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

加川貴章 (Takaaki KAGAWA)

1. k を実二次体とし, $\mathcal{O}_k$, $\mathcal{O}_k^\times$ でそれぞれ k の整数環, 単数群を表すとする. 不定方程式

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

を考える. この方程式を考える理由は以下の通りである：

E_1, E_2 を, $\mathcal{O}_k$ 係数の Weierstrass 方程式で定義される楕円曲線で, 判別式 $\Delta(E_1), \Delta(E_2)$ が $\mathcal{O}_k^\times$ に属するものとする. E_1 から E_2 への k 上定義された 3 次の isogeny があるとする. この時 j 不変量 $j(E_1)$, $j(E_2)$ は以下のような特別な形をしている ([5])：

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

但し $J(X) = (X + 27)(X + 3)^3/X$. (これは modular curve $Y_0(3)$ のパラメータ表示に他ならない.) $j(E_i) \in \mathcal{O}_k (i = 1, 2)$ であり (cf. [6], Propostion 5.1), t_i はモニック多項式 $(X + 27)(X + 3)^3 - j(E_i)X \in \mathcal{O}_k[X]$ の根であるので, $t_1, t_2 \in \mathcal{O}_k$ である. また単項イデアル (t_i) はイデアルの 6 乗でなくてはならないことがわかる ([3], p.234). よって

$$(t_1) = \begin{cases} (1), \ (3^6) & (3 \text{ が } k \text{ で惰性する時}), \\ (1), \ (3^3), \ (3^6) & (3 \text{ が } k \text{ で分岐する時}), \\ (1), \ \mathfrak{p}^6, \ \mathfrak{p}'^6, \ (3^6) & ((3) = \mathfrak{p}\mathfrak{p}', \ \mathfrak{p} \neq \mathfrak{p}' \text{ の時}). \end{cases}$$

$\mathfrak{p}$, $\mathfrak{p}'$ は単項イデアルかどうかわからないし, 仮に単項イデアルとしても生成元は体に依存した量に成るだろうから, 取り扱いは難しいと思われる. よって $(t_1) = (1), (3^3), (3^6)$ の場合を扱うことにする. $(t_1) = (1)$ ならば

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

$(t_1) = (3^6)$ ならば

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

となり

$$X^3 = u + 27v, \quad X \in \mathcal{O}_k - \{0\}, \quad u, v \in \mathcal{O}_k^\times \tag{2}$$

が得られる. $(t_1) = (3^3)$ ならば

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

となり (1) が得られる. 方程式 (2) に関しては次の結果がある :

定理 1 ([4])**.** p を $p \equiv 3 \pmod 4$, $p \neq 3$ である素数とし, $k = \mathbb{Q}(\sqrt{3p})$ とおく. この時 (2) が解を持つ $\iff$ $k = \mathbb{Q}(\sqrt{33})$.

よって (1) を考えるのである.

2. 以降 k を定理 1 にあるような実二次体とする. 定理 1 のような条件をつける理由は, 上述のように 3 が分岐する場合にのみ $X^3 = u + v$ が関わることと, k の類数 h_k が奇数となるからである. (類数が 6 と素なら k 上至る所 good reduction を持つ楕円曲線が global minimal equation で定義される. すなわち, $\mathcal{O}_k$ 係数で判別式が $\mathcal{O}_k^\times$ であるような方程式で定義される. 周知の通り, 実二次体の類数が奇数であるか否かは容易にコントロールできるが, 3 で割れるかどうかはコントロールが難しいので, せめて類数を奇数にはしておきたい.) この時任意の $w \in \mathcal{O}_k^\times$ に対し $N_{k/\mathbb{Q}}(w) = 1$ であることに注意しておく.

(1) に 3 乗数を掛ける, 共役を取るなどして, $u = 1$ または $u = \varepsilon$ (> 1 は k の基本単数) としてよい. 即ち

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

及び

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

を解けばよい.

命題 2. 方程式 (3) は解を持たない.

