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

Takaaki Kagawa

Abstract

This paper is a remix of author's papers [7], [8] and [9].

1 Introduction

Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field, where m is a square-free integer greater than 1. In our previous papers [5] and [6], we determined all elliptic curves with everywhere good reduction over k when $m = 37$ and 29, respectively. There, 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 [18]) 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 [6], [10], [12], the proof is given for the nonexistence of elliptic curves with everywhere good reduction over k when $m = 3, 21$ and the determination of such curves is done 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 $j(E)$ and $\Delta(E)$ by the j-invariant and the discriminant of E, respectively.

2010 *Mathematics Subject Classification*: 11G05.

2 Results

Let $k = \mathbb{Q}(\sqrt{33})$. The fundamental unit of k is $\varepsilon = 23 + 4\sqrt{33}$. In [12], the following elliptic curve with everywhere good reduction over k is given:

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

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

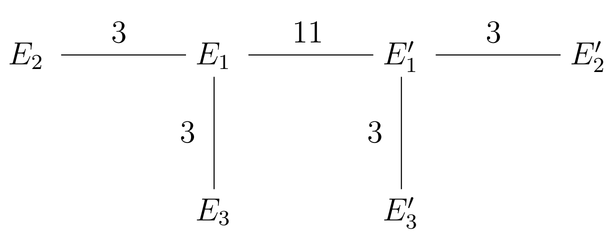
$$V_1 = E_1(k)_{\mathrm{tors}} = \langle (0,0) \rangle, \quad V_2 = \langle (-6-\sqrt{33}, y_1) \rangle,$$

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 [22], we obtain the following defining equations of E_2 and E_3:

$$\begin{aligned} E_2 &: y^2 + (5+\sqrt{33})xy + \varepsilon y = x^3 - (1235 + 215\sqrt{33})x - (35915 + 6252\sqrt{33}), \\ &\quad \varDelta(E_2) = -\varepsilon, \quad j(E_2) = -(5+\sqrt{33})^3(5588 + 972\sqrt{33})^3\varepsilon^{-1}, \\ E_3 &: y^2 + (5+\sqrt{33})xy + \varepsilon y = x^3 + (85 + 15\sqrt{33})x + (730 + 127\sqrt{33}), \\ &\quad \varDelta(E_3) = -\varepsilon^5, \quad j(E_3) = -(5-\sqrt{33})^3(5588 - 972\sqrt{33})^3\varepsilon. \end{aligned}$$

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 $\varDelta(E_1)/\varDelta(E_1') = \varDelta(E_2)/\varDelta(E_3') = \varepsilon^6$ is not a 12-th 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 twist 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 among the related elliptic curves:



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 to d. Let $S_d = S_2(\Gamma_0(d), \chi_d)$ be the space of cuspforms of Neben-type of weight 2 and level d. It is conjectured (cf. [16]) 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 [17], the j-invariants of E and $\overline{E}$ can be written as

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

(This is nothing other than a parameterization of the modular curve $Y_0(3)$.) Moreover, let $c_4(E)$ and $c_6(E)$ be the usual quantities associated to 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* E, $\overline{E}$, t *and* $\overline{t}$ *be as above. Then*

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

(b) *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* $(\overline{t})$ *are integral and sixth-powers.*

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

(b) 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 12-th 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 $t\bar{t} = 3^6$. 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 in which 3 does not split 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 [20]). Thus it follows from Lemma 3, (b) that

$$(t) = \begin{cases} (1),\ (729) & \text{if 3 is inert,} \\ (1),\ (27),\ (729) & \text{if 3 ramifies.} \end{cases}$$

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 $(t) = (1)$,

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

if $(t) = (729)$, and

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

if 3 is ramified and $(t) = (27)$. Note that $c_4(E) \neq 0$ since $j(E) \neq 0$.

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

$$X^3 = u + 27v, \quad X^3 = u + v$$

in $X \in \mathcal{O}_k \setminus \{0\}$, $u, v \in \mathcal{O}_k^{\times}$. We will study them in the next subsection.

3.2 Some Diophantine equations

Using the software KASH, SageMath or Magma, we obtain the following lemma.

