ACTA ARITHMETICA
LXXVII.2 (1996)

# On a characterization of Shimura's elliptic curve over $\mathbb{Q}(\sqrt{37})$

by

Masanari Kida (Baltimore, Md., and Yamagata)

**1.** Let $k$ be the real quadratic field $\mathbb{Q}(\sqrt{37})$, $\widetilde{\chi}$ the associated Legendre character modulo 37, $\sigma$ the generator of the Galois group $\mathrm{Gal}(k/\mathbb{Q})$, and

$$\mathit{\Gamma}_0 = \mathit{\Gamma}_0(37) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \pmod{37} \right\}.$$

Then

$$\chi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \widetilde{\chi}(a)$$

is a homomorphism of $\mathit{\Gamma}_0$ onto $\{\pm 1\}$. Set $\mathit{\Gamma}_\chi = \ker(\chi)$. Denote by $X_0$ (resp. $X_\chi$) the modular curve corresponding to $\mathit{\Gamma}_0$ (resp. $\mathit{\Gamma}_\chi$) with Jacobian $J_0$ (resp. $J_\chi$). Put $J = \mathrm{coker}(J_0 \to J_\chi)$, where the map $J_0 \to J_\chi$ is induced by the natural inclusion $\mathit{\Gamma}_\chi \to \mathit{\Gamma}_0$. The algebraic variety $J$ is an abelian variety of dimension 2 defined over $\mathbb{Q}$ that is obtained from the eigenform in the space $S_2(\mathit{\Gamma}_0, \widetilde{\chi})$ of cusp forms of "Neben"-type of weight two. Moreover, $J$ splits over $k$ as a product $E_{37} \times E_{37}^{\sigma}$ of elliptic curves defined over $k$, where $E_{37}^{\sigma}$ stands for the conjugate curve of $E_{37}$. It is also shown that the Hasse–Weil $L$-function of $E_{37}$ has an analytic continuation to the whole complex plane and satisfies the functional equation (cf. [13]). Note that the elliptic curve $E_{37}$ has no complex multiplication (cf. [11]). Further, the curve $E_{37}$, which we call *Shimura's elliptic curve* over $k$, has the following interesting properties:

(I) $E_{37}$ has good reduction at every finite place of the ring of algebraic integers in $k$ (see [2] and [5], V, 3.7(ii));

(II) $E_{37}$ is isogenous to $E_{37}^{\sigma}$.

It is known that the degree of the isogeny in (II) is one, i.e., $E_{37}$ is isomorphic to its Galois conjugate. (Such elliptic curves are usually called $\mathbb{Q}$-*curves*.) For the fact cited above, we refer to [13], §§7.5, 7.7, [14], and [15].

In this paper, we shall give the following characterization of Shimura's elliptic curve $E_{37}$.

THEOREM. *Every elliptic curve defined over $k$ with good reduction everywhere that is isomorphic to its Galois conjugate is isogenous to Shimura's elliptic curve $E_{37}$ over $k$.*

To prove this, we shall find all elliptic curves with the above properties. In the next section, by using Setzer's result [12], we reduce the problem to solving a set of Diophantine equations and, in Section 3, we solve these equations by the method of Steiner [18] and Tzanakis–de Weger [19]. We prove the theorem in the last section.

Here we should mention a result of Shiota. In his paper [16], he computed an explicit model of $E_{37}$ and characterized it by its torsion point structure. Our characterization, on the other hand, is more intrinsic (see the end of Section 4).

The notations introduced in this section will be used throughout the paper. In addition, for an elliptic curve $E$, let $j(E)$ denote the $j$-invariant of $E$.

**2.** An elliptic curve defined over $k$ is called *special* if it has good reduction everywhere and is isomorphic to the conjugate curve. Now let $E$ be a special curve. Since $E$ and $E^{\sigma}$ are isomorphic, we have $j(E) = j(E^{\sigma}) = j(E)^{\sigma}$. Therefore the $j$-invariant of a special curve is rational. Further, it is a rational integer, because the curve has good reduction at every finite place.

Let $\mathcal{A}$ be the set consisting of rational integers $A$ that satisfy the three conditions below:

(P1) If 2 divides $A$, then 16 divides $A$ or $A - 4$.
(P2) If 3 divides $A$, then 27 divides $A - 12$.
(P3) The square free part of $A^3 - 1728$ divides 37.

PROPOSITION 1. *There is a one-to-one correspondence between $\mathcal{A}$ and the set of special curves over $k$.*

Remark. The two sets appearing in the statement of this proposition are both finite. The finiteness of $\mathcal{A}$ follows from Siegel's theorem ([17], §IX.3) and Shafarevich's theorem ([17], §IX.6) guarantees that of the latter set.

Proof of Proposition 1. Put

$\mathcal{R}$ = the set of elliptic curves over $k$ having good reduction everywhere with rational $j$-invariant,
$\mathcal{S}$ = the set of special curves over $k$.

By the argument above, we have $\mathcal{S} \subset \mathcal{R}$.

For $A$ $(\neq 0, 12) \in \mathbb{Z}$, $u \in k^\times$, define the elliptic curve $E_{A,u}$ by

$$y^2 = x^3 - 3A(A^3 - 1728)u^2x - 2(A^3 - 1728)^2u^3.$$

We have $j(E_{A,u}) = A^3$.

