BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 59, No. 1, 2011

NUMBER THEORY

The Diophantine Equation $X^3 = u + v$ over Real Quadratic Fields

by

Takaaki KAGAWA

Presented by Jerzy KACZOROWSKI

This paper is dedicated to Professor Norio Adachi
on the occasion of his seventieth birthday

Summary. Let k be a real quadratic field and let $\mathcal{O}_k$ and $\mathcal{O}_k^\times$ be the ring of integers and the group of units, respectively. A method of solving the Diophantine equation $X^3 = u+v$ ($X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$) is developed.

1. Let k be a real quadratic field, $\mathcal{O}_k$ the ring of integers of k, and $\mathcal{O}_k^\times$ the group of units of k. We consider the Diophantine equation

$$X^3 = u + v \tag{1}$$

in $X \in \mathcal{O}_k - \{0\}$ and $u, v \in \mathcal{O}_k^\times$. The reason why we consider this equation is as follows:

Let E_1 and E_2 be elliptic curves defined by Weierstrass equations over $\mathcal{O}_k$ with unit discriminants $\Delta(E_1)$ and $\Delta(E_2)$, respectively. Suppose that there exists an isogeny from E_1 to E_2 defined over k with degree 3. Then, by Pinch [6], the j-invariants $j(E_1)$ and $j(E_2)$ can be written as

$$j(E_1) = J(t_1), \quad j(E_2) = J(t_2), \quad t_1, t_2 \in k, \quad t_1 t_2 = 3^6,$$

where $J(X) = (X+27)(X+3)^3/X$. (This is nothing other than a parametrization of the modular curve $Y_0(3)$.) As explained in [4], $j(E_i) \in \mathcal{O}_k$, $t_i \in \mathcal{O}_k$

2010 *Mathematics Subject Classification*: 11D99, 11G05.
Key words and phrases: Diophantine equation over real quadratic fields, elliptic curves with everywhere good reduction.

DOI: 10.4064/ba59-1-1

and the principal ideals (t_i) are 6th powers $(i = 1, 2)$. Thus

$$(t_1) = \begin{cases} (1),\ (3^6) & \text{when 3 is inert in } k, \\ (1),\ (3^3),\ (3^6) & \text{when 3 is ramified in } k, \\ (1),\ \mathfrak{p}^6,\ \mathfrak{p}'^6,\ (3^6) & \text{when } (3) = \mathfrak{p}\mathfrak{p}',\ \mathfrak{p} \neq \mathfrak{p}'. \end{cases}$$

It depends on k whether $\mathfrak{p}$ and $\mathfrak{p}'$ are principal ideals or not, and even if they are, their generators depend on k and hence are difficult to deal with. Thus, in the following, we consider the cases $(t_1) = (1)$, (3^3) and (3^6). If $(t_1) = (1)$, then

$$\left(\frac{c_4(E_1)}{t_1+3}\right)^3 = \Delta(E_1)(1 + 27w) \quad (w = 1/t_1 \in \mathcal{O}_k^\times).$$

If $(t_1) = (3^6)$ then

$$\left(\frac{3c_4(E_1)}{t_1+3}\right)^3 = \Delta(E_1)(w + 27) \quad (w = 3^6/t_1 \in \mathcal{O}_k^\times),$$

whence we get the equation

$$X^3 = u + 27v \tag{2}$$

in $X \in \mathcal{O}_k - \{0\}$ and $u, v \in \mathcal{O}_k^\times$. Here $c_4(E_1)$ is the usual quantity associated with a defining equation of E_1. (See [8].) Note that, from Theorem 2.1(a) of [7], $j(E_1) \neq 0$ and thus $c_4(E_1) \neq 0$. If $(t_1) = (3^3)$, then we get equation (1) as follows:

$$\left(\frac{c_4(E_1)}{t_1+3}\right)^3 = \Delta(E_1)(1 + w) \quad (w = 3^3/t_1 \in \mathcal{O}_k^\times).$$

For equation (2), we already have the following:

Theorem 1 ([5]). *Let p be a prime number with $p \equiv 3 \pmod 4$, $p \neq 3$, and let $k = \mathbb{Q}(\sqrt{3p})$. Then equation* (2) *has a solution if and only if $p = 11$, i.e. $k = \mathbb{Q}(\sqrt{33})$.*

Thus, in the following, we treat equation (1).

