The Diophantine equation $X^3 = u + v$ over real quadratic fields

加川貴章 (Takaaki KAGAWA)
立命館大学(Ritsumeikan Univ.)

k : real quadratic field, $\mathcal{O}_k$: ring of integers,
$\mathcal{O}_k^\times$: group of units

We consider the Diophantine equation

$$
\begin{aligned}
&X^3 = u + v, \\
&X \in \mathcal{O}_k - \{0\},\ u, v \in \mathcal{O}_k^\times.
\end{aligned}
\tag{1}
$$

Motivation

$E_1, E_2/\mathcal{O}_k$: elliptic curves with unit discriminants.

Suppose

$\exists f : E_1 \longrightarrow E_2$ isogeny of deg. 3 $/k$.

Then the j-invariants $j(E_1)$, $j(E_2)$ are of the form

$$\begin{aligned} &j(E_1) = J(t_1), \quad j(E_2) = J(t_2), \\ &t_1, t_2 \in k, \quad t_1 t_2 = 3^6, \end{aligned}$$

(where $J(X) = (X+27)(X+3)^3/X$).

Since $j(E_1), j(E_2) \in \mathcal{O}_k$, we have $t_1, t_2 \in \mathcal{O}_k$.

$c_4(E_1), c_6(E_1)$: as usual
$\Delta(E_1) \in \mathcal{O}_k^\times$: discriminant of E_1
$\Longrightarrow$

$$j(E_1) = \frac{c_4(E_1)^3}{\Delta(E_1)} \tag{2}$$
$$= \frac{(t_1+27)(t_1+3)^3}{t_1},$$
$$j(E_1) - 1728 = \frac{c_6(E_1)^2}{\Delta(E_1)} \tag{3}$$
$$= \frac{(t_1^2+18t_1-27)^2}{t_1}.$$

Since $(\Delta(E_1)) = (1)$ and $j(E_1) \neq 0, 1728$, by (2) and (3), the principal ideal (t_1) is 6-th power. Thus

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

$$(t_1) = (1)$$

$$\implies \left(\frac{c_4(E_1)}{t_1+3}\right)^3 = \Delta(E_1)(1+27w),$$

$$w = \frac{1}{t_1} \in \mathcal{O}_k^\times$$

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

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

$$\implies \left(\frac{3c_4(E_1)}{t_1+3}\right)^3 = \Delta(E_1)(w+27),$$

$$w = \frac{3^6}{t_1} \in \mathcal{O}_k^\times.$$

$$\implies X^3 = u + 27v$$

$$(t_1) = (3^3)$$

$$\implies \left(\frac{c_4(E_1)}{t_1+3}\right)^3 = \Delta(E_1)(1+w),$$

$$w = \frac{3^3}{t_1} \in \mathcal{O}_k^\times.$$

$$\implies X^3 = u + v$$

Theorem 1 (to appear in TJM).
Let $k = \mathbb{Q}(\sqrt{3p})$, p : *prime*, $\neq 3$, $\equiv 3 \pmod 4$.
Then $X^3 = u + 27v$ *has a solution*
in $X \in \mathcal{O}_k - \{0\}$, $u, v \in \mathcal{O}_k^\times$
$\Longleftrightarrow$
$k = \mathbb{Q}(\sqrt{33})$. ∎

Thus, we pay attention to (1).

Throughout, let k be as in Theorem 1
($\Longrightarrow N(w) = 1, \forall w \in \mathcal{O}_k^\times$ ($N := N_{k/\mathbb{Q}}$)
and the class number h_k of k is odd)

We may suppose $u = 1$
or $u = \varepsilon\,(> 1 :$ the fundamental unit of $k)$;
i.e. we must solve

$$X^3 = 1 + v, \qquad (4)$$
$$X \in \mathcal{O}_k - \{0\},\ v \in \mathcal{O}_k^\times$$

and

$$X^3 = \varepsilon + v, \qquad (5)$$
$$X \in \mathcal{O}_k - \{0\},\ v \in \mathcal{O}_k^\times.$$

