ACTA ARITHMETICA
LXXXIII.3 (1998)

Determination of elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{37})$

by

Takaaki Kagawa (Tokyo)

1. Let k be a number field. It is a fascinating problem to determine the elliptic curves with everywhere good reduction over k. It is well known that there is no such curve over the field of rational numbers. When k is an imaginary quadratic field, Stroeker [Str] showed that such a curve does not admit a global minimal model, and also that there is no such curve over k provided that the class number of k is prime to 6. Hence the problem is essentially solved in this case.

It is natural that we next turn to the case where k is a real quadratic field. Another reason we are interested in this case is related to Shimura's elliptic curves obtained in the following way. Let N be a positive fundamental discriminant and let χ_N be the associated Dirichlet character. When the space $S_2(\Gamma_0(N), \chi_N)$ of cuspforms of Neben-type of weight two has a 2-dimensional $\mathbb{Q}$-simple factor, Shimura [Shim] constructed an abelian surface A defined over $\mathbb{Q}$. Over the real quadratic field $k = \mathbb{Q}(\sqrt{N})$, A splits as $B \times B'$, where B is an elliptic curve defined over k and B' is the conjugate of B. We call B Shimura's elliptic curve over k. It is known that B is isogenous to B' over k ([Shim]), and that B has everywhere good reduction over k (cf. [Ca], [DR], [KM]). Conversely, an elliptic curve E over a real quadratic field k with the properties stated above is conjectured by Pinch [Pi1] to be isogenous over k to Shimura's elliptic curve. For related topics concerning modularity of elliptic curves over number fields, see [Ha1], [HHM].

Hence the case of a real quadratic field is especially interesting. In this case, the following is known:

- Several examples are known [Co], [Is], [Set], [Shio], etc.).
- There is a method of constructing $\mathbb{Q}$-curves with everywhere good reduction over real quadratic fields ([Um]). Recall that a $\mathbb{Q}$-*curve* is

1991 *Mathematics Subject Classification*: Primary 11G05; Secondary 11D25, 11J86.

an elliptic curve defined over $\overline{\mathbb{Q}}$ which is isogenous over $\overline{\mathbb{Q}}$ to any of its Galois conjugates.

- There is no curve with everywhere good reduction over $\mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\sqrt{13})$ ([Pi1], [Is]).
- Determination of such curves has been made under certain conditions ([Co], [Ki1]).

However, as far as the author knows, there is no result determining all elliptic curves with everywhere good reduction over a real quadratic field.

In the present paper, we shall determine all elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{37})$ by means of diophantine equations.

2. The space $S_2(\Gamma_0(37), \chi_{37})$ is 2-dimensional and $\mathbb{Q}$-simple by Shimura [Shim]. Hence Shimura's abelian variety is uniquely determined (up to $\mathbb{Q}$-isogeny) and we denote it by A_{37}. The matrix

$$\frac{1}{\sqrt{37}}\begin{pmatrix} 0 & -1 \\ 37 & 0 \end{pmatrix}$$

induces an automorphism η of A_{37} defined over $k = \mathbb{Q}(\sqrt{37})$. Shimura's elliptic curve over k is defined as $B_{37} := (1+\eta)A_{37}$. A defining equation of B_{37} is given in [Shio]:

$$B_{37}: \quad y^2 - \varepsilon y = x^3 + \frac{3\varepsilon+1}{2}x^2 + \frac{11\varepsilon+1}{2}x, \quad \Delta = \varepsilon^6, \quad j = 2^{12},$$

where Δ is the discriminant and j is the j-invariant. From this equation, we see that $B_{37}(k)_{\text{tors}} = \langle(0,0)\rangle \cong \mathbb{Z}/5\mathbb{Z}$. Kida ([Ki1]) proved that the elliptic curves with everywhere good reduction over k with $j \in \mathbb{Z}$ are isomorphic over k to either $C_1 := B_{37}$ given above or $C_2 := C_1/\langle(0,0)\rangle$ given by

$$C_2: \quad y^2 - \varepsilon y = x^3 + \frac{3\varepsilon+1}{2}x^2 - \frac{1669\varepsilon+139}{2}x - 7(5449\varepsilon+451),$$
$$\Delta = \varepsilon^6, \quad j = 3376^3.$$

We see that $C_2(k)_{\text{tors}}$ is trivial (Proposition A.3 of [Shio]; see also Table 8 in [MSZ]).

The purpose of the present paper is to determine all elliptic curves with everywhere good reduction over k without any restriction on the j-invariant. As a matter of fact, we prove:

THEOREM. *Up to isomorphism over $k = \mathbb{Q}(\sqrt{37})$, C_1 and C_2 above are the only elliptic curves with everywhere good reduction over k. In particular, Pinch's conjecture is true for the field k.*

Consequently, all such curves are the ones already obtained in [Ki1].

REMARK. Shimura ([Shim]) showed that $S_2(\Gamma_0(41), \chi_{41})$ is also 2-dimensional $\mathbb{Q}$-simple, and hence Shimura's elliptic curve over $\mathbb{Q}(\sqrt{41})$ is unique, the one denoted by B_{41}. Shiota [Shio] computed a defining equation of B_{41}. Kida and the author ([KK]) have recently determined all elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{41})$. They are the curves E_i ($i = 23, \ldots, 28$) in the table in §5 of [Co] (E_{26} is isomorphic over $\mathbb{Q}(\sqrt{41})$ to B_{41}), and they are isogenous over $\mathbb{Q}(\sqrt{41})$. In particular, Pinch's conjecture is true also for $\mathbb{Q}(\sqrt{41})$. We also find that there are no such curves over $\mathbb{Q}(\sqrt{N})$ ($N = 17, 21, 73, 97, 149, 173, 181$). Note that $S_2(\Gamma_0(N), \chi_N)$ has no 2-dimensional $\mathbb{Q}$-simple factor for these N and for $N = 5, 13$ ([Ha2], [Shim]). Hence the conjecture is true also for these 10 values of N.

3. Notation. For a number field F, we denote by $\mathcal{O}_F$ (resp. $\mathcal{O}_F^\times$) its ring of integers (resp. its group of units). If F is a quadratic field and $x \in F$, we denote the conjugate of x by x'.

Throughout this paper, we denote the real quadratic field $\mathbb{Q}(\sqrt{37})$ by k. Set $\omega = (1 + \sqrt{37})/2$, and let $\pi = (7 + \sqrt{37})/2$ be a prime element dividing 3 in k. Observe that $\pi\pi' = 3$. We denote by ε the fundamental unit of k larger than 1, namely $\varepsilon = 6 + \sqrt{37}$. Observe that $N_{k/\mathbb{Q}}(\varepsilon) = -1$.