2. In the following, let k be as in Theorem 1. Then $N_{k/\mathbb{Q}}(w) = 1$ for all $w \in \mathcal{O}_k^\times$.

Multiplying cubes or considering the conjugate of (1), we may assume that $u = 1$ or $u = \varepsilon$ (> 1) is the fundamental unit of k. Hence we solve

$$X^3 = 1 + v, \quad X \in \mathcal{O}_k - \{0\},\ v \in \mathcal{O}_k^\times, \tag{3}$$

and

$$X^3 = \varepsilon + v, \quad X \in \mathcal{O}_k - \{0\},\ v \in \mathcal{O}_k^\times. \tag{4}$$

Proposition 2. *Equation* (3) *has no solutions.*

Proof. Suppose the contrary. Since $X^3 - 1 = (X-1)(X^2+X+1) = v \in \mathcal{O}_k^\times$, we have $X - 1 =: v_1 \in \mathcal{O}_k^\times$ and $X^2 + X + 1 =: v_2 \in \mathcal{O}_k^\times$. Eliminating X yields $v_1^2 + 3v_1 + 3 = v_2$. Noting that the norm of a unit is 1 and taking norms yields

$$\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2 + 4\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1) + 4 = 0.$$

But from this we get $v_1 = -1$, i.e. $X = 0$, a contradiction. ∎

Thus, from now on, we deal with equation (4).

LEMMA 3. *εv is a cube in k.*

Proof. Let $'$ be the conjugation of $k/\mathbb{Q}$. Noting $\varepsilon\varepsilon' = N_{k/\mathbb{Q}}(\varepsilon) = 1$ and $vv' = N_{k/\mathbb{Q}}(v) = 1$, we have

$$\left(\frac{X}{X'}\right)^3 = \frac{\varepsilon + v}{\varepsilon' + v'} = \frac{\varepsilon v(\varepsilon + v)}{\varepsilon v(\varepsilon' + v')} = \varepsilon v \frac{\varepsilon + v}{\varepsilon\varepsilon' v + \varepsilon v v'} = \varepsilon v \frac{\varepsilon + v}{v + \varepsilon} = \varepsilon v. \;\blacksquare$$

From this lemma, the form of the v is restricted. In fact, we have:

$v =$	εv is	Existence of a solution
$\pm\varepsilon^{6n+1}$	not a cube	$\times$
$\pm\varepsilon^{6n+2}$	a cube and not a $\pm\Box_k$	?
$\pm\varepsilon^{6n+4}$	not a cube	$\times$
$\pm\varepsilon^{6n+5}$	a cube and a $\pm\Box_k$	?

(where $\Box_k$ stands for a square element of k).

LEMMA 4. $v \neq -\varepsilon^{6n+5}$.

Proof. Suppose the contrary. Then there exists a $w \in \mathcal{O}_k^\times$ such that $w^2 = -\varepsilon' v$, whence

$$\begin{aligned} N_{k/\mathbb{Q}}(X)^3 &= N_{k/\mathbb{Q}}(\varepsilon + v) = (\varepsilon + v)(\varepsilon' + v') \\ &= 2 - (w^2 + w'^2) = 2 - (w + w')^2 + 2 \\ &= 4 - \mathrm{Tr}_{k/\mathbb{Q}}(w)^2. \end{aligned}$$

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

When $v = \varepsilon^{6n+5}$, there exists a $w \in \mathcal{O}_k^\times$ such that $\varepsilon' v = w^2$. Taking norms, we have

$$\begin{aligned} N_{k/\mathbb{Q}}(X)^3 &= N_{k/\mathbb{Q}}(\varepsilon + v) = (\varepsilon + v)(\varepsilon' + v') \\ &= 2 + (w^2 + w'^2) = 2 + (w + w')^2 - 2 \\ &= \mathrm{Tr}_{k/\mathbb{Q}}(w)^2. \end{aligned}$$

Thus $(N_{k/\mathbb{Q}}(X), \mathrm{Tr}_{k/\mathbb{Q}}(w))$ is an integer point on the singular cubic $y^2 = x^3$ and thus we cannot handle this case as in Lemma 4. But $\mathrm{Tr}_{k/\mathbb{Q}}(w)$ is a cube in $\mathbb{Z}$, and the following proposition holds:

