p}}(c_4^3/\Delta) \geq 0$. Moreover, $\mathrm{ord}_{\mathfrak{p}}(j) \equiv \mathrm{ord}_{\mathfrak{p}}(c_4^3) \equiv 0 \pmod 3$, and similarly $j - 1728 = c_6^2/\Delta$ implies $\mathrm{ord}_{\mathfrak{p}}(j-1728) \equiv 0 \pmod 2$. Hence $\mathrm{ord}_{\mathfrak{p}}(w) \equiv 0 \pmod 6$. Thus $w \in K(\mathcal{S}, 6)$. Moreover, if we set $u = \Delta/(c_4c_6)$ then we have

$$\Delta = u^6 j^2 (j-1728)^3 = u^6 w,$$

from which we see that the class of $w \in K(\mathcal{S}, 6)$ lifts to $K(\mathcal{S}, 12)$.

For the converse, suppose that $j \in \mathcal{O}_{K,\mathcal{S}}$ with $w = j^2(j-1728)^3 \in K(\mathcal{S}, 6)_{12}$. Since $jw \in K^{*3}$ and $(j-1728)w \in K^{*2}$ we see that $j \in K(\mathcal{S}, 3)$ and $j - 1728 \in K(\mathcal{S}, 2)$.

Since $w \in K(\mathcal{S}, 6)_{12}$ there exists $u \in K^*$ such that $(3u)^6 w \in K(\mathcal{S}, 12)$. We claim that the elliptic curve

$$E: \qquad Y^2 = X^3 - 3u^2 j(j-1728)X - 2u^3 j(j-1728)^2$$

(which does have $j(E) = j$) has good reduction at all primes $\mathfrak{p} \notin \mathcal{S}$ with $\mathrm{ord}_{\mathfrak{p}}(6) = 0$. Let $\mathfrak{p}$ be such a prime. Let $\mathrm{ord}_{\mathfrak{p}}(j) = 3e_1 \geq 0$ and $\mathrm{ord}_{\mathfrak{p}}(j-1728) = 2e_2 \geq 0$. The invariants of E are

$$\begin{aligned} c_4 &= (12u)^2 j(j-1728), \\ c_6 &= (12u)^3 j(j-1728)^2, \\ \Delta &= (12u)^6 j^2 (j-1728)^3 = 2^{12}(3u)^6 w. \end{aligned}$$

Hence $\mathrm{ord}_{\mathfrak{p}}(\Delta) = 12e$ where $e = \frac{1}{2}(\mathrm{ord}_{\mathfrak{p}}(u) + e_1 + e_2) \in \mathbb{Z}$ (by choice of u). Also, $\mathrm{ord}_{\mathfrak{p}}(c_4) = 2\,\mathrm{ord}_{\mathfrak{p}}(u) + 3e_1 + 2e_2 = 4e + e_1 \geq 4e$, and $\mathrm{ord}_{\mathfrak{p}}(c_6) = 3\,\mathrm{ord}_{\mathfrak{p}}(u) + 3e_1 + 4e_2 = 6e + e_2 \geq 6e$. Lemma 3.1 now implies that E has good reduction at $\mathfrak{p}$.

If there are primes $\mathfrak{p}$ dividing 6 and not in $\mathcal{S}$, E may not have good reduction at $\mathfrak{p}$ but we have at least ensured that $\mathrm{ord}_{\mathfrak{p}}(\Delta) \equiv 0 \pmod{12}$. □

The strategy of our algorithm will be to consider each class $w \in K(\mathcal{S}, 6)_{12}$ in turn, and determine for each the possible $j \in \mathcal{O}_{K,\mathcal{S}}$ with $w \equiv j^2(j-1728)^3$ (modulo K^{*6}). There are finitely many classes w to consider; for each w there is only a finite set of possible values of j (see next proposition), and for each (w, j) pair there are only finitely many suitable curves.

Proposition 3.3. *Let K be a number field and $\mathcal{S}$ a finite set of primes of K. Let $w \in K(\mathcal{S}, 6)$. Each $j \in \mathcal{O}_{K,\mathcal{S}} \setminus \{0, 1728\}$ with $j^2(j-1728)^3 \equiv w \pmod{K^{*6}}$ has the form $j = x^3/w = 1728 + y^2/w$, where $P = (x, y)$ is an $\mathcal{S}$-integral point on the elliptic curve*

$$E_w : \qquad Y^2 = X^3 - 1728w$$

with $xy \neq 0$.