Here we give the outline of the proof. Let E be an elliptic curve with everywhere good reduction over k. Since the class number of k is 1, E has a model

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

with coefficients $a_i \in \mathcal{O}_k$ ($i = 1, 2, 3, 4, 6$) and discriminant $\Delta = \pm\varepsilon^n \in \mathcal{O}_k^\times$. In view of the formulae for an admissible change of variables, we may assume that $-6 \le n < 6$. The discriminant Δ and the quantities $c_4, c_6 \in \mathcal{O}_k$ defined as usual are algebraically dependent, namely $c_4^3 - c_6^2 = 1728\Delta$. This means that (c_4, c_6) is an $\mathcal{O}_k$-integral point of one of the elliptic curves

$$E_n^\pm : \quad y^2 = x^3 \pm 1728\varepsilon^n, \qquad -6 \le n < 6.$$

Thus to determine the elliptic curves with everywhere good reduction over k, we first determine the sets

$$E_n^\pm(\mathcal{O}_k) = \{(x, y) \in \mathcal{O}_k \times \mathcal{O}_k \mid y^2 = x^3 \pm 1728\varepsilon^n\}.$$

We need not determine all the sets though, because the discriminant of E is a cube, as will be proved in §4. Further, the map

$$E_n^\pm(\mathcal{O}_k) \to E_{n+6}^\pm(\mathcal{O}_k), \qquad (x, y) \mapsto (x\varepsilon^2, y\varepsilon^3)$$

is a bijection, and the map $(x, y) \mapsto (x'\varepsilon^2, y'\varepsilon^3)$ is also a bijection from $E_n^\pm(\mathcal{O}_k)$ to $E_{6-n}^\pm(\mathcal{O}_k)$ (resp. from $E_n^\pm(\mathcal{O}_k)$ to $E_{6-n}^\mp(\mathcal{O}_k)$) if n is even (resp. odd). Therefore it suffices to determine the following three sets:

$$E_0^\pm(\mathcal{O}_k), \qquad E_3^+(\mathcal{O}_k).$$

The determination will be done in §5.

Next in §7, for each $(x,y)\in E_n^{\pm}(\mathcal{O}_k)$, we check whether x,y occur as the quantities c_4,c_6 of a Weierstrass equation with coefficients in $\mathcal{O}_k$.

4. This section is devoted to the proof of the following proposition:

PROPOSITION 1. *An elliptic curve with everywhere good reduction over k has cubic discriminant.*

Note that the discriminant being a cube or not is independent of the choice of a model.

To prove Proposition 1, suppose that, on the contrary, there is an elliptic curve E_1 with everywhere good reduction over k given by a global minimal Weierstrass equation whose discriminant Δ is not a cube.

LEMMA 1. *Let M be a real quadratic field. Assume that* 3 *is unramified in M and the class number of $M(\sqrt{-3})$ is prime to* 3. *Let E be an elliptic curve with everywhere good reduction over M given by a global minimal equation whose discriminant Δ is not a cube in M. Then E has ordinary good reduction at all primes of M lying above* 3.

Proof. (The essential part of the proof is due to Kida [Ki2].) Let $\mathfrak{p}$ be a prime ideal of M dividing 3, u_0 a fundamental unit of M, and set $F=M(\sqrt{-3})$ and $K=M(\sqrt[3]{\Delta})=M(\sqrt[3]{u_0})$. Also let L be the extension of M generated by the coordinates of all points of order 3. Note that $M\subset K\subset FK\subset L$ ([Ser], p. 305 and [Sil], p. 98), and that the extension L/M is unramified outside 3 and the archimedean primes by the criterion of Néron–Ogg–Shafarevich ([Sil], p. 184). Also note that $\mathfrak{p}$ is ramified in K and F: $\mathfrak{P}_F^2=\mathfrak{p}\mathcal{O}_F$. Suppose that E has supersingular reduction at $\mathfrak{p}$. Then the decomposition group of $\mathfrak{p}$ is a 2-group (see §1.11 and §2.2 of [Ser]). Hence $\mathfrak{p}$ cannot be totally ramified in K/M. Therefore $\mathfrak{p}\mathcal{O}_K=\mathfrak{P}_K^2\mathfrak{P}_K'$, where $\mathfrak{P}_K$ and $\mathfrak{P}_K'$ are distinct prime ideals of K. Since FK/M is a Galois extension, we have $\mathfrak{p}\mathcal{O}_{FK}=(\mathfrak{P}\mathfrak{P}'\mathfrak{P}'')^2$ with three distinct prime ideals $\mathfrak{P},\mathfrak{P}',\mathfrak{P}''$ of FK. It follows that $\mathfrak{P}_F$ splits completely in FK.

Hence, if 3 remains prime in M, then FK/F is an unramified extension of degree three. This is a contradiction.

Next consider the case where 3 decomposes in M: $3\mathcal{O}_M=\mathfrak{p}\mathfrak{p}'$, $3\mathcal{O}_F=(\mathfrak{P}_F\mathfrak{P}_F')^2$. Since $FK=F(\sqrt[3]{u_0})$ is a Kummer extension of degree 3 over F, we see, by Theorem 119 of [He], that $\mathfrak{P}_F$ splits completely in FK if and only if the congruence

$$X^3\equiv u_0 \pmod{\mathfrak{P}_F^4} \tag{1}$$

is solvable in $\mathcal{O}_F$. Let σ be an element of $\mathrm{Gal}(F/\mathbb{Q})$ such that $\sigma|_M$ is the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q})$. Applying σ to the congruence (1), we have a solution $N(u_0)X^\sigma$ of the congruence

$$Y^3\equiv u_0^{-1} \pmod{\mathfrak{P}_F'^4}.$$

This means that $\mathfrak{P}'_F$ also decomposes in FK. Hence FK/F is again an unramified extension of degree three. ∎

Suppose that E_1 does not admit any 3-isogeny defined over k.

LEMMA 2. *Let M and E be as in Lemma* 1 *and let u_0 be a fundamental unit of M. If the class number of $K = M(\sqrt[3]{u_0})$ is odd*, *then E admits a* 3-*isogeny defined over M.*

Proof. Let L be the extension of M generated by the coordinates of all points of order 3 and let $F = M(\sqrt{-3})$. We may regard $G = \mathrm{Gal}(L/M)$ as a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. Since L contains $M(\sqrt[3]{\Delta}) = K$, which is a cubic extension of M, the order of G is divisible by 3. Therefore G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ or it contains $\mathrm{SL}_2(\mathbb{F}_3)$ by Proposition 15 of [Ser]. The former case is equivalent to the assertion that E admits a 3-isogeny defined over M. Suppose that E does not admit any 3-isogeny defined over M. Then $G \supset \mathrm{SL}_2(\mathbb{F}_3)$, which is equivalent to the assertion that $G = \mathrm{GL}_2(\mathbb{F}_3)$, since $\det : G \to \mathbb{F}_3^\times$ is surjective by the commutative diagram

$$\begin{tikzcd} G \arrow[r] \arrow[d, "\mathrm{Res}"'] & \mathrm{GL}_2(\mathbb{F}_3) \arrow[d, "\det"] \\ \mathrm{Gal}(F/M) \arrow[r, "\sim"] & \mathbb{F}_3^\times \end{tikzcd}$$