Theorems 1 and 2(a) of [12] yield that every curve in $\mathcal{R}$ is isomorphic to $E_{A,u}$ for some $A \in \{A \in \mathbb{Z} \mid A \text{ satisfies (P1) and (P2)}\}$ and $u \in k^\times$. From Theorem 2(b) in the same paper, it follows that the square-free part of $A^3 - 1728$ must divide the discriminant of $k$. The same theorem shows that there is only one $u \in k^\times$ for $A \in \mathcal{A}$. So we have shown that $A \mapsto E_{A,u}$ gives a one-to-one correspondence between $\mathcal{A}$ and $\mathcal{R}$.

For $E = E_{A,u} \in \mathcal{R}$, the conjugate curve $E^\sigma$ has good reduction everywhere and the same $j$-invariant as $E$. Therefore $E^\sigma$ is of the form $E_{A,u'}$. By the uniqueness of $u$ for $A$, $E^\sigma$ is isomorphic to $E$. Hence $\mathcal{R} \subset \mathcal{S}$. ∎

**3.** In this section, we explicitly determine the set $\mathcal{A}$ defined at the beginning of the previous section.

We first consider the condition (P3). To find $A$'s satisfying it, the following Diophantine equations must be solved in rational integers $A$ and $B$:

$$A^3 - 1728 = B^2, \tag{1}$$

$$A^3 - 1728 = -B^2, \tag{2}$$

$$A^3 - 1728 = 37B^2, \tag{3}$$

$$A^3 - 1728 = -37B^2. \tag{4}$$

LEMMA 1. *The Diophantine equations* (1) *and* (2) *have only one solution* $(A, B) = (12, 0)$.

Proof. Setting $x = A/4$ (resp. $x = -A/4$) and $y = B/8$, we obtain

$$C1 : y^2 = x^3 - 27, \qquad C2 : y^2 = x^3 + 27,$$

respectively. These equations define elliptic curves over $\mathbb{Q}$ and their Mordell–Weil groups are cyclic of order 2. In fact, $C1$ (resp. $C2$) is the curve 36C (resp. 144C) in the tables in [1] (see also [4]). It is easy to see that the point $(x, y) = (3, 0)$ (resp. $(-3, 0)$) generates the group. ∎

To solve the equations (3) and (4), we need the following result due to Hemer.

LEMMA 2 (Hemer [6], Theorems 4 and 5). *Consider the equation* $y^2 - \kappa f^2 = x^3$, *where* $\kappa$ *is a square-free integer* $\neq 1$, $f \in \mathbb{Z}$, *and* $\gcd(f, x^3)$ *is cube-free. Suppose that the class number of the quadratic field* $L = \mathbb{Q}(\sqrt{\kappa})$ *is not divisible by* 3. *Denote by* $\varepsilon$ *the fundamental unit of* $L$ *if* $\kappa > 1$.

(i) *If $2f$ does not contain primes that decompose in $L$, then all the integral solutions of the equation $y^2-\kappa f^2=x^3$ can be found by solving the equations*

$$\pm y+f\sqrt{\kappa}=\eta\alpha^3,$$

*where $\alpha$ is an integer in $L$ and $\eta=1$ or $\varepsilon$ if $\kappa>1$ and $\eta=1$ if $\kappa<0$ and also $\eta=(1+\sqrt{-3})/2$ if $\kappa=-3$.*

(ii) *If $2f$ contains $r$ different primes that decompose in $L$, say, $p_i=P_iP_i'$, then all the integral solutions of the equation $y^2-\kappa f^2=x^3$ can be found by solving the equations*

$$\prod_{i=1}^{r}p_i^{q_i}(\pm y+f\sqrt{\kappa})=\prod P_i^{h_i}\alpha^3=\eta\beta\alpha^3,$$

*where $\alpha$ is an integer in $L$ and $h_i=0$ or the least positive integer such that $P_i^{h_i}$ is a principal ideal and all combinations of these values are considered. When $h_i=0$, we put $q_i=0$, and when $h_i>0$ (and thus $h_i\not\equiv 0 \pmod 3$), we put*

$$q_i=\begin{cases}h_i-2 & \text{if } h_i\equiv 1 \pmod 3,\\ h_i-1 & \text{if } h_i\equiv 2 \pmod 3.\end{cases}$$

*Further, if $\kappa>0$, then $\eta=1,\varepsilon$, or $\varepsilon'$ (the conjugate of $\varepsilon$). If $\kappa<0$ and $\kappa\neq-3$, then $\eta=1$, and if $\kappa=-3$, then $\eta=1$ or $(1+\sqrt{-3})/2$.*

We solve the equation (4) first.

Lemma 3. *The Diophantine equation* (4) *has only one solution $(A,B)=(12,0)$.*

Proof. Multiplying the equation by $37^3$ and setting $x=-37A$ and $y=37^2B$, we have

$$y^2-111(2^3\cdot 3\cdot 37)^2=x^3. \tag{5}$$

Assume first that $\gcd(f,x^3)$ is not cube-free. In this case, $x$ is divisible by 2. Then an elementary argument shows that $2^2\mid x$ and $2^3\mid y$. Setting $x=2^2x'$ and $y=2^3y'$, we obtain

$$y'^2-111(3\cdot 37)^2=x'^3.$$

Since $2,3$, and 37 do not decompose in $L=\mathbb{Q}(\sqrt{111})$ and the class number of $L$ is 2, we can apply Lemma 2(i) with $\kappa=111$ and $f=3\cdot 37$. Thus all the integral solutions of (5) are contained in the solutions of the equations

$$\pm y'+3\cdot 37\sqrt{111}=\eta\alpha^3, \tag{6}$$

where $\eta=1$ or $\varepsilon=295+28\sqrt{111}$. We set $\alpha=a+b\sqrt{111}$.