Proof. For each such j there exists $v \in K^*$ such that $w = j^2(j-1728)^3 v^6$. Then $wj = x^3$ with $x = j(j-1728)v^2$ and $w(j-1728) = y^2$ with $y = j(j-1728)^2 v^3$. We then trivially have $x^3 - y^2 = 1728w$, so $P = (x, y)$ has the properties stated: x, y are $\mathcal{S}$-integral since $x^3 = wj \in \mathcal{O}_{K,\mathcal{S}}$ and $y^2 = w(j-1728) \in \mathcal{O}_{K,\mathcal{S}}$. Conversely, if $P = (x, y)$ is an $\mathcal{S}$-integral point on E_w such that $j = x^3/w \in \mathcal{O}_{K,\mathcal{S}}$, then $j^2(j-1728)^3 = v^{-6}w$ where $v = w/(xy)$. □

This shows that the number of possible j-invariants is finite, for each w and hence overall, since for each w the number of $\mathcal{S}$-integral points on E_w is finite. To find this finite set of j we consider each elliptic curve E_w in turn and determine the complete set of $\mathcal{S}$-integral points on it.

We do not claim that for each $\mathcal{S}$-integral point on each E_w the value $j = x^3/w$ is $\mathcal{S}$-integral. Moreover, not every $\mathcal{S}$-integral value of j which arises from an $\mathcal{S}$-integral point on some E_w is necessarily the j-invariant of a suitable elliptic curve; but if we restrict to j-invariants coming from $w \in K(\mathcal{S}, 6)_{12}$, then we will see that there exist suitable curves for each j found (at least if $\mathcal{S}$ contains all primes dividing 6) and we can determine them all precisely.

Proposition 3.4. *Let K be a number field and $\mathcal{S}$ a finite set of primes of K. Let $w \in K(\mathcal{S}, 6)_{12}$. Let $j \in \mathcal{O}_{K,\mathcal{S}} \setminus \{0, 1728\}$ with $j^2(j-1728)^3 \equiv w \pmod{K^{*6}}$. Choose $u_0 \in K^*$ such that $(3u_0)^6 w \in K(\mathcal{S}, 12)$; then the elliptic curve*

$$E : \qquad Y^2 = X^3 - 3xu_0^2 X - 2yu_0^3$$

(where x and y are as in Proposition 3.3) has j-invariant j and good reduction outside $\mathcal{S}^{(6)}$. Moreover, the complete set of curves with good reduction outside $\mathcal{S}^{(6)}$ having j-invariant j is the set of quadratic twists $E^{(u)}$ for $u \in K(\mathcal{S},2)$.

Proof. The first part follows from the proof of Proposition 3.2, since the curve E is the one considered there with $u = u_0 v$ where $w = j^2(j-1728)^3 v^6$, and $(3u)^6 j^2 (j-1728)^3 = (3u_0)^6 w \in K(\mathcal{S},12)$.

Any other curve with the same j-invariant is a quadratic twist $E^{(u)}$ with $u \in K^*$ (modulo K^{*2}). The last statement of the proposition is that such a quadratic twist has good reduction outside $\mathcal{S}^{(6)}$ if and only if $u \in K(\mathcal{S},2)$.

In one direction, twisting by $u \in K(\mathcal{S},2)$ has the effect of replacing u_0 by uu_0 which does not affect the condition $(3u_0)^6 w \in K(\mathcal{S},12)$; so these twists do have good reduction outside $\mathcal{S}^{(6)}$.

Conversely, since twisting E by u multiplies Δ by u^6 we see that for $E^{(u)}$ to have good reduction at a prime $\mathfrak{p} \notin \mathcal{S}$ it is necessary to have $\mathrm{ord}_{\mathfrak{p}}(u)$ even. □

These propositions together give an algorithm for computing all elliptic curves defined over K with good reduction outside $\mathcal{S}$ and j-invariant neither 0 nor 1728:

1. Compute $K(\mathcal{S},6)$ from $K(\mathcal{S},2)$ and $K(\mathcal{S},3)$, and the subgroup $K(\mathcal{S},6)_{12}$, as in the previous section; hence determine a (finite) representative set W of $\mathcal{S}$-integers $w \in K(\mathcal{S},6)_{12}$; for each such w, compute $u_0 \in K^*$ such that $(3u_0)^6 w \in K(\mathcal{S},12)$. The following steps are then carried out for each w in turn.

2. Find all $\mathcal{S}$-integral points (x,y) on the elliptic curve E_w such that $j = x^3/w$ is $\mathcal{S}$-integral.