PROPOSITION 5. *Let p ($\neq 3$) be a prime (not necessarily $p \equiv 3 \pmod 4$), and let $K := \mathbb{Q}(\sqrt{3p})$. If there exist an $a \in \mathbb{Z}$ and a $w \in \mathcal{O}_K^\times$ such that $\mathrm{Tr}_{K/\mathbb{Q}}(w) = a^3$, then $p = 5$ and $w = \pm 4 \pm \sqrt{15}$.*

Proof. Let $w = (a^3 + b\sqrt{3p})/2$, $b \in \mathbb{Z}$. Since $N_{k/\mathbb{Q}}(w) = (a^6 - 3pb^2)/4 = 1$, we have $3pb^2 = (a^3+2)(a^3-2)$.

(I) If a is even, then $(a^3+2, a^3-2) = 2$. Thus one of the following conditions holds:

(a) $a^3 + 2 = 2\Box$, $a^3 - 2 = 6p\Box$ ($\Box$ denotes a square element of $\mathbb{Z}$),
(b) $a^3 + 2 = -2\Box$, $a^3 - 2 = -6p\Box$,
(c) $a^3 + 2 = 6p\Box$, $a^3 - 2 = 2\Box$,
(d) $a^3 + 2 = -6p\Box$, $a^3 - 2 = -2\Box$,
(e) $a^3 + 2 = 6\Box$, $a^3 - 2 = 2p\Box$,
(f) $a^3 + 2 = -6\Box$, $a^3 - 2 = -2p\Box$,
(g) $a^3 + 2 = 2p\Box$, $a^3 - 2 = 6\Box$,
(h) $a^3 + 2 = -2p\Box$, $a^3 - 2 = -6\Box$.

The following lemma is obtained by using the free soft-ware KASH:

LEMMA 6.

(1) $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 2y^2 = x^3 + 2\} = \{(0, \pm 1)\}$.
(2) $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 2y^2 = x^3 - 2\} = \emptyset$.
(3) $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 6y^2 = x^3 + 2\} = \emptyset$.
(4) $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 6y^2 = x^3 - 2\} = \{(2, \pm 1)\}$.

Therefore $a = \pm 2$, $2p\Box = \pm 10$ and $w = \pm 4 \pm \sqrt{15}$.

(II) If a is odd, then $(a^3+2, a^3-2) = 1$. Thus one of the following conditions holds:

(a) $a^3 + 2 = \Box$, $a^3 - 2 = 3p\Box$ ($\Box$ denotes a square element of $\mathbb{Z}$),
(b) $a^3 + 2 = -\Box$, $a^3 - 2 = -3p\Box$,
(c) $a^3 + 2 = 3p\Box$, $a^3 - 2 = \Box$,
(d) $a^3 + 2 = -3p\Box$, $a^3 - 2 = -\Box$,
(e) $a^3 + 2 = 3\Box$, $a^3 - 2 = p\Box$,
(f) $a^3 + 2 = -3\Box$, $a^3 - 2 = -p\Box$,
(g) $a^3 + 2 = p\Box$, $a^3 - 2 = 3\Box$,
(h) $a^3 + 2 = -p\Box$, $a^3 - 2 = -3\Box$.

By using KASH again, we obtain the following:

LEMMA 7.

(1) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y^2 = x^3 + 2\} = \{(-1, \pm 1)\}$.
(2) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y^2 = x^3 - 2\} = \{(3, \pm 5)\}$.
(3) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 3y^2 = x^3 - 2\} = \emptyset$.
(4) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 3y^2 = x^3 + 2\} = \{(1, \pm 1)\}$.

Therefore $w = (\pm 27 \pm 5\sqrt{29})/2$ or $(\pm 1 \pm \sqrt{-3})/2$, none of which is in K. ∎

Thus, if there exists a solution (X, v) of (4), then there exists an $n \in \mathbb{Z}$ such that $v = \pm\varepsilon^{6n+2}$. In the $+$ case and in the $-$ case, there may exist a solution. Indeed, we have:

p	$p \bmod 3$	v	X	$N_{k/\mathbb{Q}}(X)$
23	2	ε^2	$(9 + \sqrt{69})/2$	3
31	1	$-\varepsilon^2$	$(-9 - \sqrt{93})/2$	-3
431	2	ε^2	$72 + 2\sqrt{1293}$	$12 = 3 \times 2^2$
439	1	$-\varepsilon^2$	$(-5625 - 155\sqrt{1317})/2$	$-75 = -3 \times 5^2$

From this table, we find interesting things. If $p \equiv 1 \pmod 3$, then $N_{K/\mathbb{Q}}(X) = -3\square$ and v is of the form $-\varepsilon^{6n+2}$ (in fact, $n = 0$), while if $p \equiv 2 \pmod 3$, then $N_{K/\mathbb{Q}}(X) = 3\square$ and v is of the form ε^{6n+2} (in fact, $n = 0$). We will show that these assertions are always true. (See Theorem 10 below.)

