MATHEMATICS OF COMPUTATION
Volume 68, Number 228, Pages 1679–1685
S 0025-5718(99)01129-1
Article electronically published on May 21, 1999

REDUCTION OF ELLIPTIC CURVES OVER CERTAIN REAL QUADRATIC NUMBER FIELDS

MASANARI KIDA

Abstract. The main result of this paper is that an elliptic curve having good reduction everywhere over a real quadratic field has a 2-rational point under certain hypotheses (primarily on class numbers of related fields). It extends the earlier case in which no ramification at 2 is allowed. Small fields satisfying the hypotheses are then found, and in four cases the non-existence of such elliptic curves can be shown, while in three others all such curves have been classified.

Introduction

From a modular point of view, it is obvious that there is no elliptic curve having good reduction at every finite place over the field $\mathbb{Q}$ of the rational numbers.

In our previous paper [4], we obtained a similar non-existence theorem for some quadratic fields in which 2 does not ramify. For example, we proved the non-existence of such elliptic curves over $\mathbb{Q}(\sqrt{17})$ and $\mathbb{Q}(\sqrt{21})$.

In this paper, we shall show a similar result in the case of quadratic fields admitting ramification at 2. To be precise, one of our consequences is:

Theorem. *There is no elliptic curve having good reduction everywhere over the following real quadratic fields:*

$$\mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{47}),\ \mathbb{Q}(\sqrt{94}).$$

In all subsequent sections, we use the following terminology for the sake of brevity. An elliptic curve defined over a number field F is said to have *good reduction* if it has good reduction at *every* finite prime of the ring of integers of F. 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 two sections. In the first section, we study a property of rational 2-torsion points on such elliptic curves, and in the second section, we give a proof of the above theorem.

1. Points of order 2

In this section, we shall prove the following theorem, which is a refinement of a result due to Bertolini and Canuto ([1], Proposition 1) for quadratic fields.

Received by the editor January 31, 1997 and, in revised form, January 2, 1998.

1991 *Mathematics Subject Classification.* Primary 11G05.

This research was supported in part by a Grant-in-Aid for Scientific Research from the Ministry of Education, Science, Sports and Culture, Japan.

Theorem 1. *Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field, with m a square-free integer that is not congruent to 1 modulo 4. We denote by ε a fundamental unit of k and by $\mathfrak{p}$ the prime ideal of k lying above 2.*

Suppose that the real quadratic field k satisfies the following assumptions:

1. *The class number of k is prime to 6.*
2. *The prime ideal $\mathfrak{p}$ is principal. Let π be a generator of $\mathfrak{p}$.*
3. *The class numbers of the following fields are all prime to 3:*
$$k(\sqrt{-1}),\ k(\sqrt{\varepsilon}),\ k(\sqrt{-\varepsilon}),\ k(\sqrt{\pi}),\ k(\sqrt{-\pi}),\ k(\sqrt{\varepsilon\pi}),\ k(\sqrt{-\varepsilon\pi}).$$
4. *If the prime ideal $\mathfrak{p}$ is inert in the genus field $\widetilde{k}$ of k, then the ray class number of $\widetilde{k}$ modulo $\mathfrak{p}$ is prime to 3.*

Then every elliptic curve defined over k having good reduction outside 2 has a k-rational point of order 2.

Proof. Let E be an elliptic curve defined over the field k that has good reduction outside 2, and E_2 the kernel of the multiplication-by-2 map in an algebraic closure of k. We set $L = k(E_2)$.

Suppose that E has no k-rational point of order 2. Then there is an intermediate field K between L and k such that the extension L/K is a cyclic extension of degree 3. Now it follows from the reduction property of E that L/k is unramified outside 2. Thus, in particular, K/k is an unramified extension outside 2 whose extension degree is at most 2.

