Journal de Théorie des Nombres
de Bordeaux **13** (2001), 201–209

Good reduction of elliptic curves over imaginary quadratic fields

par Masanari KIDA

Résumé. Nous montrons que l'invariant modulaire j d'une courbe elliptique définie sur un corps quadratique imaginaire ayant partout bonne réduction vérifie certaines équations diophantiennes, sous réserve que soient vérifiées certaines hypothèses relatives à l'arithmétique du corps. En résolvant explicitement ces équations dans l'anneau des entiers du corps, nous montrons que de telles courbes n'existent pas sur certains corps quadratiques imaginaires. Nos résultats généralisent des résultats antérieurs de Setzer et Stroeker.

Abstract. We prove that the j-invariant of an elliptic curve defined over an imaginary quadratic number field having good reduction everywhere satisfies certain Diophantine equations under some hypothesis on the arithmetic of the quadratic field. By solving the Diophantine equations explicitly in the rings of quadratic integers, we show the non-existence of such elliptic curve for certain imaginary quadratic fields. This extends the results due to Setzer and Stroeker.

Introduction

It is well-known that there is no elliptic curve having good reduction everywhere over the field $\mathbb{Q}$ of rational numbers. This result is further generalized to certain quadratic fields and some other fields (see [9] and the references there).

In this paper, we are particularly interested in the case of imaginary quadratic fields. For this case, the following nice result due to Setzer and Stroeker is known.

Theorem (Setzer [11, Theorem 5], Stroeker [16, (1.9) Theorem]). *Let k be an imaginary quadratic field. If the class number of k is prime to 6, then there is no elliptic curve defined over k having good reduction everywhere.*

Manuscrit reçu le 26 octobre 1999.

This research was supported in part by Grant-in-Aid for Encouragement of Young Scientists (No. 11740009), Ministry of Education, Science, Sports and Culture, Japan.

Moreover, Setzer gives a criterion for the non-existence of elliptic curves having good reduction everywhere by using certain Galois-theoretic properties of the two division fields of the elliptic curves ([11, p. 249, Proposition]).

The aim of this paper is to prove the non-existence of such elliptic curves under somewhat weaker assumptions than Setzer and Stroeker's in the above theorem. For that purpose, we reduce the problem of finding such curves to solving certain Diophantine equations (cf. Theorem 2) under some hypothesis. Solving these Diophantine equations explicitly, we shall show the following theorem.

Theorem 1. *There is no elliptic curve having good reduction everywhere over the following four imaginary quadratic fields:*

$$\mathbb{Q}(\sqrt{-35}),\ \mathbb{Q}(\sqrt{-37}),\ \mathbb{Q}(\sqrt{-51}),\ \mathbb{Q}(\sqrt{-91}).$$

The class numbers of these four fields are all 2. Therefore the non-existence of elliptic curves having good reduction everywhere for these fields does not follow from Setzer and Stroeker's theorem above. Moreover, Setzer's criterion cannot be applied to these fields (cf. [11, Theorem 4 (a)]).

This paper consists of three sections. In the first section, we show that the j-invariant of an elliptic curve over an imaginary quadratic number field having good reduction everywhere satisfies a set of Diophantine equations. In the second section, we explain how to solve these Diophantine equations. Some numerical examples and the proof of Theorem 1 are given in the third section.

1. Diophantine equations

We shall prove the following theorem in this section. For the definition of the j-invariant of an elliptic curve, we refer to [1, p. 364 (7.1)].

Theorem 2. *Let k be an imaginary quadratic field. Suppose k satisfies the following assumptions:*

(i) *The unit group of k consists of ± 1;*
(ii) *The class number of k is prime to 3;*
(iii) *If the class number of k is divisible by 2, then every ideal class of order 2 contains an ideal $\mathfrak{c}$ such that $\mathfrak{c}^2 = (r)$ with some rational integer r.*

Then the j-invariant j of an elliptic curve defined over k having good reduction everywhere satisfies the following set of Diophantine equations in the ring of integers of k:

$$C_t^{\pm}:\ y^2 = x^3 \pm 1728t^3, \quad (t = 1, r), \tag{1}$$

where j and x are related by $j = \pm\left(\dfrac{x}{t}\right)^3$.