LEMMA 8. *Let $k = \mathbb{Q}(\sqrt{3p})$, ε be as above, and let w be an odd power of ε.*

(a) *If $p \equiv 1 \pmod 3$, then $\mathrm{Tr}_{k/\mathbb{Q}}(w) + 2 = p\square$ and $\mathrm{Tr}_{k/\mathbb{Q}}(w) - 2 = 3\square$.*
(b) *If $p \equiv 2 \pmod 3$, then $\mathrm{Tr}_{k/\mathbb{Q}}(w) + 2 = 3\square$ and $\mathrm{Tr}_{k/\mathbb{Q}}(w) - 2 = p\square$.*

Proof. Let $w = (a + b\sqrt{3p})/2$, where a, b are odd. Since $N_{k/\mathbb{Q}}(\varepsilon) = (a^2 - 3pb^2)/4 = 1$, we obtain $3pb^2 = (a + 2)(a - 2)$.

It follows from $(a + 2, a - 2) = 1$ that $\{a + 2, a - 2\} = \{\square, 3p\square\}$ or $\{p\square, 3\square\}$. Supposing $\{a + 2, a - 2\} = \{\square, 3p\square\} = \{x^2, 3py^2\}$, we obtain $(a + b\sqrt{3p})/2 = \{(x + y\sqrt{3p})/2\}^2$, which contradicts our hypothesis. Thus $\{a + 2, a - 2\} = \{p\square, 3\square\}$.

If $a + 2 = p\square, a - 2 = 3\square$, then $p\square - 4 = 3\square$ and $p \equiv 1 \pmod 3$, and if $a + 2 = 3\square, a - 2 = p\square$, then $p \equiv 2 \pmod 3$.

When $w = a + b\sqrt{3p}$ $(a, b \in \mathbb{Z})$, a similar proof works. ∎

LEMMA 9. *Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field (where m is a square-free integer), and let ε (> 1) be the fundamental unit of K.*

(a) *If $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$ is odd, then $m \equiv 5 \pmod 8$.*
(b) *Suppose that $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$ is odd. Then $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon^n)$ is even if and only if $3 \mid n$.*

Proof. (a) If $\varepsilon = (a + b\sqrt{m})/2$ (where $a = \mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$ and $b \in \mathbb{N}$ are odd), then $a^2 - mb^2 = \pm 4$. Since $a^2 \equiv b^2 \equiv 1 \pmod 8$, we have $m \equiv mb^2 = a^2 \mp 4 \equiv 5 \pmod 8$.

(b) The assertion follows easily from $(\mathcal{O}_K/(2))^\times = \mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$. ∎

The next theorem is our main result:

THEOREM 10. *Let X, v be a solution of equation* (4).

(a) *If $p \equiv 1 \pmod 3$, then:*

- *There exists an $n \in \mathbb{Z}$ such that $v = -\varepsilon^{6n+2}$.*
- *Letting $\varepsilon^{6n+1} = (a + b\sqrt{3p})/2$ $(a, b \in \mathbb{N})$ and $c = N_{k/\mathbb{Q}}(X)$, we have $c^3 = 2 - a = -3\Box$ and c is odd, $3pb^2 = c^6 - 4c^3 = a^2 - 4$, and $c^3 - 4 = -p\Box$.*
- *$p \equiv 7 \pmod 8$.*

(b) *If $p \equiv 2 \pmod 3$ then:*

- *There exists an $n \in \mathbb{Z}$ such that $v = \varepsilon^{6n+2}$.*
- *Letting $\varepsilon^{6n+1} = (a + b\sqrt{3p})/2$ $(a, b \in \mathbb{N})$ and $c = N_{k/\mathbb{Q}}(X)$, we have $c^3 = 2 + a = 3\Box$, $3pb^2 = c^6 - 4c^3 = a^2 - 4$, and $c^3 - 4 = p\Box$.*
- *$p \equiv 7 \pmod 8$.*