Hence $\mathrm{Gal}(L/K)$ is a 2-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. By an appropriate choice of a basis of the group of 3-torsion points, we may assume that

$$\mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle, \quad \text{where} \quad \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Since, by Lemma 1, E has ordinary good reduction at any primes of M lying above 3, we can apply the argument in the proof of Proposition 5.6 of [BK] to this case and we see that the fixed field of $\langle \sigma, \tau^2 \rangle$ is an unramified quadratic extension of K. ∎

The class numbers of $k(\sqrt{-3})$, $k(\sqrt[3]{\varepsilon}) = \mathbb{Q}(\sqrt[3]{\varepsilon})$ are 4, 1, respectively (the computation of the class number of $\mathbb{Q}(\sqrt[3]{\varepsilon})$ takes less than 10 seconds on Sparc station SS4 by using KASH Version 1.7). Therefore E_1 admits a 3-isogeny defined over k. We show that this leads to a contradiction. More precisely, we prove

PROPOSITION 2. *Let E_1 be an elliptic curve with everywhere good reduction over k. Then E_1 does not admit any* 3-*isogeny defined over k.*

To prove the proposition, suppose, on the contrary, that there exists a 3-isogeny $f : E_1 \to E_2$ defined over k. We define a rational function $J(x)$ by

$$J(x) = \frac{(x+27)(x+3)^3}{x}.$$

Then, by Pinch [Pi2], the j-invariant $j(E_i)$ of E_i $(i = 1, 2)$ can be written as

$$j(E_1) = J(\tau_1), \quad j(E_2) = J(\tau_2), \quad \tau_1, \tau_2 \in k, \ \tau_1\tau_2 = 3^6$$

(the parametrization of the j-invariant used in [Ha1] and [Um] is $J(27x)$, which is given by Fricke [Fr]). Moreover, let c_4, c_6 be the usual quantities associated with the defining equation of E_1. Then

$$j(E_1) = \frac{c_4^3}{\Delta} = \frac{(\tau_1+27)(\tau_1+3)^3}{\tau_1},$$
$$j(E_1) - 1728 = \frac{c_6^2}{\Delta} = \frac{(\tau_1^2+18\tau_1-27)^2}{\tau_1}.$$

Since E_1 and E_2 have everywhere good reduction over k, $j(E_1)$ and $j(E_2)$ are integers in k and the principal ideals $(j(E_i))$ and $(j(E_i)-1728)$ $(i = 1, 2)$ are a cube and a square, respectively. Thus we can write

$$\tau_1 = \pi^a\pi'^b u, \quad \tau_2 = \pi^{6-a}\pi'^{6-b}u^{-1}, \quad a, b = 0, 6, \ u \in \mathcal{O}_k^\times.$$

Considering the dual isogeny $\widehat{f} : E_2 \to E_1$ and the conjugate $f' : E_1' \to E_2'$, we may suppose that $(a, b) = (0, 0)$ or $(0, 6)$. We have $\tau_1 \neq -3$, since an elliptic curve defined over a quadratic field with $j = 0$ has at least one prime of bad reduction ([Set]). In case $(a, b) = (0, 0)$, if we put $X = c_4/(\tau_1+3)$, $u_1 = \Delta$ and $u_2 = \Delta/u$, we obtain

$$X^3 = u_1 + 27u_2. \tag{2}$$

In case $(a, b) = (0, 6)$, if we put $X = c_4\pi'/(\tau_1+3)$, $u_1 = \Delta$ and $u_2 = \Delta/u$, we obtain

$$X^3 = \pi'^3 u_1 + \pi^3 u_2. \tag{3}$$

Since $u_1, u_2 \in \mathcal{O}_k^\times$, we have $X \in \mathcal{O}_k$ in both cases.

LEMMA 3. *The map $x + y\omega \mapsto x$ $(x, y \in \mathbb{Z})$ gives rise to a canonical isomorphism $\mathcal{O}_k/\pi^2 \cong \mathbb{Z}/9\mathbb{Z}$. In particular*, $\varepsilon \equiv 5 \pmod{\pi^2}$ *and ε is not a cube modulo π^2.*

LEMMA 4. *Equations* (2) *and* (3) *have no solutions.*

Proof. We prove the assertion only for equation (2) since a similar proof works for (3).

Suppose that there exist $X \in \mathcal{O}_k$ and $u_1, u_2 \in \mathcal{O}_k^\times$ satisfying (2). Then, by Lemma 3, we see that u_1 is a cube. Clearly, without loss of generality, we may suppose that $u_1 = 1$. Writing (2) as

$$27u_2 = X^3 - 1 = (X-1)(X^2+X+1),$$

we have

$$X-1 = \pi^a\pi'^b u_3, \quad X^2+X+1 = \pi^{3-a}\pi'^{3-b}u_4, \quad u_3, u_4 \in \mathcal{O}_k^\times,\ 0 \le a, b \le 3,$$

whence

$$\pi^{2a}\pi'^{2b}u_3^2 + 3\pi^a\pi'^b u_3 + 3 = \pi^{3-a}\pi'^{3-b}u_4. \tag{4}$$

Without loss of generality, we may assume that $a \ge b$. Each case of $b = 0, 1$ and $a = 3$ immediately leads to a contradiction. The remaining case $(a, b) = (2, 2)$ leads to a contradiction as follows. Taking the norms of both sides of (4), we have

$$\begin{aligned} N_{k/\mathbb{Q}}(u_4) = 3^3 \operatorname{Tr}_{k/\mathbb{Q}}(u_3)^2 &+ (3^2 + 3^5 N_{k/\mathbb{Q}}(u_3)) \operatorname{Tr}_{k/\mathbb{Q}}(u_3) \\ &+ (3^6 + 1 + 3^3 N_{k/\mathbb{Q}}(u_3)). \end{aligned}$$

For all possible signs of the norms, $\operatorname{Tr}_{k/\mathbb{Q}}(u_3)$ cannot be rational, a contradiction. ■

Hence the assumption that E_1 admits a 3-isogeny defined over k yields a contradiction. This completes the proof of Proposition 2, and hence of Proposition 1.

5. We now determine $E_n^{\pm}(\mathcal{O}_k)$.

PROPOSITION 3. *The Mordell–Weil group of E_0^+ over k is $\langle(-12, 0)\rangle \cong \mathbb{Z}/2\mathbb{Z}$. In particular*, $E_0^+(\mathcal{O}_k) = \{(-12, 0)\}$.