Proof. It is known that the j-invariant j of an elliptic curve having good reduction everywhere satisfies the following conditions for every discrete valuation v of the ring of integers of k (see [2, (1.3)]):

(2a) $$v(j) \geq 0,$$

(2b) $$v(j) \equiv 0 \pmod 3,$$

(2c) $$v(j - 1728) \equiv 0 \pmod 2.$$

It follows from (2a) that j is an algebraic integer. Furthermore, j generates an ideal which is a cube by (2b): $(j) = \mathfrak{b}^3$. By the assumption on the class number of k, the ideal $\mathfrak{b}$ is principal, i.e., $\mathfrak{b} = (x)$. Hence, we have

(3) $$j = \pm x^3.$$

Here we used the assumption on the unit group. It is easy to see that the generator x can be taken in the ring of algebraic integers of k.

Now by (2c), there exists an ideal $\mathfrak{a}$ such that

(4) $$(j - 1728) = \mathfrak{a}^2.$$

Suppose first that $\mathfrak{a}$ in (4) is principal, say $\mathfrak{a} = (y)$. Then we get $j - 1728 = \pm y^2$ with some $y \in k$. It is readily seen from this equation that y is an algebraic integer. Combining this with (3), we obtain $\pm y^2 = \pm x^3 - 1728$. Changing the signs of the variables, we have $C_1^{\pm} :\ y^2 = x^3 \pm 1728$.

If $\mathfrak{a}$ is not principal, then the class of $\mathfrak{a}$ is of order 2 in the ideal class group. The class of $\mathfrak{a}$ contains an ideal $\mathfrak{c}$ such that $\mathfrak{c}^2 = (r)$ with $r \in \mathbb{Z}$ by the third assumption. This means that there exists $y \in k$ satisfying $\mathfrak{a} = (y)\mathfrak{c}$. Hence it follows $\mathfrak{a}^2 = (y^2)\mathfrak{c}^2 = (ry^2)$. Combining this with (4), we have $j - 1728 = \pm ry^2$. This implies that ry^2 is an algebraic integer. Substituting (3) into this equation and, if necessary, changing the signs of the variables, we obtain $ry^2 = x^3 \pm 1728$. Multiplying by r^3 then yields $(r^2y)^2 = (rx)^3 \pm 1728r^3$. Since $(r^2y)^2 = r^3 \cdot ry^2$, we see that r^2y is integral. Replacing (rx, r^2y) by (x, y), we have $C_r^{\pm}$. We have thus proved Theorem 2. □

Some remarks are in order. The first assumption in Theorem 2 is satisfied if k is neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$. The class number of each field is one. Hence the non-existence for these two fields follows from Setzer and Stroeker's theorem.

The resulting Diophantine equations $C_t^{\pm}$ in Theorem 2 define elliptic curves over $\mathbb{Q}$. Thus, to apply the theorem to a specific imaginary quadratic field, we have to determine the integral points in the ring of quadratic integers of an elliptic curve defined over $\mathbb{Q}$. This is actually possible by the method we will explain in the next section.

2. Integral points on an elliptic curve

Let $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field where m is a square-free rational integer and $\mathbb{Z}_k$ the ring of integers of k. Let E be an elliptic curve given by a short Weierstrass equation

$$y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$. In this section, we discuss how to find the integral points of E in $\mathbb{Z}_k$.

First we consider the method of computing the Mordell-Weil group $E(k)$.

We denote by $E(-m)$ the quadratic twist of E corresponding to the quadratic extension $k/\mathbb{Q}$, which is defined by the equation

$$Y^2 = X^3 + a(-m)^2 X + b(-m)^3.$$

These two curves E and $E(-m)$ are both defined over $\mathbb{Q}$ and are isomorphic over k. An explicit isomorphism over k is given by

$$\begin{array}{rccc} \vartheta\colon & E(-m) & \longrightarrow & E \\ & (X,Y) & \longmapsto & \left(\dfrac{-X}{m}, \dfrac{-Y}{m\sqrt{-m}}\right). \end{array} \tag{5}$$

By this isomorphism, we have $\vartheta(E(-m)(\mathbb{Q})) \subset E(k)$. Note that the generator σ of the Galois group of the quadratic extension $k/\mathbb{Q}$ acts on $\vartheta(E(-m)(\mathbb{Q}))$ by $P \mapsto -P$.

