Non-existence of elliptic curves with everywhere good reduction over some real quadratic fields

Yokoyama, Shun'ichi
Graduate School of Mathamatics, Kyushu University

Shimasaki, Yu
Graduate School of Mathamatics, Kyushu University

出版情報：Journal of Math-for-Industry (JMI). 3 (B), pp.113-117, 2011-10-12. Faculty of Mathematics, Kyushu University
バージョン：
権利関係：

Journal of Math-for-Industry, Vol. 3 (2011B-4), pp. 113–117

Math-for-industry
Education & Research Hub

Non-existence of elliptic curves with everywhere good reduction over some real quadratic fields

Shun'ichi Yokoyama and Yu Shimasaki

Received on August 25, 2011

Abstract. We prove the non-existence of elliptic curves having good reduction everywhere over some real quadratic fields. These results of computations give best-possible data including structures of Mordell-Weil groups over real quadratic fields $\mathbb{Q}(\sqrt{m})$ up to 100 via two-descent.

Keywords. Elliptic curves having everywhere good reduction, Mordell-Weil groups, Two-descent.

1. Introduction

Throughout this paper, let K_m be the real quadratic field $\mathbb{Q}(\sqrt{m})$ where m is a square-free positive integer with $m \leq 100$ and $\mathcal{O}_{K_m}$ the ring of integers of K_m. We already know the following results concerning elliptic curves with everywhere good reduction over real quadratic fields ([2, 4, 5, 6, 7, 8, 12, 13, 14, 18, 25]):

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

2. *The elliptic curves with everywhere good reduction over K_m are determined completely for $m = 6, 7, 14, 22, 29, 33, 37, 38, 41, 65$ and 77.*

3. *There are elliptic curves with everywhere good reduction over K_m if $m = 26, 79$ and 86* (cf. [4, 16] and Cremona's table [3]).

In this paper, we prove the non-existence of elliptic curves with everywhere good reduction over three real quadratic fields not appearing in Theorem 1.1. Here is the main theorem:

Theorem 1.2. *If $m = 43, 46$ and 59, there are no elliptic curves with everywhere good reduction over K_m.*

The following cases are still unknown whether an elliptic curve with everywhere good reduction over K_m exists or not:

$$m = 51, 62, 67, 71, 87, 91.$$

For three of them, we prove the following conditional (but best-possible) result:

Theorem 1.3. *If $m = 62, 67$ and 71, there are no elliptic curves with everywhere good reduction over K_m which have cubic discriminant.*

Remark 1.4. In some cases (e.g. $m = 77$, cf. [8]), we can prove that there exists an elliptic curve with everywhere good reduction over K_m having cubic discriminant.

Our strategy for the proof is close to that of T. Kagawa [8]. However, we use different kinds of computer softwares and computational techniques. In [8], all computations were carried out by using KASH [11] and SIMATH [21]. Unfortunately, development of SIMATH had already stopped and some fatal bugs (Tate's algorithm over number fields, for example) remain even now. Thus we switched environment of computation completely and started from a check experiment of Kagawa's results by using Magma [15], Pari-GP [17] and Sage [19].

Acknowledgment It is our pleasure to thank Takaaki Kagawa for his reading the first version of our paper and making various comments including the references to his pioneer works. We would like to thank Masanari Kida and Yuichiro Taguchi who gave us some useful advice. Our thanks also go to Iwao Kimura and Denis Simon who pointed out that there were some bugs of programs what we used.