Lemma 4. (a) *The equation* $27y^2 = x^3 - 676$ $(x, y \in \mathbb{Z})$ *has no solutions.*

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

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

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

Lemma 5. *Let* k *be a real quadratic field. If there exist* $u, v \in \mathcal{O}_k^\times$, $X \in \mathcal{O}_k$ *such that*

$$X^3 = u + 27v \tag{3.6}$$

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

Proof. 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 (3.6), we have

$$N_{k/\mathbb{Q}}(X)^3 = 730 + 27\,\mathrm{Tr}_{k/\mathbb{Q}}(uv^{-1}). \tag{3.7}$$

Since $uv = \pm\square_k$ and $N_{k/\mathbb{Q}}(v) = 1$, we have $uv^{-1} = uv/v^2 = \pm w^2$ 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 4 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 $(7) = \mathfrak{p}_7\mathfrak{p}_7'$, $\mathfrak{p}_7 \neq \mathfrak{p}_7'$.

If the sign is $-$, then

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

It follows from Lemma 4 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 $(2) = \mathfrak{p}_2^3$, $(13) = \mathfrak{p}_{13}\mathfrak{p}_{13}'$, $\mathfrak{p}_{13} \neq \mathfrak{p}_{13}'$. 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 an $n \in \mathbb{Z}$ such that $v = \pm\varepsilon^{3n-1}$, $X = \pm\varepsilon^{n-1}$, or $v = \pm\varepsilon^{3n+1}$, $X = \pm\varepsilon^{n+1}$. $\square$

Remark. Lemma 5 is a generalization of Proposition 2.3 in [15] 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 $X = -1$.

Using the software mentioned above, we obtain the following.

Lemma 6. (a) *There are no integer solutions of* $y^2 = x^3 - 784$.

(b) *The only integer solutions of* $y^2 = x^3 + 676$ *are* $(x, y) = (0, \pm 26)$.

(c) *The only integer solutions of* $y^2 = x^3 - 676$ *are* $(x, y) = (10, \pm 18)$, $(13, \pm 39)$, $(26, \pm 130)$, $(130, \pm 1482)$, $(338, \pm 6214)$ *and* $(901, \pm 27045)$.

(d) *The integer solutions of* $y^2 = x^3 + 784$ *are* $(x, y) = (-7, \pm 21)$, $(0, \pm 28)$, $(8, \pm 36)$ *and* $(56, \pm 420)$.

Proposition 7. *Let p be a prime number such that $p = 2$ or $p \equiv 3 \pmod 4$, $p > 3$. Let $k = \mathbb{Q}(\sqrt{3p})$. Then equation (3.6) has a solution in $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$ only when $k = \mathbb{Q}(\sqrt{6})$ or $\mathbb{Q}(\sqrt{33})$, in which cases, the only solutions are $(X, u, v) = (w_1(4 \pm \sqrt{6}), w_1^3, w_1^3(5 \pm 2\sqrt{6}))$, $(-w_2(5 \pm \sqrt{33}), w_2^3, -w_2^3(23 \pm 4\sqrt{33}))$, respectively. Here w_1 (resp. w_2) is any unit of $\mathbb{Q}(\sqrt{6})$ (resp. $\mathbb{Q}(\sqrt{33})$). Note 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. The case $uv = \pm \square_k$ are treated in Lemma 5 and shown no solutions exist. Thus we assume that $uv^{-1} = \pm \varepsilon w^2$, $w \in \mathcal{O}_k^\times$. Taking norm of (3.6), we have (3.7). There exists a $\pi \in \mathcal{O}_k$ such that $(\pi)^2 = (3)$, since 3 ramifies in k and the class number of k is odd. (see [3], Theorems 39 and 41.) The facts that $\pi^2/3 > 0$ and $k \neq \mathbb{Q}(\sqrt{3})$ imply $\sqrt{3\varepsilon} = \pi\varepsilon^n \in \mathcal{O}_k$ (for some $n \in \mathbb{Z}$). Thus

$$27 \operatorname{Tr}_{k/\mathbb{Q}}(uv^{-1}) = \pm 9 \operatorname{Tr}_{k/\mathbb{Q}}((\sqrt{3\varepsilon}\, w)^2) = \pm 9 \bigl\{ \operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w)^2 - 2 N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}) \bigr\}. \tag{3.8}$$

When $N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}) = -3$, equations (3.7) and (3.8) give

$$\bigl\{3 \operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w)\bigr\}^2 = \begin{cases} N_{k/\mathbb{Q}}(X)^3 - 784 & \text{if } uv^{-1} = \varepsilon w^2, \\ \bigl\{-N_{k/\mathbb{Q}}(X)\bigr\}^3 + 676 & \text{if } uv^{-1} = -\varepsilon w^2. \end{cases}$$

Thus there is no solution in this case.