Proof. We first calculate the rank. In general, if E is an elliptic curve defined over $\mathbb{Q}$, then the rank of $E(\mathbb{Q}(\sqrt{m}))$ is calculated from the formula

$$\operatorname{rank} E(\mathbb{Q}(\sqrt{m})) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E^{(m)}(\mathbb{Q}),$$

where $E^{(m)}$ is the quadratic twist by m (for a proof, see [Ro]). Let E be the curve E_0^+ or its twist $(E_0^+)^{(37)}$ and let $L(E/\mathbb{Q}, s)$ be the Hasse–Weil L-function of E. Since E has complex multiplication by $\mathbb{Z}[(1+\sqrt{-3})/2]$ and

$$L(E/\mathbb{Q}, 1) = \begin{cases} 1.2143\ldots & \text{if } E = E_0^+, \\ 3.1941\ldots & \text{if } E = (E_0^+)^{(37)} \end{cases}$$

(which are calculated by SIMATH Version 3.9), we have, by Theorem 1 of Coates–Wiles [CW], $\operatorname{rank} E(\mathbb{Q}) = 0$. Therefore $\operatorname{rank} E_0^+(k) = 0$.

Next, we compute the torsion subgroup. Let $\mathfrak{p}_p$ be a prime ideal lying above a prime number p and let $(E_0^+)_{\mathfrak{p}_p}$ be the reduction modulo $\mathfrak{p}_p$. Since

$$\#(E_0^+)_{\mathfrak{p}_7}(\mathcal{O}_k/\mathfrak{p}_7) = 2^2, \quad \#(E_0^+)_{\mathfrak{p}_{41}}(\mathcal{O}_k/\mathfrak{p}_{41}) = 2\cdot 3\cdot 7,$$

we have, by Theorem 1 of [MSZ], $\#E_0^+(k)_{\mathrm{tors}} \le 2$. This completes the proof. ■

REMARK. The rank of $E_0^+(\mathbb{Q})$ is easily computed by 2-descent, whereas it is hard to compute the rank of $(E_0^+)^{(37)}(\mathbb{Q})$ by the same method, since the (conjectural) order of the Shafarevich–Tate group $Ш$ of $(E_0^+)^{(37)}/\mathbb{Q}$ is 4. This is why the author resorts to L-functions.

REMARK. E. Liverance pointed out that $\operatorname{rank}(E_0^+)^{(37)}(\mathbb{Q}) = 0$ follows from a result in [Sa] without using the L-function. By other results in the same paper, we know that the 3-primary part of $Ш$ is trivial. Hence, combining this with the main result of [Ru], in which the above value of the L-function appears, we see that the order of $Ш$ is exactly 4.

LEMMA 5. *Let u_1, u_2 stand for units in k and A for an integer in k. Then*

(a) *The equation $64u_1 + u_2 = A^2$ has no solution.*
(b) *The solutions of the equation $8u_1 + u_2 = A^2$ are*

$$(u_1, u_2, A) = (w^2, w^2, \pm 3w) \quad (w \in \mathcal{O}_k^\times).$$

(c) *The equation $16u_1 + 2u_2 = A^2$ has no solution.*
(d) *The solutions of the equation $u_1 + u_2 = A^2$ are*

$$(u_1, u_2, A) = (w, -w, 0),\ (w^2\varepsilon^3, w^2\varepsilon'^3, \pm 42w),\ (w^2\varepsilon'^3, w^2\varepsilon^3, \pm 42w) \quad (w \in \mathcal{O}_k^\times).$$

Proof. (a) is a special case of Lemma 2.1 of Ishii [Is]. A key point of his proof is that 64 is divisible by 4. Hence (b) can be proved similarly to (a). The assertion (c) is clear since $8u_1 + u_2$ is prime to 2.

(d) If $A \neq 0$, then Proposition 2 of [Co] implies that

$$u_1 = w^2 u_0, \quad u_2 = w^2 u_0', \quad w, u_0 \in \mathcal{O}_k^\times,\ \operatorname{Tr}_{k/\mathbb{Q}}(u_0) = x^2,\ x \in \mathbb{Z}.$$

We may suppose that u_1 is positive, and hence $u_0 = \varepsilon^n$ for some $n \in \mathbb{Z}$. By Theorem 1 of [KT], $\operatorname{Tr}_{k/\mathbb{Q}}(\varepsilon^n) = x^2$ holds only for $n = 3$, $x = \pm 42$. ■

PROPOSITION 4.

$$E_3^+(\mathcal{O}_k) = \{(-12\varepsilon, 0), (12(588 - \varepsilon^{-3}), \pm 3024(196 + \varepsilon^{-3}))\}.$$

Proof. Factorizing $x^3 = y^2 - 1728\varepsilon^3$ in $L = k(\sqrt{3\varepsilon})$, we have

$$x^3 = (y + 24\varepsilon\sqrt{3\varepsilon})(y - 24\varepsilon\sqrt{3\varepsilon}).$$

Hence, to determine $E_3^+(\mathcal{O}_k)$, we use the following data for L obtained with KASH:

(a) $\mathcal{O}_L = \mathcal{O}_k \oplus \mathcal{O}_k\sqrt{3\varepsilon}$.
(b) A system of fundamental units is ε, $\varepsilon_1 = \varepsilon + 2\sqrt{3\varepsilon}$. Note that $N_{L/k}(\varepsilon_1) = 1$.
(c) 2, π and π' decompose as $(2) = \mathfrak{P}_2^2$, $(\pi) = \mathfrak{P}_3^2$ and $(\pi') = \mathfrak{P}_3'^2$.
(d) The class number of L is 2.

We denote the conjugation of L over k by $^{-}$. Let $(y + 24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{A}\mathfrak{C}^3$, $(y - 24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{B}\mathfrak{D}^3$, where $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ are integral ideals in L such that $\mathfrak{A}, \mathfrak{B}$ are cube-free, $\mathfrak{A}\mathfrak{B}$ is a cube and $\overline{\mathfrak{A}} = \mathfrak{B}$. If a prime ideal $\mathfrak{P}$ in L divides $\mathfrak{A}$, then it divides both of $(y \pm 24\varepsilon\sqrt{3\varepsilon})$. Thus $\mathfrak{P} \mid 48\varepsilon\sqrt{3\varepsilon}$ and we can write

$$\mathfrak{A} = \mathfrak{P}_2^{a_2}\mathfrak{P}_3^{a_3}\mathfrak{P}_3'^{a_3'}, \quad 0 \le a_2, a_3, a_3' < 3.$$