3. For each $\mathcal{S}$-integral point $(x,y) \in E_w(K)$, consider the elliptic curve $E : Y^2 = X^3 - 3xu_0^2 X - 2yu_0^3$ (with the value of u_0 found in step 1 for the current w), which certainly has good reduction outside $\mathcal{S}^{(6)}$. If there are any primes $\mathfrak{p}$ dividing 6 not in $\mathcal{S}$, check whether E has good reduction at each such $\mathfrak{p}$ (say by using Tate's algorithm), and discard E if not.

4. Repeat the preceding step for each quadratic twist $E^{(u)}$ as u runs through representatives for $K(\mathcal{S},2)$.

As an alternative to Step 3, we may consider the following more self-contained version, which requires only a value $j \in \mathcal{O}_{K,\mathcal{S}}$ satisfying $j^2(j-1728)^3 \in K(\mathcal{S},6)_{12}$, as in Proposition 3.2:

3′. For each $\mathcal{S}$-integral j for which $j^2(j-1728)^3 \in K(\mathcal{S},6)_{12}$, determine $u_0 \in K^*$ such that $(3u_0)^6 j^2 (j-1728)^3 \in K(\mathcal{S},12)$, and consider the elliptic curve $E : \quad Y^2 = X^3 - 3j(j-1728)u_0^2 X - 2j(j-1728)^2 u_0^3$; this has good reduction outside $\mathcal{S}^{(6)}$. If there are any primes $\mathfrak{p}$ dividing 6 not in $\mathcal{S}$, check whether E has good reduction at each such $\mathfrak{p}$ (say by using Tate's algorithm), and discard E if not.

When $K = \mathbb{Q}$, the determination of W is of course trivial. Writing $\mathcal{S} = \{p_1, \ldots, p_n\}$, we may take

$$W = \{\pm \prod_{i=1}^{n} p_i^{e_i} \mid 0 \le e_i \le 5 \quad \forall i\}$$

so that $\#W = 2 \cdot 6^n$. In this case we certainly have $K(\mathcal{S}, 6) = K(\mathcal{S}, 6)_{12}$ (the class number being 1); for Step 3 we may take $u_0 = 3$ if $3 \notin \mathcal{S}$, otherwise $u_0 = 1$ (for all w). In the self-contained Step 3′ we may take u_0 to be the product of those primes $p \notin \mathcal{S}$ such that $\mathrm{ord}_p(3^6 j^2 (j - 1728)^3) \equiv 6 \pmod{12}$.

When the set $\mathcal{S}$ contains some or all of the primes dividing 2 and 3 we may be able to replace the curves E_w by curves which are closer to minimal at these primes, by dividing the coefficient $1728w$ by a sixth power. We omit the details.

4 Curves with j-invariants 0 and 1728

Elliptic curves with j-invariant 0 all have models of the form

$$Y^2 = X^3 + w,$$

and are sextic twists of the curve $Y^2 = X^3 + 1$, with w unique modulo K^{*6}. Similarly, elliptic curves with j-invariant 1728 all have models of the form

$$Y^2 = X^3 + wX,$$

and are quartic twists of the curve $Y^2 = X^3 + X$, with w unique modulo K^{*4}.

To have good reduction outside $\mathcal{S}$ we will see that the twisting factor w is restricted to lie in $K(\mathcal{S}', 6)$ or $K(\mathcal{S}', 4)$ for a certain set $\mathcal{S}'$ (defined precisely below) with

$$\mathcal{S} \subseteq \mathcal{S}' \subseteq \mathcal{S}^{(6)} = \mathcal{S} \cup \{\mathfrak{p} \mid \mathrm{ord}_{\mathfrak{p}}(6) > 0\}.$$

Proposition 4.1 (For curves with $j = 0$). *If $\mathcal{S}$ does not contain all primes $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(3)$ odd then there are no elliptic curves E defined over K, with j-invariant 0 and good reduction outside $\mathcal{S}$. Otherwise every such curve is isomorphic to $Y^2 = X^3 + w$ with $w \in K^*$, uniquely determined modulo K^{*6}, representing a class in $K(\mathcal{S}', 6)$, where*

$$\mathcal{S}' = \mathcal{S} \cup \{\mathfrak{p} \mid \mathrm{ord}_{\mathfrak{p}}(2) \equiv \pm 1 \pmod 3\} \cup \{\mathfrak{p} \mid \mathrm{ord}_{\mathfrak{p}}(3) \equiv 2 \pmod 4\},$$

such that

- $\mathrm{ord}_{\mathfrak{p}}(w) \equiv \mp 2 \pmod 6$ *for all* $\mathfrak{p} \in \mathcal{S}' \setminus \mathcal{S}$ *with* $\mathrm{ord}_{\mathfrak{p}}(2) \equiv \pm 1 \pmod 3$*;*
- $\mathrm{ord}_{\mathfrak{p}}(w) \equiv 3 \pmod 6$ *for all* $\mathfrak{p} \in \mathcal{S}' \setminus \mathcal{S}$ *with* $\mathrm{ord}_{\mathfrak{p}}(3) \equiv 2 \pmod 4$.