Hereafter, for a finitely generated Abelian group A, let A_n be the kernel of the multiplication-by-n map and set $A\langle 2\rangle = A/A_{2^\infty}$.

We now consider the following map:

$$\begin{array}{rccc} \varphi\colon & E(\mathbb{Q})\langle 2\rangle + \vartheta(E(-m)(\mathbb{Q}))\langle 2\rangle & \longrightarrow & E(k)\langle 2\rangle \\ & (P,Q) & \longmapsto & P+Q. \end{array}$$

In the map definition, the addition is that of the group law on E. Is is easy to see that the map is a homomorphism. By considering the action of σ, it is verified that the intersection of $E(\mathbb{Q})$ and $\vartheta(E(-m)(\mathbb{Q}))$ is a subset of $E(\mathbb{Q})_2$. Therefore, the sum of the groups on the left hand side is direct. Similarly, it can be seen that the map is injective. Moreover, the cokernel of φ is killed by the multiplication-by-2 map. Indeed, for any $P \in E(k)\langle 2\rangle$, take $(P + P^\sigma, P - P^\sigma) \in E(\mathbb{Q})\langle 2\rangle \oplus \vartheta(E(-m)(\mathbb{Q}))\langle 2\rangle$, then we have $\varphi(P + P^\sigma, P - P^\sigma) = 2P$.

Summing up the above arguments, we can compute $E(k)$ by the following procedure.

Step 1 Compute the generators of $E(\mathbb{Q})$ and $\vartheta((E(-m)(\mathbb{Q}))\langle 2\rangle)$. For this purpose, several pseudo algorithms are known (see [18]) and they are implemented in some number theory packages such as SIMATH ([6]).

Step 2 Determine whether the generators found in the preceding step and all possible sums of them have a half point (i.e., a point Q such that $P = 2Q$ for a given P) in $E(k)$ or not. If there exists a half point, then compute it and enlarge the group. This can be done by an algorithm due to Washington ([17, Proposition 4]). Repeat this step until no more half point exists.

Step 3 Fill up the 2-power torsion points. An explicit computation of the division polynomials, for example, enables us to accomplish it.

It should be emphasized that we can compute $E(k)$ because the curve E is defined over $\mathbb{Q}$. Computing Mordell-Weil groups over an algebraic number field larger than $\mathbb{Q}$ is still difficult in general (cf. [3]).

Having computed the Mordell-Weil group, we now turn our attention to computing the integral points.

Let $P_1, P_2, \dots, P_s$ be the generators of $E(k)$. Suppose that $P = p_1P_1 + p_2P_2 + \cdots + p_sP_s \in E(k)$ is an integral point with $p_1, p_2, \dots, p_s \in \mathbb{Z}$. Using Baker's theory for elliptic logarithms (cf. [5]), Smart and Stephens ([14], see also [15, Chapter XIII]) give a small computable upper bound for $\max\{|p_1|, |p_2|, \dots, |p_s|\}$. Hence we are able to find all the integral points in $E(k)$.

Here we make some remarks for a practical computation. To use the Smart-Stephens algorithm, local minimal models of the curve E and the canonical heights and the elliptic logarithms of the generators of $E(k)$ are required. We implemented the algorithms (Tate's algorithm [13, Chapter IV, §9], Silverman's algorithm [12] and Algorithm 7.4.8 in [1], respectively) for computing these invariants on KASH ([4]). We refer to [10] for more details.

Though Algorithm 7.4.8 in [1] only describes how to compute the elliptic logarithm of a point in the real locus of an elliptic curve, it is enough for our purpose as the following proposition shows.

Proposition. *Let Φ (resp. $\Phi_{(-m)}$) be the elliptic logarithm on E (resp. $E(-m)$) and Λ (resp. Λ_{-m}) the corresponding period lattice. Then the following diagram is commutative:*

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\times\frac{1}{\sqrt{-m}}} & \mathbb{C}/\Lambda_{-m} \\ \uparrow{\scriptstyle\Phi} & & \uparrow{\scriptstyle\Phi_{-m}} \\ E & \xleftarrow{\vartheta} & E(-m), \end{array}$$

where the map ϑ is defined by (5).

