TOKYO J. MATH.
VOL. 24, NO. 2, 2001

Computing Elliptic Curves Having Good Reduction Everywhere over Quadratic Fields

Masanari KIDA

The University of Electro-Communications

(Communicated by K. Komatsu)

Introduction.

The first example of an elliptic curve having good reduction everywhere over a quadratic field is given by Tate (see [16]). His example

$$y^2 + xy + \left(\frac{5+\sqrt{29}}{2}\right)^2 y = x^3$$

has good reduction at every finite place of the ring of integers of $\mathbf{Q}(\sqrt{29})$. Other examples of such elliptic curves are found by several authors (see for example [17] and [5]).

The aim of this paper is to give a systematic method to compute all such elliptic curves defined over quadratic number field for a given modular invariant. In other words, we give an algorithm for finding all twists having good reduction everywhere. For the case of rational j-invariants, Setzer ([17, Lemma]) gives some conditions which these twists must satisfy. But his characterization is not easy to use for a practical computation. In this paper, using twists of elliptic curves explicitly, we shall clarify his argument and give a general method that is relevant to explicit computation. Our method mainly involves a computation of quartic fields with given discriminant.

As an application, we compute elliptic curves having good reduction everywhere over certain real quadratic fields that have rational or singular j-invariants.

Throughout this paper, we use the following notation.

For an algebraic number field K, let K^* be the multiplicative group of K and $\mathcal{O}_K$ the ring of algebraic integers of K. Suppose that L/K is a field extension of finite degree. We denote by $d_{L/K}$ the discriminant of the extension. If the base field K is equal to the field $\mathbf{Q}$ of rational numbers, we use d_L instead of $d_{L/\mathbf{Q}}$ for simplicity. The symbol $N_{L/K}$ stands for the

Received September 18, 2000
Revised April 2, 2001
This research was supported in part by Grant-in-Aid for Encouragement of Young Scientists (No. 09740012), Ministry of Education, Science, Sports and Culture, Japan.

norm map. Moreover, if the extension L/K is a Galois extension, let $\mathrm{Gal}(L/K)$ be its Galois group.

For an elliptic curve E defined over K, let $j(E)$ be the modular invariant of E and $\mathrm{Cond}_L(E_L)$ the conductor over L where E_L is the base change $E \times_K L$.

We also use the following term for the sake of brevity. An elliptic curve E defined over K is said to have *good reduction* (over K) if it has good reduction at *every* finite prime of $\mathcal{O}_K$. When we refer to the reduction at a specific prime, we always say that the curve has good reduction *at* the prime.

This paper consists of four sections. In the first section, we recall the theory of twist in brief. Our algorithm for finding appropriate twists will be given in the second section. In the third section, we count the number of the twists. In the fourth section, we compute some examples of elliptic curves having good reduction over certain real quadratic fields.

1. Preliminaries.

Let E be an elliptic curve defined over a number field K whose j-invariant is neither 0 nor 1728. We take a short Weierstrass equation for E:

$$y^2 = x^3 + a_4 x + a_6 .$$

Then the quadratic twist E^u corresponding to an element $u \in K^*/K^{*2}$ is an elliptic curve defined over K given by the Weierstrass equation

$$y^2 = x^3 + u^2 a_4 x + u^3 a_6 . \tag{1.1}$$

The curves E and E^u are isomorphic over the quadratic extension $K(\sqrt{u})$ of K, hence, in particular, we have $j(E) = j(E^u)$.

We also need a notion of quartic twists. Let M/K be a quartic extension with a quadratic intermediate field L. We write $M = L(\sqrt{u})$ with $u \in L^*/L^{*2}$. For an elliptic curve E defined over K, we call the elliptic curve $(E_L)^u$ defined over L the *quartic twist* corresponding to u. We denote it also by E^u, if no confusion will be made. Note that, in this notation, a model of the quartic twist is also given by (1.1).

The following proposition describes the variation of the conductor of an elliptic curve by a quadratic twist.

PROPOSITION 1.1. *Let $L = K(\sqrt{u})$ be a quadratic extension of a number field K and E an elliptic curve defined over K. Then we have*

$$N_{L/K}(\mathrm{Cond}_L(E_L)) \cdot (d_{L/K})^2 = \mathrm{Cond}_K(E) \cdot \mathrm{Cond}_K(E^u) . \tag{1.2}$$

PROOF. This proposition follows immediately from [15, Proposition 1] and [12, Theorem]. See also [21, Proposition 5.2]. □

2. Finding twists.

Let $k = \mathbf{Q}(\sqrt{m})$ be a quadratic number field where m is a square-free integer. Suppose that an integer $j \in \mathcal{O}_k$ is given. In this section, we describe an algorithm to find all the elliptic curves defined over k having good reduction whose j-invariant is this given j.

We do not really need to known whether there is such an elliptic curve in advance, because our algorithm also answers the question of the existence.

We remark also that our assumption on the integrality of j is justified by the fact that an elliptic curve has potential good reduction if and only if its j-invariant is integral ([19,VII.5.5]).

