On Elliptic Curves with Everywhere Good Reduction over Certain Number Fields

Shun’ichi Yokoyama
Faculty of Mathematics, Kyushu University, Fukuoka, Japan
Email: s-yokoyama@math.kyushu-u.ac.jp

Received September 1, 2012; revised October 21, 2012; accepted November 6, 2012

ABSTRACT

We prove the existence and nonexistence of elliptic curves having good reduction everywhere over certain real quadratic fields \( \mathbb{Q}(\sqrt{m}) \) for \( m \leq 200 \). These results of computations give best-possible data including structures of Mordell-Weil groups over some real quadratic fields via two-descent. We also prove similar results for the case of certain cubic fields. Especially, we give the first example of elliptic curve having everywhere good reduction over a pure cubic field using our method.

Keywords: Elliptic Curves over Number Fields; Mordell-Weil Group; Two-Descent

1. Introduction

Tables of elliptic curves over \( \mathbb{Q} \) have been of great value in mathematical research. In particular, some databases are very famous and useful in number theory, and Cremona’s index (classification of elliptic curves over \( \mathbb{Q} \)) becomes popular. Nowadays, modularity theorem that explains correspondence between elliptic curves and modular forms becomes one of the most important facts in number theory and arithmetic geometry.

Meanwhile, computing elliptic curves (rank of curves, Mordell-Weil groups etc.) over general number fields is still hard. There are only a few databases of such curves and these databases use Cremona-Lingham’s general algorithm over number fields. It seems ideal from the viewpoint of computational approach, and we can also observe the case of elliptic curves over cubic fields that are not totally real. However, updating of this algorithm with supplementary tables had been stopped since September 2005. In addition, though we apply this general algorithm, we have to determine many Mordell-Weil groups (=sets of rational points) and this task is the most difficult in creating databases.

Therefore, we have to find a more efficient way (reducing the number of Mordell-Weil groups that we have to determine) to achieve this project and also easy-to-read sorted tables of such curves, including information (with references) which case is already known and which case is still open.

Let \( K_m \) be the real quadratic field \( \mathbb{Q}(\sqrt{m}) \) where \( m \) is a square-free positive integer with \( m \leq 200 \) and \( O_{K_m} \) the ring of integers of \( K_m \). We already know the following results concerning elliptic curves with everywhere good reduction over certain real quadratic fields [1-16]:

Theorem 1.1.
1) There are no elliptic curves with everywhere good reduction over \( K_m \) if
   \[ m = 2, 3, 5, 10, 11, 13, 15, 17, 19, 21, 23, 30, 31, 34, 35, 39, 42, 47, 53, 55, 57, 58, 61, 66, 69, 70, 73, 74, 78, 82, 83, 85, 89, 93, 94, 95 \text{ and } 97. \]

2) The elliptic curves with everywhere good reduction over \( K_m \) are determined completely for
   \[ m = 6, 7, 14, 22, 29, 33, 37, 38, 41, 65 \text{ and } 77. \]

3) There are elliptic curves with everywhere good reduction over \( K_m \) if \( m = 26, 79 \) and 86.

We can also consider the pure cubic field case. Let \( L_m \) be the pure cubic field \( \mathbb{Q}(\sqrt[3]{m}) \) where \( m \) is cube-free, positive integer with \( m \leq 200 \) and \( O_{L_m} \) the ring of integers of \( L_m \). The first known result is given by Bertolini-Canuto [17]:

Theorem 1.2. Let \( L \) be the field \( \mathbb{Q}(\alpha) \) where \( \alpha \) is the real cube root of 2 (i.e. \( L = L_2 \)). Then there are no elliptic curves over \( L \) with good reduction everywhere.

Recently, N. Takeshi applied Bertolini-Canuto’s method and showed the following criterion in her master’s thesis.

Theorem 1.3. ([18]) Let \( L \) be the cubic field (not only
pure cubic) satisfying the following conditions:

a) 2 does not split on \( L/\mathbb{Q} \),

b) The narrow class number of \( L \) is coprime to 6.

Then there are no admissible curves over \( L = \) elliptic curves with everywhere good reduction over \( L \) which have \( L \)-rational point of order 2).