Proof. Let e_1, e_2 and e_3 be the roots of the polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$ where b_2, b_4 and b_6 are the standard invariants of E (for the definitions, see [1, p. 364 (7.1)] for example) and e'_1, e'_2 and e'_3 the corresponding objects for $E(-m)$. It is easy to see that they are related by

$$e'_i = -m\, e_i \ (i = 1, 2, 3).$$

Hence we have

$$\Lambda = \sqrt{-m}\, \Lambda_{-m} \tag{6}$$

by an easy change of variables in the period integrations.

Noting that the inverse map of Φ (resp. Φ_m) is given by

$$z \mapsto \left(\wp(z;\Lambda), \tfrac{1}{2}\wp'(z;\Lambda)\right) \quad \left(\text{resp. } z \mapsto \left(\wp(z;\Lambda_{-m}), \tfrac{1}{2}\wp'(z;\Lambda_{-m})\right)\right)$$

where $\wp(z;\Lambda)$ (resp. $\wp(z;\Lambda_{-m})$) is the Weierstrass $\wp$-function relative to the lattice Λ (resp. Λ_{-m}), we have to show

$$\left(\frac{-\wp\left(\frac{z}{\sqrt{-m}};\Lambda_{-m}\right)}{m}, \frac{-\wp'\left(\frac{z}{\sqrt{-m}};\Lambda_{-m}\right)}{2m\sqrt{-m}}\right) = \left(\wp(z;\Lambda), \frac{1}{2}\wp'(z;\Lambda)\right).$$

The first half is obtained from the following elementary calculations:

$$\begin{aligned}
\wp\left(\frac{z}{\sqrt{-m}};\Lambda_{-m}\right) &= \frac{-m}{z^2} + \sum_{\omega\in\Lambda_{-m}\setminus\{0\}} \left(\frac{1}{\left(\frac{z}{\sqrt{-m}}+\omega\right)^2} - \frac{1}{\omega^2}\right) \\
&= \frac{-m}{z^2} + \sum_{\omega'\in\Lambda\setminus\{0\}} \left(\frac{1}{\left(\frac{z}{\sqrt{-m}}+\frac{\omega'}{\sqrt{-m}}\right)^2} - \frac{1}{\left(\frac{\omega'}{\sqrt{-m}}\right)^2}\right) \qquad \text{by (6)} \\
&= \frac{-m}{z^2} + \sum_{\omega'\in\Lambda\setminus\{0\}} \left(\frac{-m}{(z+\omega')^2} - \frac{-m}{\omega'^2}\right) \\
&= -m\,\wp(z;\Lambda).
\end{aligned}$$

Differentiating the both sides of the above obtained equation by z, we have

$$\wp'\left(\frac{z}{\sqrt{-m}};\Lambda_{-m}\right) = -m\sqrt{-m}\,\wp'(z;\Lambda).$$

This completes the proof of the proposition. $\square$

If $P = 2Q$ holds, then it is easy to see that $\Phi(Q)$ agrees with either $\frac{\Phi(P)}{2}$, $\frac{\Phi(P)}{2} + \frac{\omega_i}{2}$ ($i = 1$ or 2) or $\frac{\Phi(P)}{2} + \frac{\omega_1+\omega_2}{2}$, where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. We can choose the correct one by computing the $\wp$ function at these values.

Since the generators of $E(k)$ always arise from the points in $E(\mathbb{Q})$ or $E(-m)(\mathbb{Q})$, it is enough to compute Φ or Φ_{-m} for the $\mathbb{Q}$-rational points.

3. Examples

In this section, we apply Theorem 2 to certain specific imaginary quadratic fields.

Among 61 imaginary quadratic fields $k = \mathbb{Q}(\sqrt{-m})$ ($1 < m < 100$, m is square-free), the non-existence of an elliptic curve having good reduction is proved for the following 44 values of m by Setzer and Stroeker's Theorem in the introduction and Setzer's criterion ([11, Thereom 4(a)]):

$$\begin{aligned} m =\,&\mathbf{1}, \mathbf{2}, \mathbf{3}, 5, 6, \mathbf{7}, 10, \mathbf{11}, 13, 14, 15, 17, \mathbf{19}, 21, 22, 30, 33, 34, 39, 41, 42, \mathbf{43}, 46 \\ &\mathbf{47}, 55, 57, 58, 62, 66, \mathbf{67}, 69, 70, \mathbf{71}, 73, 77, 78, \mathbf{79}, 82, 85, 86, 93, 94, 95, 97. \end{aligned}$$