In the rest of this paper, we do not treat the cases where $j = 0$ and 1728, since Setzer showed that any elliptic curve having these j-invariants must have bad reduction at some prime over any quadratic field ([17, Theorem 2 (a)]). In fact, it is known that these j-values behave even worse (see [8]).

If an elliptic curve has good reduction, then the ideal generated by the discriminant of the curve is a 12-th power. Thus it easily follows that the conditions

$$v(j) \equiv 0 \pmod 3 \quad \text{and} \quad v(j - 1728) \equiv 0 \pmod 2 \tag{2.1}$$

are necessary for every discrete valuation v of $\mathcal{O}_k$.

We separate the description of our algorithm into two cases depending on the degree of the given integer j.

2.1. The case where j is rational. Since k is a quadratic field, we can write $j = A^3$ with some $A \in \mathbf{Z}$ by (2.1).

ALGORITHM 1.
Input: $A \in \mathbf{Z}$, $(A \neq 0, 12)$.
Output: All elliptic curves having good reduction with $j = A^3$.

Step 1: Let E_A be an elliptic curve defined by

$$y^2 = x^3 - 3A(A^3 - 1728)x - 2(A^3 - 1728)^2 . \tag{2.2}$$

The j-invariant of E_A is A^3 and the discriminant is $2^{12} \cdot 3^6 \cdot (A^3 - 1728)^3$.

This is the same notation as one used in Setzer's paper [17].

Step 2: The curve E_A itself cannot have good reduction over $\mathbf{Q}$ by a well-known theorem of Tate. Furthermore, since we want to find elliptic curves defined over k which are isomorphic to E_A over an algebraic closure of k (in fact, over a quadratic extension of k), we have to find appropriate quartic twists E_A^u of the curve E_A or equivalently the quartic fields $K = k(\sqrt{u})$.

The following proposition enables us to find the candidates for K.

PROPOSITION 2.1. *Let $k = \mathbf{Q}(\sqrt{m})$, $K = k(\sqrt{u})$ and E_A be as above. If the quartic twist E_A^u corresponding to K has good reduction over k, then we have*

$$(N_{k/\mathbf{Q}}(d_{K/k}) \cdot d_k)^2 = \mathrm{Cond}_{\mathbf{Q}}(E_A)\mathrm{Cond}_{\mathbf{Q}}(E_A^m) . \tag{2.3}$$

PROOF. Here we simply write E for E_A. First we write down the identity (1.2) in Proposition 1.1 for the quadratic extensions $k/\mathbf{Q}$ and K/k. They are

$$N_{k/\mathbf{Q}}(\mathrm{Cond}_k(E_k)) \cdot (d_{k/\mathbf{Q}})^2 = \mathrm{Cond}_{\mathbf{Q}}(E) \cdot \mathrm{Cond}_{\mathbf{Q}}(E^m) \tag{2.4}$$

and

$$N_{K/k}(\mathrm{Cond}_K(E_K)) \cdot (d_{K/k})^2 = \mathrm{Cond}_k(E_k) \cdot \mathrm{Cond}_k(E_k^u)\,. \tag{2.5}$$

If E_k^u has good reduction, then we have $\mathrm{Cond}_k(E_k^u) = \mathcal{O}_k$. Since E_k is isomorphic to E_K^u, it follows from [19, VII.5.4] that $N_{K/k}(\mathrm{Cond}_K(E_K)) = \mathcal{O}_k$. Now the equality (2.5) becomes

$$(d_{K/k})^2 = \mathrm{Cond}_k(E_k)\,.$$

Substituting this into (2.4), we obtin (2.3). □

The conductor of an elliptic curve can be computed by Tate's algorithm ([20, IV.9]). Therefore by the above proposition, we can calculate $N_{k/\mathbf{Q}}(d_{K/k})$. We thus have the absolute discriminant d_K of K modulo the sign from the relation $|d_K| = |N_{k/\mathbf{Q}}(d_{K/k}) \cdot d_k^2|$.

Step 3: The problem of finding appropriate quartic twists is now reduced to the problem of finding quartic fields with given discriminant. We can carry out this procedure by the following proposition.

PROPOSITION 2.2 (Buchmann, Ford, Pohst). *Let K be a quartic field over $\mathbf{Q}$ with a quadratic intermediate field k. Denote by $\omega = \frac{\sigma+\sqrt{d_k}}{2}$ an integral base of k where we take $\sigma \in \{0, 1\}$ so that $\sigma \equiv d_k \pmod 4$. Then we can take a generator of K whose minimal polynomial*

$$x^2 - \alpha x + \beta \in \mathcal{O}_k[x]\,, \quad (\alpha = a_1 + a_2\omega, \beta = b_1 + b_2\omega)$$

overe k satisfies the following inequalities:

$$a_1 \in \{0, 1\}\,, \quad a_2 \in \{0, 1, 2, 3\}\,,$$

$$\frac{A_2 - \sqrt{2}M}{4} \le b_2 \le \frac{A_2 + M}{4}\,,$$

$$\frac{1}{16}(A_1 - 8b_2\sigma - \sqrt{2}N) \le b_1 \le \frac{1}{16}(A_1 - 8b_2\sigma + \sqrt{2}N)\,,$$

where A_1, A_2, M and N are defined as follows:

$$A_1 = 4a_1^2 + 4a_1a_2\sigma + a_2^2(d_k + \sigma)\,, \quad A_2 = a_2(2a_1 + a_2\sigma)\,,$$

$$M = \left\lfloor 2\sqrt{\frac{|d_K|}{3|d_k|^2}} \right\rfloor\,, \quad N = \left\lfloor 4\sqrt{\frac{|d_K|}{3|d_k|}} \right\rfloor\,.$$

PROOF. This proposition is a consequence of [1, Proposition 2.25], [10, Proposition 4.1] and [2, Proposition 3]. □

Of course, two different polynomials may generate isomorphic fields. We can find such field isomorphisms by an algorithm described in Cohen's textbook ([3, Section 4.5.4]). In this way, the redundant polynomials are eliminated.

Step 4: Again by Tate's algorithm, we compute the conductor of E_A^u over k for each $K = k(\sqrt{u})$ obtained in the preceding step and check if the conductor $\mathrm{Cond}_k(E_A^u)$ is trivial or not to determine which curves have good reduction.

2.2. The case where j is quadratic. If j is a quadratic integer, our algorithm is as follows.

ALGORITHM 2.
Input: A quadratic integer j.
Output: All elliptic curves having good reduction with given j-invariant.

Step 1: Let $E(j)$ be a plane curve defined by

$$y^2 = x^3 - 3j(j-1728)x - 2j(j-1728)^2 . \tag{2.6}$$

This curve is an elliptic curve if $j \neq 0, 1728$. Then the modular invariant of $E(j)$ is j and its discriminant is $2^{12} \cdot 3^6 \cdot j^2(j-1728)^3$.

Step 2: We have to find quadratic twists of $E(j)$. By the same argument as in the proof of Proposition 2.1, we can derive the next proposition.

PROPOSITION 2.3. *Let $K = k(\sqrt{u})$ be a quadratic extension over $k = \mathbf{Q}(\sqrt{m})$. If the quadratic twist $E(j)^u$ corresponding to K has good reduction over k, then we have*

$$(d_{K/k})^2 = \mathrm{Cond}_k(E(j)) . \tag{2.7}$$

Again, by this proposition, we can compute the absolute discriminant d_K of K modulo the sign.

Steps 3 and 4: These steps are the same as the corresponding steps in the previous case.

REMARK 2.4. We may start with any model having the given j-invariant in Step 1 in the above algorithms. But starting with a model with smaller discriminant usually reduces the amount of computation.

We now illustrate our method by the following example.

EXAMPLE 2.5. Let $j = A^3 = 4^3$ and $k = \mathbf{Q}(\sqrt{442})$. We use Algorithm 1.

Step 1: The elliptic curve E_4 is

$$E_4 : \ y^2 = x^3 + 19968x - 5537792 .$$

Step 2: We have

$$d_k = 1768 = 2^3 \cdot 13 \cdot 17 ,$$

$$\mathrm{Cond}_{\mathbf{Q}}(E_4) = 2^8 \cdot 3^2 \cdot 13^2 , \quad \mathrm{Cond}_{\mathbf{Q}}(E_4^{442}) = 2^8 \cdot 3^2 \cdot 13^2 \cdot 17^2 .$$

Here and hereafter, we mainly used TECC ([14]) to compute conductors. Now it readily follows from (2.3) that $N_{k/\mathbf{Q}}(d_{K/k}) = \pm 2^5 \cdot 3^2 \cdot 13$, where K is a quartic field

we want to find. It yields

$$d_K = \pm 2^{11} \cdot 3^2 \cdot 13^3 \cdot 17^2 . \tag{2.8}$$

Step 3: In the present case, the constants in Proposition 2.2 are

$$M = 70, \quad N = 5941 .$$

As a result, we find 40 polynomials which generate number fields with the given discriminant (2.8) and they are divided into 8 isomorphism classes. A set of representatives is

$$\begin{aligned} &x^4 + 156x^2 + 2106, && x^4 + 312x^2 + 8424, && x^4 + 312x^2 - 11466, \\ &x^4 + 312x^2 - 170586, && x^4 + 624x^2 - 2106, && x^4 - 156x^2 + 2106, \\ &x^4 - 312x^2 + 8424, && x^4 - 312x^2 - 11466. \end{aligned}$$