When $\eta=1$, the equation (6) yields $37=b(a^2+37b^2)$. It is easy to solve this equation and we get only one solution $(a,b)=(0,1)$, from which we obtain $(x',y')=(-111,0)$ and $(A,B)=(12,0)$.

If $\eta = \varepsilon$, then we have

$$111 = 28a^3 + 885a^2b + 9324ab^2 + 32745b^3.$$

It is readily seen that $a \equiv 0 \pmod 3$. Putting $a = 3a'$ gives

$$37 = 252a'^3 + 2655a'^2b + 9324a'b^2 + 10915b^3.$$

Reducing this equation modulo $3^2$ yields $7b^3 \equiv 1 \pmod{3^2}$, which is impossible. So there is no solution in this case.

Next we consider the case where $\gcd(f, x^3)$ is cube-free. Applying Lemma 2(i) with $\kappa = 111$ and $f = 2^3 \cdot 3 \cdot 37$, we get the equations

$$\pm y + 2^3 \cdot 3 \cdot 37\sqrt{111} = \eta\alpha^3.$$

A similar argument to that above shows that the equation has one solution $(x, y) = (-444, 0)$, which does not meet the condition on $\gcd(f, x^3)$. ■

The rest of this section is devoted to solving the Diophantine equation (3). We prove:

LEMMA 4. *The solutions of the Diophantine equation* (3) *are*

$$(A, B) = (12, 0), (16, \pm 8), (120, \pm 216), (3376, \pm 32248).$$

Proof. As in the preceding lemma, multiplying the equation by $37^3$ and setting $x = 37A$ and $y = 37^2B$, we get

$$y^2 + 111(2^3 \cdot 3 \cdot 37)^2 = x^3. \tag{7}$$

First suppose that $\gcd(f, x^3)$ is cube-free. Put $\kappa = -111$ and $f = 2^3 \cdot 3 \cdot 37$. It is readily shown that the class number of $L = \mathbb{Q}(\sqrt{-111})$ is 8 and that, among the prime divisors of $f$, only 2 splits in $L$. Also we can show

$$2^8 = \left(\frac{5 + 3\sqrt{-111}}{2}\right)\left(\frac{5 - 3\sqrt{-111}}{2}\right)$$

is the least power of 2 dividing into principal ideals. That is, the prime ideals lying above 2 have order 8 in the ideal class group of $L$. According to Lemma 2(ii), we have to solve the equations below:

$$\pm\, y + 2^3 \cdot 3 \cdot 37\sqrt{-111} = \left(\frac{a + b\sqrt{-111}}{2}\right)^3, \tag{8}$$

$$2^7(\pm y + 2^3 \cdot 3 \cdot 37\sqrt{-111}) = \left(\frac{5 + 3\sqrt{-111}}{2}\right)\left(\frac{a + b\sqrt{-111}}{2}\right)^3. \tag{9}$$

The equation (8) yields $b\,(a^2 - 37b^2) = 2^6 \cdot 37$, from which we can derive the solution $(a, b) = (0, -4)$. The corresponding solution of (7) does not satisfy the condition on $\gcd(f, x^3)$.

From (9), it follows that

$$a^3 + 5a^2b - 333ab^2 - 185b^3 = 606208.$$

Set $a = x + y$ and $b = y$. We obtain

$$x^3 + 8x^2y - 320xy^2 - 512y^3 = 606208.$$

It is easily seen that $x \equiv 0 \pmod 8$. Writing $x = 8x'$, we get

$$x'^3 + x'^2y - 5x'y^2 - y^3 = 1184.$$

By putting $x' = A + B$ and $y = A$, this yields

$$-4A^3 + 4AB^2 + B^3 = 1184.$$

By an easy argument, this implies $2 \mid A$ and $4 \mid B$. On setting $A = -2X, B = 4Y$, the equation finally becomes

$$X^3 - 4XY^2 + 2Y^3 = 37. \tag{10}$$

Next we assume that $\gcd(f, x^3)$ is not cube-free. Then 2 divides $x$. As before, it can be shown that $4 \mid x$ and $8 \mid y$. Replacing $x$ (resp. $y$) by $4x'$ (resp. $8y'$) in (7), we obtain

$$y'^2 + 111(3 \cdot 37)^2 = x'^3.$$

Applying Lemma 2(ii) with $\kappa = -111$ and $f = 3 \cdot 37$, we have the following equations:

$$\pm y' + 3 \cdot 37\sqrt{-111} = \left(\frac{a + b\sqrt{-111}}{2}\right)^3,$$

$$2^7(\pm y' + 3 \cdot 37\sqrt{-111}) = \left(\frac{5 + 3\sqrt{-111}}{2}\right)\left(\frac{a + b\sqrt{-111}}{2}\right)^3.$$

The first equation yields $2^3 \cdot 37 = b\,(a^2 - 37b^2)$. So we have the solution $(a, b) = (0, -2)$, which implies $(A, B) = (12, 0)$.