2. Setup

In this section, we introduce the strategy to prove our results. Henceforth, we assume that the class number of K_m is 1 and every elliptic curve E with everywhere good reduction over K_m has no K_m-rational point of order 2 because Comalada [1] determines all admissible curves (= elliptic curves having good reduction everywhere and a K_m-rational point of order 2) defined over K_m with $m \leq 100$ and such curves do not exist over K_m which we consider in this paper. First we use the following result:

Proposition 2.1 (Setzer [20])**.** *Let E be an elliptic curve over K_m. If the class number of K_m is prime to 6 then E has a global minimal model.*

Let E be an elliptic curve with everywhere good reduction over K_m. By Proposition 2.1, E has a global minimal model

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

with coefficients $a_i \in \mathcal{O}_{K_m}$ $(i=1,2,3,4,6)$. The discriminant of E (denoted by $\Delta(E)$) is

$$\Delta(E)=\frac{c_4^3-c_6^2}{1728}$$

where $c_4, c_6 \in \mathcal{O}_{K_m}$ are, as in [24] (Chapter III, p.42), written as polynomials in the a_i's with integer coefficients. Moreover, the following conditions are equivalent (cf. [24], Chapter VII, Prop. 5.1):

- E has everywhere good reduction over K_m,
- $\Delta(E) \in \mathcal{O}_{K_m}^{\times}$.

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

$$E_n^{\pm}(\mathcal{O}_{K_m})=\left\{(x,y)\in \mathcal{O}_{K_m}\times\mathcal{O}_{K_m} \mid\ y^2=x^3\pm 1728\varepsilon^n\right\}$$

with $0 \le n < 12$. However, the set of coefficients $(a_1,a_2,a_3,a_4,a_6) \in \mathcal{O}_{K_m}^{\oplus 5}$, which gives rise to $(c_4,c_6) \in \mathcal{O}_{K_m}^{\oplus 2}$, does not necessarily exist. Therefore, we check whether the curve

$$E_C:\ y^2=x^3-27c_4x-54c_6, \tag{1}$$

which is isomorphic to E over K_m, has trivial conductor for each $(c_4,c_6) \in E_n^{\pm}(\mathcal{O}_{K_m})$.

Actually, it is very hard to compute all $E_n^{\pm}(\mathcal{O}_{K_m})$ 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. In [8], Kagawa shows a criterion whether the discriminant of an elliptic curve with everywhere good reduction over K_m is a cube in K_m:

Lemma 2.2 ([8], Prop. 1)**.** *If the following five conditions hold, then the discriminant of every elliptic curve with everywhere good reduction over K_m is a cube in K_m:*

1. *The class number of K_m is prime to 6;*
2. *$K_m/\mathbb{Q}$ is unramified at 3;*
3. *The class number of $K_m(\sqrt{-3})$ is prime to 3;*
4. *The class number of $K_m(\sqrt[3]{\varepsilon})$ is odd;*
5. *For some prime ideal $\mathfrak{p}$ of K_m dividing 3, the congruence $X^3 \equiv \varepsilon \pmod{\mathfrak{p}^2}$ does not have a solution in $\mathcal{O}_{K_m}$.*

Using the criterion, Kagawa shows the following:

Lemma 2.3 ([10])**.** *If $m=46$ or 59, every elliptic curve with everywhere good reduction over K_m has a global minimal model whose discriminant is a cube in K_m.*

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

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

Lemma 2.4 ([8], Prop. 4)**.** *Let E be an elliptic curve defined over K_m. If E has good reduction outside 2 and has no K_m-rational point of order 2, then $K_m(E[2])/K_m(\sqrt{\Delta(E)})$ is a cyclic cubic extension unramified outside 2. In particular, the ray class number of $K_m(\sqrt{\Delta(E)})$ modulo $\prod_{\mathfrak{p}|2}\mathfrak{p}$ is a multiple of 3.*

Note that $K_m(\sqrt{\Delta(E)})$ is either K_m, $K_m(\sqrt{-1})$ or $K_m(\sqrt{\pm\varepsilon})$. Thus we compute the ray class number of $K_m(\sqrt{\Delta(E)})$ modulo $\prod_{\mathfrak{p}|2}\mathfrak{p}$. The following computations are carried out by using Pari/GP [17] (Same type results were obtained in [9] by using KASH [11]). The bold-faced numbers in this table are the ones divisible by 3.

m	K_m	$K_m(\sqrt{-1})$	$K_m(\sqrt{\varepsilon})$	$K_m(\sqrt{-\varepsilon})$
43	1	**3**	10	1
46	1	4	1	**3**
59	1	**9**	**6**	1

