TOKYO J. MATH.
VOL. 33, NO. 1, 2010

The Diophantine Equation $X^3 = u + 27v$ over Real Quadratic Fields

Takaaki KAGAWA

Ritsumeikan University

(Communicated by M. Ohta)

Abstract. Let k be a real quadratic field. The Diophantine equation $X^3 = u + 27v$ in $X \in \mathcal{O}_k$ (the ring of integers of k), $u, v \in \mathcal{O}_k^\times$ (the group of units of k) is solved under some assumptions on k.

1. Main theorem

Let k be a real quadratic field. Throughout, $\mathcal{O}_k$ and $\mathcal{O}_k^\times$ denote the ring of integers of k and the group of units of k, respectively. The Diophantine equation

$$X^3 = u + 27v \tag{1}$$

in $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$ arises from the study of elliptic curves with everywhere good reduction over k. (See [2], [3], [4] and [6].) We treat this equation and prove the following theorem:

THEOREM. *Let $k = \mathbf{Q}(\sqrt{6})$ or $k = \mathbf{Q}(\sqrt{3p})$, where p is a prime number such that $p \neq 3$ and $p \equiv 3 \pmod 4$. If equation* (1) *has solutions in $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$, then $k = \mathbf{Q}(\sqrt{6})$ or $k = \mathbf{Q}(\sqrt{33})$, and the only solutions are*

$$(X, u, v) = (w_1(4 \pm \sqrt{6}), w_1^3, w_1^3(5 \pm 2\sqrt{6}))$$

for any $w_1 \in \mathcal{O}_{\mathbf{Q}(\sqrt{6})}^\times$, or

$$(X, u, v) = (w_2(5 \pm \sqrt{33}), -w_2^3, w_2^3(23 \pm 4\sqrt{33}))$$

for any $w_2 \in \mathcal{O}_{\mathbf{Q}(\sqrt{33})}^\times$. (Note that $5 + 2\sqrt{6}$ and $23 + 4\sqrt{33}$ are the fundamental units of $\mathbf{Q}(\sqrt{6})$ and $\mathbf{Q}(\sqrt{33})$, respectively.)

This Theorem and a theorem in [5] imply the following criterion :

Received February 26, 2009; revised August 6, 2009
2000 *Mathematics Subject Classification*: 11D99, 11G05

CORALLARY 1. *Let p be a prime such that $p \neq 3, 11$, $p \equiv 3 \pmod 8$, let $k := \mathbf{Q}(\sqrt{3p})$, and let $\varepsilon > 1$ be the fundamental unit of k. If the following conditions are satisfied, then there are no elliptic curves with everywhere good reduction over k.*

(1) $(h_k, 3) = 1$,

(2) $4 \nmid h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_1^{(\infty)}\mathfrak{P}_2^{(\infty)})$ *or* $4 \nmid h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((3))$.

Here, for a number field K and a divisor $\mathfrak{m}$ of K, $h_K(\mathfrak{m})$ is the ray class number of K modulo $\mathfrak{m}$, and $\mathfrak{P}_1^{(\infty)}, \mathfrak{P}_2^{(\infty)}$ are the infinite primes of $k(\sqrt[3]{\varepsilon})$.

PROOF. Let E be an elliptic curve with everywhere good reduction over k. We may suppose that the discriminant of E is not a cube, because such a curve exists only on $\mathbf{Q}(\sqrt{6})$ and $\mathbf{Q}(\sqrt{33})$. (See [3].) By Proposition 12 of [4], E admits a 3-isogeny defined over k. Thus $X^3 = u + 27v$ or $X^3 = u + v$ has a solution in $X \in \mathcal{O}_k - \{0\}$, $u, v \in \mathcal{O}_k^\times$. But by Theorem in this paper, the former equation has no solutions, and from a result in [5], which requires $p \equiv 3 \pmod 8$, the latter equation has no solutions. □

As a corollary, we have

CORALLARY 2. *If $m = 129, 177, 201$ or 249, then there are no elliptic curves with everywhere good reduction over $\mathbf{Q}(\sqrt{m})$.*