From the second equation, we have

$$a^3 + 5a^2b - 333ab^2 - 185b^3 = 75776.$$

Setting $a = x + y$ and $b = y$ yields

$$x^3 + 8x^2y - 320xy^2 - 512y^3 = 75776.$$

It is easily seen that $x \equiv 0 \pmod 8$. Putting $x = 8x'$, we get

$$x'^3 + x'^2y - 5x'y^2 - y^3 = 148.$$

The substitution $x' = -A + B$ and $y = -A$ yields

$$4A^3 - 4AB^2 + B^3 = 148.$$

Finally, by putting $A = X$ and $B = 2Y$, we again obtain the equation (10).

Therefore our problem is reduced to finding the solutions of the Thue equation (10).

Here we should note that, in his paper [18], Steiner solved the Thue equation

$$X^3 - 4XY^2 + 2Y^3 = 1.$$

So we make use of a part of his computation.

Let $F(X,Y) = X^3 - 4XY^2 + 2Y^3$ be the left hand side of (10) and set $g(X) = F(X,1)$. The equation $g(X) = 0$ has three real roots. We denote one of them by $\vartheta$ and consider the cubic field $K = \mathbb{Q}(\vartheta)$. By Steiner's computation (cf. [18]), the ring of integers of $K$ has a basis $(1, \vartheta, \vartheta^2)$ and the fundamental units are given by

$$\varepsilon_1 = 1 - \vartheta, \qquad \varepsilon_2 = 1 - 2\vartheta.$$

Define

$$\mu_1 = 13 - 2\vartheta - 3\vartheta^2, \qquad \mu_2 = 1 + \vartheta + \vartheta^2$$

and $M = \{\pm\mu_1, \pm\mu_2\}$. Then we have a factorization $37 = \mu_1\mu_2^2$ in $K$. Now the equation (10) implies $N(X - Y\vartheta) = 37$, where $N$ is the norm map from $K$ to $\mathbb{Q}$. Thus we obtain

$$X - Y\vartheta = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\mu, \qquad a_1, a_2 \in \mathbb{Z}, \mu \in M. \tag{11}$$

In the range $H = \max(|a_1|, |a_2|) < 26$, we can find the following solutions by a machine computation:

$$\begin{aligned}(\mu, a_1, a_2; X, Y) = {} & (\mu_1, -2, 1; -3, 2), \\ & (-\mu_1, -1, 2; -5, -9), \\ & (\mu_2, -2, 0; 7, -3), \\ & (-\mu_2, 1, 0; -3, -4), \\ & (-\mu_2, 9, -4; -67, -40).\end{aligned} \tag{12}$$

On the other hand, by searching solutions of (10) in the range $|X|$ and $|Y| < 500$, we again get the above five solutions. We claim that these are all the integral solutions of (10).

To show this, we use the algorithm due to Tzanakis and de Weger [19] (see also [20]). In the following, we explain the algorithm and present the computed numerical values. Let $\vartheta^{(1)}, \vartheta^{(2)}, \vartheta^{(3)}$ be the roots of $g(X) = 0$:

$$\begin{aligned}\vartheta^{(1)} &\doteq -2.21431974337753519, \\ \vartheta^{(2)} &\doteq 0.53918887281088912, \\ \vartheta^{(3)} &\doteq 1.67513087056664607.\end{aligned}$$

Set $\beta^{(i)} = X - \vartheta^{(i)}Y$ ($i \in I$), where $I = \{1, 2, 3\}$. We define $\varepsilon_1^{(i)}$, etc., in a similar way. Moreover, we put

$$\begin{aligned}
C_1 &= \frac{2^2\cdot 37}{\min_{i\in I}|g'(\vartheta^{(i)})|} = \frac{2^2\cdot 37}{|g'(\vartheta^{(2)})|} \doteq 47.31720891589014404,\\
C_2 &= \frac{\min_{i,j\in I,i<j}|\vartheta^{(i)}-\vartheta^{(j)}|}{2} = \frac{|\vartheta^{(2)}-\vartheta^{(3)}|}{2} \doteq 0.567970998877878477,\\
Y_1 &= [(4C_1)] = 189.
\end{aligned}$$

Lemma 5 ([19], Lemma 1.1). *If* $|Y| > Y_1$, *then* $X/Y$ *is a convergent of the continued fraction expansion of* $\vartheta^{(i_0)}$, *where* $i_0 \in I$ *is taken such that* $|\beta^{(i_0)}| = \min_{i\in I}|\beta^{(i)}|$.