Table 1. Ray class number of $K_m(\sqrt{\Delta(E)})$ $(m=43,46,59)$ modulo $\prod_{\mathfrak{p}|2}\mathfrak{p}$

As a result, if $m=46$ the discriminant $\Delta(E)$ is $-\varepsilon^{6n+3}$ and if $m=59$ the discriminant is $-\varepsilon^{6n}$ or ε^{6n+3}. We can conclude that it is enough to determine $E_3^+(\mathcal{O}_{K_{46}})$, $E_0^+(\mathcal{O}_{K_{59}})$ and $E_3^-(\mathcal{O}_{K_{59}})$ to prove Theorem 1.2 for $m=46$ and 59.

However, the case $m=43$ remains because some of the conditions in Lemma 2.2 do not hold. In this case, it is known that the discriminant is $-\varepsilon^{2n}$ (cf. [9] and Lem. 2.3) so we need to compute the three sets, $E_0^+(\mathcal{O}_{K_{43}})$, $E_2^+(\mathcal{O}_{K_{43}})$ and $E_4^+(\mathcal{O}_{K_{43}})$.

3. Results of the computation

3.1. Computing Mordell-Weil groups and integral points

To compute $E_n^{\pm}(\mathcal{O}_{K_m})$, we first compute the Mordell-Weil group $E_n^{\pm}(K_m)$. It is decomposed into a direct-sum of $E_n^{\pm}(K_m)_{\mathrm{tors}}$ (torsion part) and $E_n^{\pm}(K_m)_{\mathrm{free}}$ (free part, which is not canonical). 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 $E_n^{\pm}(K_m)/2E_n^{\pm}(K_m)$ to $E_n^{\pm}(K_m)$).

Proposition 3.1. *A basis of $E_n^{\pm}(K_m)$ is as follows:*

1. (Case $m=43$)

(a) $E_0^+(K_{43}) \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ *and a basis is* $\{T_{43}, P_{43A}\}$ *where* $T_{43} = (-12, 0)$ *is 2-torsion and*

$$P_{43A} = \left(-\frac{104}{9}, -\frac{56}{27}\sqrt{43}\right)$$

is a generator of the free-part.

(b) $E_2^+(K_{43}) \simeq \mathbb{Z}$ *and a basis is* $\{P_{43B}\}$ *where*

$$P_{43B} = \left(3200 - 488\sqrt{43}, 294088 - 44848\sqrt{43}\right).$$

(c) $E_4^+(K_{43}) \simeq \mathbb{Z}$ *and a basis is* $\{P_{43C}\}$ *where* $P_{43C} = (x, y)$ *with*

$$x = -727456 + 110936\sqrt{43}$$
$$y = 496115392 - 75656888\sqrt{43}$$

2. (Case $m = 46$) $E_3^+(K_{46})$ *is isomorphic to* $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ *with a basis* $\{T_{46}, P_{46}\}$ *where* $T_{46} = (-12\varepsilon, 0)$ ($\varepsilon = 24335 + 3588\sqrt{46}$) *is 2-torsion and* $P_{46} = (x, y)$ *with*

$$x = \frac{1044823225}{6084} + \frac{987505}{39}\sqrt{46}$$
$$y = \frac{116177050458217}{474552} + \frac{73202442649}{2028}\sqrt{46}$$

is a generator of the free-part.

3. (Case $m = 59$)

(a) $E_0^+(K_{59}) \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ *and a basis is* $\{T_{59A}, P_{59A}\}$ *where* $T_{59A} = (-12, 0)$ *is 2-torsion and*

$$P_{59A} = \left(-\frac{133}{16}, \frac{283}{64}\sqrt{59}\right)$$

is a generator of the free-part.