Step 4: Computing the conductors of the corresponding quartic twists, we find that the following two polynomials give the twisted curves having good reduction:

$$\begin{aligned} &x^4 - 156x^2 + 2106, && \pm\sqrt{78 \pm 3\sqrt{442}}, \\ &x^4 - 312x^2 + 8424, && \pm\sqrt{156 \pm 6\sqrt{442}}, \end{aligned}$$

where the numbers on the right are the roots of the polynomials on the left. The Galois group of each polynomial is isomorphic to the dihedral group D_4 of order 8, hence, in particular, the extension $K/\mathbf{Q}$ is not Galois. As a consequence, two isomorphism classes result from each polynomial:

$$\begin{aligned} C_1 &= E_4^{(78+3\sqrt{442})}, \quad C_2 = C_1^{\sigma} = E_4^{(78-3\sqrt{442})}, \\ C_3 &= E_4^{(156+6\sqrt{442})}, \quad C_4 = C_3^{\sigma} = E_4^{(156-6\sqrt{442})}. \end{aligned}$$

Here σ is the generator of $\mathrm{Gal}(k/\mathbf{Q})$.

The explicit equations can be calculated by the formula (1.1):

$$\begin{aligned} C_1 : y^2 =& x^3 + (200918016 + 9345024\sqrt{442})x - 7782835027968 \\ &- 369315348480\sqrt{442}, \\ C_2 : y^2 =& x^3 + (200918016 - 9345024\sqrt{442})x - 7782835027968 \\ &+ 369315348480\sqrt{442}, \\ C_3 : y^2 =& x^3 + (803672064 + 37380096\sqrt{442})x - 62262680223744 \\ &- 2954522787840\sqrt{442}, \\ C_4 : y^2 =& x^3 + (803672064 - 37380096\sqrt{442})x - 62262680223744 \\ &+ 2954522787840\sqrt{442}. \end{aligned}$$

Consequently, these four curves are all the elliptic curves having good reduction over $\mathbf{Q}(\sqrt{442})$ with j-invariant 4^3.

REMARK 2.6 In general, we need a lot of time to find the candidates for the quartic fields in the third step, since the constants M and N are sometimes large.

For this reason, we propose the following alternative. Let us write $K = k(\sqrt{u})$ with $u \in k^*$. Assume that the class number of k is 1. Then we can impose some restrictions on u mod $(k^*)^2$ by the ramification theory of Kummer extension. Namely, the possible prime divisors of u are the ramifying primes (we know all of them from d_K) and the primes above 2. Checking the discriminants of the fields generated by these possible u's, we obtain candidates of polynomials in the third step.

This method sometimes works even if the class number is greater than one and it is empirically faster than the preceding method. It is thus worth trying this method first.

Professor Lemmermeyer kindly pointed out to the author that recent results on computing ray class fields (see [4]) may be used for our purpose.

3. Counting the number of curves having good reduction.

Once we find an elliptic curve having good reduction for a given j-invariant, it is natural to ask how many isomorphism classes over k there are. The answer to the question is provided by the following more or less known proposition.

In what follows, by an unramified extension of an algebraic number field, we mean an unramified extension in the *narrow* sense, namely an extension unramified outside the archimedean primes.

PROPOSITION 3.1. *Let K be an algebraic number field and E an elliptic curve defined over K having good reduction. Then every quadratic twist of E having good reduction is a twist of E by an unramified quadratic extension over K, and vice versa.*

We include a proof of this proposition for completeness.

PROOF. Let E^u be a quadratic twist of E having good reduction. Set $L = K(\sqrt{u})$. Using [19, VII.5.4] again, we have

$$N_{L/K}(\mathrm{Cond}_L(E_L)) = \mathcal{O}_K .$$

It immediately follows from Proposition 1.1 that $d_{L/K} = \mathcal{O}_K$. This shows that L/K is an unramified extension.

Conversely, assume $L = K(\sqrt{u})$ is an unramified quadratic extension of K. We shall show that the conductor of an elliptic curve remains unchanged under the unramified quadratic twist by u. Let $\mathcal{D}(E/K)$ (resp. $\mathcal{D}(E^u/K)$) be the minimal discriminant (for the definition, see [19, p. 224]) of E/K (resp. E^u/K). By Ogg's formula ([20, IV.11]), we have, for each discrete valuation v of K,

$$v(\mathrm{Cond}_K(E)) = v(\mathcal{D}(E/K)) + 1 - m_v ,$$
$$v(\mathrm{Cond}_K(E^u)) = v(\mathcal{D}(E^u/K)) + 1 - m_v^u ,$$

where m_v (resp. m_v^u) is the number of irreducible components counted without multiplicity on the special fiber of the minimal proper regular model of E (resp. E^u) at v. Subtracting the first equality from the second one, we obtain

$$v(\mathrm{Cond}_K(E^u)) - v(\mathrm{Cond}_K(E)) = v(\mathcal{D}(E^u/K)) - v(\mathcal{D}(E/K)) - m_v^u + m_v\,. \tag{3.1}$$

Now we need a result due to Silverman.