When $N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}) = 3$, equations (3.7) and (3.8) give

$$\bigl\{3 \operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w)\bigr\}^2 = \begin{cases} N_{k/\mathbb{Q}}(X)^3 - 676 & \text{if } uv^{-1} = \varepsilon w^2, \\ \bigl\{-N_{k/\mathbb{Q}}(X)\bigr\}^3 + 784 & \text{if } uv^{-1} = -\varepsilon w^2. \end{cases}$$

In case $uv^{-1} = \varepsilon w^2$, Lemma 6 implies that $\operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = \pm 6, \pm 13, \pm 247$ or ± 9015, and

$$\sqrt{3\varepsilon}\, w = \begin{cases} 3 \pm \sqrt{6} & \text{if } \operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = 6, \\ -3 \pm \sqrt{6} & \text{if } \operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = -6, \\ (\pm 13 \pm \sqrt{157})/2 & \text{if } \operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = \pm 13, \\ \pm 247 \pm \sqrt{3 \cdot 503 \cdot 53857} & \text{if } \operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = \pm 247, \\ \pm 9015 \pm \sqrt{2 \cdot 11 \cdot 47 \cdot 59} & \text{if } \operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = \pm 9015. \end{cases}$$

Thus $k = \mathbb{Q}(\sqrt{6})$ and $\varepsilon = 5 + 2\sqrt{6}$. Since $\sqrt{3\varepsilon} = 3 + \sqrt{6}$ and $\sqrt{3\varepsilon}\,\varepsilon' = 3 - \sqrt{6}$, we have

$$uv^{-1} = \varepsilon w^2 = \begin{cases} \varepsilon & \text{if } \sqrt{3\varepsilon}\, w = \pm(3 + \sqrt{6}), \\ \varepsilon' & \text{if } \sqrt{3\varepsilon}\, w = \pm(3 - \sqrt{6}). \end{cases}$$

When $uv^{-1} = \varepsilon$, since $u + 27v = v(\varepsilon + 27) = v\varepsilon(4 - \sqrt{6})^3$, there exists a $w_1 \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{6})}$ such that $v = w_1^3\varepsilon'$, $u = w_1^3$ and $X = w_1(4 - \sqrt{6})$. When $uv^{-1} = \varepsilon'$, since $u + 27v = v(\varepsilon' + 27) = v\varepsilon'(4 + \sqrt{6})^3$, there exists a $w_1 \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{6})}$ such that $v = w_1^3\varepsilon$, $u = w_1^3$ and $X = w_1(4 + \sqrt{6})$. In case $uv^{-1} = -\varepsilon w^2$, Lemma 6 implies that $\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = \pm 7, \pm 12$, or ± 140, and

$$\sqrt{3\varepsilon}\, w = \begin{cases} (\pm 7 \pm \sqrt{37})/2 & \text{if } \mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = \pm 7, \\ 6 \pm \sqrt{33} & \text{if } \mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = 12, \\ -6 \pm \sqrt{33} & \text{if } \mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = -12, \\ \pm 70 \pm \sqrt{59 \cdot 83} & \text{if } \mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\, w) = \pm 140. \end{cases}$$

Thus $k = \mathbb{Q}(\sqrt{33})$ and $\varepsilon = 23 + 4\sqrt{33}$. Since $\sqrt{3\varepsilon} = 6 + \sqrt{33}$ and $\sqrt{3\varepsilon}\,\varepsilon' = 6 - \sqrt{33}$, we have

$$uv^{-1} = -\varepsilon w^2 = \begin{cases} -\varepsilon & \text{if } \sqrt{3\varepsilon}\, w = \pm(6 + \sqrt{33}), \\ -\varepsilon' & \text{if } \sqrt{3\varepsilon}\, w = \pm(6 - \sqrt{33}). \end{cases}$$

