ACTA ARITHMETICA
XCVI.3 (2001)

Determination of elliptic curves with everywhere good reduction over real quadratic fields $\mathbb{Q}(\sqrt{3p})$

by

Takaaki Kagawa (Kusatsu)

1. Introduction. Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field, where m is a squarefree integer greater than 1. In our previous papers [4] and [5], we determined all elliptic curves with everywhere good reduction over k when $m = 37$ and 29, respectively. In the course of the determination, we constructed some unramified abelian extensions by applying Serre's results (the corollary to Proposition 11 and Proposition 12 in [14]) to the field of 3-division points. Unfortunately, we cannot apply them to the case $m \equiv 0 \pmod 3$ because of their assumption. However, without them, we can construct certain abelian extensions unramified outside 3 and the infinite primes. Thus assuming certain conditions on ray class numbers, we can deduce some criteria, and using them we can treat the case $m \equiv 0 \pmod 3$.

If $1 < m < 100$, $m \equiv 0 \pmod 3$, and the class number of k is prime to 6, then $m = 3, 6, 21, 33, 57, 69$ or 93. In [5], [7], [9], the proof is given for the nonexistence of elliptic curves with everywhere good reduction over k when $m = 3, 21$ and all such curves are determined when $m = 6$, while the cases $m = 33$, 57, 69 and 93 are still open. In this paper, we determine all elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{33})$ and show the nonexistence of such curves over $\mathbb{Q}(\sqrt{57})$, $\mathbb{Q}(\sqrt{69})$ and $\mathbb{Q}(\sqrt{93})$.

We use the following notation throughout this paper. For an algebraic number field k, $\mathcal{O}_k$, $\mathcal{O}_k^\times$ and h_k denote the ring of integers, group of units and class number of k, respectively. If $\mathfrak{m}$ is a divisor of k (that is, a formal product of a fractional ideal of k and some infinite primes of k), $h_k(\mathfrak{m})$ denotes the ray class number modulo $\mathfrak{m}$. If k is a real quadratic field, then ε and $'$ denote the fundamental unit greater than 1 and the conjugation of k, respectively.

For an elliptic curve E, we denote by $j(E)$ and $\Delta(E)$ the j-invariant and the discriminant of E, respectively.

2000 *Mathematics Subject Classification*: Primary 11G05.

2. Results. Let $k = \mathbb{Q}(\sqrt{33})$. The fundamental unit of k is $\varepsilon = 23 + 4\sqrt{33}$. In [9], the following elliptic curve with everywhere good reduction over k is given:

$$E_1 : y^2 + (5+\sqrt{33})xy + \varepsilon y = x^3, \quad \Delta(E_1) = -\varepsilon^3, \quad j(E_1) = -32768.$$

This curve contains two k-rational subgroups V_1, V_2 of order 3, namely

$$V_1 = E_1(k)_{\mathrm{tors}} = \langle (0,0)\rangle, \quad V_2 = \langle(-6-\sqrt{33}, y_1)\rangle,$$

where $y_1 = (40 + 7\sqrt{33} + \sqrt{-\varepsilon})/2 = (40 + 7\sqrt{33} + 2\sqrt{-3} + \sqrt{-11})/2$. Let $E_2 := E_1/V_1$, $E_3 := E_1/V_2$. Using Vélu's formula [18], we obtain the following defining equations of E_2 and E_3:

$$E_2 : y^2 + (5+\sqrt{33})xy + \varepsilon y = x^3 - (1235 + 215\sqrt{33})x - (35915 + 6252\sqrt{33}),$$
$$\Delta(E_2) = -\varepsilon, \quad j(E_2) = -(5+\sqrt{33})^3(5588 + 972\sqrt{33})^3\varepsilon^{-1},$$

$$E_3 : y^2 + (5+\sqrt{33})xy + \varepsilon y = x^3 + (85 + 15\sqrt{33})x + (730 + 127\sqrt{33}),$$
$$\Delta(E_3) = -\varepsilon^5, \quad j(E_3) = -(5-\sqrt{33})^3(5588 - 972\sqrt{33})^3\varepsilon.$$

Although $j(E_1) = j(E_1')$ (resp. $j(E_2) = j(E_3')$), E_1 and E_1' (resp. E_2 and E_3') are not isomorphic over k, since $\Delta(E_1)/\Delta(E_1') = \Delta(E_2)/\Delta(E_3') = \varepsilon^6$ is not a 12th power. Hence there are at least six k-isomorphism classes of elliptic curves with everywhere good reduction over k.

By definition, E_2 and E_3 are 3-isogenous over k to E_1. Further we see that E_1 and E_1' are 11-isogenous over k, since E_1 and E_1' are quadratic twists by $-\pi_{11}/11$ and $\pi_{11}'/11^2$ of the curves 121B1 and 121B2 in Table 1 of [2], respectively, 121B1 and 121B2 are 11-isogenous over $\mathbb{Q}$, and $(-\pi_{11}/11)(\pi_{11}'/11^2) = 1/11^2$. Here $\pi_{11} = 11 + 2\sqrt{33}$ is a prime element of k dividing 11. Below is the isogeny graph of the related elliptic curves:

$$\begin{array}{ccccccc} E_2 & \overset{3}{\text{———}} & E_1 & \overset{11}{\text{———}} & E_1' & \overset{3}{\text{———}} & E_2' \\ & & \Big| {\scriptstyle 3} & & \Big| {\scriptstyle 3} & & \\ & & E_3 & & E_3' & & \end{array}$$

Here, for a prime p and elliptic curves E and $\overline{E}$ defined over k, the graph

$$E \overset{p}{\text{———}} \overline{E}$$

means that E and $\overline{E}$ are p-isogenous over k. Hence there is at least one k-isogeny class of elliptic curves with everywhere good reduction over k.

In this paper we prove

THEOREM 1. *Up to isomorphism over $k = \mathbb{Q}(\sqrt{33})$, the six curves listed above are all the elliptic curves with everywhere good reduction over k. In particular, there is exactly one k-isogeny class of such curves.*

We simultaneously prove the following theorem:

THEOREM 2. *There are no elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{m})$ *if* $m = 57$, 69 *or* 93.

Let d be the discriminant of a real quadratic field and χ_d the Dirichlet character associated with d. Let $S_d = S_2(\Gamma_0(d), \chi_d)$ be the space of cusp-forms of Neben-type of weight 2 and level d. It is conjectured (cf. [12]) that any elliptic curve having everywhere good reduction over the real quadratic field $\mathbb{Q}(\sqrt{d})$ and admitting an isogeny over $\mathbb{Q}(\sqrt{d})$ to its conjugate should be isogenous over $\mathbb{Q}(\sqrt{d})$ to so-called Shimura's elliptic curve which arises from a 2-dimensional $\mathbb{Q}$-simple factor of S_d. When $d = 33$, 57, 69, 93, it is known that S_d is 2-dimensional and $\mathbb{Q}$-simple, 4-dimensional and $\mathbb{Q}$-simple, 6-dimensional and $\mathbb{Q}$-simple, 8-dimensional and $\mathbb{Q}$-simple, respectively. Thus Theorems 1 and 2 confirm the conjecture for these four values of d.