Since $\overline{\mathfrak{A}} = \mathfrak{B}$ and (c), we see that $\mathfrak{A} = \mathfrak{B}$. Moreover, since $\mathfrak{A}\mathfrak{B}$ is a cube, we have $a_2 = a_3 = a_3' = 0$. Hence

$$(y + 24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{C}^3.$$

By (a) and (d), we can write $\mathfrak{C} = (a + b\sqrt{3\varepsilon})$ with $a, b \in \mathcal{O}_k$, and hence $y + 24\varepsilon\sqrt{3\varepsilon} = \eta(a + b\sqrt{3\varepsilon})^3$ with $\eta \in \mathcal{O}_L^\times$. We may write $\eta = \varepsilon^l\varepsilon_1^m$ $(-1 \le l, m \le 1)$ since -1, ε^3 and ε_1^3 can be absorbed in the cube. By (b), taking the norm from L to k yields

$$x^3 = \varepsilon^{2l}\{(a + b\sqrt{3\varepsilon})(a - b\sqrt{3\varepsilon})\}^3,$$

whence $l = 0$ and

$$y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1^m(a + b\sqrt{3\varepsilon})^3, \quad m = 0, \pm 1.$$

If $m = -1$, then taking conjugation yields

$$-y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1(-a + b\sqrt{3\varepsilon})^3.$$

Therefore it is sufficient to solve the following:

$$\pm y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1^m(a + b\sqrt{3\varepsilon})^3, \quad a, b, y \in \mathcal{O}_k,\ m = 0, 1.$$

Case 1: $m = 1$. Equating the coefficients of $\sqrt{3\varepsilon}$ yields

$$2a^3 + 3\varepsilon a^2 b + 18\varepsilon ab^2 + 3\varepsilon^2 b^3 = 24\varepsilon.$$

We see that a is divisible by 3, whence $\varepsilon b^3 \equiv -1 \pmod{\pi^2}$, which is impossible by Lemma 3.

Case 2: $m = 0$. Equating the coefficients yields

$$8\varepsilon = b(a^2 + \varepsilon b^2), \quad \pm y = a(a^2 + 9\varepsilon b^2). \tag{5}$$

From the first equation of (5), we have $b = u, 2u, 4u$ or $8u$ for some positive unit u of k (note that 2 is prime in k). If $b = 8u$, then $a^2 = \varepsilon u^{-1} - 64\varepsilon u^2$, which has no solutions by Lemma 5(a). If $b = u$, then Lemma 5(b) implies that $u^3 = -1$, which contradicts $u > 0$. If $b = 4u$, then $a^2 = -16\varepsilon u^2 + 2\varepsilon u^{-1}$, which has no solutions by Lemma 5(c). If $b = 2u$, then

$$\left(\frac{a}{2}\right)^2 = \varepsilon u^{-1} - \varepsilon u^2. \tag{6}$$

By Lemma 5(d), we see that (6) holds only for $u = 1, \varepsilon^{-2}$, from which we obtain $(a, b) = (0, 2)$, $(\pm 84, 2\varepsilon^{-2})$. By the second equation of (5), the corresponding values of y are 0, $\pm 3024(196 + \varepsilon^{-3})$, respectively. ■

Proposition 5. *The set* $E_0^-(\mathcal{O}_k)$ *consists of the following* 15 *elements*:

$$(12,0),\ (16,\pm 8\sqrt{37}),\ (120,\pm 216\sqrt{37}),\ (3376,\pm 32248\sqrt{37}),$$
$$(44+4\sqrt{37},\pm(320\pm 40\sqrt{37})),\ (572+92\sqrt{37},\pm(19040\pm 3128\sqrt{37})).$$

Proof. Let $L=k(\sqrt{-3})$. To prove the proposition, we use the following data for L obtained with KASH:

(a) $\mathcal{O}_L=\mathcal{O}_k\oplus\mathcal{O}_k\zeta$, where $\zeta=(1+\sqrt{-3})/2$.

(b) $\mathcal{O}_L^\times=\langle\varepsilon\rangle\times\langle\zeta\rangle\cong\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$.

(c) 2, π and π' decompose as $(2)=\mathfrak{P}_2\overline{\mathfrak{P}}_2$ ($\mathfrak{P}_2\neq\overline{\mathfrak{P}}_2$), $(\pi)=\mathfrak{P}_3^2$ and $(\pi')=\mathfrak{P}_3'^2$.

(d) The ideal class group is a cyclic group of order 4 generated by the class of $\mathfrak{P}_2$.

(e) $\mathfrak{P}_2^4=(1+\omega-3\zeta)$.

Arguing similarly to Proposition 4 over the field L, we see that it suffices to solve

$$(\pm y+24\sqrt{-3})=\mathfrak{P}_2^{a_2}\overline{\mathfrak{P}}_2^{\overline{a}_2}\mathfrak{C}^3$$

for $(a_2,\overline{a}_2)=(0,0),(2,1)$, $y\in\mathcal{O}_k$ and an integral ideal $\mathfrak{C}$ of L.

Case 1: $(a_2,\overline{a}_2)=(0,0)$. Since $(\pm y+24\sqrt{-3})=\mathfrak{C}^3$ and, by (d), the class number of L is prime to 3, we see that $\mathfrak{C}$ is a principal ideal. Hence, by (a) and (b), $\pm y+24\sqrt{-3}=\varepsilon^m\zeta^n(a+b\zeta)^3$, $a,b\in\mathcal{O}_k$, $m=0,\pm1$ and $n=0,\pm1$. Taking the norm from L to k of both sides, we obtain $m=0$, and considering the conjugate, we may suppose that $n=0$ or 1.

If $n=0$, equating the coefficients gives

$$\pm y=\frac{1}{2}(a-b)(2a+b)(a+2b), \tag{7}$$
$$16=ab(a+b). \tag{8}$$

From (8) we obtain

$$(a+b,ab)=(u,16u^{-1}),\ (2u,8u^{-1}),\ (4u,4u^{-1}),\ (8u,2u^{-1}),\ (16u,u^{-1})$$

for some unit u of k. If $(a+b,ab)=(4u,4u^{-1})$, then a and b are the roots of the quadratic polynomial

$$X^2-4uX+4u^{-1}.$$

The discriminant of the polynomial is $16(u^2-u^{-1})$, which must be a square. Then, by Lemma 5(d), $(u^2,-u^{-1})=(w,-w),(w^2\varepsilon^3,w^2\varepsilon'^3)$ for some unit w of k. The first case leads to $u=1$, $a=b=2$, and we get $y=0$ by (7). The second case leads to $w^2=\varepsilon$, a contradiction. If $(a+b,ab)=(2u,8u^{-1})$, then the quadratic polynomial satisfied by a and b is

$$X^2-2uX+8u^{-1},$$

whose discriminant $4(u^2-8u^{-1})$ must be a square. By Lemma 5(b), we obtain $u=-1$, $(a,b)=(2,-4),(-4,2)$, and, by (7), $y=0$. For $(a,b)=(u,16u^{-1}),(8u,2u^{-1})$ or $(16u,u^{-1})$, the discriminant of the quadratic polynomials which a,b satisfy are

$$u^2+64u^{-1},\ 4(16u^2-2u^{-1}),\ 4(64u^2-u^{-1}),$$

respectively, none of which is a square by Lemma 5(a), (c).