In this paper, we extend Theorem 1.1 and apply our method to determine the existence and nonexistence of elliptic curves having good reduction everywhere over certain pure cubic fields. The following two theorems are our main result:

Theorem 1.4.

1) There are no elliptic curves with everywhere good reduction over \( K_m \) if \( m = 43, 46, 59, 62, 67, 71, 103, 107, 127, 137, 139, 151 \) and 163.

2) The elliptic curves with everywhere good reduction over \( K_m \) are determined completely for \( m = 109 \).

3) There are admissible curves over \( K_m \) if \( m = 118, 134, 161 \) and 166.

4) There are no admissible curves over \( K_m \) if \( m = 131, 179 \) and 199.

5) There is an elliptic curve \( E \) with everywhere good reduction and not having \( K_m \)-rational point of order 2 if \( m = 158 \) and 161.

Theorem 1.5.

1) There are no elliptic curves with everywhere good reduction over \( L_m \) if
\[ m = 3, 5, 6, 10, 12, 17, 18, 29, 116, 137, 173 \] and 197.

2) If \( m = 23, 44, 45, 75 \) and 87, there are no admissible curves and elliptic curves with everywhere good reduction over \( L_m \) which have cubic discriminant.

3) There is an elliptic curve \( E \) with everywhere good reduction and not having \( L_m \)-rational point of order 2 over \( L_m \) if \( m = 46 \).

We would like to remark that this result is an extension of the author’s previous result [19].

2. Strategy

In this section, we introduce the strategy to prove our results. Our strategy for the proof is close to that of T. Kagawa [7]. However, we use different kinds of computer softwares and computational techniques.

Important processes of our result are the following: At first, we divide all elliptic curves having everywhere good reduction into two types. One is “admissible case”, and the other is “nonadmissible case”. Next we consider some criteria of S. Comalada to determine whether admissible curves exist or not (Section 2.1). After that, we observe (non)existence of all nonadmissible curves using some criteria from algebraic number theory (Section 2.2). Using this method, we can get the list of important invariants having constraint condition, and this condition can be expressed using certain elliptic curves over \( K_m \) or \( L_m \). Finally, we directly compute Mordell-Weil groups of specific elliptic curves (Section 2.3). Explicit data are given from Section 2.4 to 2.6. We note that easy-to-read sorted tables will be given in Chapter 3.

2.1. For the Case of Admissible Curves

First of all, S. Comalada [20] determines all admissible curves defined over \( K_m \) with \( m \leq 100 \). Comalada also gives some criteria to find admissible curves over \( K_m \) for an arbitrary \( m \).

Definition 2.1. An elliptic curve defined over \( K_m \) is called g-admissible if it is admissible and has a global minimal model.

Proposition 2.2. The following two conditions are equivalent:

1) There exists a g-admissible elliptic curve over \( K_m \).

2) \( m = 1023 \) or either of these sets of diophantine equations has a solution:

a) \( x^2 - 4my^2 = -7 \), \( 7 \mid m \),

b) \( x^2 - 4my^2 = 65 \), \( 65 \mid m \),

c) \( x^2 - my^2 = -2 \), \( m = -2 \mod 8 \),

d) \( x^2 - my^2 = -8 \) and \( r^2 - ms^2 = \pm 256 \), \( r \) is odd, \( m = 1 \mod 8 \),

e) \( r^2 - ms^2 = -16384 \) and \( r^2 - mw^2 = 8r \), \( r = 3 \mod 4 \), \( (t, r) = 1 \), \( 128w = st \mod r \), \( m = 1 \mod 8 \).

Thus we can find some admissible curves appearing Theorem 1.4 using Comalada’s method.

2.2. For the Case of Nonadmissible Curves

Next we assume that a number field \( K \) is \( K_m \) or \( L_m \). We also assume that the class number of \( K \) is 1 and every elliptic curve \( E \) with everywhere good reduction over \( K \) has no \( K \)-rational point of order 2. For our convenience, we say “nonadmissible” if \( E \) has everywhere good reduction over \( K \) with no \( K \)-rational point of order 2. First we use the following result:

Proposition 2.3. ([21]) Let \( E \) be an elliptic curve over a number field \( K \). If the class number of \( K \) is prime to 6 then \( E \) has a global minimal model.