証明. $X^3 - 1 = (X-1)(X^2+X+1) = v \in \mathcal{O}_k^\times$ だから, $X - 1 =: v_1 \in \mathcal{O}_k^\times$, $X^2 + X + 1 =: v_2 \in \mathcal{O}_k^\times$ である. X を消去して, $v_1^2 + 3v_1 + 3 = v_2$ を得る. 単数のノルムが 1 であることに注意してノルムを取ると,

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

が得られるが, これから $v_1 = -1$, 即ち $X = 0$ となり矛盾である. ∎

よって以降方程式 (4) を扱う.

補題 3. εv は k の 3 乗数である.

証明. $'$ で $k/\mathbb{Q}$ の共役を表すとする. $\varepsilon\varepsilon' = N_{k/\mathbb{Q}}(\varepsilon) = 1$, $vv' = N_{k/\mathbb{Q}}(v) = 1$ に注意して計算すると,

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

が得られる. ∎

この補題により, v の形が大分絞られてくる. 実際,

$v =$	εv は	解の有無
$\pm\varepsilon^{6n+1}$	3 乗数でない	$\times$
$\pm\varepsilon^{6n+2}$	3 乗数であり, $\pm\square_k$ でない.	?
$\pm\varepsilon^{6n+4}$	3 乗数でない	$\times$
$\pm\varepsilon^{6n+5}$	3 乗数であり, $\pm\square_k$ である.	?

(但し $\square_k$ で k の平方数を表すとする.)

補題 4. $\varepsilon v \neq -\square_k$.

証明. $\varepsilon v = -\square_k$ とする. この時 $w^2 = -\varepsilon' v$ となる $w \in \mathcal{O}_k^\times$ が存在するので,

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

よって $\mathrm{Tr}_{k/\mathbb{Q}}(w)^2 = \{-N_{k/\mathbb{Q}}(X)\}^3 + 4$ が成り立つが, Cremona [1] によると $y^2 = x^3 + 4$ (108A1) の (affine) $\mathbb{Q}$ 有理点は $(0, \pm 2)$ だけなので, $X = 0$ でなくてはならず, 不可能である. ∎

$v = \varepsilon^{6n+5}$ の時はどうかと言うと, $\varepsilon' v = w^2$ となる $w \in \mathcal{O}_k^\times$ が存在するので,

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

となり楕円曲線でなくなってしまうので, $v = -\varepsilon^{6n+5}$ の時のようにはいかない. しかし $\mathrm{Tr}_{k/\mathbb{Q}}(w)$ が立方数であることは言える. そして次が成り立つ.

命題 5. p を 3 でない素数とし ($p \not\equiv 3 \pmod 4$ は仮定しない), $K := \mathbb{Q}(\sqrt{3p})$ とおく. $\mathrm{Tr}_{K/\mathbb{Q}}(w) = a^3$ を満たす $a \in \mathbb{Z}$, $w \in \mathcal{O}_K^\times$ が存在すれば, $p = 5$, $w = \pm 4 \pm \sqrt{15}$ でなくてはならない.

証明. $w = (a^3 + b\sqrt{3p})/2$, $b \in \mathbb{Z}$ とする. この時 $N_{k/\mathbb{Q}}(w) = (a^6 - 3pb^2)/4 = 1$ であるので, $3pb^2 = (a^3+2)(a^3-2)$ である.

(I) a が偶数ならば $(a^3+2, a^3-2) = 2$ だから,
(a) $a^3+2 = 2\square$, $a^3-2 = 6p\square$ ($\square$ で $\mathbb{Z}$ の平方数を表すとする.)
(b) $a^3+2 = -2\square$, $a^3-2 = -6p\square$
(c) $a^3+2 = 6p\square$, $a^3-2 = 2\square$
(d) $a^3+2 = -6p\square$, $a^3-2 = -2\square$
(e) $a^3+2 = 6\square$, $a^3-2 = 2p\square$
(f) $a^3+2 = -6\square$, $a^3-2 = -2p\square$
(g) $a^3+2 = 2p\square$, $a^3-2 = 6\square$
(h) $a^3+2 = -2p\square$, $a^3-2 = -6\square$
のいずれかが成り立つ.