3. Preliminaries. Later we will give criteria for every elliptic curve with everywhere good reduction over a real quadratic field k to admit a 3-isogeny defined over k (Propositions 11 and 12 below). Thus we first study elliptic curves with 3-isogeny and some diophantine equations arising from the investigation of such curves. Further, since a key tool to prove the criteria is the field $L = k(E[3])$ of 3-division points and $\mathrm{Gal}(L/k)$ can be viewed as a subgroup of the general linear group $\mathrm{GL}_2(\mathbb{F}_3)$, we will also study subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$.

3.1. *Elliptic curves with 3-isogeny.* Let E and $\overline{E}$ be elliptic curves defined over a number field k which are 3-isogenous over k. We define a rational function $J(x)$ by

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

Then, by Pinch [13], the j-invariants of E and $\overline{E}$ can be written as

$$j(E) = J(t), \quad j(\overline{E}) = J(\bar{t}), \quad t, \bar{t} \in k,\ t\bar{t} = 729 = 3^6.$$

(This is nothing but a parametrization of the modular curve $Y_0(3)$.) Moreover, let $c_4(E)$ and $c_6(E)$ be the usual quantities associated with E. Then the following relations hold:

$$j(E) = \frac{c_4(E)^3}{\Delta(E)} = \frac{(t+27)(t+3)^3}{t}, \tag{3.1}$$

$$j(E) - 1728 = \frac{c_6(E)^2}{\Delta(E)} = \frac{(t^2+18t-27)^2}{t}. \tag{3.2}$$

LEMMA 3. *Let* k, E, $\overline{E}$, t *and* $\bar{t}$ *be as above. Then*

(1) *If* $j(E) \neq 1728$, *then* $t/\Delta(E)$ *is a square in* k.

(2) *If E and $\overline{E}$ have everywhere good reduction over k and $j(E), j(\overline{E}) \neq 0, 1728$, then the principal ideals (t) and $(\bar{t})$ are integral and sixth powers.*

Proof. (1) follows immediately from (3.2).

(2) It suffices to prove the assertions only for t. Equation (3.1) and the assumption that E has everywhere good reduction over k imply that t is an integer in k. By the same assumption, the principal ideal $(\Delta(E))$ is a 12th power, say $(\Delta(E)) = \mathfrak{a}^{12}$. Since $j(E) \neq 1728$, we see from (3.2) that $(t) = ((t^2 + 18t - 27)/c_6(E))^2\mathfrak{a}^{12}$ is a square. To show that (t) is a cube, it is enough to show that $\mathrm{ord}_\mathfrak{p}(t) \equiv \mathrm{ord}_\mathfrak{p}(27) \pmod 3$ for any prime ideal $\mathfrak{p}$ dividing 3, where $\mathrm{ord}_\mathfrak{p}$ is the normalized valuation corresponding to $\mathfrak{p}$, since $t, \bar{t} \in \mathcal{O}_k$ and $t\bar{t} = 3^6$. We may suppose that $\mathrm{ord}_\mathfrak{p}(t) \geq \mathrm{ord}_\mathfrak{p}(27)$. If $\mathrm{ord}_\mathfrak{p}(t) = \mathrm{ord}_\mathfrak{p}(27)$, then there is nothing to prove. If $\mathrm{ord}_\mathfrak{p}(t) > \mathrm{ord}_\mathfrak{p}(27)$, then $\mathrm{ord}_\mathfrak{p}((t+27)/t) = \mathrm{ord}_\mathfrak{p}(27) - \mathrm{ord}_\mathfrak{p}(t)$. On the other hand, since $j(E) \neq 0$, we see from (3.1) that $((t+27)/t) = (c_4(E)/(t+3))^3/\mathfrak{a}^{12}$ is a cube. Hence $\mathrm{ord}_\mathfrak{p}(t) \equiv \mathrm{ord}_\mathfrak{p}(27) \pmod 3$. ∎

Let k be a real quadratic field and let E be an elliptic curve having everywhere good reduction over k and admitting a 3-isogeny defined over k with $j(E) = J(t)$. In this case, $j(E)$ is neither 0 nor 1728 (Theorem 2(a) in [16]). Thus it follows from Lemma 3(2) that

$$(t) = \begin{cases} (1),\ (729) & \text{if 3 is inert,} \\ (1),\ (27),\ (729) & \text{if 3 ramifies,} \\ (1),\ \mathfrak{p}^6,\ \mathfrak{p}'^6,\ (729) & \text{if } (3) = \mathfrak{p}\mathfrak{p}',\ \mathfrak{p} \text{ and } \mathfrak{p}' \text{ are distinct prime ideals.} \end{cases}$$

From (3.1), we have

$$\left(\frac{c_4(E)}{t+3}\right)^3 = \Delta(E)(1 + 27u), \quad u = \frac{1}{t} \in \mathcal{O}_k^\times \tag{3.3}$$

if $(t) = (1)$,

$$\left(\frac{3c_4(E)}{t+3}\right)^3 = \Delta(E)(u + 27), \quad u = \frac{729}{t} \in \mathcal{O}_k^\times \tag{3.4}$$

if $(t) = 729$, and

$$\left(\frac{c_4(E)}{t+3}\right)^3 = \Delta(E)(1 + u), \quad u = \frac{27}{t} \in \mathcal{O}_k^\times \tag{3.5}$$

if 3 is ramified and $(t) = (27)$. Suppose that 3 decomposes in k as $\mathfrak{p}\mathfrak{p}'$, that $(t) = \mathfrak{p}^6$, and that $(h_k, 6) = 1$. Then $\mathfrak{p}$ is principal, say $\mathfrak{p} = (\pi)$, $\pi \in \mathcal{O}_k$. From (3.1) we have

$$\left(\frac{\pi c_4(E)}{t+3}\right)^3 = \Delta(E)(\pi^3 \pm \pi'^3 u), \quad u = \frac{\pi^6}{t} \in \mathcal{O}_k^\times. \tag{3.6}$$

Similarly, if $(3) = \mathfrak{p}\mathfrak{p}'$, $(t) = \mathfrak{p}'^6 = (\pi'^6)$, then

$$\left(\frac{\pi' c_4(E)}{t+3}\right)'^3 = \Delta(E)'(\pi^3 \pm \pi'^3 u), \quad u = \frac{\pi^6}{t'} \in \mathcal{O}_k^\times. \tag{3.7}$$

Note that $c_4(E) \neq 0$ since $j(E) \neq 0$.