Let \( E \) be an elliptic curve with everywhere good reduction over a number field \( K \). By Proposition 2.3, \( E \) has a global minimal model

\[ E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \]

with coefficients \( a_i \in O_K \ (i = 1, 2, 3, 4, 6) \).

The discriminant of \( E \) (denoted by \( \Delta(E) \)) is

\[ \Delta(E) = \frac{c_4^3 - c_6}{1728} \]
where \( c_1, c_6 \in \mathcal{O}_K \) are, as in [22] (Chapter III, p. 42), written as polynomials in the \( a_i \)'s with integer coefficients. Moreover, the following conditions are equivalent (cf. [22], Chapter VII, Prop. 5.1):

1) \( E \) has everywhere good reduction over \( K \), 
2) \( \Delta(E) \in \mathcal{O}_K^* \).

In our case, all elements of \( \mathcal{O}_K^* \) are written in the form \( \pm \epsilon^m \) where \( \epsilon \) is a fundamental unit of \( K \) (let us fix \( \epsilon \) for each \( m \)). Thus to determine the elliptic curves with everywhere good reduction over \( K \), we shall compute the sets

\[
E_n^\pm(\mathcal{O}_K) = \{(x,y) \in \mathcal{O}_K \times \mathcal{O}_K \mid y^2 = x^3 \pm 1728\epsilon^m \} \quad (0 \leq n < 12).
\]

However, the set of coefficients \((a_1, a_2, a_3, a_4, a_6) \in \mathcal{O}_K^{25} \), which gives rise to \((c_1, c_6) \in \mathcal{O}_K^{25} \), does not necessarily exist. Therefore, we check whether the curve

\[
E_{c} : y^2 = x^3 - 27c_4x - 54c_6,
\]

which is isomorphic to \( E \) over \( K \), has trivial conductor for each \((c_1, c_6) \in E_n^\pm(\mathcal{O}_K) \).

Actually, it is very hard to compute all \( E_n^\pm(\mathcal{O}_K) \) because of the limitation of efficiency of equipments. To reduce the amount of computation, we show that some values of \( n \) are irrelevant by using Kagawa’s results. Before that, we can easily reduce for the cases of \( 6 \leq n < 12 \) because the map

\[
E_n^\pm(\mathcal{O}_K) \to E_{n+6}(\mathcal{O}_K), (x,y) \mapsto (x\epsilon^3, y\epsilon^3)
\]

is a bijection. Hence, we observe \( E_n^\pm(\mathcal{O}_K) \) only for \( 0 \leq n < 6 \).

In [7], Kagawa shows a criterion whether the discriminant of an elliptic curve with everywhere good reduction over \( K \) is a cube in \( K \):

Lemma 2.4. If the following five conditions hold, then the discriminant of every elliptic curve with everywhere good reduction over \( K \) is a cube in \( K \):

1) The class number of \( K \) is prime to 6;
2) \( K/\mathbb{Q} \) is unramified at 3; 
3) The class number of \( K(\sqrt{-3}) \) is prime to 3;
4) The class number of \( K(\sqrt[3]{3}) \) is odd;
5) For some prime ideal \( P \) of \( K \), dividing 3, the congruence \( x^3 \equiv \epsilon \mod{P^2} \) does not have a solution in \( \mathcal{O}_K \).

Using the criterion, Kagawa shows the following:

Lemma 2.5. ([23]) If \( m = 107, 127, 161, 166 \) or 193, every elliptic curve with everywhere good reduction over \( K \) has a global minimal model whose discriminant is a cube in \( K \).

Therefore, we have \( \Delta(E) = \pm \epsilon^{3n} \) for some \( n \in \mathbb{Z} \). 

By applying the next lemma, we can further discard some cases:

Lemma 2.6. ([7]) Let \( K \) be a number field and \( E \) an elliptic curve defined over \( K \). If \( E \) has good reduction outside 2 and has no \( K \)-rational point of order 2, then \( K[\{E[2]\}] / K(\sqrt{\Delta(E)}) \) is a cyclic cubic extension unramified outside 2. In particular, the ray class number of \( K(\sqrt{\Delta(E)}) \) modulo \( \mathfrak{m} = \prod_{P} P \) is a multiple of 3.