Propositon 2. *Equation* (4) *has no solutions.*

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

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

$\therefore\ v_1 = -1,\ X = 0 \quad \cdots \quad$ impossible. ∎

Therefore, we treat equation (5)

Lemma 3. *εv is a cube*

Proof. Let $'$ be the conjugation of $k/\mathbb{Q}$. Then

$$\begin{aligned}\left(\frac{X}{X'}\right)^3 &= \frac{\varepsilon + v}{\varepsilon' + v'} \\ &= \frac{\varepsilon v(\varepsilon + v)}{\varepsilon v(\varepsilon' + v')} \\ &= \varepsilon v \frac{\varepsilon + v}{\varepsilon\varepsilon' v + \varepsilon v v'} \\ &= \varepsilon v \frac{\varepsilon + v}{v + \varepsilon} \\ &= \varepsilon v\end{aligned}$$

∎

$v =$	εv is	
$\pm\varepsilon^{6n+1}$	not a cube	$\times$
$\pm\varepsilon^{6n+2}$	a cube, $\neq \pm\square_k$	?
$\pm\varepsilon^{6n+4}$	not a cube	$\times$
$\pm\varepsilon^{6n+5}$	a cube, $\pm\square_k$	?

($\square_k$ = a square in k)

Lemma 4. $\varepsilon v \neq -\Box_k$.

Proof. Suppose the contrary. Then

$$\begin{aligned} N(X)^3 &= N(\varepsilon + v) \\ &= (\varepsilon + v)(\varepsilon' + v') \\ &= \varepsilon\varepsilon' + (\varepsilon v' + \varepsilon' v) + vv' \\ &= 2 - (w^2 + w'^2) \quad (\text{where } w^2 = -\varepsilon' v) \\ &= 2 - (w + w')^2 + 2 \\ &= 4 - T(w)^2. \end{aligned}$$

$\therefore T(w)^2 = \{-N(X)\}^3 + 4$

Since the only (affine) $\mathbb{Q}$-rational points of $y^2 = x^3 + 4$ are $(0, \pm 2)$, X must be $0 \cdots$ impossible.

∎

Remaining: $v = \varepsilon^{6n+5}$, $\pm\varepsilon^{6n+2}$

When $v = \varepsilon^{6n+5}$, then $\varepsilon v = \square_k$. Thus

$$\begin{aligned}
N(X)^3 &= N(\varepsilon + v) \\
&= (\varepsilon + v)(\varepsilon' + v') \\
&= \varepsilon\varepsilon' + (\varepsilon v' + \varepsilon' v) + vv' \\
&= 2 + (w^2 + w'^2) \qquad\qquad (\text{where } w^2 = \varepsilon' v) \\
&= 2 + (w + w')^2 - 2 \\
&= T(w)^2 \\
&\cdots \text{not an elliptic curve!}
\end{aligned}$$

But we have $T(w) =$ a cube.

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

Proof. Let $w = (a^3 + b\sqrt{3p})/2$, $b \in \mathbb{Z}$. Then
$N(w) = (a^6 - 3pb^2)/4 = 1$.
$\therefore 3pb^2 = (a^3 - 2)(a^3 + 2)$.

(I) a : even $\Longrightarrow (a^3 - 2, a^3 + 2) = 2 \Longrightarrow$
(a) $a^3 - 2 = 2\Box$, $a^3 + 2 = 6p\Box$ ($\Box =$ a square in $\mathbb{Z}$)
or
(b) $a^3 - 2 = -2\Box$, $a^3 + 2 = -6p\Box$
or
(c) $a^3 - 2 = 6p\Box$, $a^3 + 2 = 2\Box$
or
(d) $a^3 - 2 = -6p\Box$, $a^3 + 2 = -2\Box$
or
(e) $a^3 - 2 = 6\Box$, $a^3 + 2 = 2p\Box$
or

(f) $a^3 - 2 = -6\Box$, $a^3 + 2 = -2p\Box$

or

(g) $a^3 - 2 = 2p\Box$, $a^3 + 2 = 6\Box$

or

(h) $a^3 - 2 = -2p\Box$, $a^3 + 2 = -6\Box$

Lemma 6.