Consequently, to investigate elliptic curves having everywhere good reduction over a real quadratic field k with unit discriminant and admitting a 3-isogeny defined over k, we need to study the equations

$$X^3 = u + 27v, \qquad X^3 = u + v, \qquad X^3 = \pi^3 u + \pi'^3 v$$

in $X \in \mathcal{O}_k \backslash \{0\}$, $u, v \in \mathcal{O}_k^\times$, where $\pi \in \mathcal{O}_k$, $N_{k/\mathbb{Q}}(\pi) = \pm 3$. We will study them in the next subsection.

3.2. *Some Diophantine equations*

LEMMA 4. *Let k be a quadratic field with $(h_k, 6) = 1$. Then the equation*

$$X^3 = 1 + 27u, \qquad X \in \mathcal{O}_k, \ u \in \mathcal{O}_k^\times, \tag{3.8}$$

has a solution only when $k = \mathbb{Q}(\sqrt{6})$ or $\mathbb{Q}(\sqrt{33})$, in which cases, the only solutions are $(X, u) = (4 \pm \sqrt{6}, 5 \pm 2\sqrt{6})$, $(-(5 \pm \sqrt{33}), -(23 \pm 4\sqrt{33}))$, respectively. Note that $h_{\mathbb{Q}(\sqrt{6})} = h_{\mathbb{Q}(\sqrt{33})} = 1$, and that $5 + 2\sqrt{6}$ (resp. $23 + 4\sqrt{33}$) is the fundamental unit of $\mathbb{Q}(\sqrt{6})$ (resp. $\mathbb{Q}(\sqrt{33})$).

Proof. First consider the case where 3 is ramified. Since h_k is odd, we have $(3) = (\pi^2)$, $\pi \in \mathcal{O}_k$. By (3.8) we have

$$X - 1 = \pi^a v, \qquad X^2 + X + 1 = \pi^{6-a} w, \qquad v, w \in \mathcal{O}_k^\times, \ a \in \mathbb{Z}, \ 0 \le a \le 6,$$

whence

$$\pi^{2a} v^2 + 3\pi^a v + 3 = \pi^{6-a} w. \tag{3.9}$$

If $a = 0, 2, 3, 5$ or 6, then the π-adic values of both sides of (3.9) cannot be equal. If $a = 1$, then taking the norm of both sides of (3.9) yields

$$\mathrm{Tr}_{k/\mathbb{Q}}(\pi v)^2 + (N_{k/\mathbb{Q}}(\pi v) + 3)\,\mathrm{Tr}_{k/\mathbb{Q}}(\pi v) + (N_{k/\mathbb{Q}}(\pi v) + 6) = \pm 3^4.$$

If $N_{k/\mathbb{Q}}(\pi v) = -3$, then $\mathrm{Tr}_{k/\mathbb{Q}}(\pi v)$ cannot be rational. If $N_{k/\mathbb{Q}}(\pi v) = 3$, then $\mathrm{Tr}_{k/\mathbb{Q}}(\pi v) = -12$ or 6. The former corresponds to $(X, u) = (-(5 \pm \sqrt{33}), -(23 \pm 4\sqrt{33}))$, the latter to $(X, u) = (4 \pm \sqrt{6}, 5 \pm 2\sqrt{6})$. If $a = 4$, then we similarly obtain

$$\mathrm{Tr}_{k/\mathbb{Q}}(\pi^4 v)^2 + (N_{k/\mathbb{Q}}(\pi^4 v) + 3)\,\mathrm{Tr}_{k/\mathbb{Q}}(\pi^4 v) + (N_{k/\mathbb{Q}}(\pi^4 v) + 3 + 3^7) = \pm 3.$$

For all possibilities of the values of $N_{k/\mathbb{Q}}(\pi^4 v)$ and the signs of the right hand side, $\mathrm{Tr}_{k/\mathbb{Q}}(\pi^4 v)$ cannot be rational.

If 3 is inert, a similar argument works and we can show that there are no solutions in this case.

Finally, consider the case where $(3) = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$. Then, for some $a, a' \in \mathbb{Z}$, $0 \le a, a' \le 3$, we have

$$(X-1) = \mathfrak{p}^a \mathfrak{p}'^{a'}, \qquad (X^2+X+1) = \mathfrak{p}^{3-a}\mathfrak{p}'^{3-a'}.$$

If $a = a'$, then we have $(X-1) = (3)^a$, $(X^2+X+1) = (3)^{3-a}$. Hence a similar argument works and we can show that there are no solutions in this case. Suppose that $a \neq a'$. Considering the conjugate of (3.8) if necessary, we may assume that $a < a'$. Then $(X-1) = (\mathfrak{p}\mathfrak{p}')^a \mathfrak{p}'^{a'-a} = (3)^a \mathfrak{p}'^{a'-a}$, and $a' - a = 1, 2, 3$. Since $(h_k, 6) = 1$, it follows that $\mathfrak{p}$ and $\mathfrak{p}'$ are both principal. Thus a similar argument leads to the conclusion that there are no solutions also in this case. ∎

We can prove the following three lemmas similarly.

LEMMA 5 (Kida [6]). *Let k be a quadratic field. Then the equation*

$$X^3 = u + 27, \qquad X \in \mathcal{O}_k,\ u \in \mathcal{O}_k^\times,$$

has no solutions.

LEMMA 6. *Let k be a quadratic field. Then the only solution of the equation*

$$X^3 = 1 + u, \qquad X \in \mathcal{O}_k,\ u \in \mathcal{O}_k^\times,$$

is $(X, u) = (0, -1)$.

LEMMA 7. *Let k be a real quadratic field in which 3 splits into two principal prime ideals with generators π and π'. Then the equation*

$$X^3 = \pi^3 + \pi'^3 u, \qquad X \in \mathcal{O}_k,\ u \in \mathcal{O}_k^\times,$$

has no solutions.

We give two more results on these equations.

LEMMA 8. *If the norm of the fundamental unit of a real quadratic field k is 1 and*

$$X^3 = u - v, \qquad X \in \mathcal{O}_k,\ u, v \in \mathcal{O}_k^\times,\ uv \in \mathcal{O}_k^{\times 2}, \tag{3.10}$$

then $X = 0$.