PROOF. Using KASH, we obtain ray class numbers appeared in Collorary 1 as follows:

p	$m = 3p$	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	1	$2^2 \cdot 3$	$\mathbf{2 \cdot 3^3}$
59	177	1	$\mathbf{2 \cdot 3}$	
67	201	1	$2^2 \cdot 3$	$\mathbf{2 \cdot 3^3}$
83	249	1	$\mathbf{2 \cdot 3}$	

Thus Corollary 1 implies the assertion. □

2. Proof of Theorem

Let k be a real quadratic field.

When $uv = \square_k$ (a square in k) or $uv = -\square_k$, we already have the following ([4]):

LEMMA 1. *If there exist $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$ satisfying (1) and $uv = \pm\square_k$, then $k = \mathbf{Q}(\sqrt{29})$ and $(X, u, v) = (\pm\varepsilon_{29}^n, \mp\varepsilon_{29}^{3n+4}, \pm\varepsilon_{29}^{3n+2})$, $(\pm\varepsilon_{29}^n, \mp\varepsilon_{29}^{3n-4}, \pm\varepsilon_{29}^{3n-2})$ $(n \in \mathbf{Z})$. (Here and in what follows, ε_m (> 1) is the fundamental unit of the real quadratic field $\mathbf{Q}(\sqrt{m})$).*

The outline of the proof of Lemma 1 is as follows. By changing (u, v, X) to (u^4, u^3v, uX) if necessary, we may assume that $N_{k/\mathbf{Q}}(u) = N_{k/\mathbf{Q}}(v) = 1$. Thus taking norm of (1), we have

$$N_{k/\mathbf{Q}}(X)^3 = 730 + 27\,\mathrm{Tr}_{k/\mathbf{Q}}(uv^{-1})\,. \tag{2}$$

By assumption, there exists a $w \in \mathcal{O}_k^\times$ such that $uv^{-1} = \pm w^2$. When $uv^{-1} = w^2$, we have

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

When $uv^{-1} = -w^2$, we have

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

Thus the problem is reduced to computing the integer points of some elliptic curves.

When $uv \neq \pm\Box_k$, we cannot use the above method. However, as we shall see later, we can use similar method under the assumption of Theorem. The following lemma is vital:

LEMMA 2. *Let k be as in the assumption of Theorem and ε (> 1) the fundamental unit of k. Then $3\varepsilon = \Box_k$.*

PROOF. There exists a $\pi \in \mathcal{O}_k$ such that $(\pi)^2 = (3)$, since 3 is ramified in k and the class number of k is odd (see [1] for example). The facts that $\pi^2/3 > 0$ and $k \neq \mathbf{Q}(\sqrt{3})$ imply $3\varepsilon = (\pi\varepsilon^n)^2$ for some $n \in \mathbf{Z}$. $\Box$

Now we treat the case $uv \neq \pm\Box_k$. From now on, let k be as in the assumption of Theorem and ε (> 1) the fundamental unit of k. Taking norm of (1), we have (2) again. (Note that $N_{k/\mathbf{Q}}(\eta) = 1$ for all $\eta \in \mathcal{O}_k^\times$, since 3 is ramified in k.) Let $uv^{-1} = \pm\varepsilon w^2$, $w \in \mathcal{O}_k^\times$. Then Lemma 2 implies, in k, that

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

When $N_{k/\mathbf{Q}}(\sqrt{3\varepsilon}) = -3$, equations (2) and (3) give

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

Using the software KASH, we obtain the following.

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

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

Thus there is no solution in this case.

When $N_{k/\mathbf{Q}}(\sqrt{3\varepsilon}) = 3$, equations (2) and (3) give

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

Using KASH again, we obtain the following.

LEMMA 4. (a) *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* $(901, \pm 27045)$.