On the basis of the above observation, we can impose a restriction on the candidates for K by an elementary argument of the ramification theory of Kummer extensions. Write $K = k(\sqrt{\alpha})$ with $\alpha \in k$. Because K/k is unramified outside 2, we have $\alpha\mathcal{O} = \mathfrak{p}^e\mathfrak{a}^2$, where $\mathcal{O}$ is the ring of integers in k and the ideal $\mathfrak{a}$ is prime to $\mathfrak{p}$ and $e = 0$ or 1. Since $\mathfrak{p}$ is principal and the class number of k is prime to 2, this implies that $\mathfrak{a}$ is also principal. Hence we may assume $\alpha = \pm\varepsilon^{e_1}\pi^{e_2}$ $(e_1, e_2 = 0 \text{ or } 1)$. Consequently, K is k itself or one of the fields listed in the third condition.

Now we claim that the prime ideal $\mathfrak{p}$ cannot remain prime in K provided that K is a quadratic extension of k. Suppose to the contrary that it remains prime. Then K is unramified over k outside the archimedian places. Since the class number of k is prime to 2, K is the genus field $\widetilde{k}$ of k. This yields that L is a cubic extension of the genus field unramified outside $\mathfrak{p}$. This contradicts the fourth assumption.

Therefore we may assume that the inertia index of $\mathfrak{p}$ in K/k is 1. Because the class number of K is prime to 3, any prime ideal of K lying above $\mathfrak{p}$ ramifies in the extension L/K and the ramification is total and tame. Consequently, we have an injection of the Galois group of L/K into the multiplicative group of the residue field $\mathcal{O}/\mathfrak{p}$. This is impossible. This completes the proof of Theorem 1. □

Remark. In our previous paper [4], we used Serre's results in [7] to find the candidates for the intermediate field K. This is why we could not handle the fields with ramification at 2. However, we should note that Serre's result enabled us to reduce the number of the candidates.

2. Non-existence theorem

The aim of this section is to find some examples of quadratic fields over which there is no elliptic curve having good reduction.

We begin by searching for fields that satisfy the hypotheses in Theorem 1.

2.1. **Notation.** We hereafter make use of the following notation. Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field, where m is a square-free integer, and $\mathcal{O}$ the ring of integers of k. Let ε denote the fundamental unit that is larger than one and N the norm map from k to $\mathbb{Q}$, unless otherwise specified.

By the second assumption in Theorem 1, there is a generator, say π, of the prime ideal $\mathfrak{p}$ of $\mathcal{O}$ lying above 2. Further, we define rational integers σ, τ by the formula $\pi' = (-1)^{\sigma}\varepsilon^{\tau}\pi$. Here the symbol $'$ stands for the conjugate. Multiplying π by a unit if necessary, we can take $(\sigma, \tau) = (1,1)$ or $(0,1)$.

We denote the fields in the third assumption in Theorem 1 as follows:

$$K_1 = k(\sqrt{-1}),\ K_2 = k(\sqrt{\varepsilon}),\ K_3 = k(\sqrt{-\varepsilon}),$$

$$K_4 = k(\sqrt{\pi}),\ K_5 = k(\sqrt{-\pi}),\ K_6 = k(\sqrt{\varepsilon\pi}),\ K_7 = k(\sqrt{-\varepsilon\pi}).$$

2.2. **The first assumption.** In the range $1 < m < 100$, the following 21 m's ($m \not\equiv 1 \pmod 4$) satisfy the first assumption:

$$m = 2, 3, 6, 7, 11, 14, 19, 22, 23, 31, 38, 43, 46, 47, 59, 62, 67, 71, 83, 86, 94.$$

In fact, all of the corresponding quadratic fields $\mathbb{Q}(\sqrt{m})$ have class number one.

2.3. **The case $m = 2$.** We first consider the case $m = 2$, which is exceptional. It is easy to see that

$$\pi = \sqrt{2},\ \varepsilon = 1 + \sqrt{2},\ \sigma = 1,\ \tau = 0,\ N\varepsilon = -1.$$

Thus we obtain the following isomorphisms among the fields in the third condition:

$$K_2 \cong K_3,\ K_4 \cong K_5,\ K_6 \cong K_7.$$

Hence we have to compute the class numbers of the fields

$$K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{-1}),\ K_2 = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right),\ K_4 = \mathbb{Q}(\sqrt[4]{2}),\ K_6 = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right).$$

As a result, the class numbers of these fields are all one. (Throughout this paper, we use PARI-GP, version 1.39.03, to compute class groups and units of number fields). Since $N\varepsilon = -1$, there is no non-trivial genus field. Therefore $\mathbb{Q}(\sqrt{2})$ satisfies all the hypotheses in the theorem.