Note that \( K(\sqrt{-1}) \) or \( K(\sqrt{\pm \epsilon}) \). Thus we compute the ray class number of \( K(\sqrt{\Delta(E)}) \) modulo \( \mathfrak{m} \). The following computations in Tables 1 and 2 are carried out by using Pari/GP [24] (Same type results were obtained in [25] by using KASH [26]). The bold-faced numbers in this table are the ones divisible by 3.

Remark 2.7. Using Lemma 2.6 with some arguments, we conclude that if the class number of \( K \) is 2 and the ray class numbers of \( K(\sqrt{-1}) \) and \( K(\sqrt{\pm \epsilon}) \) are

<table>
<thead>
<tr>
<th>( m )</th>
<th>( K(\sqrt{-1}) )</th>
<th>( K(\sqrt{\epsilon}) )</th>
<th>( K(\sqrt{-\epsilon}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>3</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>46</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>59</td>
<td>9</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>62</td>
<td>8</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>67</td>
<td>3</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>71</td>
<td>7</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>103</td>
<td>5</td>
<td>1</td>
<td>20</td>
</tr>
<tr>
<td>107</td>
<td>9</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>109</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>127</td>
<td>5</td>
<td>3</td>
<td>16</td>
</tr>
<tr>
<td>131</td>
<td>15</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>137</td>
<td>4</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>139</td>
<td>9</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>151</td>
<td>7</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>161</td>
<td>8</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>163</td>
<td>3</td>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>179</td>
<td>15</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>193</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>199</td>
<td>9</td>
<td>20</td>
<td>1</td>
</tr>
</tbody>
</table>
all prime to 3 then each elliptic curve with everywhere good reduction over $K$ is admissible (See [25], Cor. 2.3). In this way, we compute them for $K_m$ with $m = 118$, $134$, $158$, $166$ and we conclude that the it cannot be determined for these 4 cases whether there is an elliptic curve with everywhere good reduction over $K_m$ which have no $K_m$-rational point of order 2. Meanwhile, we can show the (non)existence of an admissible curve (see the next section).

For example, the case of $m = 46$, we can conclude that $K_m\left(\sqrt{\Delta(E)}\right) = K_m\left(\sqrt{-e}\right)$ thus the discriminant has the form $\Delta(E) = -e^{2k+1}$ ($k \in \mathbb{Z}_{\geq 0}$). Hence we should determine three sets of integral points $E^+_m\left(O_{K_m}\right)$, $E^+_1\left(O_{K_m}\right)$ and $E^+_1\left(O_{K_m}\right)$.

### 2.3. Computing Mordell-Weil Basis and Integral Points

To compute $E^+_m\left(O_K\right)$, we first compute the Mordell-Weil group $E^+_m\left(K\right)$

$E^+_m\left(K\right) = \left\{(x, y) \in K \times K \left| y^2 = x^3 + 1728e^x\right| (0 \leq n < 6)\right\}.$

It is decomposed into a direct-sum of $E^+_m\left(K\right)_{\text{tors}}$ (torsion part) and $E^+_m\left(K\right)_{\text{free}} = \mathbb{Z}^{2r}$ (free part, which is not canonical, with $r \geq 0$). The torsion part can be determined by observing reduction at good primes and decomposition of division polynomials. On the other hand, the free part can be computed by applying two-descent and infinite descent (the process of decompression from $E^*_m(K)/2E^*_m(K)$ to $E^*_1(K)$). We used Denis Simon’s two-descent program (cf. [27]) on Pari-GP. To compute some related data efficiently, we executed the Pari-GP program on Sage [28] as a built-in software. We also use Magma [29] for verification.

The procedure of explicit computation of $E(K)$ is the following:

1) Determine $p_1, \ldots, p_r$ whose images in $E(K)/E(K)_{\text{tors}}$ generate a subgroup of finite index of $E(K)/E(K)_{\text{tors}}$. Usually, these are obtained by performing an $m$-descent for some $m \geq 2$, especially we often choose $m = 2$.

2) Compute an upper bound on the index: $\left[E(K)/E(K)_{\text{tors}} : \langle p_1, \ldots, p_r \rangle\right]$.

3) A sieving procedure (See [30], Section 4) is then used to deduce a Mordell-Weil basis for $E(K)$.