Now assume $|Y| > Y_1$. Choose $j,k \in I$ such that $i_0$, $j$, $k$ are pairwise distinct. We eliminate $X$ and $Y$ from two of $\beta^{(i)}$ $(i = i_0, j, k)$ and obtain

$$\beta^{(i_0)}(\vartheta^{(j)}-\vartheta^{(k)}) + \beta^{(j)}(\vartheta^{(k)}-\vartheta^{(i_0)}) + \beta^{(k)}(\vartheta^{(i_0)}-\vartheta^{(j)}) = 0,$$

or equivalently

$$\frac{\vartheta^{(i_0)}-\vartheta^{(j)}}{\vartheta^{(i_0)}-\vartheta^{(k)}}\cdot\frac{\beta^{(k)}}{\beta^{(j)}} - 1 = -\frac{\vartheta^{(k)}-\vartheta^{(j)}}{\vartheta^{(k)}-\vartheta^{(i_0)}}\cdot\frac{\beta^{(i_0)}}{\beta^{(j)}}. \tag{13}$$

Combining this with (11) yields

$$\begin{aligned}
&\frac{\vartheta^{(i_0)}-\vartheta^{(j)}}{\vartheta^{(i_0)}-\vartheta^{(k)}}\cdot\frac{\mu^{(k)}}{\mu^{(j)}}\cdot\left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right)^{a_1}\cdot\left(\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}\right)^{a_2} - 1\\
&\qquad\qquad = -\frac{\vartheta^{(k)}-\vartheta^{(j)}}{\vartheta^{(k)}-\vartheta^{(i_0)}}\cdot\frac{\mu^{(i_0)}}{\mu^{(j)}}\cdot\left(\frac{\varepsilon_1^{(i_0)}}{\varepsilon_1^{(j)}}\right)^{a_1}\cdot\left(\frac{\varepsilon_2^{(i_0)}}{\varepsilon_2^{(j)}}\right)^{a_2}.
\end{aligned}$$

Define

$$\varLambda = \log\left|\frac{\vartheta^{(i_0)}-\vartheta^{(j)}}{\vartheta^{(i_0)}-\vartheta^{(k)}}\cdot\frac{\mu^{(k)}}{\mu^{(j)}}\right| + a_1\log\left|\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right| + a_2\log\left|\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}\right|, \tag{14}$$

and $H = \max(a_1, a_2)$. We shall give an upper and a lower bound for $|\varLambda|$ in terms of $H$. Put

$$\begin{aligned}
C_3 &= \max_{i_1\ne i_2\ne i_3\ne i_1}\left|\frac{\vartheta^{(i_1)}-\vartheta^{(i_2)}}{\vartheta^{(i_1)}-\vartheta^{(i_3)}}\right| = \left|\frac{\vartheta^{(1)}-\vartheta^{(3)}}{\vartheta^{(2)}-\vartheta^{(3)}}\right| \doteq 3.42398698316326030168,\\
Y_2^* &= \max(Y_1, [(2C_1C_3/C_2)^{1/3}]) = Y_1 = 189,\\
\mu_- &= \min_{i\in I,\mu\in M}|\mu^{(i)}| = \mu_1^{(3)} \doteq 1.231547958290,\\
\mu_+ &= \max_{i\in I,\mu\in M}|\mu^{(i)}| = \mu_1^{(2)} \doteq 11.049448332688,\\
C_4 &= \frac{1+2\max_{1\le i_1<i_2\le 3}|\vartheta^{(i_1)}-\vartheta^{(i_2)}|}{2\mu_-} = \frac{1+2|\vartheta^{(1)}-\vartheta^{(3)}|}{2\mu_1^{(3)}}\\
&\doteq 3.56417351382.
\end{aligned}$$

For a subset $I' = \{h_1, h_2\}$ of $I$, let

$$U_{I'} = \begin{pmatrix} \log|\varepsilon_1^{(h_1)}| & \log|\varepsilon_2^{(h_1)}| \\ \log|\varepsilon_1^{(h_2)}| & \log|\varepsilon_2^{(h_2)}| \end{pmatrix}.$$

Since $\det U_{I'} = \pm$ the regulator of $K$, we can set

$$U_{I'}^{-1} = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}, \qquad N[U_{I'}^{-1}] = \max_i(|u_{i1}| + |u_{i2}|).$$

Now we define

$$\begin{aligned} C_5 &= \min(2\min_{I'\subset I} N[U_{I'}^{-1}], \max_{I'\subset I} N[U_{I'}^{-1}]) \\ &= \max N[U_{I'}^{-1}] = N[U_{\{1,2\}}^{-1}] \doteq 2.54936575324381, \end{aligned}$$

and

$$C_6 = \frac{1.39C_1C_3C_4^3}{C_2} \doteq 17952.14631285.$$

Then an upper bound is given by

$$|\Lambda| < C_6 \exp\left(\frac{-3}{C_5}H\right), \tag{15}$$

if $|Y| > Y_2$ ([19], Lemma 2.2), where

$$Y_2 = \max(Y_2^*, 2\sqrt[3]{37}, \mu_+/C_2) = Y_2^* = 189.$$

We now need a special case of Waldschmidt's theorem [22] (cf. [19], Appendix II) to get a lower bound for $|\Lambda|$.

LEMMA 6. *Let $\alpha_1, \ldots, \alpha_n$ be nonzero algebraic numbers and $b_1, \ldots, b_n$ rational integers ($n \ge 2$). Set $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$. Define the absolute logarithmic height for $\alpha_i$ by*

$$h(\alpha_i) = \frac{1}{d}\log\Big(a_0\prod_{j=1}^{d}\max(1, |\alpha_i^{(j)}|)\Big),$$