m	t	$\pm$	$C_t^{\pm}(\mathbb{Q}(\sqrt{-m}))$	Group Structure
35	1	+	$\left\langle\left(-\frac{27452}{361}, \frac{767312}{6859}\sqrt{-35}\right), (-12,0)\right\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
		−	$\langle(-8, 8\sqrt{-35}), (12,0)\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
	5	+	$\langle(-1275, 7695\sqrt{-35}), (-60,0)\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
		−	$\langle(-20, 80\sqrt{-35}), (60,0)\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
37	1	+	$\left\langle(-16, 8\sqrt{-37}), \left(-\frac{3144}{37}, \frac{176040}{1369}\sqrt{-37}\right), (-12,0)\right\rangle$	$\mathbb{Z}^{\oplus 2}\oplus\mathbb{Z}/2\mathbb{Z}$
		−	$\langle(12,0)\rangle$	$\mathbb{Z}/2\mathbb{Z}$
	2	+	$\left\langle\left(-\frac{2220328}{38025}, \frac{524683936}{7414875}\sqrt{-37}\right), (-24,0)\right\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
		−	$\langle(40,224), (24,0)\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
51	1	+	$\langle(-12,0)\rangle$	$\mathbb{Z}/2\mathbb{Z}$
		−	$\langle(12,0)\rangle$	$\mathbb{Z}/2\mathbb{Z}$
	3	+	$\langle(72,-648)\rangle$	$\mathbb{Z}/6\mathbb{Z}$
		−	$\langle(36,0)\rangle$	$\mathbb{Z}/2\mathbb{Z}$
91	1	+	$\left\langle\left(-\frac{5988}{175}, \frac{125712}{6125}\sqrt{-91}\right), (-12,0)\right\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
		−	$\left\langle\left(-\frac{24}{7}, \frac{216}{49}\sqrt{-91}\right), (12,0)\right\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
	7	+	$\langle(28,784), (-84,0)\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
		−	$\langle(1785,75411), (84,0)\rangle$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$

TABLE 1. The Mordell-Weil groups $C_t^{\pm}(\mathbb{Q}(\sqrt{-m}))$

The bold-faced numbers corresponds to the fields whose class numbers are prime to six.

In our forthcoming paper [8], we show the non-existence for $m = 74$ by a different method.

On the other hand, the only known examples of elliptic curves having good reduction everywhere defined over an imaginary quadratic field of small discriminant are the eight curves (up to isomorphism) defined over $\mathbb{Q}(\sqrt{-65})$ found by Setzer [11].

Among the fifteen fields which remain, the following four fields satisfy the assumptions on the class number in Theorem 2 and they also satisfy the third assumption of the theorem on the existence of the rational integer r.

m	class number	r
35	2	5, 7
37	2	2
51	2	3, 17
91	2	7, 13

Note that r is a rational integer that necessarily divides the discriminant of the quadratic field, since r satisfies $\mathfrak{c}^2 = (r)$ in k. Although there may be more than one r for one field, as for the Mordell-Weil group computation, the results are essentially unchanged whichever r we choose. Indeed, let r_1

and r_2 be the r's. In each case, $m = r_1 r_2$ holds. Then we have the following isomorphism over $\mathbb{Q}$:

$$C^+_{r_1}(-m) = C^+_{r_1}(-r_1 r_2) = C^+_{-r_1^2 r_2} \simeq C^+_{-r_2} = C^-_{r_2}.$$

Similarly we can show

$$C^+_{r_1} \simeq C^-_{r_2}(-m),\ C^-_{r_1} \simeq C^+_{r_2}(-m),\ C^-_{r_1}(-m) \simeq C^+_{r_2}.$$

Generally speaking, the smaller r we choose, the faster the computation is.

The Mordell-Weil groups and the integral points of the curves $C^\pm_t(k)$ ($t =$ 1 or r) are compiled in Table 1 and Table 2, respectively.