PROPOSITION 3.2 (Silverman [18, Theorem 3]). *Let E be an elliptic curve defined over K and $L = K(\sqrt{u})$ a quadratic extension of K. Assume that L/K is unramified at all primes of K lying above 2 and at all primes for which E has bad reduction. Then*

$$\mathcal{D}(E^u/K) = \mathcal{D}(E/K)(d_{L/K})^6\,. \tag{3.2}$$

REMARK 3.3. Silverman proved the above theorem using somewhat finer invariants than the usual minimal discriminants and the usual field discriminants. A generalization of the formula (3.2) is obtained by Comalada [6].

We return to the proof of Proposition 3.1. Since E has good reduction and L/K is unramified, the assumptions in the preceding proposition are satisfied. Taking the valuations of (3.2) and substituting it into (3.1), we get

$$v(\mathrm{Cond}_K(E^u)) - v(\mathrm{Cond}_K(E)) = 6v(d_{L/K}) - m_v^u + m_v\,.$$

On the other hand, it follows from our assumption that

$$v(d_{L/K}) = 0\,, \quad v(\mathrm{Cond}_K(E)) = 0\,, \quad m_v = 1\,.$$

Therefore it yields $v(\mathrm{Cond}_K(E^u)) = 1 - m_v^u$. Since $v(\mathrm{Cond}_K(E^u)) \geq 0$ and $m_v^u \geq 1$, we have $v(\mathrm{Cond}_K(E^u)) = 0$. This completes the proof of Proposition 3.1. □

Applying Proposition 3.1 to the case where K is a quadratic field, we have the following corollary.

COROLLARY 3.4. *Let E be an elliptic curve defined over a quadratic field k having good reduction. Let s denote the number of the ramifying primes in the extension $k/\mathbf{Q}$. Then the number of the twists of E having good reduction is 2^{s-1}.*

PROOF. By the genus theory (see [11]), there are exactly $2^{s-1} - 1$ unramified quadratic extensions over k. Therefore, the number of the twists is 2^{s-1} in total. □

For the case of elliptic curves having rational j-invariants, the above corollary is already proved by Setzer ([17, Theorem 2]) by a different method.

EXAMPLE 3.5. Proposition 3.1 gives an alternative method to compute the twists. Namely, if we find one twist having good reduction, then others can be found by unramified quadratic twists according to Proposition 3.1. In Example 2.5, suppose that we found C_1. There are $2^{3-1} - 1 = 3$ unramified quadratic extensions of $k = \mathbf{Q}(\sqrt{422})$. Specifically, they

are

$$\mathbf{Q}(\sqrt{26}, \sqrt{17}) = \mathbf{Q}(\sqrt{43 + 2\sqrt{442}}),$$
$$\mathbf{Q}(\sqrt{34}, \sqrt{13}) = \mathbf{Q}(\sqrt{47 + 2\sqrt{442}}),$$
$$\mathbf{Q}(\sqrt{2}, \sqrt{221}) = \mathbf{Q}(\sqrt{223 + 2\sqrt{442}}).$$

The other three curves C_2, C_3, C_4 arise as twists corresponding to these biquadratic fields. Indeed, we can verify the following isomorphisms:

$$C_1^{(43+2\sqrt{442})} \simeq C_2, \quad C_1^{(47+2\sqrt{442})} \simeq C_4, \quad C_1^{(223+2\sqrt{442})} \simeq C_3.$$

4. Computing elliptic curves having good reduction.

In this section, we apply our method developed in Section 2 to the computation of elliptic curves having good reduction over real quadratic fields.

For that purpose, we first find possible pairs of a real quadratic field k and an integer j for which there is an elliptic curve defined over k having good reduction whose j-invariant is j.

4.1. Rational j-invariants. Comalada and Nart [7] study the properties of j-invariants of elliptic curves having good reduction. We use their result to find the candidates of rational integers that appear as the j-invariants of elliptic curves having good reduction over $\mathbf{Q}(\sqrt{m})$ $(1 < m < 100)$ (see [13] for the detail).

TABLE 1. Rational j-invariants for $\mathbf{Q}(\sqrt{m})$.

m	6	7	14	22	26	37	38	65	77	79	86
j	20^3	-15^3 255^3	-15^3 255^3	20^3	4^3 -2876^3	16^3 3376^3	20^3	17^3 257^3	-15^3 255^3	39^3	20^3

In fact, as our computation below will show, all these values in Table 1 do appear. In this table, $j = -15^3, 20^3, 255^3$ are singular j-invariants. The values 255^3 and -15^3 always appear in pairs, because there is a 2-isogeny between curves having these j-invariants and the good reduction property is invariant under an isogeny ([19, VII.7.2.]).

4.2. Singular j-invariants. Next we shall find all singular j-invariants that appear as the j-invariants of elliptic curves with good reduction.

For the thirteen imaginary quadratic orders of class number one, we first check if j is a cube of a rational integer. For example, $j(\sqrt{-3}) = 5400 = 2 \cdot 30^3$ does not appear as a j-invariant of an elliptic curve having good reduction. Then we apply the results in [7] and obtain the following table (Table 2).