*where $d = [\mathbb{Q}(\alpha_i) : \mathbb{Q}]$, $a_0$ is the positive leading coefficient of the minimal polynomial of $\alpha_i$ over $\mathbb{Z}$, and $\alpha_i^{(j)}$'s are the conjugates of $\alpha_i$. Further, let $V_0 = 1/D$, $V_j \ge \max(h(\alpha_j), |\log\alpha_j|/D, V_{j-1})$ for $1 \le j \le n$, and $V_j^+ = \max(V_j, 1)$ for $j = n, n-1$. Finally, put*

$$\Lambda = b_1\log\alpha_1 + \ldots + b_n\log\alpha_n,$$

*where* log *is a fixed determination of the logarithm. If $\Lambda \ne 0$, then*

$$|\Lambda| > \exp(-C_7(\log H + C_8)), \tag{16}$$

*where the constants are defined as follows*:

$$\begin{aligned} H &= \max_{1\le i\le n} |b_i|,\\ C_7 &= 2^{e(n)} n^{2n} D^{n+2} V_1 \dots V_n \log(eDV_{n-1}^+),\\ C_8 &= \log(eDV_n^+),\\ e(n) &= \min(8n+51, 10n+33, 9n+39). \end{aligned}$$

Let us return to our $\Lambda$ defined by (14). Since the right hand side of (13) is not zero, we have $\Lambda \neq 0$. So we can apply Waldschmidt's theorem with $b_1 = a_1$, $b_2 = a_2$, $b_3 = 1$ and

$$\alpha_1 = \frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}, \quad \alpha_2 = \frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}, \quad \alpha_3 = \frac{\vartheta^{(i_0)} - \vartheta^{(j)}}{\vartheta^{(i_0)} - \vartheta^{(k)}} \cdot \frac{\mu^{(k)}}{\mu^{(j)}}.$$

Moreover, log is taken as $\log|\cdot|$. For a fixed $i_0$, even if we interchange $k$ and $j$, the absolute value of $\Lambda$ remains unchanged. Hence we may choose the pair of subscripts that make $|\alpha_2| > 1$. Note that, since $\alpha_1$ and $\alpha_2$ are units, the leading coefficients of their minimal equations are both 1 and their absolute logarithmic heights are

$$h(\alpha_1) \doteq 0.647460923, \qquad h(\alpha_2) \doteq 1.412669734.$$

Depending on the choices of $i_0 \in I$ and $\mu \in M$, we have the following result.

Case 1: $\mu = \pm\mu_1$. The leading coefficient of the minimal polynomial of $\alpha_3$ is $37^3$ and $h(\alpha_3) \doteq 2.683099165$.

(1) $i_0 = 1$, $j = 2$, $k = 3$, or
(2) $i_0 = 2$, $j = 3$, $k = 1$, or
(3) $i_0 = 3$, $j = 2$, $k = 1$:

$$V_1 \doteq 0.64746092309, \quad V_2 \doteq 1.41266973468, \quad V_3 \doteq 2.68309916596,$$

$$C_7 \doteq 402529807284373736011187653.22971161315132497876,$$

$$C_8 \doteq 3.77873200084140223037.$$

Case 2: $\mu = \pm\mu_2$. The leading coefficient of the minimal polynomial of $\alpha_3$ is 1 and $h(\alpha_3) \doteq 0.4271368408$.

(1) $i_0 = 1$, $j = 2$, $k = 3$, or
(2) $i_0 = 2$, $j = 3$, $k = 1$, or
(3) $i_0 = 3$, $j = 2$, $k = 1$:

$$V_1 \doteq 0.64746092309, \quad V_2 \doteq 1.41263459880, \quad V_3 \doteq 1.41263459880,$$

$$C_7 \doteq 211929376309360982692463534.89361820091842195339,$$

$$C_8 \doteq 3.13721593991530433503.$$

From the inequalities (15) and (16) on $\Lambda$ and a result of Pethö and de Weger [9], an upper bound for $H$ is obtained.

LEMMA 7 ([19], Lemma 2.4). *If $|Y| > Y_2$, then $H < C_9$. The constant $C_9$ is given by*

$$C_9 = \frac{2C_5}{3}\left(\log C_6 + C_7C_8 + C_7 \log \frac{C_5C_7}{3}\right) < 4.44 \cdot 10^{28},$$

*where the bound on the right hand side takes care of all the cases.*

Remark. In general, $Y_2$ is much larger than $Y_1$. The solutions in the gap $Y_1 < |Y| < Y_2$ can be found by Lemma 5.

To lower the bound, we use the generalized lemma of Davenport.

LEMMA 8 (Davenport, cf. [18], Lemma 1). *Let $\theta, \beta$ be given real numbers, $M, B, p, q$ rational integers satisfying $6 < B$, $1 \le q \le MB$, $|\theta q - p| < 2/(MB)$. Set $H = \max(|b_1|, |b_2|)$. If $\|q\beta\| \ge 3/B$, then there is no solution of the inequality*

$$|b_1\theta + b_2 - \beta| \le K^{-H}$$

*in rational integers $b_1, b_2$ with $\log(B^2M)/\log K \le H \le M$, where $\|x\|$ denotes the distance between $x$ and the nearest integer.*

From (15), we have

$$\begin{aligned}|a_1 \log\alpha_1 + a_2 \log\alpha_2 + \log\alpha_3| &< 17952.147 \exp\left(\frac{-3}{2.549}H\right)\\ &\le \exp(9.795464 - 1.17693H)\\ &< \exp(-0.8H) \qquad \text{for } H \ge 26.\end{aligned}$$