(b) $E_3^-(K_{59}) \simeq \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/2\mathbb{Z}$ *and a basis is* $\{T_{59B}, P_{59B}, P_{59C}\}$ *where* $T_{59B} = (12\varepsilon, 0)$ ($\varepsilon = -530 + 69\sqrt{59}$) *is 2-torsion and* $P_{59B} = (x, y)$ *with*

$$x = 9275 - \frac{2415}{2}\sqrt{59}$$
$$y = -\frac{5810733}{4} + \frac{756493}{4}\sqrt{59}$$

and $P_{59C} = (z, w)$ *with*

$$z = \frac{50000200}{59} - \frac{6509460}{59}\sqrt{59}$$
$$w = \frac{65094772968}{59} - \frac{500002437752}{3481}\sqrt{59}$$

are generators of the free-part.

Here we used Denis Simon's two-descent program (cf. [22]) on Pari-GP [17]. To compute some related data efficiently, we executed the Pari-GP program on Sage [19] as a built-in software.

Warning: Simon's two-descent program is also available as a Sage's built-in function that does not require the Pari-GP platform. However, this function has fatal bugs (errors) that come from the same bugs in the previous edition of Simon's original (Pari-GP) program. For the Pari-GP platform, this problem has already been fixed by himself completely, but it is not yet for the Sage platform.

To compute the subset $E_n^{\pm}(\mathcal{O}_{K_m})$ of integral points in $E_n^{\pm}(K_m)$, we use the method of elliptic logarithm to compute the linear form:

$$P = \sum_{i=1}^{r} m_i P_i + nT \in E_n^{\pm}(\mathcal{O}_{K_m}) \qquad (m_1, ..., m_r, n \in \mathbb{Z})$$

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

$$M := \max\{|m_1|, ..., |m_r|, |n|\}$$

can be bounded using the LLL-algorithm (by Lenstra-Lenstra-Lovász, cf. [23]).

Proposition 3.2. *The set of integral points* $E_n^{\pm}(\mathcal{O}_{K_m})$ *is as follows:*

1. (Case $m = 43$)
   (a) $E_0^+(\mathcal{O}_{K_{43}}) = \{O, T_{43}, T_{43} \pm P_{43A}\}$,
   (b) $E_2^+(\mathcal{O}_{K_{43}}) = \{O, \pm P_{43B}, \pm 2P_{43B}\}$,
   (c) $E_4^+(\mathcal{O}_{K_{43}}) = \{O, \pm P_{43C}, \pm 2P_{43C}\}$.
2. (Case $m = 46$) $E_3^+(\mathcal{O}_{K_{46}}) = \{O, T_{46}\}$.
3. (Case $m = 59$)
   (a) $E_0^+(\mathcal{O}_{K_{59}}) = \{O, T_{59A}\}$,
   (b) $E_3^-(\mathcal{O}_{K_{59}}) = \{O, T_{59B}\}$.

Finally, we compute that the elliptic curve (1) has trivial conductor. As a result, there are no pairs $(c_4, c_6) \in E_n^{\pm}(\mathcal{O}_{K_m})$ for which (1) has trivial conductor. Therefore, the non-existence of the curves follows.

In the same way, we can prove Theorem 1.3. For $m = 62, 67$ and 71, by the assumption of cubic discriminants, it is enough to determine $E_{3n}^{\pm}(\mathcal{O}_{K_m})$ ($n \in \mathbb{Z}$). To apply Lemma 2.4, we compute the ray class number of $K_m(\sqrt{\Delta(E)})$ modulo $\prod_{\mathfrak{p}|2} \mathfrak{p}$.

m	K_m	$K_m(\sqrt{-1})$	$K_m(\sqrt{\varepsilon})$	$K_m(\sqrt{-\varepsilon})$
62	1	8	**3**	1
67	1	**3**	14	1
71	1	7	**3**	4

Table 2. Ray class number of $K_m(\sqrt{\Delta(E)})$ ($m = 62, 67, 71$) modulo $\prod_{\mathfrak{p}|2} \mathfrak{p}$

Finally it is enough to determine $E_3^-(\mathcal{O}_{K_{62}})$, $E_0^+(\mathcal{O}_{K_{67}})$ and $E_3^-(\mathcal{O}_{K_{71}})$. Here is the result of computing Mordell-Weil groups and sets of integral points.