If $n=1$, then we obtain

$$a^3+3a^2b-b^3=48.$$

We see that $a\equiv b \pmod 3$. Letting $a=3A+b, A\in\mathcal{O}_k$ and reducing modulo π^2, we obtain $b^3\equiv 7 \pmod{\pi^2}$, which contradicts Lemma 3.

Case 2: $(a_2,\overline{a}_2)=(2,1)$. Multiplying both sides by $(4)=(\mathfrak{P}_2\overline{\mathfrak{P}}_2)^2$ and considering (e) yields

$$(4)(\pm y+24\sqrt{-3})=\mathfrak{P}_2^4(\overline{\mathfrak{P}}_2\mathfrak{C})^3=(1+\omega-3\zeta)(\overline{\mathfrak{P}}_2\mathfrak{C})^3,$$

whence, by (d),

$$4(\pm y+24\sqrt{-3})=\zeta^n(1+\omega-3\zeta)(a+b\zeta)^3,\qquad a,b\in\mathcal{O}_k,\ n=0,\pm1.$$

If $n=0$, then equating the coefficients yields

$$-64=a^3-(\omega-2)a^2b-(\omega+1)ab^2-b^3, \tag{9}$$

$$\pm4y-96=(\omega+1)a^3+9a^2b-3(\omega-2)ab^2-(\omega+1)b^3. \tag{10}$$

As we will see later, the solutions of (9) are the following:

$(4,-4),\ (0,4),\ (-4,0),$
$(-3+\sqrt{37},-2\sqrt{37}),\ (-2\sqrt{37},3+\sqrt{37}),\ (3+\sqrt{37},-3+\sqrt{37}),$
$(-40-4\sqrt{37},8\sqrt{37}),\ (8\sqrt{37},40-4\sqrt{37}),\ (40-4\sqrt{37},-40-4\sqrt{37}),$
$(-2,3+\sqrt{37}),\ (-1-\sqrt{37},-2),\ (3+\sqrt{37},-1-\sqrt{37}),$
$(-3+\sqrt{37},2),\ (1-\sqrt{37},-3+\sqrt{37}),\ (2,1-\sqrt{37}),$
$(-19-3\sqrt{37},16+2\sqrt{37}),\ (16+2\sqrt{37},3+\sqrt{37}),\ (3+\sqrt{37},-19-3\sqrt{37}),$
$(-16+2\sqrt{37},19-3\sqrt{37}),\ (-3+\sqrt{37},-16+2\sqrt{37}),\ (19-3\sqrt{37},-3+\sqrt{37}).$

Substituting them in (10), we get all the values of y except 0.

If $n=1$ or $n=-1$, then we obtain

$$192=(-2+\omega)a^3+3(1+\omega)a^2b+9ab^2+(2-\omega)b^3,$$
$$-192=(1+\omega)a^3+9a^2b+3(1+\omega)a^2b-(2-\omega)b^3,$$

respectively. They are shown to be impossible similarly to the case $n=1$ in Case 1. ∎

Remark. The rank of $E_0^-(k)=(E_0^-)^{(37)}(\mathbb{Q})$ is 2, which is easily seen by 2-descent.

6. In [dW2], de Weger solves the Thue equation

$$x^3 + (9 + 2\sqrt{13})x^2y - (12 + \sqrt{13})xy^2 - \frac{11 + 3\sqrt{13}}{2}y^3 = \left(\frac{3 + \sqrt{13}}{2}\right)^n$$

with variables x, y in $\mathcal{O}_{\mathbb{Q}(\sqrt{13})}$ and n in $\mathbb{Z}$. To the author's knowledge, this is the only example in the literature where a Thue equation over a real quadratic field is solved completely. By imitating his proof, we can solve the Thue equation (9) as follows.

Let $(a, b) \in \mathcal{O}_k \times \mathcal{O}_k$ be a solution of (9). Putting $A = -a - (\omega + 2)b$ we have

$$A^3 + (4\omega + 4)A^2b + (16\omega + 48)Ab^2 + (32\omega + 80)b^3 = 64.$$

It is easy to see that $4 \mid A$ and $2 \mid b$. By putting $A = 4X, b = 2Y$, we have

$$X^3 + 2(\omega + 1)X^2Y + 4(\omega + 3)XY^2 + 2(2\omega + 5)Y^3 = 1. \tag{11}$$

Hence it suffices to prove the following:

PROPOSITION 6. *The only* $(X, Y) \in \mathcal{O}_k \times \mathcal{O}_k$ *satisfying* (11) *are*

$$\begin{gathered}
(-2 - 9\omega, 22 - 4\omega),\ (-23 - 8\omega, -4 + 8\omega),\ (25 + 17\omega, -18 - 4\omega),\\
(21 + 8\omega, -8 - 3\omega),\ (-9 - 3\omega, 1 + \omega),\ (-12 - 5\omega, 7 + 2\omega),\\
(9 + 2\omega, 1 - 2\omega),\ (-3 - \omega, -2 + \omega),\ (-6 - \omega, 1 + \omega),\\
(-5 - 2\omega, 1 + \omega),\ (1 + \omega, -1),\ (4 + \omega, -\omega),\\
(-2 - \omega, 2),\ (1, 0),\ (1 + \omega, -2),\\
(3 + \omega, 1 - \omega),\ (-\omega, 1),\ (-3, -2 + \omega),\\
(7 - 2\omega, 11 - 3\omega),\ (1 + \omega, -9 + 2\omega),\ (-8 + \omega, -2 + \omega).
\end{gathered}$$

Proof. Let $F(X, Y)$ be the left hand side of (11), θ a root of the polynomial $F(X, 1)$ and let $L = \mathbb{Q}(\theta)$. Then $k \subset L$, $[L : \mathbb{Q}] = 6$ and $\mathcal{O}_L = \mathbb{Z}[\xi]$, where $\xi = (12 + 18\theta - 4\theta^3 - \theta^4)/20$. In particular, $\theta = 4\xi - 5\xi^2 - 4\xi^3 + 4\xi^4 + \xi^5$ and $\sqrt{37} = 3 - 12\xi - 8\xi^2 + 8\xi^3 + 2\xi^4$. The extension $L/\mathbb{Q}$ is Galois with Galois group $\langle \sigma, \tau \rangle$, where σ and τ are given by

$$\begin{aligned}
\sigma(\xi) &= -14 - 6\xi + 49\xi^2 + 9\xi^3 - 28\xi^4 - 6\xi^5,\\
\tau(\xi) &= -1 - 3\xi + 5\xi^2 + 4\xi^3 - 4\xi^4 - \xi^5,
\end{aligned}$$

and they satisfy $\sigma^3 = 1, \tau^2 = 1$ and $\sigma\tau = \tau\sigma^2$. Thus $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the symmetric group of degree 3. The conjugates of ξ in L are numbered as follows:

$$\begin{aligned}
\xi^{(1)} &= \xi = -4.6017164\ldots,\\
\xi^{(2)} &= \sigma(\xi) = -0.5284180\ldots,\\
\xi^{(3)} &= \sigma^2(\xi) = -0.4112467\ldots,\\
\xi^{(4)} &= \tau(\xi) = -1.2776453\ldots,
\end{aligned}$$

$$\xi^{(5)} = \tau\sigma(\xi) = 0.6985045\ldots,$$
$$\xi^{(6)} = \tau\sigma^2(\xi) = 1.1205221\ldots$$