Proof. Every curve defined over K with j-invariant 0 is isomorphic to a curve of the given form, where w is determined up to sixth powers. The discriminant of $Y^2 = X^3 + w$ is $\Delta = -2^4 3^3 w^2$; a necessary condition for the curve to have good reduction at $\mathfrak{p}$ is $\mathrm{ord}_{\mathfrak{p}}(\Delta) \equiv 0 \pmod{12}$. This is impossible if $\mathrm{ord}_{\mathfrak{p}}(3)$ is odd, since then $\mathrm{ord}_{\mathfrak{p}}(\Delta)$ is also odd; this establishes the first statement. For the rest it suffices to observe that we require

- $\mathrm{ord}_{\mathfrak{p}}(w) \equiv 0 \pmod 6$ if $\mathrm{ord}_{\mathfrak{p}}(3) \equiv 0 \pmod 4$ and $\mathrm{ord}_{\mathfrak{p}}(2) \equiv 0 \pmod 3$;
- $\mathrm{ord}_{\mathfrak{p}}(w) \equiv 3 \pmod 6$ if $\mathrm{ord}_{\mathfrak{p}}(3) \equiv 2 \pmod 4$;
- $\mathrm{ord}_{\mathfrak{p}}(w) \equiv \mp 2 \pmod 6$ if $\mathrm{ord}_{\mathfrak{p}}(2) \equiv \pm 1 \pmod 3$.

The first condition in ensured by requiring $w \in K(\mathcal{S}', 6)$ with $\mathcal{S}'$ as in the statement of the proposition. □

Remarks. 1. When $\mathcal{S}$ already contains the primes dividing 6, we may observe that the curves we consider with $j = 0$ are precisely the ones considered in the first part of the algorithm.

2. Over $\mathbb{Q}$, we can omit $j = 0$ unless $3 \in \mathcal{S}$, and if $2 \notin \mathcal{S}$ then we set $\mathcal{S}' = \mathcal{S} \cup \{2\}$ and use only those $w \in K(\mathcal{S}', 6)$ with $\mathrm{ord}_2(w) \equiv 4 \pmod 6$. This just amounts to taking $w = 16w_1$ where $w_1 \in K(\mathcal{S}, 6)$.

Proposition 4.2 (For curves with $j = 1728$). *Every elliptic curve E defined over K with j-invariant 1728 and with good reduction outside $\mathcal{S}$ is isomorphic to $Y^2 = X^3 + wX$, with $w \in K^*$ uniquely determined modulo K^{*4}, representing a class in $K(\mathcal{S}', 4)$ where $\mathcal{S}' = \mathcal{S} \cup \{\mathfrak{p} \mid \mathrm{ord}_{\mathfrak{p}}(2) \equiv 1 \pmod 2\}$, such that for all $\mathfrak{p} \in \mathcal{S}' \setminus \mathcal{S}$ (if any), $\mathrm{ord}_{\mathfrak{p}}(w) \equiv 2 \pmod 4$.*

Proof. Every curve defined over K with j-invariant 1728 is isomorphic to a curve of the given form, where w is determined up to fourth powers. The discriminant of $Y^2 = X^3 + wX$ is -2^6w^3, so a necessary condition for the curve to have good reduction at $\mathfrak{p}$ is $\mathrm{ord}_{\mathfrak{p}}(w) \equiv 0 \pmod 4$ if $\mathrm{ord}_{\mathfrak{p}}(2)$ is even (this includes all $\mathfrak{p} \nmid 2$), and $\mathrm{ord}_{\mathfrak{p}}(w) \equiv 2 \pmod 4$ if $\mathrm{ord}_{\mathfrak{p}}(2)$ is odd; hence we must have $w \in K(\mathcal{S}', 4)$, and w must also satisfy the last condition of the statement. □

Remark. Over $\mathbb{Q}$, we set $\mathcal{S}' = \mathcal{S} \cup \{2\}$ and if $2 \notin \mathcal{S}$ we use only those $w \in K(\mathcal{S}', 4)$ with $\mathrm{ord}_2(w) \equiv 2 \pmod 4$. This just amounts to taking $w = 4w_1$ where $w_1 \in K(\mathcal{S}, 4)$.