Proof. By assumption, we have $uv' = w^2$ for some $w \in \mathcal{O}_k^\times$. Taking the norm of both sides of (3.10) and noting $N_{k/\mathbb{Q}}(u) = N_{k/\mathbb{Q}}(v) = N_{k/\mathbb{Q}}(w) = 1$, we obtain

$$\mathrm{Tr}_{k/\mathbb{Q}}(w)^2 = \{-N_{k/\mathbb{Q}}(X)\}^3 + 4.$$

It then follows that $X = 0$, since the only (affine) $\mathbb{Q}$-rational points of the elliptic curve $y^2 = x^3 + 4$, which is the curve 108A1 in Table 1 of [2], are $(0, \pm 2)$. ∎

LEMMA 9. *Let k be one of the real quadratic fields $\mathbb{Q}(\sqrt{33})$, $\mathbb{Q}(\sqrt{57})$, $\mathbb{Q}(\sqrt{69})$ and $\mathbb{Q}(\sqrt{93})$. Then the equation*

$$X^3 = u + 27v, \qquad X \in \mathcal{O}_k,\ u, v \in \mathcal{O}_k^\times,\ u \notin k^{\times 3}, \tag{3.11}$$

has no solutions.

Proof. Equation (3.11) has no solutions modulo 3, 3, 9 or $(31+3\sqrt{93})/2$ according as $k = \mathbb{Q}(\sqrt{33})$, $\mathbb{Q}(\sqrt{57})$, $\mathbb{Q}(\sqrt{69})$ or $\mathbb{Q}(\sqrt{93})$. Note that

$$\mathcal{O}_{\mathbb{Q}(\sqrt{93})}/((31+3\sqrt{93})/2) \cong \mathbb{Z}/31\mathbb{Z}. \ \blacksquare$$

3.3. *Subgroups of* $\mathrm{GL}_2(\mathbb{F}_3)$ *as a Galois group.* Let k be an algebraic number field not containing $\sqrt{-3}$. Let E be an elliptic curve defined over k, let $E[3] = \{P \in E \mid 3P = O\}$ be the group of 3-division points of E, and let $L = k(E[3])$ be the field generated over k by the points of $E[3]$. We may regard $G = \mathrm{Gal}(L/k)$ as a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ by the faithful representation $G \to \mathrm{GL}_2(\mathbb{F}_3)$ induced by the action of G on $E[3]$. Here we study what group G can be. We mention that Naito [10] studied the same problem for elliptic curves defined over $\mathbb{Q}$.

LEMMA 10. *Let G be as above. Let $\varrho = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_3)$, which satisfy the relations $\varrho^2 = \sigma^2 = \tau^8 = 1$, $\sigma\tau\sigma^{-1} = \tau^3$. Then*

(1) *G is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to one of the following*:

- (i) $\langle\varrho\rangle \cong \mathbb{Z}/2\mathbb{Z}$.
- (ii) $\langle -1\rangle \times \langle\varrho\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- (iii) $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \cong S_3$ (*the symmetric group of degree* 3).
- (iv) $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \cong S_3$.
- (v) $\langle\sigma, \tau^2\rangle \cong D_8$ (*the dihedral group of order* 8).
- (vi) $\langle\tau\rangle \cong \mathbb{Z}/8\mathbb{Z}$.
- (vii) $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$.
- (viii) $\langle\sigma, \tau\rangle \cong SD_{16}$ (*the semi-dihedral group of order* 16).
- (ix) $\mathrm{GL}_2(\mathbb{F}_3)$.

(2) *$\Delta(E)$ is a cube in k if and only if G is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to one of the groups in* (i), (ii), (v), (vi) *or* (viii). *For each case, $G \cap \mathrm{SL}_2(\mathbb{F}_3) = \mathrm{Gal}(L/k(\sqrt{-3}))$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to $\{1\}$, $\langle -1\rangle \cong \mathbb{Z}/2\mathbb{Z}$, $\langle\tau^2\rangle \cong \mathbb{Z}/4\mathbb{Z}$, $\langle\tau^2\rangle \cong \mathbb{Z}/4\mathbb{Z}$, $\langle\sigma\tau, \tau^2\rangle \cong Q_8$ (the quaternion group), respectively.*

(3) *E admits a 3-isogeny defined over k if and only if G is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to one of the groups in* (i), (ii), (iii), (iv) *or* (vii).

REMARK. $\mathrm{GL}_2(\mathbb{F}_3)$ is of order $2^4 \cdot 3$ and hence SD_{16} is a 2-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$.

P r o o f (of Lemma 10). (1) We have $\#G \geq 2$, since $k(\sqrt{-3}) \subset L$ ([17], p. 98) and $[k(\sqrt{-3}) : k] = 2$. The special linear group $\mathrm{SL}_2(\mathbb{F}_3)$ does not contain G, since we have $\mathrm{Gal}(L/k(\sqrt{-3})) = G \cap \mathrm{SL}_2(\mathbb{F}_3)$ by the commutativity of the diagram

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_3) \\ {\scriptstyle\mathrm{Res}}\downarrow & & \downarrow{\scriptstyle\det} \\ \mathrm{Gal}(k(\sqrt{-3})/k) & \xrightarrow{\sim} & \mathbb{F}_3^\times \end{array}$$

From these together with the classification of the subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$ (cf. [10]), we obtain the assertion.

(2) The first part is clear from the fact that $\Delta(E)$ is a cube in k if and only if $[L : k]$ is not divisible by 3 ([14], §5.3). The second part follows from direct calculation.

(3) Since admitting a 3-isogeny defined over k is equivalent to the existence of a point P of order 3 such that $\sigma(P) = \pm P$ for any $\sigma \in G$, we may assume, by an appropriate choice of a basis of $E[3]$, that G is a subgroup of $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$. The groups appearing in (1) which are subgroups of this group are those in (i), (ii), (iii), (iv) and (vii). ■

4. Some criteria. In this section, we use the following notation: For subgroups H and N of $\mathrm{GL}_2(\mathbb{F}_3)$, $H \sim N$ means that H is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to N.

PROPOSITION 11. *Let k be a real quadratic field. Assume* $h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}) \not\equiv 0 \pmod 4$, *where $\mathfrak{p}_\infty^{(1)}$ and $\mathfrak{p}_\infty^{(2)}$ are the real primes of k, or* $h_{k(\sqrt{-3})}((3)) \not\equiv 0 \pmod 4$. *Then every elliptic curve E with everywhere good reduction over k whose discriminant $\Delta(E)$ is a cube in k admits a 3-isogeny defined over k.*