The conjugates of θ are numbered in accordance with the numbering of the conjugates of ξ. A system of fundamental units of L is given by

$$\begin{aligned}
\varepsilon_1 &= -\xi,\\
\varepsilon_2 &= -5 - 4\xi + 18\xi^2 + 5\xi^3 - 9\xi^4 - 2\xi^5,\\
\varepsilon_3 &= -6 - 8\xi + 23\xi^2 + 9\xi^3 - 13\xi^4 - 3\xi^5,\\
\varepsilon_4 &= 1 + 3\xi - 5\xi^2 - 4\xi^3 + 4\xi^4 + \xi^5,\\
\varepsilon_5 &= -16 - 15\xi + 63\xi^2 + 18\xi^3 - 36\xi^4 - 8\xi^5.
\end{aligned}$$

The actions of σ and τ on the units are as follows:

$$\sigma(\varepsilon_i) = \begin{cases} \varepsilon_3^{-1} & \text{if } i = 1,\\ \varepsilon_4^{-1} & \text{if } i = 2,\\ \varepsilon_1\varepsilon_3^{-1} & \text{if } i = 3,\\ \varepsilon_2\varepsilon_4^{-1} & \text{if } i = 4,\\ \varepsilon_1\varepsilon_2^{-1}\varepsilon_3^{-1}\varepsilon_4\varepsilon_5 & \text{if } i = 5, \end{cases} \qquad \tau(\varepsilon_i) = \begin{cases} \varepsilon_4 & \text{if } i = 1,\\ \varepsilon_3 & \text{if } i = 2,\\ \varepsilon_2 & \text{if } i = 3,\\ \varepsilon_1 & \text{if } i = 4,\\ -\varepsilon^{-1}\varepsilon_2\varepsilon_3\varepsilon_4^{-1}\varepsilon_5^{-1} & \text{if } i = 5. \end{cases}$$

Since (11) is equivalent to $N_{L/k}(X - Y\theta) = 1$, we have $\eta := X - Y\theta = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_4^{a_4}$ for some $a_1, \ldots, a_4 \in \mathbb{Z}$ (note that $N_{L/k}(\varepsilon_i) = 1$ $(i = 1, 2, 3, 4)$ and $N_{L/k}(\varepsilon_5) = \varepsilon$). Eliminating X, Y we obtain

$$(\sigma(\theta) - \sigma^2(\theta))\eta + (\sigma^2(\theta) - \theta)\sigma(\eta) + (\theta - \sigma(\theta))\sigma^2(\eta) = 0,$$

hence

$$\frac{\theta - \sigma^2(\theta)}{\theta - \sigma(\theta)} \cdot \frac{\sigma(\eta)}{\sigma^2(\eta)} - 1 = -\frac{\sigma(\theta) - \sigma^2(\theta)}{\sigma(\theta) - \theta} \cdot \frac{\eta}{\sigma^2(\eta)},$$

or equivalently

$$-\varepsilon_1^{b_1}\varepsilon_2^{b_2}\varepsilon_3^{b_3}\varepsilon_4^{b_4} - 1 = \varepsilon_1^{d_1}\varepsilon_2^{d_2}\varepsilon_3^{d_3}\varepsilon_4^{d_4}, \tag{12}$$

where

$$b_1 = a_1 + 2a_3, \quad b_2 = a_2 + 2a_4 - 1, \quad b_3 = -2a_1 - a_3 + 1, \quad b_4 = -2a_2 - a_4,$$
$$d_1 = -b_3, \quad d_2 = -b_4, \quad d_3 = b_1 + b_3, \quad d_4 = b_2 + b_4.$$

As in [Ki1], [TdW], [dW1] or [dW2], we estimate linear forms in the logarithms

$$\Lambda_i = \sum_{j=1}^{4} b_j \log|\varepsilon_j^{(i)}| = \begin{cases} \log\left|\dfrac{\theta^{(i)} - \sigma^2(\theta^{(i)})}{\theta^{(i)} - \sigma(\theta^{(i)})} \cdot \dfrac{\sigma(\eta^{(i)})}{\sigma^2(\eta^{(i)})}\right| & (1 \le i \le 3),\\[2ex] \log\left|\dfrac{\theta^{(i)} - \sigma(\theta^{(i)})}{\theta^{(i)} - \sigma^2(\theta^{(i)})} \cdot \dfrac{\sigma^2(\eta^{(i)})}{\sigma(\eta^{(i)})}\right| & (4 \le i \le 6). \end{cases}$$

Let $i_0 \in \{1, \ldots, 6\}$ be the index such that $|\eta^{(i_0)}| = \min_{1\le i\le 6}\{|\eta^{(i)}|\}$. By a similar argument to that given in [dW2] (we omit the details) we find that

$$|\Lambda_{i_0}| < 4.1069 \exp(-0.24457B),$$

subject to the condition $B := \max\{|b_1|, |b_2|, |b_3|, |b_4|\} \geq 100$. As explained in [dW1], §3.2, we may suppose that $i_0 = 1$. By the main result of [BW] (again we omit the details), we find

$$\log|\Lambda_1| > -4.1810 \cdot 10^{18} \log(B).$$

Combining these bounds we have $B \leq 1.5142 \cdot 10^{21}$.

Applying Proposition 3.1 of [TdW] to our case by taking the parameter c_0 appearing there to be 10^{100}, we get a much smaller bound $B \leq 719$. We again apply the same proposition by taking $c_0 = 10^{18}$ and we get $B \leq 141$.