We certainly wish to have an upper bound for $\left[E(K)/E(K)_{\text{tors}} : \langle p_1, \ldots, p_r \rangle\right]$ as small as possible. In particular, $p_1, \ldots, p_r$ will certainly be a Mordell-Weil basis of $E(K)$ if the value is equal to 1.

To compute the subset $E^+_m\left(O_K\right)$ of integral points in $E^+_m\left(K\right)$, we use the method of elliptic logarithm to compute the linear form: $L = \sum_{i=1}^{r} m_i p_i + n T \in E^+_m\left(O_K\right)$ ($m_i, \ldots, m_r, n \in \mathbb{Z}$) where $p_i$‘s and $T$ are generators of the free part and the torsion part. Moreover, the maximum of the absolute values of the coefficients of the linear form $M = \max \left|\left|m_1, \ldots, m_r, n\right|\right|$ can be bounded using the LLL-algorithm (by Lenstra-Lenstra-Lovasz, cf. [31]).

Finally, we compute that the elliptic curve $E^+_C: y^2 = x^3 - 27c_4x - 54c_6$ has trivial conductor.

### 2.4. Computation I: Admissible Curves for Real Quadratic Case

First we prove the (non)existence of $g$-admissible curves: Proposition 2.8.

1) There are no $g$-admissible curves over $K_m$ if $m = 103, 107, 109, 127, 131, 137, 139, 151, 158, 163, 179, and 199.

2) There are $g$-admissible curves over $K_m$ if $m = 118, 134, 161$ and 166.

Proof. For all $m$‘s appearing in 1), the third equivalent conditions a)-e) of Proposition 2.2 does not be satisfied.
For $m = 118, 134$ and $166$, we can find a solution of 2)-c) of Prop. 2.2. The equation has the form
\[ x^2 - my^2 = -2 \]
and we can get the following solutions:

- (Case $m = 118$) $554^2 - 118 \cdot 51^2 = -2$,
- (Case $m = 134$) $382^2 - 134 \cdot 33^2 = -2$,
- (Case $m = 166$) $41242^2 - 166 \cdot 3201^2 = -2$.

For $m = 161$, we can find a solution of 2)-a) of Prop. 2.2. The equation has the form
\[ x^2 - 4my^2 = -7 \]
and we can get the following solution
\[ 203^2 - 4 \cdot 161 \cdot 8^2 = -7 . \]

Remark 2.9. In fact, [20] proved that the number of g-admissible elliptic curves over $K_m$ (up to isomorphism) for $m = 118, 134, 166$ is $2$ if
\[ x^2 - my^2 = -2 \]
is solvable and $m \neq 6$. Thus we conclude that the number of admissible elliptic curves over $K_m$ for $m = 118, 134, 166$ is greater than or equal to $2$. Note that it is not true in general that all admissible curves defined over $K_m$ are g-admissible. However, assume the class number of $K_m$ is odd, it is true except some cases.

2.5. Computation II: Nonadmissible Curves for Real Quadratic Case

Proposition 2.10. If $m = 43, 46, 59, 62, 67, 71, 107, 127, 139, 151$ and $163$, there are no elliptic curves with everywhere good reduction over $K_m$.

Proof. We compute Mordell-Weil bases and the sets of integral points for each of the 11 cases using method appearing in Section 2.3. In this paper, we omit data of bases of $E^+_m(K_m)$ and the sets of integral points to avoid being intricate. A complete data are available from the author’s website:

http://www2.math.kyushu-u.ac.jp/~s-yokoyama/ECTable.html (*).

As a result, there are no pairs $(c_4, c_6) \in E^+_m(O_{K_m})$ for which the elliptic curve $E_C$ has trivial conductor.

For the case $m = 109$, we can find $(c_4, c_6)$ (that gives the elliptic curve with everywhere good reduction appearing in Theorem 1.4) from $E^+_4(O_{K_{109}})$.

Proposition 2.11. The elliptic curves with everywhere good reduction over $K_m$ are determined completely for $m = 109$.

Proof. First, we compute Mordell-Weil bases:

1) $E^+_4(K_{109}) = \mathbb{Z}/2\mathbb{Z}$; basis is \{ $T_{109}$ \} \{ $T_{109} = (-12, 0)$ \}.