P r o o f. Let E be an elliptic curve with everywhere good reduction over k with $\Delta(E) \in k^{\times 3}$. Set $L := k(E[3])$, $G := \mathrm{Gal}(L/k)$ and $H := \mathrm{Gal}(L/k(\sqrt{-3})) = G \cap \mathrm{SL}_2(\mathbb{F}_3)$. By Lemma 10(2), G is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to $\langle \sigma, \tau \rangle \cong SD_{16}$, $\langle \tau \rangle \cong \mathbb{Z}/8\mathbb{Z}$, $\langle \sigma, \tau^2 \rangle \cong D_8$, $\langle -1 \rangle \times \langle \varrho \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or $\langle \varrho \rangle \cong \mathbb{Z}/2\mathbb{Z}$. If $G \sim \langle \tau \rangle$ or $\langle \sigma, \tau^2 \rangle$, then it is clear that G has a normal subgroup N such that G/N is of order 4. Further, by Lemma 10(2), $H \cong \mathbb{Z}/4\mathbb{Z}$ in these cases. If $G \sim \langle \sigma, \tau \rangle$, then G has a normal subgroup of N with $G/N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Indeed, $\langle \sigma, \tau \rangle / \langle \tau^2 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Further $H \sim \langle \sigma\tau, \tau^2 \rangle \cong Q_8$ and $\langle \sigma\tau, \tau^2 \rangle / \langle \tau^2 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus in view of the criterion of Néron–Ogg–Shafarevich ([17], p. 184), our assumptions on ray class numbers imply that $G \sim \langle \varrho \rangle$ or $\langle -1 \rangle \times \langle \varrho \rangle$. We therefore see from Lemma 10(3) that E admits a 3-isogeny defined over k. ■

PROPOSITION 12. *Let k be a real quadratic field with $(h_k, 6) = 1$. Let ε be the fundamental unit of k and let $\mathfrak{P}_\infty^{(1)}$ and $\mathfrak{P}_\infty^{(2)}$ be the real primes of $k(\sqrt[3]{\varepsilon})$.*

(1) *If $h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)}) \not\equiv 0 \pmod 4$ or $h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3)) \not\equiv 0 \pmod 4$, then every elliptic curve E with everywhere good reduction over k whose discriminant $\Delta(E)$ is not a cube in k admits a 3-isogeny defined over k.*

(2) *If $h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)}) \not\equiv 0 \pmod 4$ or $h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3)) \not\equiv 0 \pmod 2$, then every elliptic curve E with everywhere good reduction over k whose discriminant $\Delta(E)$ is not a cube in k has a k-rational subgroup V of order 3, and either E or E/V has a k-rational point of order 3.*

Proof. (1) Let E be an elliptic curve with everywhere good reduction over k and let $L = k(E[3])$, $G = \mathrm{Gal}(L/k)$. By the corollary to Theorem 1 of [15], which states that every elliptic curve with everywhere good reduction over k has a global minimal model provided $(h_k, 6) = 1$, and the assumption that $\Delta(E)$ is not a cube, we have $k(\sqrt[3]{\Delta(E)}) = k(\sqrt[3]{\varepsilon})$. Since L contains $k(\sqrt[3]{\Delta(E)})$ ([14], p. 305), we have $[L : k] \equiv 0 \pmod 3$. Thus, by Lemma 10(2), we have $G \sim \left(\begin{smallmatrix}1&*\\0&*\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}*&*\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)$ or $\mathrm{GL}_2(\mathbb{F}_3)$. Suppose that E admits no 3-isogeny defined over k. Then, by Lemma 10(3), we have $G = \mathrm{GL}_2(\mathbb{F}_3)$, $\mathrm{Gal}(L/k(\sqrt[3]{\varepsilon})) \sim \langle\sigma, \tau\rangle$ and $\mathrm{Gal}(L/k(\sqrt[3]{\varepsilon}, \sqrt{-3})) = \mathrm{Gal}(L/k(\sqrt[3]{\varepsilon})) \cap \mathrm{SL}_2(\mathbb{F}_3) \sim \langle\sigma\tau, \tau^2\rangle$. The criterion of Néron–Ogg–Shafarevich and the fact that $\langle\sigma, \tau\rangle/\langle\tau^2\rangle$ and $\langle\sigma\tau, \tau^2\rangle/\langle\tau^2\rangle$ are both isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ imply $h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)}) \equiv 0 \pmod 4$ and $h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3)) \equiv 0 \pmod 4$.

(2) According to (1), we have $G \sim \left(\begin{smallmatrix}1&*\\0&*\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}*&*\\0&1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)$. Supposing $G \sim \left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)$, the criterion of Néron–Ogg–Shafarevich implies that $L/k(\sqrt[3]{\varepsilon})$ is an abelian extension of degree 4 unramified outside $\{3, \mathfrak{P}_\infty^{(1)}, \mathfrak{P}_\infty^{(2)}\}$ and $L/k(\sqrt[3]{\varepsilon}, \sqrt{-3})$ is a quadratic extension unramified outside 3. These contradict our assumptions. ∎

5. Proof of Theorems 1 and 2. Let k be one of the real quadratic fields $\mathbb{Q}(\sqrt{33})$, $\mathbb{Q}(\sqrt{57})$, $\mathbb{Q}(\sqrt{69})$ and $\mathbb{Q}(\sqrt{93})$. The fundamental unit of k is

$$\varepsilon = \begin{cases} 23 + 4\sqrt{33} & \text{if } k = \mathbb{Q}(\sqrt{33}),\\ 151 + 20\sqrt{57} & \text{if } k = \mathbb{Q}(\sqrt{57}),\\ (25 + 3\sqrt{69})/2 & \text{if } k = \mathbb{Q}(\sqrt{69}),\\ (29 + 3\sqrt{93})/2 & \text{if } k = \mathbb{Q}(\sqrt{93}). \end{cases}$$

Note that $N_{k/\mathbb{Q}}(\varepsilon) = 1$. Let E be an elliptic curve with everywhere good reduction over k. Table 1 and Propositions 11 and 12 imply that E admits a 3-isogeny defined over k.

Table 1. Ray class numbers

k	$h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)})$	$h_{k(\sqrt{-3})}((3))$	$h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)})$	$h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3))$
$\mathbb{Q}(\sqrt{33})$	2	1	$2\cdot 3^3$	3^5
$\mathbb{Q}(\sqrt{57})$	**4**	2	$\mathbf{2^2\cdot 3}$	$2\cdot 3^3$
$\mathbb{Q}(\sqrt{69})$	6	9	$2\cdot 3$	3^2
$\mathbb{Q}(\sqrt{93})$	**12**	18	$\mathbf{2^2\cdot 3}$	$2\cdot 3^2$

In the case where $\Delta(E)$ is a cube in k, k is $\mathbb{Q}(\sqrt{33})$ and E is isomorphic over k to E_1 or E_1'. More generally we have the following:

PROPOSITION 13. *Let k be a quadratic field with $(h_k, 6) = 1$. If there is an elliptic curve E which has everywhere good reduction over k and admits a 3-isogeny defined over k, and whose discriminant $\Delta(E)$ is a cube in k, then k is equal to $\mathbb{Q}(\sqrt{6})$ or $\mathbb{Q}(\sqrt{33})$. If $k = \mathbb{Q}(\sqrt{6})$ (resp. $k = \mathbb{Q}(\sqrt{33})$), then such a curve E is isomorphic over k to*

$$E_4 : y^2 + (4+\sqrt{6})xy + (5+2\sqrt{6})y = x^3,\ \Delta(E_4) = (5+2\sqrt{6})^3,\ j(E_4) = 8000$$

or E_4' (resp. to E_1 or E_1').