(a) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 2y^2 = x^3 - 2\} = \emptyset$.

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

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

(d) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 6y^2 = x^3 + 2\} = \emptyset$.

$\therefore a = \pm 2$, $2p\Box = \pm 10$. $\therefore u = \pm 4 \pm \sqrt{15}$.

(II) a : odd $\cdots$ similar. ∎

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

Thus, if (5) has a solution, then $\exists n \in \mathbb{Z}$, s.t. $v = \pm\varepsilon^{6n+2}$.

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

Lemma 7. *$k := \mathbb{Q}(\sqrt{3p})$, ε : as above,*
$w = \varepsilon^{odd}$

(1) $p \equiv 1 \pmod 3$
$\Longrightarrow T(w) + 2 = p\square,\ T(w) - 2 = 3\square$

(2) $p \equiv 2 \pmod 3$
$\Longrightarrow T(w) + 2 = 3\square,\ T(w) - 2 = p\square$

Proof. Suppose $w = (a + b\sqrt{3p})/2$, $a, b :$ odd. Since $N(\varepsilon) = (a^2 - 3pb^2)/4 = 1$, we have $3pb^2 = a^2 - 4 = (a+2)(a-2)$.
$(a+2, a-2) = 1$ implies
$\{a+2, a-2\} = \{\square, 3p\square\}$ or $\{p\square, 3\square\}$.
Assuming $\{a+2, a-2\} = \{3p\square, \square\} = \{3py^2, x^2\}$, we get $(a + b\sqrt{3p})/2 = \{(x + y\sqrt{3p})/2\}^2 \cdots$ contradiction.
$\therefore \{a+2, a-2\} = \{p\square, 3p\square\}$.
$a + 2 = p\square, a - 2 = 3\square \Longrightarrow p\square - 4 = 3\square$
$\Longrightarrow p \equiv 2 \pmod 3$
$a + 2 = 3\square, a - 2 = -\square \Longrightarrow p \equiv 1 \pmod 3$.

$w = a + b\sqrt{3p}$, $a, b \in \mathbb{Z} \cdots$ similar. ∎

Lemma 8. $K = \mathbb{Q}(\sqrt{m})$: *real quadratic field* (m : *square-free*), ε (> 1) : *the fundamental unit of* K

(a) $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$: *odd* $\Longrightarrow m \equiv 5 \pmod 8$.

(b) $[\exists w \in \mathcal{O}_K^\times$ *s.t.* $\mathrm{Tr}_{K/\mathbb{Q}}(w)$: *odd* $]$
$\iff$ $[\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$ *is odd* $]$

(c) *Suppose that* $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$ *is odd.*
Then $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon^n)$: *even* $\iff 3 \mid n$.

Theorem 9. *X, v : a solution of* (5).

(a) $p \equiv 1 \pmod 3 \Longrightarrow$

- $\exists n \in \mathbb{Z}$ *s.t.* $v = -\varepsilon^{6n+2}$,
- *Letting* $\varepsilon^{6n+1} = (a+b\sqrt{3p})/2$, $c = N(X)$, *we have* $c^3 = 2 - a = -3\Box$: *odd,* $(\Longrightarrow T(\varepsilon^{6n+1})$: *odd* $\Longrightarrow p \equiv 7 \pmod 8)$, $3pb^2 = c^6 - 4c^3 = a^2 - 4$, $c^3 - 4 = -p\Box$.