Proposition 3.3. *A basis of $E_n^{\pm}(K_m)$ and the set of integral points $E_n^{\pm}(\mathcal{O}_{K_m})$ are as follows:*

1. (Case $m = 62$) $E_3^-(K_{62})$ *is isomorphic to* $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ *with a basis* $\{T_{62}, P_{62}\}$ *where* $T_{62} = (12\varepsilon, 0)$ ($\varepsilon = -63 + 8\sqrt{62}$) *is 2-torsion and*

$$P_{62} = \left(\frac{30492}{25} - \frac{3872}{25}\sqrt{62}, -\frac{8377936}{125} + 8512\sqrt{62}\right)$$

is a generator of the free-part. The set of integral points is

$$E_3^-(\mathcal{O}_{K_{62}}) = \{O, T_{62}\}.$$

2. (Case $m = 67$) $E_0^+(K_{67})$ *is isomorphic to* $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ *with a basis* $\{T_{67}, P_{67}\}$ *where* $T_{67} = (-12, 0)$ *is 2-torsion and*

$$P_{67} = \left(-\frac{584}{49}, \frac{248}{343}\sqrt{67}\right)$$

is a generator of the free-part. The set of integral points is

$$E_0^+(\mathcal{O}_{K_{67}}) = \{O, T_{67}, T_{67} \pm P_{67}\}.$$

3. (Case $m = 71$) $E_3^-(K_{71})$ *is isomorphic to* $\mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/2\mathbb{Z}$ *with a basis* $\{T_{71}, P_{71A}, P_{71B}\}$ *where* $T_{71} = (12\varepsilon, 0)$ ($\varepsilon = 3480 + 413\sqrt{71}$) *is 2-torsion and* $P_{71A} = (x, y)$ *with*

$$x = 165300 + \frac{39235}{2}\sqrt{71}$$
$$y = \frac{377098253}{4} + \frac{44753329}{4}\sqrt{71}$$

and $P_{71B} = (z, w)$ *with*

$$z = \frac{1560462848}{3025} + \frac{185192868}{3025}\sqrt{71}$$
$$w = -\frac{87152513410872}{166375} - \frac{10343100438152}{166375}\sqrt{71}$$

are generators of the free-part. The set of integral points is

$$E_3^-(\mathcal{O}_{K_{71}}) = \{O, T_{71}, \pm P_{71A} \mp P_{71B}, T_{71} \pm P_{71A} \mp P_{71B}\}.$$
(*double sign in the same order*)

Moreover, there are no pairs $(c_4, c_6) \in E_n^{\pm}(\mathcal{O}_{K_m})$ *for which the elliptic curve* (1) *has trivial conductor.*

3.2. Trial of computation

In this subsection, we show examples of computation times of running Simon's two-descent program to compute Mordell-Weil groups. Simon's two-descent is mainly controlled by four parameters:

- `lim1`: limit on trivial points on binary quartic forms ("quartics" for short),
- `lim3`: limit on points on ELS (everywhere locally solvable) quartics,
- `limtriv`: limit on trivial points on elliptic curve,
- `limbigprime`: distinguish between small and large prime numbers to use probabilistic tests for large primes,

and there are some supplemental parameters (`maxprob`, `bigint`, `nbideaux`, etc.).

Now we fix the set of main parameters (`lim1`, `lim3`, `limtriv`, `limbigprime`) $= (40, 60, 40, 30)$ that were chosen to compute the case $m = 43$. The total running times of these computations are as follows:

m	$E_n^{\pm}$	desired	actual	CPU time (sec.)	S/F
43	E_0^+	1	1	570.168	success
	E_2^+	1	1	120.916	success
	E_4^+	1	1	112.554	success
46	E_3^+	1	1	670.117	success
59	E_0^+	1	1	195.500	success
	E_3^-	2	1	300.582	failure
62	E_3^-	1	1	317.216	success
67	E_0^+	1	0	976.785	failure
71	E_3^-	2	2	279.413	success