For the proof of this lemma and for later use, we first give a lemma.

LEMMA 14 (Kida [8]). *Let E be an elliptic curve having everywhere good reduction over a quadratic field k. Let s denote the number of ramifying rational primes in the extension $k/\mathbb{Q}$. Then the number of twists of E having everywhere good reduction over k is 2^{s-1}.*

Proof (of Proposition 13). By the argument in Subsection 3.1, $j(E)$ is of the form $J(t)$, $t \in \mathcal{O}_k$, $t \mid 3^6$, and the principal ideal (t) is a sixth power. By (3.3)–(3.7), we see that there exist $X \in \mathcal{O}_k \setminus \{0\}$ and $u \in \mathcal{O}_k^\times$ such that

(5.1) $\quad X^3 = 1 + 27u \quad$ if $(t) = (1)$,

(5.2) $\quad X^3 = u + 27 \quad$ if $(t) = (729)$,

(5.3) $\quad X^3 = 1 + u \quad$ if 3 is ramified, and $(t) = (27)$,

(5.4) $\quad X^3 = \pi^3 + \pi'^3 u \quad$ if $3 = \pm\pi\pi'$, and $(t) = (\pi^6)$ or (π'^6).

Note that in equation (5.1), $u = 1/t$, $X = c_4(E)/((t+3)v)$, where $\Delta(E) = v^3$, $v \in \mathcal{O}_k \setminus \{0\}$. From Lemmas 5–7, none of the equations (5.2)–(5.4) has solutions. From Lemma 4, the only units u satisfying equation (5.1) are $u = 5 \pm 2\sqrt{6}$ and $-(23 \pm 4\sqrt{33})$. If $u = 5 \pm 2\sqrt{6}$ (resp. $u = -(23 \pm 4\sqrt{33})$), then $j(E) = J(5 \mp 2\sqrt{6}) = 8000$ (resp. $j(E) = J(-(23 \mp 4\sqrt{33})) = -32768$). We have two elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{6})$ (resp. $\mathbb{Q}(\sqrt{33})$) with j invariant 8000 (resp. -32768), namely E_4 and E_4' (resp. E_1 and E_1'). Lemma 14 therefore implies our assertion. ∎

REMARK. All elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{6})$ have been determined in [5], [7].

Consider the case where $\Delta(E)$ is not a cube in k. The field $K := k(\sqrt{\Delta(E)})$ is one of the fields k, $k(\sqrt{-1})$ or $k(\sqrt{\pm\varepsilon})$, since we may assume that $\Delta(E)$ is a unit (see the above-cited result in [15]). The field generated over k by the points of order 2 of E is a cyclic cubic extension of K, since in [1], it is shown that E has no k-rational points of order 2. This means that, in view of the criterion of Néron–Ogg–Shafarevich, $h_K^{(2)} := h_K(\prod_{\mathfrak{p}|2}\mathfrak{p})$ is divisible by 3. Thus Table 2 implies that $\Delta(E) = -\varepsilon^{2n+1}$ $(n \in \mathbb{Z})$.

Table 2. $h_K^{(2)}$ $(K = k, k(\sqrt{-1}), k(\sqrt{\pm\varepsilon}))$

k	$h_K^{(2)}$			
	$K = k$	$K = k(\sqrt{-1})$	$K = k(\sqrt{\varepsilon})$	$K = k(\sqrt{-\varepsilon})$
$\mathbb{Q}(\sqrt{33})$	1	2	1	**3**
$\mathbb{Q}(\sqrt{57})$	1	2	1	**3**
$\mathbb{Q}(\sqrt{69})$	1	4	1	**3**
$\mathbb{Q}(\sqrt{93})$	1	2	1	**3**

In view of the formulae for an admissible change of variables, we may assume that $\Delta(E) = -\varepsilon^{\pm 1}$ or $-\varepsilon^{\pm 5}$. We may further assume that $\Delta(E) = -\varepsilon^{6n+1}$ $(n = 0, -1)$ by considering the conjugate of E.

Suppose first that $(t) = (1)$. By (3.3), we obtain

$$X^3 = \varepsilon + 27u, \qquad X = \frac{-c_4(E)}{(t+3)\varepsilon^{2n}} \in \mathcal{O}_k, \qquad u = \frac{\varepsilon}{t} \in \mathcal{O}_k^\times,$$

which is impossible by Lemma 9.

Suppose next that $(t) = (27)$. Then, by (3.5), we obtain

$$X^3 = \varepsilon + \varepsilon u, \qquad X = \frac{-c_4(E)}{(t+3)\varepsilon^{2n}} \in \mathcal{O}_k \backslash \{0\}, \qquad u = \frac{27}{t} \in \mathcal{O}_k^\times.$$

Let

$$\pi = \begin{cases} 6 + \sqrt{33} & \text{if } k = \mathbb{Q}(\sqrt{33}), \\ 15 + 2\sqrt{57} & \text{if } k = \mathbb{Q}(\sqrt{57}), \\ (9 + \sqrt{69})/2 & \text{if } k = \mathbb{Q}(\sqrt{69}), \\ (9 + \sqrt{93})/2 & \text{if } k = \mathbb{Q}(\sqrt{93}) \end{cases}$$

be a prime element of k dividing 3. Lemma 3(1) and the fact that $\pi^2 = 3\varepsilon$ imply $u = -\varepsilon^{2m}$, $m \in \mathbb{Z}$, whence

$$X^3 = \varepsilon - \varepsilon^{2m+1}, \qquad X \neq 0,$$

which is impossible by Lemma 8.

Finally, suppose that $(t) = (729)$. Since $t/\Delta(E) = -t/\varepsilon^{6n+1}$ is a square by Lemma 3(1), we have $729/t = -\varepsilon^{2m-1}$ for some $m \in \mathbb{Z}$, and hence by (3.4) we have

$$\left(\frac{3c_4(E)}{(t+3)\varepsilon^{2n}}\right)^3 = \varepsilon^{2m} - 27\varepsilon.$$

By Lemma 9, m must be a multiple of 3. Letting $l = m/3 \in \mathbb{Z}$, we have

$$X^3 = 1 - 27\varepsilon^{1-6l}, \qquad X = \frac{3c_4(E)}{(t+3)\varepsilon^{2n+2l}} \in \mathcal{O}_k.$$

By Lemma 4, this is possible only if $k = \mathbb{Q}(\sqrt{33})$, $l = 0$, whence $j(E) = J(-729\varepsilon) = -(5+\sqrt{33})^3(5588 + 972\sqrt{33})^3\varepsilon^{-1}$, which equals $j(E_2)$ and $j(E_3')$. Lemma 14 therefore implies that E is isomorphic over $\mathbb{Q}(\sqrt{33})$ to E_2 or E_3' according as $\Delta(E) = -\varepsilon$ or $\Delta(E) = -\varepsilon^{-5}$.