2.4. **Class numbers of K_1, K_2, K_3.** As for the other quadratic fields, we notice that $N\varepsilon = 1$, because their discriminants are of the form $2^{\ell} \cdot p$, where p is a prime number congruent to 3 modulo 4 and ℓ is 2 or 3.

To reduce the amount of computation, we first study the class numbers of the fields K_1, K_2, K_3. Since these fields are biquadratic (Galois) extensions over $\mathbb{Q}$, the divisibility of the class numbers follows immediately from the following lemmas.

The first lemma is easy to prove.

Lemma 1. *Let t be the trace from k to $\mathbb{Q}$ of the unit ε. Then we have*

$$K_2 = k(\sqrt{\varepsilon}) = \mathbb{Q}(\sqrt{t+2}, \sqrt{t-2}),$$
$$K_3 = k(\sqrt{-\varepsilon}) = \mathbb{Q}(\sqrt{-t+2}, \sqrt{-t-2}).$$

For biquadratic extensions, we can apply the next lemma.

TABLE 1. Class numbers of the quadratic fields associated with K_1, K_2 and K_3

m	$t = \mathrm{Tr}\ (\varepsilon)$	Class numbers				
		$\mathbb{Q}(\sqrt{-m})$	$\mathbb{Q}(\sqrt{t+2})$	$\mathbb{Q}(\sqrt{-t+2})$	$\mathbb{Q}(\sqrt{t-2})$	$\mathbb{Q}(\sqrt{-t-2})$
3	4	1	1	1	1	2
6	10	2	1	1	1	1
7	16	1	1	4	1	1
11	20	1	1	1	1	2
14	30	4	1	1	1	1
19	340	1	1	1	1	**6**
22	394	2	1	1	1	1
23	48	**3**	1	4	1	1
31	3040	**3**	1	8	1	1
38	74	**6**	1	1	1	1
43	6964	1	1	1	1	10
46	48670	4	1	**3**	1	1
47	96	5	1	8	1	1
59	1060	**3**	1	1	1	**6**
62	126	8	1	**3**	1	1
67	97684	1	1	1	1	14
71	6960	7	1	4	**3**	1
83	164	**3**	1	1	1	10
86	20810	10	1	1	1	1
94	4286590	8	1	5	1	1

Lemma 2 (Masley [6], Lemma 11). *Let L/K be an abelian extension with Galois group of type $(2,2)$, and p an odd prime. Let h_K and h_L denote the class numbers of K and L, respectively. If p is prime to h_K and p divides h_L, then the class number of one of the three intermediate fields of L/K is divisible by p.*

Accordingly, to verify the third condition for K_1, K_2, K_3, we have only to compute the class numbers of the following five quadratic fields:

$$\mathbb{Q}(\sqrt{-m}),\ \mathbb{Q}\left(\sqrt{\pm(t+2)}\right),\ \mathbb{Q}\left(\sqrt{\pm(t-2)}\right).$$

The result of the computation is shown in Table 1. In the table the bold-faced numbers are those that do *not* satisfy the assumption.

2.5. **Class numbers of $K_4, \dots, K_7$.** Now let us proceed to the assumption on the fields $K_4, \dots, K_7$. There are isomorphisms among these fields (note that $N(\varepsilon) = 1$),

$$\begin{cases} K_4 \cong K_7 \text{ and } K_5 \cong K_6 & \text{if } (\sigma, \tau) = (1,1), \\ K_4 \cong K_6 \text{ and } K_5 \cong K_7 & \text{if } (\sigma, \tau) = (0,1). \end{cases}$$

Hence it is enough to compute the class numbers of K_4 and K_5. Table 2 shows the result of the computation. In the table, we set $w = \sqrt{m}$. Again the bold-faced numbers are those that fail to satisfy the assumption.