2) $E^+_4(K_{109}) = \mathbb{Z}[\sqrt{2}]$; basis is \{ $p_{109, 4}$ \} \{ $p_{109, 9}$ \} where
\[
\begin{align*}
p_{109, 4} &= (-5688/25 - (544/25)\sqrt{109}, \\
&\quad -307444/125 - (29452/125)\sqrt{109}), \\\np_{109, 9} &= (3026/9 + (290/9)\sqrt{109}, \\
&\quad -277340/27 - (26564/27)\sqrt{109}).
\end{align*}
\]

3) $E^+_4(K_{109}) = \mathbb{Z}[\sqrt{2}]$; basis is \{ $p_{109C, p_{109D}}$ \} where
\[
\begin{align*}p_{109C} &= (-5596 - 536\sqrt{109}, -1286204 - 123196\sqrt{109}), \\
p_{109D} &= (916346/81 + (87770/81)\sqrt{109}, \\
&\quad 1613792380/729 - (154573276/729)\sqrt{109}).
\end{align*}
\]

The sets of integral points are

1) $E^+_4(O_{K_{109}}) = \{O, T_{109}\}$,

2) $E^+_4(O_{K_{109}}) = \{O, \pm p_{109A} \pm p_{109B}, \pm 2p_{109A} \pm 2p_{109B}\}$,

3) $E^+_4(O_{K_{109}}) = \{O, \pm p_{109C}, \pm 2p_{109C}, \pm 3p_{109C} \pm p_{109D}\}$.

From $2p_{109C}$ in $E^+_4(O_{K_{109}})$, we can construct the elliptic curve having everywhere good reduction over $K_{109}$ as follows:

\[
y^2 + 1 + \sqrt{109} y x y = x^3 - 3 + \sqrt{109} x^2 - (274 + 29\sqrt{109}) x - (3259 + 315\sqrt{109}).
\]

According to [16], there are no elliptic curves having good reduction everywhere and no $K_{109}$-rational point of order $2$ (= non-admissible) except the above up to isogenies.

For the case $m = 158$, the class number of $K_m$ is $2$ so our strategy cannot apply. However, we can find one elliptic curve with everywhere good reduction over $K_m$ with computing $E^+_4(O_{K_{118}})$.

Proposition 2.12. There is an elliptic curve $E$ having everywhere good reduction over $K_{158}$. $E$ is given by

\[
y^2 + xy + \sqrt{158} y = x^3 - x^2 + \left(A + B\sqrt{158}\right) x + \left(C + D\sqrt{158}\right)
\]

where
\[
\begin{align*}A &= -361817559192191668851, \\
B &= -28784659475803145415, \\
C &= 3691288333191863812738417681108, \\
D &= 293663132146367649175848062813.
\end{align*}
\]

For the case $m = 161$, we can find $(c_4, c_6)$ (that gives the elliptic curve with everywhere good reduction
appearing in Theorem 1.4) from $E_5\left(\mathbb{Q}_{16}\right)$.

Proposition 2.13. There is an elliptic curve $E$ having everywhere good reduction over $\mathbb{K}_{161}$. $E$ is given by

\[ y^2 + xy + y = x^3 - x^2 + \left(-3680 + 290\sqrt{161}\right)x + (-148482 + 11702\sqrt{161}). \]

2.6. Computation III: Nonadmissible Curves for Pure Cubic Case

Proposition 2.14. If $m = 23, 44, 75$ and 87, there are no elliptic curves with everywhere good reduction over $\mathbb{K}_m$ which have no $L_m$-rational point of order 2 (not admissible) and cubic discriminant.

Proof. In this case, it is enough to determine

\[ E_0^m\left(\mathbb{Q}_{25}\right), E_0^m\left(\mathbb{Q}_{44}\right), E_5^m\left(\mathbb{Q}_{45}\right), E_5^m\left(\mathbb{Q}_{75}\right), E_5^m\left(\mathbb{Q}_{85}\right). \]

The result of computing Mordell-Weil bases and the sets of integral points is available from the online data (*). As a result, there are no pairs $(c_5, c_6) \in E_5^m\left(\mathbb{Q}_{16}\right)$ for which the elliptic curve $E_5$ has trivial conductor.