The proof is now complete.

6. Appendix. In Section 5, we gave a characterization of elliptic curves having everywhere good reduction over a real quadratic field k, admitting a 3-isogeny defined over k, and having cubic discriminant (Proposition 13). Here we give a similar characterization of the curves whose discriminant is equal to $\square$, a square in k, or $-\square$. More precisely, we prove

PROPOSITION 15. *Let k be a real quadratic field. If there exists an elliptic curve E with everywhere good reduction over k given by a global minimal model with $j(E) = J(t)$ ($t \in \mathcal{O}_k$, $(t) = (1)$ or (729)) and $\Delta(E) = \pm\square$, then $k = \mathbb{Q}(\sqrt{29})$ and E is isomorphic over k to*

$$E_5 : y^2 + xy + \varepsilon^2 y = x^3,$$
$$\Delta(E_5) = -\varepsilon^{10}, \qquad j(E_5) = (\varepsilon^2 - 3)^3/\varepsilon^4,$$
$$E_6 : y^2 + xy + \varepsilon^2 y = x^3 - 5\varepsilon^2 x - (\varepsilon^2 + 7\varepsilon^4),$$
$$\Delta(E_6) = -\varepsilon^{14}, \qquad j(E_6) = -(1 + 216\varepsilon^2)^3/\varepsilon^{14},$$

or to their conjugates E_5', E_6'. Here $\varepsilon = (5+\sqrt{29})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{29})$ and J is the one given in Subsection 3.1.

LEMMA 16. (1) *The equation $27Y^2 = X^3 - 676$ ($X, Y \in \mathbb{Z}$) has no solutions.*

(2) *The equation $27Y^2 = X^3 + 784$ ($X, Y \in \mathbb{Z}$) has no solutions.*

(3) *The only $X, Y \in \mathbb{Z}$ satisfying $27Y^2 = X^3 + 676$ are $(X,Y) = (-1, \pm 5)$, $(26, \pm 26)$.*

(4) *The only $X, Y \in \mathbb{Z}$ satisfying $27Y^2 = X^3 - 784$ are $(X,Y) = (19, \pm 15)$, $(28, \pm 28)$.*

P r o o f. Let A be one of $\pm 676, \pm 784$. If $X, Y \in \mathbb{Z}$ satisfy $27Y^2 = X^3 + A$, then $(3X, 27Y)$ is an integral point of the elliptic curve

$$C_A : y^2 = x^3 + 27A.$$

If $A = 784$ or -676, then $C_A(\mathbb{Q}) = \{O\}$ is shown by 2-descent. The only integral points on C_{676} are

$$(-26, \pm 26), (-3, \pm 135), (13, \pm 143), (22, \pm 170), (78, \pm 702), (1573, \pm 62387),$$

among which $(-3, \pm 135) = (3\cdot(-1), \pm 27\cdot 5)$ and $(78, \pm 702) = (3\cdot 26, \pm 27\cdot 26)$ provide solutions of $27Y^2 = X^3 + 676$. The only integral points on C_{-784} are

$$(28, \pm 28), (57, \pm 405), (84, \pm 756), (1708, \pm 70588),$$

among which $(57, \pm 405) = (3\cdot 19, \pm 27\cdot 15)$ and $(84, \pm 756) = (3\cdot 28, \pm 27\cdot 28)$ provide solutions of $27Y^2 = X^3 - 784$. (The computations of the integral points of C_{676} and C_{-784} are done using KASH version 2.1.) ∎

LEMMA 17. *Let k be a real quadratic field. If there exist $u, v \in \mathcal{O}_k^\times$, $X \in \mathcal{O}_k$ such that*

$$X^3 = u + 27v, \qquad uv = \pm\square, \tag{6.1}$$

then k is equal to $\mathbb{Q}(\sqrt{29})$ and the only solutions are $(u, v, X) = (\pm\varepsilon^{3n+1}, \mp\varepsilon^{3n-1}, \mp\varepsilon^{n-1})$, $(\pm\varepsilon^{3n-1}, \mp\varepsilon^{3n+1}, \mp\varepsilon^{n+1})$ $(n \in \mathbb{Z})$, where $\varepsilon = (5 + \sqrt{29})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{29})$.

P r o o f. By changing (u, v, X) to (u^4, u^3v, uX) if necessary, we may assume that $N_{k/\mathbb{Q}}(u) = N_{k/\mathbb{Q}}(v) = 1$. Taking the norm of both sides of (6.1), we have $N_{k/\mathbb{Q}}(X)^3 = 730 + 27\,\mathrm{Tr}_{k/\mathbb{Q}}(uv')$. Since $uv = \pm\square$ and $N_{k/\mathbb{Q}}(v) = 1$, we have $uv' = uv/v^2 = \pm w^2$ for some $w \in \mathcal{O}_k^\times$. Hence

$$N_{k/\mathbb{Q}}(X)^3 = 730 \pm 27\,\mathrm{Tr}_{k/\mathbb{Q}}(w^2) = 730 \pm 27\{\mathrm{Tr}_{k/\mathbb{Q}}(w)^2 - 2N_{k/\mathbb{Q}}(w)\}.$$

If the sign is $+$, then

$$\begin{aligned} 27\,\mathrm{Tr}_{k/\mathbb{Q}}(w)^2 &= N_{k/\mathbb{Q}}(X)^3 - 730 + 54N_{k/\mathbb{Q}}(w) \\ &= \begin{cases} N_{k/\mathbb{Q}}(X)^3 - 676 & \text{if } N_{k/\mathbb{Q}}(w) = 1, \\ N_{k/\mathbb{Q}}(X)^3 - 784 & \text{if } N_{k/\mathbb{Q}}(w) = -1. \end{cases} \end{aligned}$$

It follows from Lemma 16 that $N_{k/\mathbb{Q}}(w) = -1$ and $\mathrm{Tr}_{k/\mathbb{Q}}(w) = \pm 15$ or ± 28, that is, $w = \pm(15 \pm \sqrt{229})/2$ or $\pm(14 \pm \sqrt{197})$. If $w = \pm(15 \pm \sqrt{229})/2$, then $(u + 27v) = (w^2 + 27) = \mathfrak{p}^3$, where $\mathfrak{p}$ is a prime ideal of $\mathbb{Q}(\sqrt{229})$ dividing 19. Since $\mathfrak{p}$ is not principal, $u + 27v$ is not a cube in $\mathbb{Q}(\sqrt{229})$. (Note that the class number of $\mathbb{Q}(\sqrt{229})$ is 3.) If $w = \pm(14 \pm \sqrt{197})$, then $u + 27v$ is not a cube in $\mathbb{Q}(\sqrt{197})$, since $(u + 27v) = (2^2 7(15 \pm \sqrt{197})) = (2)^3\mathfrak{p}_7^2\mathfrak{p}_7'$, where $(7) = \mathfrak{p}_7\mathfrak{p}_7'$.