TABLE 2. Class numbers of K_4 and K_5

m	π	ε	(σ,τ)	Class numbers	
				K_4	K_5
3	$1-w$	$2+w$	$(1,1)$	1	1
6	$-2+w$	$5+2w$	$(1,1)$	1	1
7	$-3+w$	$8+3w$	$(0,1)$	2	1
11	$-3+w$	$10+3w$	$(1,1)$	1	1
14	$-4+w$	$15+4w$	$(0,1)$	2	1
22	$14-3w$	$197+42w$	$(1,1)$	1	1
43	$59-9w$	$3482+531w$	$(1,1)$	1	1
47	$7-w$	$48+7w$	$(0,1)$	1	4
67	$221-27w$	$48842+5967w$	$(1,1)$	1	**3**
86	$102-11w$	$10405+1122w$	$(1,1)$	1	1
94	$1464-151w$	$2143295+221064w$	$(0,1)$	1	8

2.6. **The ray class number of genus fields.** We now examine the last hypothesis. Let us write the discriminant of the quadratic field as $2^\ell \cdot p$ ($p \equiv 3 \pmod 4$) as before. It is easily shown that the ideal $\mathfrak{p}$ of k is inert in the genus field $\widetilde{k}$ if and only if $p \equiv 3 \pmod 8$. Hence we have to check the hypothesis for $m = 3, 6, 11, 22, 43, 86$. Since the genus field $\widetilde{k}$ is nothing but $k(\sqrt{-1})$ or $k(\sqrt{-\varepsilon})$ according as $\ell = 2$ or 3, the class number of $\widetilde{k}$ is prime to 3 as we have checked in the above. Thus it readily follows from the ray class number formula that its ray class number modulo $\mathfrak{p}$ is prime to 3 if and only if there exists a unit u of $\mathcal{O}_{\widetilde{k}}$ such that $u \not\equiv 1 \pmod{\mathfrak{p}\mathcal{O}_{\widetilde{k}}}$, where $\mathcal{O}_{\widetilde{k}}$ is the ring of integers of $\widetilde{k}$. For $m = 3$ and 6, the third root of unity in $\mathcal{O}_{\widetilde{k}}$ gives u. For the other fields, since they do not contain the group of third roots of unity, it is enough to see whether the fundamental unit v of $\widetilde{k}$ works as u. Now we calculate v and the prime decomposition of $v-1$ in $\mathcal{O}_{\widetilde{k}}$.

We get Table 3, in which we use the following notation:

$$x = \begin{cases} \sqrt{-1}+\sqrt{-p} & \text{if } \ell = 2, \\ \sqrt{-2}+\sqrt{-p} & \text{if } \ell = 3; \end{cases}$$

$$\mathfrak{P}_q,\ \mathfrak{P}'_q = \text{ prime ideals of } \mathcal{O}_{\widetilde{k}} \text{ lying above a rational prime } q \text{ and } \mathfrak{P}_q \neq \mathfrak{P}'_q.$$

Thus we have $\mathfrak{P}_2 = \mathfrak{p}\mathcal{O}_{\widetilde{k}}$.

Unfortunately, none of these four fields satisfies the fourth condition in Theorem 1.

2.7. **Non-existence theorem.** Summing up the preceding computations and applying Theorem 1 to the special case of elliptic curves having good reduction, we obtain the following.

Proposition 1. *Let m be one of $2, 3, 6, 7, 14, 47, 94$ and $k = \mathbb{Q}(\sqrt{m})$. Every elliptic curve defined over k having good reduction has a k-rational point of order 2.*

Now we need the following result due to Comalada. It is worth noting that, while our theorem is field-theoretic, his result is proved by solving certain Diophantine equations explicitly.

TABLE 3. Fundamental units of the genus fields

m	Fundamental unit v	Factorization of $v-1$
11	$\frac{x^3}{20}-\frac{x^2}{4}+\frac{x}{5}-\frac{3}{2}$	$\mathfrak{P}_2\mathfrak{P}_5$
22	$\frac{2x^3}{9}+\frac{7x}{9}$	$\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}'_3\mathfrak{P}_{11}$
43	$\frac{25x^3}{84}-\frac{9x^2}{4}+\frac{193x}{21}-\frac{139}{2}$	$\mathfrak{P}_2\mathfrak{P}_{1741}$
86	$\frac{20x^3}{41}+\frac{529x}{41}$	$\mathfrak{P}_2\mathfrak{P}_{11}\mathfrak{P}'_{11}\mathfrak{P}_{43}$

Proposition 2 (Comalada [2]). *Let m be a positive square-free rational integer less than 100, and $k=\mathbb{Q}(\sqrt{m})$ a real quadratic field. There exists an elliptic curve defined over k having good reduction that has a k-rational point of order 2 if and only if m is one of* $6, 7, 14, 22, 38, 41, 65, 77, 86$.