Proof. (a) Suppose that $v = \varepsilon^{6n+2}$. Taking the norm of $X^3 = \varepsilon + \varepsilon^{6n+2}$, we have

$$\begin{aligned} c^3 = N_{k/\mathbb{Q}}(X)^3 &= (\varepsilon + \varepsilon^{6n+2})(\varepsilon^{-1} + \varepsilon^{-6n-2}) \\ &= 2 + \mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon^{6n+1}) = 2 + a. \end{aligned}$$

Since $a^2 - 3pb^2 = 4$, we have $3pb^2 = c^6 - 4c^3$. From Lemma 8, $c^3 - 4 = a - 2 = 3\Box$, but $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 3y^2 = x^3 - 4\} = \emptyset$. Thus it is impossible. Therefore $v = -\varepsilon^{6n+2}$, and from Lemma 8, $c^3 = 2 - a = -3\Box$, $c^3 - 4 = -2 - a = -p\Box$. Suppose that c is even. Then, of course, $a = 2 - c^3$ is even. From $c^3 = -3\Box$, we have $c = -3\Box$. Thus $-p\Box = c^3 - 4 \equiv -4 \pmod{64}$, and thus $-p\Box/4 = c^3/4 - 1 \equiv 3 \pmod 4$, $p \equiv 1 \pmod 4$, which is impossible. Hence c is odd. Since $a = \mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon^{6n+1})$ is odd, it follows from Lemma 9 that $p \equiv 7 \pmod 8$.

(b) Arguing similarly to (a), we have $v = \varepsilon^{6n+2}$, $a = c^3 - 2$, $c^3 = 3\Box$ and $c^3 - 4 = p\Box$ (where a, b, c are integers as in the statement). If c is odd, then a is odd and thus, from Lemma 9, we obtain $p \equiv 7 \pmod 8$. Supposing c is even, it follows from $c^3 = 3\Box$ that $c = 3\Box$. Thus $p\Box = c^3 - 4 \equiv -4 \pmod{64}$ and so $p\Box/4 = c^3/4 - 1 \equiv 7 \pmod 8$, or $p \equiv 7 \pmod 8$. ∎

COROLLARY 11. *If $p \equiv 3 \pmod 8$ and $p \neq 3$, then equation* (1) *has no solutions.*

Theorem 10 tells us how to solve equation (4). We give two examples.

Example 1. $p = 23$ ($\equiv 2 \pmod 3$).

From Theorem 10, v must be of the form ε^{6n+2} ($n \in \mathbb{Z}$). Let a, b and c be rational integers as in Theorem 10. Then we have

$$c^3 = a + 2 = 3\square,$$
$$69b^2 = c^6 - 4c^3 = a^2 - 4,$$
$$c^3 - 4 = 23\square.$$

Using KASH, we find that the only integer solutions of $23y^2 = x^3 - 4$ are $(3, \pm 1)$, whence $c = 3, a = c^3 - 2 = 25, b^2 = (25^2 - 4)/69 = 3^2$, $\varepsilon^{6n+1} = (25 + 3\sqrt{69})/2 = \varepsilon$, and $X^3 = \varepsilon + \varepsilon^2 = ((9 + \sqrt{69})/2)^3$. Therefore the only solution of (4) is $(X, v) = ((9 + \sqrt{69})/2, \varepsilon^2)$.

Example 2. $p = 199$ ($\equiv 1 \pmod 3$).

From Theorem 10, v must be of the form $-\varepsilon^{6n+2}$ ($n \in \mathbb{Z}$). Let c be a rational integer as in Theorem 10. Then we have

$$c^3 - 4 = 199\square.$$

But $199y^2 = x^3 - 4$ has no integer solutions (this is checked by KASH again). Therefore, equation (4) and hence (1) has no solutions.

Using a computer, we obtain the following:

(a) For $p \equiv 7 \pmod 8$, $7 \leq p \leq 500$, equation (4) has a solution if and only if $p = 23, 31, 431, 439$.
(b) For the above p, the number of solutions of equation (4) is 1. (See the table above.)

It would be interesting to show the number of solutions of (4) is always at most 1, or to find p such that (4) has two or more solutions.