In the column of "Examples of m", we list all m's less than 100. If there is no m in the range, we fill in the smallest m satisfying the conditions.

TABLE 2. Orders of class number 1.

Discriminant	j	Examples of m
-7	-15^3	7, 14, 77
-8	20^3	6, 22, 38, 86
-11	-32^3	33
-19	-96^3	133
-43	-960^3	989
-67	-5280^3	1541
-163	-640320^3	7661
-28	255^3	7, 14, 77

Next we consider the orders of class number two. There are twenty-nine such orders. Let E be an elliptic curve defined over $k = \mathbf{Q}(\sqrt{m})$ with complex multiplication by an imaginary quadratic order of discriminant $-d$. We first check the necessary conditions (2.1). The following pairs satisfy the conditions.

$$(-d, m) = (-20, 5), (-32, 2), (-52, 13), (-72, 6), (-99, 33), (-112, 7).$$

We apply the following lemma to these pairs.

LEMMA 4.1. *Let E be an elliptic curve defined over a real quadratic field k with complex multiplication. Assume that E has good reduction and that $k = \mathbf{Q}(j(E))$. Let K be the quotient field of the endomorphism ring of E. If the ray class number modulo 2 of Kk is prime to 3, then E has a k-rational point of order 2.*

PROOF. Let E_2 be the kernel of the multiplication-by-2 map on E in an algebraic closure of k. Note that the absolute Galois group of k acts on E_2 through a finite quotient isomorphic to a subgroup of S_3. By the theory of complex multiplication, $Kk(E_2)/Kk$ is an abelian extension (see [20, II.5.7]). Since E has good reduction, this extension is unramified outside the prime ideals dividing 2. By the assumption on the ray class number, we have $[Kk(E_2) : Kk] \leq 2$. It yields $[k(E_2) : Kk \cap k(E_2)] \leq 2$. On the other hand, we know $[Kk \cap k(E_2) : k] \leq [Kk : k] = 2$. Since $[k(E_2) : k]$ is a divisor of 6, it follows $[k(E_2) : k] \leq 2$. This implies that there exists a k-rational point of order 2 on E. □

The ray class numbers modulo 2 of $Kk = \mathbf{Q}(\sqrt{m}, \sqrt{-d})$ for the pair $(-d, m)$ are 2, 1, 2, 2, 3 and 1, respectively in the above order. Thus, among the six pairs, only $(-d, m) = (-99, 33)$ does not satisfy the assumption on the ray class number in Lemma 4.1. For the remaining 5 pairs, any corresponding elliptic curve having good reduction must have a k-rational point of order two. In connection with this, Comalada [5] makes a list of elliptic curves with good reduction having a k-rational point of order 2 for $\mathbf{Q}(\sqrt{m})$ $(1 < m < 100)$. Checking his table, we find that the following quadratic singular j-invariants appear as a modular invariant of an elliptic curve having good reduction:

$$m = 6, \quad d = -72, \quad j(3\sqrt{-2}) = 188837384000 + 77092288000\sqrt{6}, \tag{4.1}$$

$$m = 7\,, \quad d = -112\,, \quad j(2\sqrt{-7}) = 137458661985000 + 51954490735875\sqrt{7} \tag{4.2}$$

and their Galois conjugates.

As we will see below, there exist elliptic curves having good reduction corresponding to $(-d, m) = (-99, 33)$. Thus we write down the j-value here.

$$m = 33\,, \quad d = -99\,, \quad j\left(3 \cdot \frac{1+\sqrt{-11}}{2}\right) = -18808030478336 - 3274057859072\sqrt{33} \tag{4.3}$$

4.3. Computing the twists. We now compute elliptic curves having good reduction with the j-invariants we found in the above.

Our computation results are collected in Table 3 and Table 4. A name is given to each isomorphism class of elliptic curve having good reduction.

In Table 3, the quartic twist u of E_A (see (2.2)) is given by the standard basis of the quadratic field, i.e.,

$$[a, b] = a + b\left(\frac{\sigma + \sqrt{d_k}}{2}\right) \tag{4.4}$$

where $\sigma \in \{0, 1\}$, $\sigma \equiv d_k \pmod 4$.

A curve name with over-line means the Galois conjugate. For example, the curve $6\overline{B}$ is the Galois conjugate curve of $6B$.

The quartic twist of E_A by u is given by

$$E_A^u : y^2 = x^3 - 3A(A^3 - 1728)u^2x - 2(A^3 - 1728)^2u^3\,.$$

The cyclic isogenies are noted in the manner of Cremona's book [9]. For example, the entry "**2** : $\overline{A}$, **3** : B" for the curve $6A$ indicates that $6A$ is 2-isogenous to $6\overline{A}$ and 3-isogenous to $6B$. We do *not* claim that they are all isogenies they have. It is still difficult to find all isogenous curves of an elliptic curve defined over a number field larger than $\mathbf{Q}$ in general. If all the curves having good reduction are determined, however, then we are often able to find all the isogenies among them. In the following tables, this is the case when $m = 6, 7, 14, 37$.