5 Examples

In all cases the full lists of curves found may be obtained from the first author's web page `http://www.maths.nott.ac.uk/personal/jec/ftp/data/extra.html`.

5.1 Examples over $\mathbb{Q}$

Take $K = \mathbb{Q}$ and $\mathcal{S} = \{2\}$. We find the following 13 possible values of j:

$$1728, 10976, -864, 3375/2, -189613868625/128, -3456,$$
$$432, 128, -35937/4, -784446336, 8000, 287496, 6912.$$

From these, we find four elliptic curves with good reduction outside 2 for each $j \in \{128, 8000, 10976, 287496\}$, eight curves with $j = 1728$ and none for the others (which only produced curves which have bad reduction at 3).

Similarly, with $\mathcal{S} = \{2, 3\}$ we find 83 possible j-invariants. In all these cases we find a Mordell-Weil basis and the $\mathcal{S}$-integral points with no difficulties.

From these, we find a total of 752 curves; each $j \neq 0, 1728$ gives 8 curves (up to isomorphism) as expected, this being the size of $K(\mathcal{S}, 2)$, and there are also 32 with $j = 0$ and 72 with $j = 1728$. Their conductors are of the form 2^a3^b with $a \leq 8$ and $b \leq 5$. As a check, we compared with the list compiled by F.B. Coghlan in 1966 (see [3]), and found the same list.

With $\mathcal{S} = \{11\}$ we find 23 possible j-invariants:

$$1728, -32768, 13824/1331, -19008, -297, 704, 59319/121, -21024576/121,$$
$$-24729001, -122023936/161051, -121, -110592/11, 139798359/19487171,$$
$$-161700475392/11, -7077888/11, -4096/11, 13824/11, -1728/11,$$
$$-2515456/11, -51778336347648/19487171, 512/11, -8120601/11,$$
$$-52893159101157376/11.$$

Some of the curves E_w which arise deserve special mention: $w = 11^4 = 14641$ and $w = 11^5 = 161051$. Both the curves E_{14641} and E_{161051} have trivial Mordell-Weil groups (over $\mathbb{Q}$), but the standard 2-descent is not sufficient to show this, since the 2-Selmer rank in both cases is 2. However we can compute the analytic ranks, and find that (in both cases) it is 0, with the order of Ш (as predicted by the Birch Swinnerton-Dyer Conjecture) equal to 4. Neither curve has any rational torsion, so neither contributes to the list of possible j values.

Only 6 of these 23 j-invariants give rise to curves with good reduction outside 11, namely

$$-52893159101157376/11, -24729001, -32768,$$
$$-122023936/161051, -4096/11, -121.$$

For each we find two elliptic curves with good reduction away from 11, giving 12 curves in all, as in [3]: three with conductor 11 and nine with conductor 121.

For several other small sets $\mathcal{S}$ of rational primes we have also been able to determine the complete set of curves. The following examples have applications in the resolution of certain Fermat-like Diophantine equations such as those treated in [2], [1]. Previously the first author had attempted to assist such applications by finding all elliptic curves with conductors N of the given type using modular symbols techniques, as in [12], but that method becomes very arduous when the space of cusp forms of weight 2 for $\Gamma_0(N)$ has large dimension.

$N = 2^k 7^2$: Here modular symbol methods were successful in reaching the highest level $N = 2^8 7^2 = 12544$. As a check, we verified that the curves obtained by our method with $\mathcal{S} = \{2, 7\}$ include the same curves with conductor divisible by 7^2 as obtained via modular symbols.

$N = 2^k 11^2$: Here modular symbol methods were successful in reaching the highest level $N = 2^8 11^2 = 30976$ (dimension 4081). Again, we verified that the curves obtained by our method with $\mathcal{S} = \{2, 11\}$ include the same curves with conductor divisible by 11^2 as obtained via modular symbols.

$N = 2^k 13^2$: Here modular symbol methods were successful in reaching the highest level $N = 2^8 13^2 = 43264$ (dimension 5657). Again, we verified that the curves obtained by our method with $\mathcal{S} = \{2, 13\}$ include the same curves with conductor divisible by 13^2 as obtained via modular symbols.

$N = 2^k 17^2$: Modular symbol methods were successful in reaching level $N = 2^7 13^2 = 36992$ (dimension 4753), but we were (until recently) unable to compute the 9577-dimensional space at level $N = 2^8 17^2 = 73984$. With our method we found all 256 elliptic curves with good reduction outside $\{2, 17\}$, including 144 with conductor $N = 2^k 17^2$; for $k \leq 7$ these were exactly the same curves

as obtained via modular symbols, but we also find 32 curves with conductor $N = 2^8 17^2$, in 16 isogeny classes. [Recently these computations for $N = 2^8 17^2$ were verified using modular symbols.]