If the sign is $-$, then

$$27\,\mathrm{Tr}_{k/\mathbb{Q}}(w)^2 = \{-N_{k/\mathbb{Q}}(X)\}^3 + 730 + 54N_{k/\mathbb{Q}}(w) = \begin{cases} \{-N_{k/\mathbb{Q}}(X)\}^3 + 784 & \text{if } N_{k/\mathbb{Q}}(w) = 1,\\ \{-N_{k/\mathbb{Q}}(X)\}^3 + 676 & \text{if } N_{k/\mathbb{Q}}(w) = -1.\end{cases}$$

It follows from Lemma 16 that $N_{k/\mathbb{Q}}(w) = -1$ and $\mathrm{Tr}_{k/\mathbb{Q}}(w) = \pm 5$ or ± 26, that is, $w = \pm(13\pm\sqrt{170})$ or $\pm(5\pm\sqrt{29})/2$. If $w = \pm(13\pm\sqrt{170})$, then $u+27v$ is not a cube in $\mathbb{Q}(\sqrt{170})$, since $(u+27v) = (26(12\pm\sqrt{170})) = \mathfrak{p}_2^3\mathfrak{p}_{13}^2\mathfrak{p}_{13}'$, where $(2) = \mathfrak{p}_2^3$, $(13) = \mathfrak{p}_{13}\mathfrak{p}_{13}'$. If $w = \pm(5\pm\sqrt{29})/2$, then $u+27v = v\varepsilon^{\pm 2}$ ($\varepsilon = (5+\sqrt{29})/2$). Thus, if $X^3 = u+27v$, then there exists $n \in \mathbb{Z}$ such that $v = \pm\varepsilon^{3n-1}$, $X = \pm\varepsilon^{n-1}$, or $v = \pm\varepsilon^{3n+1}$, $X = \pm\varepsilon^{n+1}$. ∎

Remark. Lemma 17 is a generalization of Proposition 2.3 of [11] which states that the only $m \in \mathbb{Z}$ and $X \in \mathcal{O}_{\mathbb{Q}(\sqrt{29})}$ satisfying $X^3 = \varepsilon^{4+12m} - 27\varepsilon^2$ are $m = 0$ and $X = -1$.

Proof of Proposition 15. Suppose that there exists an elliptic curve E with properties stated in the proposition. We take $\Delta(E) \in \mathcal{O}_k^\times$. Letting

$$(X,u,v) = \begin{cases} (c_4(E)/(t+3), \Delta(E), \Delta(E)/t) & \text{if } (t) = (1),\\ (3c_4(E)/(t+3), 729\Delta(E)/t, \Delta(E)) & \text{if } (t) = (729),\end{cases}$$

we have $X^3 = u+27v$, $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$, $uv = \pm\square$ by (3.3), (3.4) and Lemma 3(1). Hence, by Lemma 17, we have $k = \mathbb{Q}(\sqrt{29})$, $u/v = -\varepsilon^2, -\varepsilon'^2$, where $\varepsilon = (5+\sqrt{29})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{29})$. If $(t) = (1)$, then $t = u/v = -\varepsilon^2, -\varepsilon'^2$, and $j(E)$ is equal to $J(-\varepsilon^2) = (\varepsilon^2-3)^3/\varepsilon^4$ or $J(-\varepsilon'^2) = (\varepsilon'^2-2)^3\varepsilon^4$. If $(t) = (729)$, then $t = 729v/u = -729\varepsilon^2$, $-729\varepsilon'^2$, and $j(E)$ is equal to $J(-729\varepsilon^2) = -(1+216\varepsilon'^2)^3\varepsilon^{14}$ or $J(-729\varepsilon'^2) = -(1+216\varepsilon^2)^3\varepsilon'^{14}$. Since the values of j-invariant obtained above are equal to $j(E_5)$, $j(E_5')$, $j(E_6')$ and $j(E_6)$ respectively, Lemma 14 implies our assertion. ∎

Using Propositions 11, 12 and 15, we can give another proof of the following theorem which is the main theorem of [5]:

Theorem 18. *Up to isomorphism over $k = \mathbb{Q}(\sqrt{29})$, the only elliptic curves with everywhere good reduction over k are E_5, E_5', E_6 and E_6'.*

Proof. Let E be an elliptic curve with everywhere good reduction over $k = \mathbb{Q}(\sqrt{29})$ and let $\Delta(E) \in \mathcal{O}_k^\times$. Since $h_k^{(2)} = h_{k(\sqrt{\pm\varepsilon})}^{(2)} = 1$, $h_{k(\sqrt{-1})}^{(2)} = 3$, and E has no k-rational point of order 2 (see [1], [3]), we have $\Delta(E) = -\varepsilon^{2n} = -\square$. Since $h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}) = 2$, $h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)}) = 2$, and the prime number 3 is inert in k, we have by Propositions 11 and 12 that $j(E)$ is of the form $J(t)$, $(t) = (1)$ or (729). Proposition 15 therefore implies that E is isomorphic over k to E_5, E_5', E_6 or E_6', as claimed. ∎

References

[1] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. 144 (1990), 237–258.

[2] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, 1997.

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

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

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

[6] M. Kida, *Arithmetic of abelian varieties under field extensions*, dissertation, Johns Hopkins Univ., 1994.

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

[8] —, *Computing elliptic curves having good reduction everywhere over quadratic fields*, preprint.

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

[10] H. Naito, *On the Galois groups of the algebraic number fields generated by the* 3-*division points of elliptic curves*, Mem. Fac. Ed. Kagawa Univ., II 36 (1986), 35–40.

[11] T. Nakamura, *On Shimura's elliptic curve over* $\mathbb{Q}(\sqrt{29})$, J. Math. Soc. Japan 36 (1984), 701–707.

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

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

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

[15] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math. 74 (1978), 235–250.

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

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

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

Department of Mathematics
Ritsumeikan University
Kusatsu, Shiga 525-8577, Japan
E-mail: kagawa@se.ritsumei.ac.jp

Received on 27.7.1999 (3657)