Table 3. Rank of $E_n^{\pm}(K_m)$ with computation time (Intel Core$^{\text{TM}}$ i5 processor (3.30GHz, dual core) and 4.0GB memory)

As above, our trials failed for two cases due to the difficulty in searching for points on these curves $E_n^{\pm}$. Thus we need to change these parameters to get our results. As a result, we succeed in computing the case $E_3^-(\mathcal{O}_{K_{59}})$ and $E_0^+(\mathcal{O}_{K_{67}})$ with the set of parameters (`lim1`, `lim3`, `limtriv`, `limbigprime`) $= (70, 80, 150, 80)$ but we need a lot of time for the computation.

m	$E_n^{\pm}$	desired	actual	CPU time (sec.)	S/F
59	E_3^-	2	2	2192.911	success
67	E_0^+	1	1	6186.093	success

Table 4. Rank of $E_n^{\pm}(K_m)$ with computation time for the case $E_3^-(\mathcal{O}_{K_{59}})$ and $E_0^+(\mathcal{O}_{K_{67}})$ (Intel Core$^{\text{TM}}$ i5 processor (3.30GHz, dual core) and 4.0GB memory)

References

[1] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. **144** (1990), 233–258.

[2] J. Cremona and M. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Exp. Math. **16** No. 3 (2007), 303–312.

[3] J. Cremona (compiled), *Elliptic Curves with Everywhere Good Reduction over Quadratic Fields*, available from his website: `http://www.warwick.ac.uk/staff/J.E.Cremona/ecegr/ecegrqf.html`.

[4] H. Ishii, *The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields*, Japan. J. Math. **12** (1986), 45–52.

[5] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{37})$, Acta Arith. **83** (1998), 253–269.

[6] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields*, Arch. Math. **73** (1999), 25–32.

[7] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields* $\mathbb{Q}(\sqrt{3p})$, Acta. Arith. **96** (2001), 231–245.

[8] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields, II*, preprint.

[9] T. Kagawa, *Elliptic curves with everywhere good reduction over real quadratic fields*, Ph.D. Thesis, Waseda University (1998).

[10] T. Kagawa, *Computing integral points of elliptic curves over real quadratic fields, and determination of elliptic curves having trivial conductor* (in Japanese), available online: `http://www.ritsumei.ac.jp/se/~kagawa/waseda.pdf`.

[11] KANT/KASH, *Computational Algebraic Number Theory*, `http://www.math.tu-berlin.de/~kant/kash.html`.

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

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

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

[15] Magma, *Computational Algebra System*, `http://magma.maths.usyd.edu.au/magma/`.

[16] H. Müller, H. Ströher and H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over quadratic fields*, J. Reine. Angew. Math. **397** (1989), 100–161.

[17] Pari(-GP), *A computer algebra system designed for fast computations in number theory*, `http://pari.math.u-bordeaux.fr/`.

[18] R. G. E. Pinch, *Elliptic curves over number fields*, Ph.D. thesis, Oxford (1982).

[19] Sage, *Open Source Mathematics Software*, `http://www.sagemath.org/`.

[20] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math. **74** (1978), no. 1, 235–250.

[21] SIMATH, *A computer algebra system*, `http://tnt.math.se.tmu.ac.jp/simath/`.

[22] D. Simon, *Computing the rank of elliptic curves over number fields*, LMS JCM, vol **5** (2002), 7–17.

[23] N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Text **41** (1998).

[24] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Graduate Texts in Mathematics **106**, Springer-Verlag (2009).

[25] T. Thongjunthug, *Heights on elliptic curves over number fields, period lattices, and complex elliptic logarithms*, Ph.D. Thesis, The University of Warwick (2011).

Shun'ichi Yokoyama and Yu Shimasaki
Graduate School of Mathematics, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
E-mail: s-yokoyama(at)math.kyushu-u.ac.jp
y-shimasaki(at)math.kyushu-u.ac.jp