Combining these two propositions, we have our non-existence theorem immediately.

Theorem 2. *There is no elliptic curve having good reduction over the following fields:*

$$\mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{47}),\ \mathbb{Q}(\sqrt{94}).$$

As a byproduct, we have also shown

Corollary. *Over the fields $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{14})$, every elliptic curve having good reduction has a rational point of order 2. Therefore all the elliptic curves having good reduction over these fields are listed in Comalada's table in* [2].

For the sake of completeness we reproduce Comalada's table for these three fields with some additional information.

In our table (Table 4), all the isomorphism classes of elliptic curves having good reduction over the three fields $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{14})$ are listed. Each isomorphism class contains a curve having a Weierstrass equation of the form

$$y^2 = x^3 + a_2x^2 + a_4x,$$

on which the point $(0,0)$ is of order 2.

For each curve, the data given in the table are a new code name, Comalada's code E_i, a_2, a_4, the j-invariant, the complex multiplication data (see below), the torsion subgroup T of the Mordell-Weil group, and the isogenies of prime degree.

Some explanations for the data may be in order.

If the new code given to a curve is of the form mX, the curve is defined over $\mathbb{Q}(\sqrt{m})$ and its conjugate curve is the curve $m\overline{X}$.

The coefficients a_2, a_4 and the j-invariant are given by expressions containing the fundamental unit ε and its Galois conjugate $\bar{\varepsilon}$. They are taken from Comalada's table, except for the curve $7\overline{D}$. This is because the isomorphism between E_{14} $(=7\overline{D})$ and the conjugate curve of E_{13} $(=7D)$ is not noticed in Comalada's table. For the values of ε, refer to Table 2.

TABLE 4. Elliptic curves having good reduction over $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{14})$