(b) $p \equiv 2 \pmod 3 \Longrightarrow$

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

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

$$\begin{aligned} c^3 &= N(X)^3 \\ &= (\varepsilon + \varepsilon^{6n+2})(\varepsilon^{-1} + \varepsilon^{-6n-2}) \end{aligned}$$

$$= 2 + T(\varepsilon^{6n+1}) = 2 + a.$$

$$\therefore a = c^3 - 2.$$

Since $a^2 - 3pb^2 = 4$, we have $3pb^2 = c^6 - 4c^3$.
From Lemma7, we have $c^3 - 4 = a - 2 = 3\square$.
But $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 3y^2 = x^3 - 4\} = \emptyset$.
Thus $v = -\varepsilon^{6n+2}$,
$c^3 = 2 - a \overset{\text{Lemma7}}{=} -3\square$,
$c^3 - 4 = -2 - a \overset{\text{Lemma7}}{=} -p\square$

Suppose that c is even.
Then $a = 2 - c^3$: even.
From $c^3 = -3\square$, we have $c = -3\square$.
$\therefore -p\square = c^3 - 4 \equiv -4 \pmod{64}$.
$\therefore -p\dfrac{\square}{4} = \dfrac{c^3}{4} - 1 \equiv 3 \pmod 4$.
$\therefore p \equiv 1 \pmod 4 \cdots$ impossible.
Thus c is odd

(b) Similar arguments yields $v = \varepsilon^{6n+2}$, $a = c^3 - 2$, $c^3 = 3\square$, $c^3 - 4 = p\square$, where a, b, c as in Theorem.

If c is odd, then, a is odd. Hence Lemma 8 implies $p \equiv 7 \pmod 8$.
If c is even, then, from $c^3 = 3\square$, we have $c = 3\square$.
$\therefore p\square = c^3 - 4 \equiv -4 \pmod{64}$.
$\therefore p\frac{\square}{4} = \frac{c^3}{4} - 1 \equiv 7 \pmod 8$.
$\therefore p \equiv 7 \pmod 8$. ∎

Corollary 10. $p \equiv 3 \pmod 8 \implies (1)$ *has no solutions.*

Theorem 9 tells us how to solve equation (5).

Example. $p = 23$ ($\equiv 2 \pmod 3$)
Consider $X^3 = \varepsilon + \varepsilon^{6n+2}$. By Theorem 9, we have

$$\begin{aligned} c^3 &= a + 2 = 3\Box, \\ 69b^2 &= c^6 - 4c^3 = a^2 - 4, \\ c^3 - 4 &= 23\Box. \end{aligned}$$

$\star\ \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 23y^2 = x^3 - 4\} = \{(3, \pm 1)\}$.

$\therefore c = 3, a = c^3 - 2 = 25, b^2 = \dfrac{25^2 - 4}{69} = 3^2$.

$\therefore \varepsilon^{6n+1} = (25 + 3\sqrt{69})/2 = \varepsilon$.

$\therefore n = 0$, $X^3 = \varepsilon + \varepsilon^2 = ((9 + \sqrt{69})/2)^3$.

Hence, the only solution is
$(X, v) = ((9 + \sqrt{69})/2, \varepsilon^2)$

$p \equiv 7 \pmod 8$, $7 \le p \le 500$

(a) (5) has solutions $\iff p = 23, 31, 431, 439.$

(b) For the above p, the number of solutions is 1.

p	$p \bmod 3$	v	X
23	2	ε^2	$\frac{9+\sqrt{69}}{2}$
31	1	$-\varepsilon^2$	$\frac{-9-\sqrt{93}}{2}$
431	2	ε^2	$72 + 2\sqrt{1293}$
439	1	$-\varepsilon^2$	$\frac{-5625-155\sqrt{1317}}{2}$

Theorem 11. *p : prime number, $p \equiv 3 \pmod 8$, $p \neq 3, 11$, $k := \mathbb{Q}(\sqrt{3p})$.*
ε (> 1) : the fundamental unit of k
$\mathfrak{P}_\infty^{(1)}, \mathfrak{P}_\infty^{(2)}$: the real primes of $k(\sqrt[3]{\varepsilon})$
If the following 2 conditions are satisfied, then there are no elliptic curves with everywhere good reducrtion 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* $4 \nmid h_{k(\sqrt[3]{\varepsilon}, \sqrt{-3})}((3))$
(*For a number field K and a divisor $\mathfrak{m}$ of K, let $h_K(\mathfrak{m})$ be the ray class number of K modulo $\mathfrak{m}$.*)

Corollary 12. *If $m = 129, 177, 201$ or 249, then there are no ellptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{m})$.*