We give some details of the computations in the preceding example, as it illustrates clearly where the difficulties with our approach lie, even in the case $K = \mathbb{Q}$. There is no difficulty in the second phase (finding the curves from their j-invariants). In the first phase (finding the j-invariants), we find 42 possible j-invariants from 72 values of w. For five w, MAGMA was not able to determine the full Mordell-Weil group of E_w, leading to extra work being necessary. For $w = -17^5$, the curve E_w has rank 0 and trivial torsion, but its 2-Selmer rank is 2 so we resorted to computing the analytic rank, by checking that $L(E_w, 1) \neq 0$. For the four values $w = 2^5 \cdot 17^5$, $w = 2^2 \cdot 17^4$, $w = -2^5 \cdot 17^4$, $w = -2^4 \cdot 17^4$ the Mordell-Weil group has rank 1, with no torsion, and a rather large generator which was not found automatically by MAGMA. In order to show that there are no $\mathcal{S}$-integral points in each of these four cases, we had to find the generator and verify that in each case it is not $\mathcal{S}$-integral. For the last three of these cases this was done by using our 2-descent program `mwrank`; for the case $w = 2^5 \cdot 17^5$, the generator has canonical height 160 (approximately) and was found by computing the Heegner point associated to the discriminant $D = -47$ to 85 decimal places. The denominator of the generator's x-coordinate is d^2 where d has 33 digits and factorization

$$d = 3 \cdot 5 \cdot 64189 \cdot 259907 \cdot 20745658643 \cdot 79102726763.$$

It would be highly desirable in cases like this to be able to decide that the generator is not $\mathcal{S}$-integral without finding it explicitly!

The computations of analytic ranks and Heegner points were originally carried out using our own `PARI/GP` programs; now these are also available within MAGMA.

$N = 2^k 19^2$: A similar calculation was carried out with $\mathcal{S} = \{2, 19\}$. The same curves were found as were already known from modular symbol calculations at levels up to $2^8 19^2 = 92416$.

$N = 2^k 23^2$: A similar calculation was carried out with $\mathcal{S} = \{2, 23\}$. For $k \leq 7$ the same curves were found as were already known from modular symbol calculations. In addition, 32 curves of conductor $N = 2^8 23^2 = 135424$ were found, in 20 isogeny classes; this level is currently beyond the range of our modular symbol computations.

5.2 Examples over quadratic fields

In the second author's thesis [23], spaces of cusp forms of weight 2 and small level $\mathfrak{N}$ were computed using the method of modular symbols for the fields $K = \mathbb{Q}(\sqrt{-23})$ and $K = \mathbb{Q}(\sqrt{-31})$ of class number 3. The newforms in these spaces which have rational Hecke eigenvalues are expected, via a conjectural generalization of the Eichler-Shimura construction over $\mathbb{Q}$, to correspond to elliptic curves defined over K with conductor $\mathfrak{N}$. (Here $\mathfrak{N}$ is an integral ideal in the ring of integers $\mathcal{O}_K$).

Lacking a way of constructing elliptic curves from newforms in this context, one has to using other methods for finding elliptic curves with small conductor defined over K. One then attempts to match up the curves found to the

newforms. For imaginary quadratic fields of class number 1 this was done systematically by the first author (see [9], [11], [13]). The first attempt to find elliptic curves with small conductor consists of searching through all integral Weierstrass equations whose 5-tuple of coefficients $[a_1, a_2, a_3, a_4, a_6]$ lies in some finite search region, eliminating those whose conductor (found using Tate's algorithm) is outside the desired range. It frequently happens that some of the expected curves are not found this way, having coefficients which are too large and so lie outside the original search region. One way of refining the search for these missing curves was described in [10], where the curves missing from [9] were all found. The method of this paper gives an alternative method which has also been successful in many cases, as we now illustrate.

We start with one case where we were able to determine that there are no curves with everywhere good reduction defined over a field for which this was not already known. In the remaining cases, we use our method for finding curves with certain conductors, but have not proved that the sets we obtained are complete.

5.2.1 $K = \mathbb{Q}(\sqrt{-23})$ and $\mathcal{S} = \emptyset$

Modular symbol calculations in [23] suggested that there exist no elliptic curves defined over $\mathbb{Q}(\sqrt{-23})$ with everywhere good reduction. As this fact was not apparently known in the literature, we applied our methods and were able to establish this.