Finally, to complete the proof of Theorem 1.5, we show the existence of an elliptic curve having everywhere good reduction over $\mathbb{K}_{46}$. We can find $(c_5, c_6)$ from $E_5^m\left(\mathbb{Q}_{16}\right)$.

Proposition 2.15. The elliptic curve $E$ as follows is having everywhere good reduction and not admissible over $\mathbb{K}_{46}$:

\begin{align*}
 y^2 + \sqrt[3]{46}xy + 1/3 &\left(\sqrt[3]{46}^2 + \sqrt[3]{46} + 1\right)y \\
 = x^3 + \left(\sqrt[3]{46} + 1\right)x^2 + C_1\sqrt[3]{46} + C_2 + C_3 &\sqrt[3]{46} + C_4x \\
 + C_5\sqrt[3]{46}^2 + C_6 &\sqrt[3]{46} + C_7
\end{align*}

where $C_i$’s $(1 \leq k \leq 6)$ are as follows:

\begin{align*}
 C_1 &= 94219593757433390681493864706,  \\
 C_2 &= 1018334709186632184731947617604,  \\
 C_3 &= 50840870355438304371288050119,  \\
 C_4 &= 23258423344479295079473275474986025640457867,  \\
 C_5 &= 82789211646292666750494613377875990377913857,  \\
 C_6 &= 326497412111533344905526205920140164426686175.
\end{align*}

Proof. We can easily compute the discriminant of the curve and the result is

\[ \Delta(E) = -\varepsilon^{24} \]

where $\varepsilon = 309\sqrt{46}^2 + 48\sqrt{46} - 4139$ is a fundamental unit of $\mathbb{K}_{46}$.

3. Tables

We give Tables 3 and 4 showing the existence or nonexistence of elliptic curves with everywhere good reduction defined over certain number fields. We note that DET = Determined, NEX = Nonexistence, PEX = Partly existence, PNEX = Partly nonexistence, UNDET = Undetermined, and $a$ is a generator of each base field, given by Magma’s setup “$\mathbb{K}<a>$: = Number Field ($f$);” where $f$ is defining polynomial of $\mathbb{K}$.

We remark that precise version of the following tables are available from the author’s website (*). These contain data of fundamental units and references.

4. Conclusion

In this paper we proved the (non)existence of elliptic curves having everywhere good reduction over certain real quadratic fields for 14 cases and partly determined the (non)existence for 9 cases. We also proved such results over certain pure cubic fields for 12 cases and partially proved for 6 cases.
Table 4. The case of pure cubic fields $L_m$.

<table>
<thead>
<tr>
<th>$m$</th>
<th>Admissible</th>
<th>Non-admissible</th>
<th>Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m \in T'$</td>
<td>No</td>
<td>No</td>
<td>NEX</td>
</tr>
<tr>
<td>$m \in T_1'$</td>
<td>No</td>
<td></td>
<td>PNX/UNDET</td>
</tr>
<tr>
<td>46</td>
<td>No</td>
<td>Yes</td>
<td>PEX/UNDET</td>
</tr>
<tr>
<td>107</td>
<td></td>
<td></td>
<td>UNDET</td>
</tr>
</tbody>
</table>

where $T' = \{2, 3, 5, 6, 10, 12, 17, 18, 29, 116, 137, 173, 197\}$ ,

$T_1' = \{23, 33, 41, 44, 45, 53, 55, 59, 69, 71, 75, 82, 87, 99, 145, 167, 177, 179, 188\}$ .

It seems extremely difficult to extend these results using same approach because of some limitations of computational tools and equipments. To improve these results, we need to discover efficient algorithms or new mathematical tools.

5. Acknowledgements

The author likes to express his gratitude to Takaaki Kagawa, Masanari Kida and Yuichiro Taguchi who guided him to the theory of elliptic curves. Their advice during the preparation of his papers on elliptic curves was very helpful.

The author would like to thank John Cremona and Denis Simon for making their programs available to him and for initially guiding him through the intricacies of the codes. He also would like to thank Iwao Kimura, Kazuo Matsuno, Yu Shimasaki and Yukihiro Uchida who gave him some useful advice and information.

This work was supported by Grant-in-Aid for JSPS fellows.

REFERENCES