When $uv^{-1} = -\varepsilon$, since $u + 27v = v\varepsilon(5 - \sqrt{33})^3$, we have $u = -w_2^3$, $v = w_2^3\varepsilon'$ and $X = w_2(5 - \sqrt{33})$ for some $w_2 \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{33})}$. When $uv^{-1} = -\varepsilon'$, we have $u + 27v = v\varepsilon'(5 + \sqrt{33})^3$. Hence there exists a $w_2 \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{33})}$ such that $u = -w_2^3$, $v = w_2^3\varepsilon$ and $X = w_2(5 + \sqrt{33})$. □

Proposition 8. *Let k be a quadratic field. Then the only solution of the equation*

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

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

Proof. Since $X^3 - 1 = (X - 1)(X^2 + X + 1) = v \in \mathcal{O}_k^\times$, $X - 1 =: v_1$, $X^2 + X + 1 =: v_2$ are units of k. Eliminating X, we have $v_1^2 + 3v_1 + 3 = v_2$. Taking norm results in

$$N_{k/\mathbb{Q}}(v_2) = 3\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2 + 3\{N_{k/\mathbb{Q}}(v_1) + 3\}\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1) + 9 + 3N_{k/\mathbb{Q}}(v_1) + 1.$$

Reducing modulo 3 yields $N_{k/\mathbb{Q}}(v_2) = 1$. Therefore $\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2 + \{N_{k/\mathbb{Q}}(v_1) + 3\}\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1) + 3 + N_{k/\mathbb{Q}}(v_1) = 0$. If $N_{k/\mathbb{Q}}(v_1) = -1$, then $\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2 + 2\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1) + 2 = 0$, which is impossible. If $N_{k/\mathbb{Q}}(v_1) = 1$ then $\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2 + 4\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1) + 4 = 0$, from which $v_1 = -1$, $X = 0$. □

Proposition 9. *If the norm of the fundamental unit of a real quadratic field k is 1 and*

$$X^3 = u - v, \quad X \in \mathcal{O}_k, \quad u, v \in \mathcal{O}_k^\times, \quad uv = \square_k \tag{3.9}$$

holds, 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 (3.9) 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 $(0, \pm 2)$. □

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 should mention that, in his paper [14], Naito studied the same problem for elliptic curves defined over $\mathbb{Q}$.

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

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

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

(b) *$\Delta(E)$ 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.*

(c) *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).

Proof. (a) We have $\#G \geq 2$, since $k(\sqrt{-3}) \subset L$ ([21], 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

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

From these together with the classification of the subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$ (cf. [14]), we obtain the assertion.

(b) 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 ([18], § 5.3). The second part follows from direct calculation.

(c) 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 $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$. Among the groups appeared in (a), the only groups which are subgroups of this group are the ones in (i), (ii), (iii), (iv) and (vii). $\square$

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 that $h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}) \not\equiv 0 \pmod 4$, where $\mathfrak{p}_\infty^{(1)}$ and $\mathfrak{p}_\infty^{(2)}$ are the real primes of k, or $h_{k(\sqrt{-3})}((\sqrt{-3})) \not\equiv 0 \pmod 4$. 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.*

Proof. 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, (b), G is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to $\langle\sigma,\tau\rangle \cong SD_{16}$, $\langle\tau\rangle \cong \mathbb{Z}/8\mathbb{Z}$, $\langle\sigma,\tau^2\rangle \cong D_8$, $\langle -1\rangle \times \langle\rho\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or $\langle\rho\rangle \cong \mathbb{Z}/2\mathbb{Z}$. 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, (b), $H \cong \mathbb{Z}/4\mathbb{Z}$ 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 ([21], p. 184), our assumptions on ray class numbers imply that $G \sim \langle\rho\rangle$ or $\langle -1\rangle \times \langle\rho\rangle$. We therefore see from Lemma 10, (c) that E admits a 3-isogeny defined over k. $\square$

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

(a) *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.*

(b) *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. (a) 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 in [19], 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 $k(\sqrt[3]{\Delta(E)})$ ([18], p. 305), we have $[L : k] \equiv 0 \pmod 3$. Thus, by Lemma 10, (b), 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, (c), 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 $h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3)) \equiv 0 \pmod 4$.

(b) According to (a), 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 ε of k larger than 1 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.

5.1 The case where $\Delta(E)$ is a cube in k

If $\Delta(E)$ is a cube in k, then k must be $\mathbb{Q}(\sqrt{33})$ and E is isomorphic over k to E_1 or E_1'. Indeed, more generally, we have the following.