Theorem 5.1. *There are no elliptic curves with everywhere good reduction defined over the field* $\mathbb{Q}(\sqrt{-23})$.

Proof. Write $\omega = (1+\sqrt{-23})/2$, so that $\mathcal{O}_K = \mathbb{Z}[\omega]$. The class group of $\mathcal{O}_K$ has order 3, generated by the class of $\mathfrak{p} = (2, \omega)$, and the only units are ± 1; a generator of $\mathfrak{p}^3$ is $2-\omega$. Hence we may take $W = \{\pm 1, \pm(1+\omega), \pm(2-\omega)\}$. Of the six curves E_w, the four with $w \neq \pm 1$ have trivial Mordell-Weil group. For example, consider $E = E_{1+\omega}$. Using MAGMA's function `RankBound()` which finds the 2-Selmer rank, we find that $E(K)$ has rank 0; and considering the reduction modulo small primes shows that $E(K)$ has no torsion, so $E(K)$ is trivial. Three other cases are similar. The curves $Y^2 = X^3 \pm 1728$ both have rank 1 over K and a 2-torsion point $(\mp 12, 0)$. Neither curve has any integral points apart from the 2-torsion points; we are grateful to E. Herrmann for verifying this for us.

Hence we find that the only possible j-invariants are $\{0, \pm 1728\}$. Now a result of Setzer [27] shows that none of these is in fact the j-invariant of an elliptic curve with everywhere good reduction over any quadratic number field, so we can conclude that there are no elliptic curves with everywhere good reduction over K. Alternatively, for the last part we may apply the general algorithm. □

5.2.2 $K = \mathbb{Q}(\sqrt{-23})$, general $\mathcal{S}$

We will denote by $\mathfrak{p}_l$ a prime of $\mathcal{O}_K$ dividing the rational prime l. Among the conductors for which we expected elliptic curves but did not find them by searching are the following:

$$\mathfrak{N}_1 = \mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}^2, \qquad \mathfrak{N}_2 = \mathfrak{p}_2^3\overline{\mathfrak{p}_2}\mathfrak{p}_3^2, \qquad \mathfrak{N}_3 = \mathfrak{p}_2^3\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}.$$

For conductor $\mathfrak{N}_1$ we expected three isogeny classes of curves, of expected rank 0, 1 and 2 (predicted from the analytic rank of the L-function of the associated newform, for compatibility with the Birch–Swinnerton-Dyer conjecture). Searching only found the curve $[1, \omega-1, 0, 2\omega-3, 5]$ of rank 0. Using the method of this paper, we also found the following curves of conductor $\mathfrak{N}_1$:

$$\begin{aligned} [0,0,0,552\omega+1221,4888\omega-34762] &\quad \text{of rank 1} \\ [0,0,0,-53160\omega-43995,-5067640\omega+19402006] &\quad \text{of rank 2} \end{aligned}$$

whose L-functions match those of the newforms as expected (comparing the first several Euler factors).

For conductors $\mathfrak{N}_2$ and $\mathfrak{N}_3$ we expected one isogeny class each, of curves with rank 0; our method did find such curves:

$$\begin{aligned} [0,0,0,-18927\omega-14202,1857222\omega-1211004] &\quad \text{of conductor } \mathfrak{N}_2 \\ [0,0,0,864\omega-26811,-95472\omega+1553094] &\quad \text{of conductor } \mathfrak{N}_3. \end{aligned}$$

However, there are still some conductors where elliptic curves are still "missing", involving bad reduction at primes above 5, 13 and 29; see [23] for more details.

5.2.3 $K = \mathbb{Q}(\sqrt{-31})$

We limit ourselves to one example. Modular symbol computations suggest the existence of an elliptic curve defined over $K = \mathbb{Q}(\sqrt{-31})$ with conductor $\mathfrak{N} = \mathfrak{p}_2\mathfrak{p}_5^2$, which was not found by our search. Using our method we find the following curve with this conductor (here $\omega = (1+\sqrt{-31})/2$):

$$[-\omega, 1-\omega, 0, \omega+8, -8\omega].$$

This model is minimal at all primes except $\mathfrak{p}_2$; its discriminant ideal is $\mathfrak{p}_2^{13}\mathfrak{p}_5^8$.

5.2.4 Real quadratic fields

Several authors have worked systematically to decide which quadratic fields possess curves with everywhere good reduction. We do not give a complete list of what is known here, but give one example which to our knowledge was not previously known, found by our method.