We search this range for solutions of (12) and find 39 solutions, 21 of which give integral (a_1, a_2, a_3, a_4); following the argument in [dW2], p. 860, the search takes less than 15 minutes on Sparc station SS4 with a C-program. For each (a_1, a_2, a_3, a_4), we see with KASH that the unit $\varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_4^{a_4}$ is of the form $X - Y\theta$. We list the solutions in Table 1. ■

Table 1. The solutions of (11) and (12)

a_1	a_2	a_3	a_4	b_1	b_2	b_3	b_4	X	Y
−3	−4	−1	5	−5	5	8	3	$-2-9\omega$	$22-4\omega$
0	4	4	0	8	3	−3	−8	$-23-8\omega$	$-4+8\omega$
5	−1	−4	−3	−3	−8	−5	5	$25+17\omega$	$-18-4\omega$
4	−1	−4	1	−4	0	−3	1	$21+8\omega$	$-8-3\omega$
−3	0	0	1	−3	1	7	−1	$-9-3\omega$	$1+\omega$
1	0	3	0	7	−1	−4	0	$-12-5\omega$	$7+2\omega$
3	−3	−3	3	−3	2	−2	3	$9+2\omega$	$1-2\omega$
−2	2	0	1	−2	3	5	−5	$-3-\omega$	$-2+\omega$
1	0	2	−2	5	−5	−3	2	$-6-\omega$	$1+\omega$
2	0	−2	1	−2	1	−1	−1	$-5-2\omega$	$1+\omega$
−1	0	0	0	−1	−1	3	0	$1+\omega$	-1
1	−1	1	1	3	0	−2	1	$4+\omega$	$-\omega$
1	0	−1	1	−1	1	0	−1	$-2-\omega$	2
0	0	0	0	0	−1	1	0	1	0
1	−1	0	1	1	0	−1	1	$1+\omega$	-2
1	1	−1	1	−1	2	0	−3	$3+\omega$	$1-\omega$
0	0	0	−1	0	−3	1	1	$-\omega$	1
1	−2	0	2	1	1	−1	2	-3	$-2+\omega$
1	−4	−1	4	−1	3	0	4	$7-2\omega$	$11-3\omega$
0	3	0	1	0	4	1	−7	$1+\omega$	$-9+2\omega$
1	0	0	−3	1	−7	−1	3	$-8+\omega$	$-2+\omega$

7. In his paper [Kr], Kraus gives local conditions on $(x, y) \in E_n^{\pm}(\mathcal{O}_k)$ which guarantee the existence of a Weierstrass equation with $(c_4, c_6) = (x, y)$. It turns out that only the following two satisfy the conditions of his results:

$$(16\varepsilon^{-2},\ -8\sqrt{37}\varepsilon^{-3}), (3376\varepsilon^{-2}, 32248\sqrt{37}\varepsilon^{-3}) \in E^-_{-6}(\mathcal{O}_k).$$

The former corresponds to Shimura's elliptic curve C_1 and the latter to C_2.

Instead of using Kraus' results, computing the conductor of the elliptic curve

$$Y^2 = X^3 - 27xX - 54y$$

by Tate's algorithm ([Ta]) also gives the result (each $(x, y) \in E^{\pm}_n(\mathcal{O}_k)$ other than the above gives an elliptic curve with good reduction outside 2). Tate's algorithm over quadratic fields is implemented by A. Umegaki on Sparc work station using PARI/GP Version 1.39. A similar algorithm is implemented in SIMATH Version 3.9, but it does not work in some cases, including ours.

Thus we complete the proof of Theorem.

Acknowledgments. We would like to express our thanks to Professor K. Hashimoto for introducing us to this subject, to K. Aoki for his information about various number theory software such as KASH and SIMATH, which were indispensable for this work. We also thank A. Umegaki for several useful discussions.

References

[BW] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. 442 (1993), 19–62.

[BK] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. 44 (1977), 715–743.

[Ca] W. Casselman, *On abelian varieties with many endomorphisms, and a conjecture of Shimura's*, Invent. Math. 12 (1971), 225–236.

[CW] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, ibid. 39 (1977), 223–251.

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

[DR] P. Deligne et M. Rapoport, *Les schémas de modules des courbes elliptiques*, in: Modular Functions of One Variable II, Lecture Notes in Math. 349, Springer, 1973, 143–316.

[Fr] R. Fricke, *Die elliptischen Funktionen und ihre Anwendungen*, Teubner, Leipzig, 1922.

[Ha1] Y. Hasegawa, *$\mathbb{Q}$-curves over quadratic fields*, Manuscripta Math., to appear.

[Ha2] —, *Table of cuspforms on $\Gamma_1(N)$ with real quadratic characters*, unpublished.

[HHM] Y. Hasegawa, K. Hashimoto and F. Momose, *Modular conjecture for $\mathbb{Q}$-curves and QM-curves*, preprint.

[He] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Grad. Texts in Math. 77, Springer, 1981.

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

[KT] T. Kagawa and N. Terai, *Squares in Lucas sequences and some Diophantine equations*, Manuscripta Math., to appear.

[KM] N. Katz and B. Mazur, *The Arithmetic Moduli of Elliptic Curves*, Princeton Univ. Press, 1985.

[Ki1] M. Kida, *On a characterization of Shimura's elliptic curve over* $\mathbb{Q}(\sqrt{37})$, Acta Arith. 77 (1996), 157–171.

[Ki2] —, private communication.

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

[Kr] A. Kraus, *Quelques remarques à propos des invariants* c_4, c_6 *et* Δ *d'une courbe elliptique*, Acta Arith. 54 (1989), 75–80.

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

[Pi1] R. G. E. Pinch, *Elliptic curves over number fields*, Ph.D. thesis, Oxford, 1982.

[Pi2] —, *Elliptic curves with good reduction away from* 3, Math. Proc. Cambridge Philos. Soc. 101 (1987), 451–459.

[Ro] M. I. Rosen, *Some confirming instances of the Birch–Swinnerton-Dyer conjecture over biquadratic fields*, in: Number Theory, R. A. Mollin (ed.), Walter de Gruyter, 1990, 493–499.

[Ru] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), 25–68.

[Sa] P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory 23 (1986), 294–317.

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

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

[Shim] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan 11, Iwanami Shoten and Princeton Univ. Press, 1971.

[Shio] K. Shiota, *On the explicit models of Shimura's elliptic curves*, J. Math. Soc. Japan 38 (1986), 649–659.

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[Str] R. J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*, Pacific J. Math. 108 (1983), 451–463.

[Ta] J. Tate, *Algorithm for determining the type of a singular fibre in an elliptic pencil*, in: Modular Functions of One Variable IV, Lecture Notes in Math. 476, Springer, 1975, 33–52.

[TdW] N. Tzanakis and B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory 31 (1989), 99–132.

[Um] A. Umegaki, *A construction of everywhere good* $\mathbb{Q}$*-curves with* p*-isogeny*, preprint.

[dW1] B. M. M. de Weger, *A hyperelliptic diophantine equation related to imaginary quadratic number fields with class number* 2, J. Reine Angew. Math. 427 (1992), 137–156; Correction: ibid. 441 (1993), 217–218.

[dW2] B. M. M. de Weger, *A Thue equation with quadratic integers as variables*, Math. Comp. 64 (1995), 855–861.

Department of Information and Computer Science
School of Science and Engineering
Waseda University
3-4-1, Ohkubo Shinjuku-ku
Tokyo 169, Japan
E-mail: kagawa@mn.waseda.ac.jp

Received on 24.3.1997
and in revised form on 3.10.1997 (3148)