		a_2	a_4	j	CM	T	Isogenies
$6A$	E_3	$-14(\varepsilon-1)$	$4\bar\varepsilon$	$64(4\varepsilon^4+1)^3/\varepsilon^4$	-72	C_2	$\mathbf{2}:\overline{A},\mathbf{3}:B$
$6\overline{A}$	E_4	$-14(\bar\varepsilon-1)$	4ε	$64(4\bar\varepsilon^4+1)^3/\bar\varepsilon^4$	-72	C_2	$\mathbf{2}:A,\mathbf{3}:\overline{B}$
$6B$	E_1	$-2(\varepsilon-1)$	4ε	20^3	-8	C_6	$\mathbf{3}:A,\mathbf{2}:\overline{B},\mathbf{3}:C$
$6\overline{B}$	E_2	$-2(\bar\varepsilon-1)$	$4\bar\varepsilon$	20^3	-8	C_6	$\mathbf{3}:\overline{A},\mathbf{2}:B,\mathbf{3}:\overline{C}$
$6C$	E_6	$14(\bar\varepsilon-1)\bar\varepsilon$	$4\bar\varepsilon$	$64(4\bar\varepsilon^4+1)^3/\bar\varepsilon^4$	-72	C_6	$\mathbf{2}:\overline{C},\mathbf{3}:B$
$6\overline{C}$	E_5	$14(\varepsilon-1)\varepsilon$	4ε	$64(4\varepsilon^4+1)^3/\varepsilon^4$	-72	C_6	$\mathbf{2}:C,\mathbf{3}:\overline{B}$
$7A$	E_9	$2(1+2\varepsilon^2)$	1	$(256\varepsilon^2+\bar\varepsilon)^3$	-112	C_4	$\mathbf{7}:\overline{A},\mathbf{2}:B$
$7\overline{A}$	E_{10}	$2(1+2\bar\varepsilon^2)$	1	$(256\bar\varepsilon^2+\varepsilon)^3$	-112	C_4	$\mathbf{7}:A,\mathbf{2}:\overline{B}$
$7B$	E_7	$-(1+2\varepsilon^2)$	$16\varepsilon^3$	255^3	-28	$C_2\times C_2$	$\mathbf{2}:A,\mathbf{7}:\overline{B},\mathbf{2}:C,\mathbf{2}:D$
$7\overline{B}$	E_8	$-(1+2\bar\varepsilon^2)$	$16\bar\varepsilon^3$	255^3	-28	$C_2\times C_2$	$\mathbf{2}:\overline{A},\mathbf{7}:B,\mathbf{2}:\overline{C},\mathbf{2}:\overline{D}$
$7C$	E_{12}	$-2(1+2\bar\varepsilon^2)$	1	$(256\bar\varepsilon^2+\varepsilon)^3$	-112	C_2	$\mathbf{7}:\overline{C},\mathbf{2}:B$
$7\overline{C}$	E_{11}	$-2(1+2\varepsilon^2)$	1	$(256\varepsilon^2+\bar\varepsilon)^3$	-112	C_2	$\mathbf{7}:C,\mathbf{2}:\overline{B}$
$7D$	E_{14}	$-(8\varepsilon-1)$	$16\varepsilon^2$	-15^3	-7	C_4	$\mathbf{7}:\overline{D},\mathbf{2}:B$
$7\overline{D}$	E_{13}	$-(8\bar\varepsilon-1)$	$16\bar\varepsilon^2$	-15^3	-7	C_4	$\mathbf{7}:D,\mathbf{2}:\overline{B}$
$14A$	E_{15}	$-3(\varepsilon-1)/2$	16ε	-15^3	-7	C_2	$\mathbf{7}:\overline{A},\mathbf{2}:B$
$14\overline{A}$	E_{16}	$-3(\bar\varepsilon-1)/2$	$16\bar\varepsilon$	-15^3	-7	C_2	$\mathbf{7}:A,\mathbf{2}:\overline{B}$
$14B$	E_{17}	$3(\varepsilon-1)$	$-\varepsilon$	255^3	-28	C_2	$\mathbf{7}:\overline{B},\mathbf{2}:A$
$14\overline{B}$	E_{18}	$3(\bar\varepsilon-1)$	$-\bar\varepsilon$	255^3	-28	C_2	$\mathbf{7}:B,\mathbf{2}:\overline{A}$

All of the curves in Table 4 have complex multiplication. For this reason, we also added the discriminant d of the quadratic order of complex multiplication.

The isogenies are given in the manner of Cremona's book [3]. For example, the entry $\mathbf{2}:\overline{A},\mathbf{3}:B$ for the curve $6A$ indicates that $6A$ is 2-isogenous to $6\overline{A}$ and 3-isogenous to $6B$. The new code is given so that the isogeny relations among the curves are easily recognizable. For instance, the curve $6\overline{A}$ has isogenies $\mathbf{2}:A,\mathbf{3}:\overline{B}$, which is obtained by taking the overline of the isogenies of $6A$. In general, finding isogenies over quadratic fields is not easy, but in our case the isogenies can be found by Kwon's theorem [5]. Connell's program apecs on Maple V also helped to compute the isogenies explicitly.

We should note that there is only one isogeny class over each quadratic field. Hence, in particular, all of the curves are $\mathbb{Q}$-curves.

REFERENCES

[1] M. Bertolini and G. Canuto, *Good reduction of elliptic curves defined over* $\mathbb{Q}(\sqrt[3]{2})$, Arch. Math. **50** (1988), 42–50. MR **89d:**10046

[2] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. **144** (1990) 237–258. MR **91e:**11058

[3] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997. CMP 98:14

[4] M. Kida and T. Kagawa, *Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields*, J. Number Theory **66** (1997) 201–210. CMP 98:02

[5] S. Kwon, *Degree of isogenies of elliptic curves with complex multiplication*, Preprint.

[6] J. Masley, On the class number of cyclotomic fields, Ph.D. Thesis, Princeton Univ., 1972.

[7] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259–331. MR **52:**8126

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF ELECTRO-COMMUNICATIONS, CHOFU, TOKYO 182-8585, JAPAN

E-mail address: kida@matha.e-one.uec.ac.jp