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

In case $uv^{-1} = \varepsilon w^2$, Lemma 4 implies that $\mathrm{Tr}_{k/\mathbf{Q}}(\sqrt{3\varepsilon}\,w) = \pm 6, \pm 13, \pm 494$ or ± 9015, and

$$\sqrt{3\varepsilon}\,w = \begin{cases} 3 \pm \sqrt{6} & \text{if } \mathrm{Tr}_{k/\mathbf{Q}}(\sqrt{3\varepsilon}\,w) = 6\,; \\ -3 \pm \sqrt{6} & \text{if } \mathrm{Tr}_{k/\mathbf{Q}}(\sqrt{3\varepsilon}\,w) = -6\,; \\ (\pm 13 \pm \sqrt{157})/2 & \text{if } \mathrm{Tr}_{k/\mathbf{Q}}(\sqrt{3\varepsilon}\,w) = \pm 13\,; \\ \pm 247 \pm \sqrt{2 \cdot 11 \cdot 47 \cdot 59} & \text{if } \mathrm{Tr}_{k/\mathbf{Q}}(\sqrt{3\varepsilon}\,w) = \pm 494\,; \\ (\pm 9015 \pm \sqrt{3 \cdot 503 \cdot 53857})/2 & \text{if } \mathrm{Tr}_{k/\mathbf{Q}}(\sqrt{3\varepsilon}\,w) = \pm 9015\,. \end{cases}$$

Thus $k = \mathbf{Q}(\sqrt{6})$ and $\varepsilon = \varepsilon_6 = 5 + 2\sqrt{6}$. Since $\sqrt{3\varepsilon_6} = 3 + \sqrt{6}$ and $\sqrt{3\varepsilon_6}\,\varepsilon_6' = 3 - \sqrt{6}$, we have

$$uv^{-1} = \varepsilon_6 w^2 = \begin{cases} \varepsilon_6 & \text{if } \sqrt{3\varepsilon_6}\,w = \pm(3 + \sqrt{6})\,; \\ \varepsilon_6' & \text{if } \sqrt{3\varepsilon_6}\,w = \pm(3 - \sqrt{6})\,. \end{cases}$$

When $uv^{-1} = \varepsilon_6$, since $u + 27v = v(\varepsilon_6 + 27) = v\varepsilon_6(4 - \sqrt{6})^3$, there exists $w_1 \in \mathcal{O}^\times_{\mathbf{Q}(\sqrt{6})}$ such that $v = w_1^3\varepsilon_6'$, $u = w_1^3$ and $X = w_1(4 - \sqrt{6})$. When $uv^{-1} = \varepsilon_6'$, since $u + 27v = v(\varepsilon_6' + 27) = v\varepsilon_6'(4 + \sqrt{6})^3$, there exists $w_1 \in \mathcal{O}^\times_{\mathbf{Q}(\sqrt{6})}$ such that $v = w_1^3\varepsilon_6$, $u = w_1^3$ and $X = w_1(4 + \sqrt{6})$.

In case $uv^{-1} = -\varepsilon w^2$, Lemma 4 implies that $\mathrm{Tr}_{k/\mathbf{Q}}(\sqrt{3\varepsilon}\,w) = \pm 7, \pm 12$, or ± 140, and

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

Thus $k = \mathbf{Q}(\sqrt{33})$ and $\varepsilon = \varepsilon_{33} = 23 + 4\sqrt{33}$. Since $\sqrt{3\varepsilon_{33}} = 6 + \sqrt{33}$ and $\sqrt{3\varepsilon_{33}}\,\varepsilon_{33}' =$

$6-\sqrt{33}$, we have

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

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

The proof of Theorem is now complete.

References

[1] A. FRÖHLICH, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemp. Math. 24, American Mathematical Society, 1983.

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

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

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

[5] T. KAGAWA, The Diophantine equation $X^3 = u + v$ over real quadratic fields, in preparation.

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

Present Address:
DEPARTMENT OF MATHEMATICAL SCIENCES,
RITSUMEIKAN UNIVERSITY,
NOJIHIGASHI, KUSASTSU, SHIGA, 525–8577 JAPAN.
e-mail: kagawa@se.ritsumei.ac.jp