If $i_0 = 1$ or 3, then it follows that

$$\left|a_1\frac{\log\alpha_1}{\log\alpha_2} + a_2 + \frac{\log\alpha_3}{\log\alpha_2}\right| < \exp(-0.8H) \qquad \text{for } H \ge 26.$$

When $i_0 = 2$, we get

$$\begin{aligned}\left|a_1\frac{\log\alpha_1}{\log\alpha_2} + a_2 + \frac{\log\alpha_3}{\log\alpha_2}\right| &< 1.1946 \exp(-0.8H) \le \exp(0.17781 - 0.8H)\\ &< \exp(-0.794H) \qquad \text{for } H \ge 26.\end{aligned}$$

Hence, for all cases,

$$\left|a_1\frac{\log\alpha_1}{\log\alpha_2} + a_2 + \frac{\log\alpha_3}{\log\alpha_2}\right| < \exp(-0.794H) \qquad \text{for } H \ge 26.$$

To apply Davenport's lemma to our case, we must find a rational approximation $p/q$ of $\delta = \log\alpha_1/\log\alpha_2$ such that $|\delta q - p| < 2/(MB)$. As Steiner

[18] pointed out, we only have to compute the convergents of the continued fraction expansion of $\delta$ to find the largest $q$ satisfying $q \le MB$ and check if

$$\|q\beta\| = \left\| -\frac{\log\alpha_3}{\log\alpha_2} q \right\| \ge 3/B$$

holds. We now apply the lemma by taking

$$M = 4.44 \cdot 10^{28}, \quad B = 100, \quad K = \exp(0.794),$$

where the constant $M$ comes from the calculation of Waldschmidt's theorem. The number $q$ for each case is given as follows:

Case 1: $\mu = \pm\mu_1$.

(1) $i_0 = 1$:

$q = 630290397095961978997661689337, \qquad \|q\beta\| > 0.07217 > 0.03,$

(2) $i_0 = 2$:

$q = 629151493674521381085747868917, \qquad \|q\beta\| > 0.32283 > 0.03,$

(3) $i_0 = 3$:

$q = 2873001635974139217734742858594, \quad \|q\beta\| > 0.11296 > 0.03.$

Case 2: $\mu = \pm\mu_2$.

(1) $i_0 = 1$:

$q = 630290397095961978997661689337, \qquad \|q\beta\| > 0.08325 > 0.03,$

(2) $i_0 = 2$:

$q = 629151493674521381085747868917, \qquad \|q\beta\| > 0.04176 > 0.03,$

(3) $i_0 = 3$:

$q = 2873001635974139217734742858594, \quad \|q\beta\| > 0.25885 > 0.03.$

Therefore we obtain $H \le \log(B^2M)/\log K \le 95$. To lower the bound more, the lemma can be applied again with $M = 95, B = 500$, and we find

Case 1: $\mu = \pm\mu_1$.

(1) $i_0 = 1$: $q = 37897, \|q\beta\| > 0.36234 > 0.006,$
(2) $i_0 = 2$: $q = 35991, \|q\beta\| > 0.33319 > 0.006,$
(3) $i_0 = 3$: $q = 17317, \|q\beta\| > 0.37880 > 0.006.$

Case 2: $\mu = \pm\mu_2$.

(1) $i_0 = 1$: $q = 37897, \|q\beta\| > 0.02617 > 0.006,$
(2) $i_0 = 2$: $q = 11573, \|q\beta\| > 0.18028 > 0.006,$
(3) $i_0 = 3$: $q = 17317, \|q\beta\| > 0.11570 > 0.006.$

Thus $H < 22$. Since we have computed all the solutions with this range and obtained the five solutions in (12), these are all solutions of our Thue equation (10) as claimed.

From (12), the integral solutions of (7) are as follows:

$$\begin{aligned}(x,y) = {} & (124912, \pm 44147512), (3144, \pm 176040), (592, \pm 10952),\\ & (1120, \pm 36296), (4440, \pm 295704).\end{aligned}$$

Since $x = 37A$ and $y = 37^2 B$, we finally obtain all the solutions of (3) listed in the statement of the lemma. ∎

Combining Lemmas 1, 3 and 4 with the conditions (P1) and (P2), we have the following complete description of the set $\mathcal{A}$.

Proposition 2. *$\mathcal{A} = \{16, 3376\}$.*

All the above calculation is executed with an accuracy of $10^{-50}$, which is sufficient for our purpose. Our programs have been implemented on NEC PC-9801NS using Yuji Kida's UBASIC86.

**4.** We are ready to prove our theorem.

By Proposition 1, for each value $A \in \mathcal{A} = \{16, 3376\}$, there is a special elliptic curve $E^A$ over $k$ with $j$-invariant $A^3$. So it is enough to show the following proposition.

Proposition 3. *There is an isogeny of degree* 5 *defined over $k$ between $E^{16}$ and $E^{3376}$.*

Proof. We shall show that $(16^3, 3376^3)$ is a noncuspidal point on the modular curve $X_0(5)$ (cf. [8]). The curve is of genus zero and the rational parametrization of the point $(j, j')$ on it is classically known ([7], IV.2.8):

$$j = j(\tau) = (\tau^2 + 10\tau + 5)^3/\tau, \quad j' = j(\tau'), \quad \tau\tau' = 125.$$

Taking $\tau = 1$, we have $j = 16^3$ and $j' = 3376^3$. The proof of the proposition is now complete. ∎

Remark. The author was informed that the elliptic curves (1)–(4) are classified and their ranks can be computed. In fact, the first two curves are 36C and 144C, respectively in the Antwerp IV tables [1]. The curve (3) is the 37-twist of 36C and (4) is the 37-twist of 144C in the same table. The rank of the curve (3) is two and all the other curves have rank zero.