Proposition 13. *Let p be a prime number such that $p = 2$ or $p \neq 3$, $p \equiv 3 \pmod 4$, and let $k := \mathbb{Q}(\sqrt{3p})$. If there is an elliptic curve E which has everywhere good reduction over k and whose discriminant $\Delta(E)$ is a cube in k, then $p = 2$ or $p = 11$. If $p = 2$ (resp. $p = 11$), then E is isomorphic over k to*

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

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

First, we give some lemmas.

Lemma 14. *Let p and q be distinct primes such that $p \equiv q \equiv 3 \pmod 4$ and let $k = \mathbb{Q}(\sqrt{pq})$. Let $\mathfrak{q}$ be the prime ideal of k dividing q. Then*
(a) *h_k is odd.*
(b) *$k(\sqrt{-\varepsilon}) = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$.*
(c) *$\varepsilon \equiv (p/q) \pmod{\mathfrak{q}}$, where $(\cdot/\cdot)$ is the Legendre symbol. In particular, $\varepsilon \equiv p \pmod{\mathfrak{q}}$ if $q = 3$.*

Proof. (a) Theorems 39 and 41 of [3].
(b) By (a), $\mathfrak{q}$ is principal. Let $\pi \in \mathcal{O}_k$ be a generator of $\mathfrak{q}$. Since $\varepsilon > 1$, k is real and $k \neq \mathbb{Q}(\sqrt{q})$, we have $q = \pi^2\varepsilon^{2n+1}$ for some $n \in \mathbb{Z}$, whence $k(\sqrt{-q}) = k(\sqrt{-\varepsilon})$.
(c) We first show that $\varepsilon \equiv \pm 1 \pmod{\mathfrak{q}}$, which is equivalent to $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon)^2 \equiv 0 \pmod q$ since $N_{k/\mathbb{Q}}(\varepsilon \pm 1) = 2 \pm \mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon)$. But this readily follows by writing ε as $\varepsilon = (\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon) + b\sqrt{pq})/2$, $b \in \mathbb{Z}$.

Let $K = k(\sqrt{-\varepsilon}) = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$. By Theorem 23 in [3], $\mathfrak{q}$ splits in K if and only if there exists an $X \in \mathcal{O}_k$ such that $X^2 \equiv -\varepsilon \pmod{\mathfrak{q}}$, which is equivalent to $\varepsilon \equiv -1 \pmod{\mathfrak{q}}$, since $\mathcal{O}_K/\mathfrak{q} \cong \mathbb{Z}/q\mathbb{Z}$ and $q \equiv 3 \pmod 4$. On the other hand, $\mathfrak{q}$ splits in K if and only if q splits in $\mathbb{Q}(\sqrt{-p})$, which is equivalent to $(p/q) = -1$. □

Corollary 15. *Let p be a prime number such that $p \equiv 3 \pmod 4$ and $p \neq 3$. Let $k = \mathbb{Q}(\sqrt{3p})$ and $K = k(\sqrt{-3})$. Then*

(a) *h_K is odd.*

(b) *The ray class number $h_K((\sqrt{-3}))$ is $2h_K$ or h_K according as $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. In particular, $h_K((\sqrt{-3}))$ is not a multiple of 4.*

Proof. (a) By [3], Corollary 3 to Theorem 74, we have $h_K = h_k h_{\mathbb{Q}(\sqrt{-p})} h_{\mathbb{Q}(\sqrt{-3})} = h_k h_{\mathbb{Q}(\sqrt{-p})}$, which is odd by Lemma 14, (a).

(b) Let $G := (\mathcal{O}_K/\sqrt{-3}\mathcal{O}_K)^\times$ and $H := \{x + \sqrt{-3}\mathcal{O}_K \mid x \in \mathcal{O}_K^\times\} \subset G$. From the formula for the ray class number (Theorem 1 of Chapter VI in [13]), it follows that $h_K((\sqrt{-3})) = h_K(G : H)$. Thus it is enough to show that

$$(G : H) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 3, \\ 1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Let $\zeta_6 = (1 + \sqrt{-3})/2$ be a primitive sixth root of unity. Since $K = k(\sqrt{-\varepsilon})$ by Lemma 14, (b) and $\zeta_6 \in K$, we have $\mathcal{O}_K^\times = \langle \zeta_6 \rangle \times \langle \sqrt{-\varepsilon} \rangle$ (cf. [3], pp. 194, 195). Hence $H = \langle \sqrt{-\varepsilon} + \sqrt{-3}\mathcal{O}_K, \zeta_6 + \sqrt{-3}\mathcal{O}_K \rangle$. Let $\mathfrak{q}$ be the prime ideal of k dividing 3.