For $m \leq 100$, all the elliptic curves having good reduction with rational j-invariant are listed. Note that $m = 33$ is lacked in Setzer's computation in [17].

TABLE 3. Rational j-invariants.

m	$j = A^3$	name	quartic twist u	CM	Isogenies
6	20^3	$6B$	$[-14, 7]$	-8	$\mathbf{3}: A, \mathbf{2}: \overline{B}, \mathbf{3}: C$
		$6\overline{B}$	$[-14, -7]$	-8	$\mathbf{3}: \overline{A}, \mathbf{2}: B, \mathbf{3}: \overline{C}$
7	255^3	$7B$	$[1197, -456]$	-28	$\mathbf{2}: A, \mathbf{7}: \overline{B}, \mathbf{2}: C, \mathbf{2}: D$
		$7\overline{B}$	$[1197, 456]$	-28	$\mathbf{2}: \overline{A}, \mathbf{7}: B, \mathbf{2}: \overline{C}, \mathbf{2}: \overline{D}$
	-15^3	$7D$	$[-21, -8]$	-7	$\mathbf{7}: \overline{D}, \mathbf{2}: B$
		$7\overline{D}$	$[-21, 8]$	-7	$\mathbf{7}: D, \mathbf{2}: \overline{B}$
14	255^3	$14B$	$[399, -114]$	-28	$\mathbf{7}: \overline{B}, \mathbf{2}: A$
		$14\overline{B}$	$[399, 114]$	-28	$\mathbf{7}: B, \mathbf{2}: \overline{A}$
	-15^3	$14A$	$[7, -2]$	-7	$\mathbf{7}: \overline{A}, \mathbf{2}: B$
		$14\overline{A}$	$[7, 2]$	-7	$\mathbf{7}: A, \mathbf{2}: \overline{B}$
22	20^3	$22A$	$[-294, 63]$	-8	$\mathbf{2}: \overline{A}$
		$22\overline{A}$	$[-294, -63]$	-8	$\mathbf{2}: A$
26	4^3	$26A$	$[78, 15]$	N.A.	$\mathbf{5}: C$
		$26B$	$[156, 30]$	N.A.	$\mathbf{5}: D$
	-2876^3	$26C$	$[294918, 56715]$	N.A.	$\mathbf{5}: A$
		$26D$	$[589836, 113430]$	N.A.	$\mathbf{5}: B$
33	-32^3	$33A$	$[126, 56]$	-11	$\mathbf{11}: \overline{A}, \mathbf{3}: B, \mathbf{3}: C$
		$33\overline{A}$	$[-224, -168]$	-11	$\mathbf{11}: A, \mathbf{3}: \overline{B}, \mathbf{3}: \overline{C}$
37	16^3	$37A$	$[-186, -72]$	N.A.	$\mathbf{5}: B$
	3376^3	$37B$	$[749766, 290232]$	N.A.	$\mathbf{5}: A$
38	20^3	$38A$	$[-126, 21]$	-8	$\mathbf{2}: \overline{A}$
		$38\overline{A}$	$[-126, -21]$	-8	$\mathbf{2}: A$
65	17^3	$65A$	$[2688, 84]$	N.A.	$\mathbf{2}: C$
		$65B$	$[2436, 588]$	N.A.	$\mathbf{2}: D$
	257^3	$65C$	$[87381, 24528]$	N.A.	$\mathbf{2}: A$
		$65D$	$[2967888, 840084]$	N.A.	$\mathbf{2}: B$
77	255^3	$77A$	$[2736, 912]$	-28	$\mathbf{7}: \overline{A}, \mathbf{2}: B$
		$77\overline{A}$	$[3648, -912]$	-28	$\mathbf{7}: A, \mathbf{2}: \overline{B}$
	-15^3	$77B$	$[48, 16]$	-7	$\mathbf{7}: \overline{B}, \mathbf{2}: A$
		$77\overline{B}$	$[64, -16]$	-7	$\mathbf{7}: B, \mathbf{2}: \overline{A}$
79	39^3	$79A$	$[-711, 80]$	N.A.	
		$79\overline{A}$	$[-711, -80]$	N.A.	
86	20^3	$86A$	$[-2142, 231]$	-8	$\mathbf{2}: \overline{A}$
		$86\overline{A}$	$[-2142, -231]$	-8	$\mathbf{2}: A$
133	-96^3	$133A$	$[52, 10]$	-19	$\mathbf{19}: \overline{A}$
		$133\overline{A}$	$[62, -10]$	-19	$\mathbf{19}: A$
989	-960^3	$989A$	$[-45654, 2814]$	-43	$\mathbf{43}: \overline{A}$
		$989\overline{A}$	$[-42840, -2814]$	-43	$\mathbf{43}: A$
1541	-5280^3	$1541A$	$[-1982946, 98518]$	-67	$\mathbf{67}: \overline{A}$
		$1541\overline{A}$	$[-1884428, -98518]$	-67	$\mathbf{67}: A$
7661	-640320^3	$7661A$	$[11290773004896, 260976456202]$	-163	$\mathbf{163}: \overline{A}$
		$7661\overline{A}$	$[11551749461098, -260976456202]$	-163	$\mathbf{163}: A$

In Table 4, we calculate the quadratic twists with respect to the curve $E(j)$ (see (2.6)) for j's given by (4.1), (4.2) and (4.3). The twists are given by the standard basis (4.4) as before.