Theorem 5.2. *Let $K = \mathbb{Q}(\sqrt{38})$ and set $\alpha = \sqrt{38}$. The elliptic curve with coefficients (of a global minimal Weierstrass model)*

$$[\alpha, \alpha+1, \alpha+1, 4\alpha+15, 4\alpha+21]$$

has everywhere good reduction over K.

Proof. The discriminant of the given equation is $32850\alpha + 202501 = \varepsilon^3$ where $\varepsilon = 6\alpha + 37$ is the fundamental unit of K. □

References

[1] M. A. Bennett and C. M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[2] M. A. Bennett, V. Vatsal, and S. Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.*, 140(6):1399–1416, 2004.

[3] B. J. Birch and W. Kuyk, editors. *Modular functions of one variable. IV.* Springer-Verlag, Berlin, 1975. Lecture Notes in Mathematics, Vol. 476.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[6] S. Comalada. Courbes elliptiques à bonne réduction d'invariant j fixé. *C. R. Acad. Sci. Paris Sér. I Math.*, 311(11):667–670, 1990.

[7] S. Comalada. Elliptic curves with trivial conductor over quadratic fields. *Pacific J. Math.*, 144(2):237–258, 1990.

[8] S. Comalada and E. Nart. Courbes elliptiques avec bonne réduction partout. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(6):223–224, 1987.

[9] J. E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Mathematica*, 51:275–323, 1984.

[10] J. E. Cremona. Addendum and errata: "Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields" [Compositio Math. **51** (1984), no. 3, 275–324; MR0743014 (85j:11063)]. *Compositio Math.*, 63(2):271–272, 1987.

[11] J. E. Cremona. Abelian varieties with extra twist, cusp forms and elliptic curves over imaginary quadratic fields. *J. London Math. Soc. (2)*, 45:404–416, 1992.

[12] J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, second edition, 1997.

[13] J. E. Cremona and E. Whitley. Periods of cusp forms and elliptic curves over imaginary quadratic fields. *Math. Comp.*, 62(205):407–429, 1994.

[14] E. Herrmann. *Bestimmung aller S-ganzen Lösungen auf elliptischen Kurven*. PhD thesis, Universität des Saarlandes, 2002.

[15] E. Herrmann and A. Pethő. S-integral points on elliptic curves. Notes on a paper of B. M. M. de Weger: "S-integral solutions to a Weierstrass equation" [J. Theór. Nombres Bordeaux **9** (1997), no. 2, 281–301; MR 99d:11027]. *J. Théor. Nombres Bordeaux*, 13(2):443–451, 2001.

[16] H. Ishii. The nonexistence of elliptic curves with everywhere good reduction over certain quadratic fields. *Japan. J. Math. (N.S.)*, 12(1):45–52, 1986.

[17] M. Kida. Reduction of elliptic curves over certain real quadratic number fields. *Math. Comp.*, 68(228):1679–1685, 1999.

[18] M. Kida. Computing elliptic curves having good reduction everywhere over quadratic fields. II. In *Algebraic number theory and Diophantine analysis (Graz, 1998)*, pages 239–247. de Gruyter, Berlin, 2000.

[19] M. Kida. Computing elliptic curves having good reduction everywhere over quadratic fields. *Tokyo J. Math.*, 24(2):545–558, 2001.

[20] M. Kida. Good reduction of elliptic curves over imaginary quadratic fields. *J. Théor. Nombres Bordeaux*, 13(1):201–209, 2001. 21st Journées Arithmétiques (Rome, 2001).

[21] M. Kida. Nonexistence of elliptic curves having good reduction everywhere over certain quadratic fields. *Arch. Math. (Basel)*, 76(6):436–440, 2001.

[22] M. Kida and T. Kagawa. Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields. *J. Number Theory*, 66(2):201–210, 1997.

[23] M. P. Lingham. *Modular forms and elliptic curves over imaginary quadratic fields*. PhD thesis, University of Nottingham, 2005. available online at `http://etheses.nottingham.ac.uk/archive/00000138/`.

[24] A. Pethő, H. G. Zimmer, J. Gebel, and E. Herrmann. Computing all S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 127(3):383–402, 1999.

[25] I. R. Šafarevič. Algebraic number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 163–176. Inst. Mittag-Leffler, Djursholm, 1963.

[26] B. Setzer. Elliptic curves over complex quadratic fields. *Pacific J. Math.*, 74(1):235–250, 1978.

[27] B. Setzer. Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant. *Illinois J. Math.*, 25(2):233–245, 1981.

[28] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106. Springer-Verlag, 1986.