Assume that $p \equiv 1 \pmod 3$. Then, since $(-p/3) = -1$, $\mathfrak{q}\mathcal{O}_K = \sqrt{-3}O_K$ is a prime ideal of K and hence G is a cyclic group of order 8. Lemma 14, (c) and the formula

$$\zeta_6 - 1 = \zeta_6^2, \quad \zeta_6^2 - 1 = \sqrt{-3}\zeta_6 \tag{5.1}$$

imply that $H = \langle \sqrt{-\varepsilon} + \sqrt{-3}\mathcal{O}_K \rangle \cong \mathbb{Z}/4\mathbb{Z}$. Thus $(G : H) = 2$.

Assume that $p \equiv 2 \pmod 3$. By Lemma 14, (c), we have $X^2 + \varepsilon \equiv (X-1)(X+1) \pmod{\mathfrak{q}}$. Hence by letting $\mathfrak{Q}_1 = (\mathfrak{q}, \sqrt{-\varepsilon} - 1)$, $\mathfrak{Q}_2 = (\mathfrak{q}, \sqrt{-\varepsilon} + 1)$, it follows from [3], Theorem 23 that

$$\sqrt{-3}\mathcal{O}_K = \mathfrak{q}\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2, \; G \cong (\mathcal{O}_K/\mathfrak{Q}_1)^\times \times (\mathcal{O}_K/\mathfrak{Q}_2)^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times.$$

The definition of $\mathfrak{Q}_i$ $(i = 1, 2)$ implies that $\sqrt{-\varepsilon} \equiv 1 \pmod{\mathfrak{Q}_1}$ and $\sqrt{-\varepsilon} \equiv -1 \pmod{\mathfrak{Q}_2}$. Further, (5.1) means that $\zeta_6 \equiv -1 \pmod{\mathfrak{Q}_i}$ $(i = 1, 2)$. Hence $H \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$, whence $(G : H) = 1$. □

Lemma 16 ([11], Corollary 3.4)**.** *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. Let E be an elliptic curve having everywhere good reduction over k and having cubic discriminant in k. Then, by Proposition 11 and Corollary 15, E admits a 3-isogeny over k. Thus by the argument in section 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), (3.4), and (3.5), we see that there exist an $X \in \mathcal{O}_k \setminus \{0\}$ and a $u \in \mathcal{O}_k^\times$ such that

$$X^3 = 1 + 27u \quad \text{if } (t) = (1), \tag{5.2}$$
$$X^3 = u + 27 \quad \text{if } (t) = (729), \tag{5.3}$$
$$X^3 = 1 + u \quad \text{if } (t) = (27). \tag{5.4}$$

From Propositions 7 and 8, neither of the equations (5.3) and (5.4) has solutions. From Proposition 7, the only units u satisfying equation (5.2) are $5 \pm 2\sqrt{6}$ 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 16 therefore implies our assertion. □

Remark. All elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{6})$ have been determined in [6], [10].

5.2 The case where $\Delta(E)$ is not a cube

Consider the case where $\Delta(E)$ is not a cube in k. Table 1 and Proposition 12 imply that E admits a 3-isogeny defined over k. Thus $j(E)$ is of the form $J(t)$, $(t) = (1), (27), (729)$.

k	$h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)})$	$h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3))$
$\mathbb{Q}(\sqrt{33})$	$2 \cdot 3^3$	3^5
$\mathbb{Q}(\sqrt{57})$	$\mathbf{2^2 \cdot 3}$	$2 \cdot 3^3$
$\mathbb{Q}(\sqrt{69})$	$2 \cdot 3$	3^2
$\mathbb{Q}(\sqrt{93})$	$\mathbf{2^2 \cdot 3}$	$2 \cdot 3^2$

Table 1: Ray class numbers

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 [19]). The field $k(E[2])$ 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, $h_K^{(2)} := h_K\left(\prod_{\mathfrak{p}|2} \mathfrak{p}\right)$ is divisible by 3. Thus Table 2 implies that $\Delta(E) = -\varepsilon^{2n+1}$ for some $n \in \mathbb{Z}$. 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

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

which is impossible by Proposition 7.