By Theorem 2, we have the candidates of the j-invariants of elliptic curves having good reduction everywhere as follows.

m	j
35	$\pm 4^3, \pm 8^3, \pm 12^3, \pm 15^3, \pm 255^3, \pm 3768^3$
37	$\pm 12^3, \pm 16^3, \pm 20^3, \pm 66^3, \pm 120^3, \pm 3376^3$
51	$\pm 12^3, \pm 24^3$
91	$\pm 4^3, \pm 12^3, \pm 16^3, \pm 15^3, \pm 255^3$

An algorithm for computing all the elliptic curves having good reduction everywhere for a given j-invariant is presented in [7]. Alternatively, we may use the criterion of Comalada and Nart in [2]. Their criterion tells us which

m	t	$\pm$	Integral Points
35	1	$+$	$(-12, 0)$
		$-$	$(12, 0), (-8, \pm 8\sqrt{-35}), (-3768, \pm 39096\sqrt{-35})$
	5	$+$	$(-60, 0), (-1275, \pm 7695\sqrt{-35})$
		$-$	$(60, 0), (-20, \pm 80\sqrt{-35}), (-75, \pm 135\sqrt{-35})$
37	1	$+$	$(-12, 0), (-16, \pm 8\sqrt{-37}), (-120, \pm 216\sqrt{-37}),$ $(-3376, \pm 32248\sqrt{-37})$
		$-$	$(12, 0)$
	2	$+$	$(-24, 0)$
		$-$	$(24, 0), (40, \pm 224), (132, \pm 1512)$
51	1	$+$	$(-12, 0)$
		$-$	$(12, 0)$
	3	$+$	$(-36, 0), (72, \pm 648), (0, \pm 216)$
		$-$	$(36, 0)$
91	1	$+$	$(-12, 0)$
		$-$	$(12, 0), (-16, \pm 8\sqrt{-91})$
	7	$+$	$(-84, 0), (28, \pm 784), (105, \pm 1323)$
		$-$	$(84, 0), (1785, \pm 75411)$

TABLE 2. The integral points on $C^\pm_t$

algebraic integers appear as the j-invariants of elliptic curves having good reduction everywhere. By either of these methods, it is shown that there is no elliptic curve having good reduction everywhere having the j-invariants in the above list. We thus obtain Theorem 1.

References

[1] H. Cohen, *A course in computational algebraic number theory*. Springer-Verlag, Berlin, 1993.

[2] S. Comalada, E. Nart, *Modular invariant and good reduction of elliptic curves*. Math. Ann. **293** (1992), no. 2, 331–342.

[3] J. E. Cremona, P. Serf, *Computing the rank of elliptic curves over real quadratic number fields of class number* 1. Math. Comp. **68** (1999), no. 227, 1187–1200.

[4] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, K. Wildanger, *KANT V4*. J. Symbolic Comput. **24** (1997), no. 3-4, 267–283, Computational algebra and number theory (London, 1993).

[5] S. David, *Minorations de hauteurs sur les variétés abéliennes*. Bull. Soc. Math. France **121** (1993), no. 4, 509–544.

[6] C. Hollinger, P. Serf, *SIMATH—a computer algebra system*. Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 331–342.

[7] M. Kida, *Computing elliptic curves having good reduction everywhere over quadratic fields*. Preprint (1998).

[8] M. Kida, *Non-existence of elliptic curves having good reduction everywhere over certain quadratic fields*. Preprint (1999).

[9] M. Kida, *Reduction of elliptic curves over certain real quadratic fields*. Math. Comp. **68** (1999), no. 228, 1679–1685.

[10] M. Kida, *TECC manual version 2.2*. The University of Electro-Communications, November 1999.

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

[12] J.H. Silverman, *Computing heights on elliptic curves*. Math. Comp. **51** (1988), no. 183, 339–358.

[13] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, New York, 1994.

[14] N.P. Smart, N.M. Stephens, *Integral points on elliptic curves over number fields*. Math. Proc. Cambridge Philos. Soc. **122** (1997), no. 1, 9–16.

[15] N.P. Smart, *The algorithmic resolution of Diophantine equations*. Cambridge University Press, Cambridge, 1998.

[16] R.J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*. Pacific J. Math. **108** (1983), no. 2, 451–463.

[17] L.C. Washington, *Class numbers of the simplest cubic fields*. Math. Comp. **48** (1987), no. 177, 371–384.

[18] H.G. Zimmer, *Basic algorithms for elliptic curves*. Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 541–595.

Masanari Kida
Department of Mathematics
The University of Electro-Communications
Chofu, Tokyo 182-8585
Japan
E-mail : kida@matha.e-one.uec.ac.jp