Lastly, we make some comments on the general cases. Let $N$ be a prime number congruent to 1 modulo 4. In a similar manner to the case $N = 37$, we can construct an abelian variety as a quotient of the Jacobian varieties of modular curves. The $\mathbb{Q}$-simple factor $J$ has even dimension $2d$ and splits over $\mathbb{Q}(\sqrt{N})$ as $J = B \times B^\sigma$, where $\dim B = d$ and $B$ is isogenous to $B^\sigma$ with degree $c(N)$ (determined only by $N$) (cf. [13]–[15]). It is known that the factors $B$ and $B^\sigma$ have good reduction everywhere (cf. [5]). Therefore the case $d = 1$ gives a construction of elliptic curves with good reduction everywhere. For some $N$, a computation has been carried out by Cremona [3] to find explicit models of the curves. Our result naturally leads to the following problem.

PROBLEM. *Consider an elliptic curve defined over $\mathbb{Q}(\sqrt{N})$ with good reduction everywhere that is isogenous to its Galois conjugate. Is it isogenous of degree $c(N)$ to Shimura's elliptic curve constructed as above?*

Pinch stated this problem as a conjecture in his thesis [10]. In fact, he showed that torsion points of the curves satisfying the conditions in the problem have the same class field theoretic properties (cf. [13], §7.7) as that of Shimura's curve.

**Appendix.** In this appendix, we give explicit global minimal models of the curves $E^{16}$ and $E^{3376}$. Such models exist, because the class number of $k = \mathbb{Q}(\sqrt{37})$ is one. Note that the model $E_{A,u}$ defined in the proof of Proposition 1 is not global minimal, since its discriminant is $2^{12}3^6(A^3 - 1728)^2u^3$.

As mentioned in the first section, Shiota [16] gave the following global minimal model of $E^{16}$:

$$y^2 - \varepsilon y = x^3 + \frac{3\varepsilon + 1}{2}x^2 + \frac{11\varepsilon + 1}{2}x,$$

where $\varepsilon = 6 + \sqrt{37}$ is the fundamental unit of $k$. On this model, the point $P_0 = (0, 0)$ is of order 5. The group generated by $P_0$ consists of

$$P_0,\ \left(\varepsilon, \frac{\varepsilon^2 + \varepsilon}{2}\right),\ \left(\varepsilon, \frac{-\varepsilon^2 + \varepsilon}{2}\right),\ (0, \varepsilon),\ \mathcal{O} \text{ (the origin)}.$$

The isogenous curve $E^{3376} = E^{16}/\langle P_0\rangle$ can be easily computed by Vélu's method [21]:

$$y^2 - \varepsilon y = x^3 + \frac{3\varepsilon + 1}{2}x^2 - \frac{1669\varepsilon + 139}{2}x - 7(5449\varepsilon + 451).$$

The discriminants of these models are $\varepsilon^6$.

## References

[1] B. J. Birch and W. Kuyk (eds.), *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer, 1975.

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

[3] J. E. Cremona, *Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction*, Math. Proc. Cambridge Philos. Soc. 111 (1992), 199–218.

[4] —, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

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

[6] O. Hemer, *On the Diophantine equation $y^2 + k = x^3$*, doctoral dissertation, Uppsala, 1952.

[7] F. Klein und R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunktionen II*, Teubner, 1892.

[8] A. P. Ogg, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc. 81 (1975), 14–27.

[9] A. Pethö and B. M. M. de Weger, *Products of prime powers in binary recurrence sequences. Part I*, *The hyperbolic case*, *with an application to the generalized Ramanujan–Nagell equation*, Math. Comp. 47 (1986), 713–727.

[10] R. G. E. Pinch, *Elliptic curves over number fields*, doctoral dissertation, Oxford University, 1982.

[11] K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. of Math. 101 (1975), 555–562.

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

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

[14] —, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. 95 (1972), 130–190.

[15] —, *On the factor of the Jacobian variety of a modular function field*, J. Math. Soc. Japan 25 (1973), 523–544.

[16] K. Shiota, *On the explicit models of Shimura's elliptic curves*, ibid. 38 (1986), 649–659.

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

[18] R. P. Steiner, *On Mordell's equation $y^2 - k = x^3$: A problem of Stolarsky*, Math. Comp. 46 (1986), 703–714.

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

[20] —, —, *How to explicitly solve a Thue–Mahler equation*, Comp. Math. 84 (1992), 223–288; Corrections 89 (1993), 241–242.

[21] M. J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A 273 (1971), 238–241.

[22] M. Waldschmidt, *A lower bound for linear forms in logarithms*, Acta Arith. 37 (1980), 257–283.

Department of Mathematics
The Johns Hopkins University
Baltimore, Maryland 21218
U.S.A.

Current address:
Department of Mathematical Sciences
Yamagata University
Yamagata, 990 Japan
E-mail: kida@kszaoh3.kj.yamagata-u.ac.jp

*Received on 23.6.1995*
*and in revised form on 25.2.1996* (2813)