3. We give some applications to elliptic curves with everywhere good reduction.

Theorem 12. *Let p be a prime number such that $p \equiv 3 \pmod 4$ and $p \neq 3, 11$, and let $k := \mathbb{Q}(\sqrt{3p})$. Let ε (> 1) be the fundamental unit of k and let $\mathfrak{P}_\infty^{(1)}$ and $\mathfrak{P}_\infty^{(2)}$ be the real primes of $k(\sqrt[3]{\varepsilon})$. If the following three conditions hold, then there are no elliptic curves with everywhere good reduction over k:*

(a) $3 \nmid h_k$, *where h_k is the class number of k.*
(b) $4 \nmid h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)})$ *or* $4 \nmid h_{k(\sqrt[3]{\varepsilon}, \sqrt{-3})}((3))$ *(where, for a number field K and a divisor $\mathfrak{m}$ of K, $h_K(\mathfrak{m})$ denotes the ray class number of K modulo $\mathfrak{m}$).*
(c) *Equation (4) has no solutions.*

Proof. Let E be an elliptic curve with everywhere good reduction over k. Combining our assumption (a) and the fact that the class number is odd (see for example [2]), E is defined by a global minimal equation. From (b), there is an isogeny of degree 3 defined over k from E to another elliptic curve ([3], [4]). Then, as proved above, there exist solutions of $X^3 = u + 27v$ or $X^3 = u + v$ in $X \in \mathcal{O}_k - \{0\}$ and $u, v \in \mathcal{O}_k^\times$. These are impossible from Theorem 1 and our hypothesis (c). Therefore, there are no such elliptic curves. ∎

Corollary 13. *If $p = 43, 47, 59, 67, 71$ or 83, then there are no elliptic curves with everywhere good reduction over $k := \mathbb{Q}(\sqrt{3p})$.*

Proof. Using KASH, the class numbers and ray class numbers appearing in Theorem 12 are computed as follows:

p	$3p$	h_k	$h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)})$	$h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3))$
43	129	$\mathbf{1}$	$2^2 \cdot 3$	$\mathbf{2 \cdot 3^3}$
47	141	$\mathbf{1}$	$\mathbf{2 \cdot 3^3}$	
59	177	$\mathbf{1}$	$\mathbf{2 \cdot 3}$	
67	201	$\mathbf{1}$	$2^2 \cdot 3$	$\mathbf{2 \cdot 3^3}$
71	213	$\mathbf{1}$	$2^2 \cdot 3$	$\mathbf{2 \cdot 3^2}$
83	249	$\mathbf{1}$	$\mathbf{2 \cdot 3}$	

(the bold-faced numbers are those which meet the assumptions of Theorem 12(a), (b)). Thus, conditions (a) and (b) are satisfied. For these p, equation (4) has no solutions. ∎

We give another corollary which is already stated in [5].

Corollary 14. *Let p be a prime number such that $p \equiv 3 \pmod 8$ and $p \neq 3, 11$, and let $k := \mathbb{Q}(\sqrt{3p})$. Let ε (> 1) be the fundamental unit of k and let $\mathfrak{P}_\infty^{(1)}$ and $\mathfrak{P}_\infty^{(2)}$ be the real primes of $k(\sqrt[3]{\varepsilon})$. If the following two conditions hold, then there are no elliptic curves with everywhere good reduction over k:*

(a) $3 \nmid h_k$,

(b) $4 \nmid h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)})$ *or* $4 \nmid h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3))$.

References

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

[2] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields*, Contemp. Math. 24, Amer. Math. Soc., 1983.

[3] T. Kagawa, *Nonexistence of elliptic curves having everywhere good reduction and cubic discriminant*, Proc. Japan Acad. Ser. A 76 (2000), 141–142.

[4] —, *Determination of elliptic curves with everywhere good reduction over real quadratic fields* $\mathbb{Q}(\sqrt{3p})$, Acta Arith. 96 (2001), 231–245.

[5] —, *The Diophantine equation* $X^3 = u + 27v$ *over real quadratic fields*, Tokyo J. Math. 33 (2010), 159–163.

[6] R. G. E. Pinch, *Elliptic curves with good reduction away from 3*, Math. Proc. Cambridge Philos. Soc. 101 (1987), 451–459.

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

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

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

Received May 2, 2011 (7831)