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**

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

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

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

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, (a) and the fact $\pi^2=3\varepsilon$ imply $u=-\varepsilon^{2m}$ for some $m\in\mathbb{Z}$, whence

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

which is impossible by Proposition 9.

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

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

By Proposition 7, this is possible only if $k=\mathbb{Q}(\sqrt{33})$ and $m=0$, whence $j(E)=J(-729\varepsilon)=-(5+\sqrt{33})^3(5588+972\sqrt{33})^3\varepsilon^{-1}$, which equals to $j(E_2)$ and $j(E_3')$. Lemma 16 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 of Theorems 1 and 2 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 $\pm\square_k$. More precisely, we prove

Proposition 17. *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 $\Delta(E) = \pm\square_k$, then $k = \mathbb{Q}(\sqrt{29})$ and E is isomorphic over k to*

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

or to their conjugates E_5', E_6'. Here $\varepsilon = (5 + \sqrt{29})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{29})$ and $J(t)$ is the one given in section 3.1.

Proof. 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 $X^3 = u + 27v$, $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$, $uv = \pm\square_k$ by (3.3), (3.4) and Lemma 3, (a). Hence, by Lemma 5, 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 16 implies our assertion. □

Using Propositions 11, 12 and 17, we can give another proof of the following theorem which is the main theorem of [6]:

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], [4]), we have $\Delta(E) = -\varepsilon^{2n} = -\square_k$. 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 17 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), 233–258.

[2] J. E. Cremona, *Algorithms for modular elliptic curves* (2nd ed.), Cambridge University Press, 1997.

[3] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge studies in advanced mathematics 27, Cambridge University Press, Cambridge, 1991.
[4] H. Ishii, *The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields*, Japan. J. Math. **12** (1986), 45–52.
[5] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{37})$, Acta Arith. **83** (1998), 253–269.
[6] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields*, Arch. Math., **73** (1999), 25–32.
[7] T. Kagawa, *Nonexistence of elliptic curves having everywhere good reduction and cubic discriminant*, Proc. Japan Acad., Ser. A **76** (2000), 141-142.
[8] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields* $\mathbb{Q}(\sqrt{3p})$, Acta Arith. **96** (2001), 231-245
[9] T. Kagawa, *The Diophantine equation* $X^3 = u + 27v$ *over real quadratic fields*, Tokyo J. Math. **33** (2010), 159-163.
[10] M. Kida, *Reduction of elliptic curves over certain real quadratic number fields*, Math. Comp. **68** (1999), 1679–1685.
[11] M. Kida, *Computing elliptic curves having good reduction everywhere over quadratic fields*, Tokyo J. Math. **24** (2001), 545–558.
[12] M. Kida and T. Kagawa, *Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields*, J. Number Theory **66** (1997), 201–210.
[13] S. Lang, *Algebraic Number Theory* (2nd ed.), Grad. Texts in Math. 110, Springer, 1994.
[14] H. Naito, *On the Galois groups of the algebraic number fields generated by the* 3*-division points of elliptic curves*, Mem. Fac. Educ. Kagawa Univ., II **36** (1986), 35–40.
[15] T. Nakamura, *On Shimura's elliptic curve over* $\mathbb{Q}(\sqrt{29})$, J. Math. Soc. Japan **36** (1984), 701–707.
[16] R. G. E. Pinch, *Elliptic curves over number fields*, Ph. D. thesis, Oxford, 1982.
[17] R. G. E. Pinch, *Elliptic curves with good reduction away from* 3, Math. Proc. Camb. Phil. Soc. **101** (1987), 451–459.
[18] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
[19] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math. **74** (1978), 235–250.
[20] B. Setzer, *Elliptic curves with good reduction everywhere over quadratic fields and having rational* j*-invariant*, Illinois J. Math. **25** (1981), 233–245.
[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.
[22] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sc. Paris **273** (1971), 238–241.

Department of Mathematical sciences
College of Science and Engineering
Ritsumeikan University
Kusatsu, Shiga 525–8577, Japan
E-mail: kagawa@se.ritsumei.ac.jp