TABLE 4. Complex multiplication by orders of class number 2.

m	j	name	quartic twist u	CM	Isogenies
6	Equation (4.1)	$6A$	[9600500, 3894730]	-72	$\mathbf{2}: \overline{A}, \mathbf{3}: B$
		$6\overline{C}$	[-94739260, -38674650]	-72	$\mathbf{2}: C, \mathbf{3}: \overline{B}$
	Galois conjugate of (4.1)	$6\overline{A}$	[9600500, -3894730]	-72	$\mathbf{2}: A, \mathbf{3}: \overline{B}$
		$6C$	[-94739260, 38674650]	-72	$\mathbf{2}: \overline{C}, \mathbf{3}: B$
7	Equation (4.2)	$7A$	[-78687840, -29795100]	-112	$\mathbf{7}: \overline{A}, \mathbf{2}: B$
		$7\overline{C}$	[29073170, 10992680]	-112	$\mathbf{7}: C, \mathbf{2}: \overline{B}$
	Galois conjugate of (4.2)	$7\overline{A}$	[-78687840, 29795100]	-112	$\mathbf{7}: A, \mathbf{2}: \overline{B}$
		$7C$	[29073170, -10992680]	-112	$\mathbf{7}: \overline{C}, \mathbf{2}: B$
33	Equation (4.3)	$33\overline{B}$	[84455, 34447]	-99	$\mathbf{3}: \overline{A}$
		$33C$	[-248976, -75544]	-99	$\mathbf{3}: A$
	Galois conjugate of (4.3)	$33B$	[118902, -34447]	-99	$\mathbf{3}: A$
		$33\overline{C}$	[-324520, 75544]	-99	$\mathbf{3}: \overline{A}$

References

[1] J. BUCHMANN and D. FORD, On the computation of totally real quartic fields of small discriminant, Math. Comp. **52** (1989), 161–174.

[2] J. BUCHMANN, D. FORD and M. POHST, Enumeration of quartic fields of small discriminant, Math. Comp. **61** (1993), 873–879.

[3] H. COHEN, *A course in computational algebraic number theory*, Springer (1993).

[4] H. COHEN, A survey of computational class field theory, J. Théor. Nombres Bordeaux **11** (1999) 1–13, Les XXèmes Journées Arithmétiques (Limoges, 1997).

[5] S. COMALADA, Elliptic curves with trivial conductor over quadratic fields, Pacific J. Math. **144** (1990), no. 2, 237–258.

[6] S. COMALADA, Twists and reduction of an elliptic curve, J. Number Theory **49** (1994), 45–62.

[7] S. COMALADA and E. NART, Modular invariant and good reduction of elliptic curves, Math. Ann. **293** (1992), 331–342.

[8] I. CONNELL, Good reduction of elliptic curves in abelian extensions, J. Reine Angew. Math. **436** (1993), 155–175.

[9] J. E. CREMONA, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press (1997).

[10] D. FORD, *Enumeration of totally complex quartic fields of small discriminant*, Computational number theory (Debrecen, 1989), de Gruyter (1991), 129–138.

[11] M. ISHIDA, *The genus fields of algebraic number fields*, Lecture Notes in Math. **555** (1976), Springer.

[12] M. KIDA, Galois descent and twists of an abelian variety, Acta Arith. **73** (1995), 51–57.

[13] M. KIDA, Computing elliptic curves having good reduction everywhere over real quadratic fields, Proceedings of Sendai Number Theory Symposium 1997, Graduate School of Information Sciences, Tohoku University (1998), 1–22 (in Japanese).

[14] M. KIDA, *TECC manual version 2.3*, The University of Electro-Communications, March 2000.

[15] J. S. MILNE, On the arithmetic of abelian varieties, Invent. Math. **17** (1972), 177–190.

[16] J.-P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331.

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

[18] J. H. SILVERMAN, Weierstrass equations and the minimal discriminant of an elliptic curve, Mathematika **31** (1984), 245–251.

[19] J. H. SILVERMAN, *The arithmetic of elliptic curves*, Springer (1986).

[20] J. H. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves.* Springer (1994).

[21] A. UMEGAKI, A construction of everywhere good **Q**-curves with p-isogeny, Tokyo J. Math. **21** (1998), 183–200.

Present Address:
DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF ELECTRO-COMMUNICATIONS,
CHOFU, TOKYO, 182–8585 JAPAN.
e-mail: kida@sugaku.e-one.uec.ac.jp