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

(この補題は, フリーのソフトウェア KASH のコマンド IntegralPoints を使うことにより得られる.)
故に $a = \pm 2$, $2p\square = \pm 10$ で. $u = \pm 4 \pm \sqrt{15}$ である.

(II) a が奇数の時も同様である. ∎

よって方程式 (4) が解を持てば, $v = \pm\varepsilon^{6n+2}$ となる $n \in \mathbb{Z}$ が存在する. 少々コンピューターを使って計算してみると, $+$ の場合も $-$ の場合も解が見付かる場合がある.

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	$-\varepsilon^2$	$(-5625-155\sqrt{1317})/2$	$-75 = -3\times 5^2$

これを見ると, 非常にはっきりした傾向が見受けられる. 実際 $p \equiv 1 \pmod 3$ なら $v = -\varepsilon^2$ が解で $N_{k/\mathbb{Q}}(X) = -3\square$, $p \equiv 2 \pmod 3$ なら $v = \varepsilon^2$ が解で $N_{k/\mathbb{Q}}(X) = 3\square$ となっている. これが常に成り立つことを以下に見ていこう.

補題 7. $k=\mathbb{Q}(\sqrt{3p})$, ε を上の通りとし, w を ε の奇数乗とする. この時
(a) $p\equiv 1 \pmod 3$ ならば, $\mathrm{Tr}_{k/\mathbb{Q}}(w)+2=p\square$, $\mathrm{Tr}_{k/\mathbb{Q}}(w)-2=3\square$ である.
(b) $p\equiv 2 \pmod 3$ ならば, $\mathrm{Tr}_{k/\mathbb{Q}}(w)+2=3\square$, $\mathrm{Tr}_{k/\mathbb{Q}}(w)-2=p\square$ である.

証明. $w=(a+b\sqrt{3p})/2$ (a,b は奇数) とする. $N_{k/\mathbb{Q}}(\varepsilon)=(a^2-3pb^2)/4=1$ だから, $3pb^2=a^2-4=(a+2)(a-2)$ が得られる.
$(a+2,a-2)=1$ より $\{a+2,a-2\}=\{\square,3p\square\}$ または $\{p\square,3\square\}$ である. $\{a+2,a-2\}=\{\square,3p\square\}=\{x^2,3py^2\}$ とすると, $(a+b\sqrt{3p})/2=\{(x+y\sqrt{3p})/2\}^2$ が得られるが, これは仮定に反する. よって $\{a+2,a-2\}=\{p\square,3p\square\}$ である.
$a+2=p\square, a-2=3\square$ ならば $p\square-4=3\square$ で $p\equiv 1 \pmod 3$, $a+2=3\square, a-2=p\square$ ならば同様に $p\equiv 2 \pmod 3$ である.
$w=a+b\sqrt{3p}$ の時も同様である. ∎

補題 8. $K=\mathbb{Q}(\sqrt{m})$ を実二次体 (m は square-free) とし, ε (>1) を K の基本単数とする.
(a) $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$ が奇数ならば $m\equiv 5 \pmod 8$ である.
(b) $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$ を奇数とする. この時「$\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon^n)$ が偶数である」 $\iff$ $3\mid n$.

証明. (a) $\varepsilon=(a+b\sqrt{m})/2$ ($a=\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)$ とし, $b\in\mathbb{N}$ は奇数) とすると, $a^2-mb^2=\pm 4$ である. $a^2\equiv b^2\equiv 1 \pmod 8$ より, $m\equiv mb^2=a^2\mp 4\equiv 5 \pmod 8$.
(b) $(\mathcal{O}_k/(2))^\times\cong\mathbb{Z}/3\mathbb{Z}$ より明らかである. ∎

次の定理が主定理である.

定理 9. X,v を (4) の解とする.
(a) $p\equiv 1 \pmod 3$ ならば,

- $\exists n\in\mathbb{Z}$ s.t. $v=-\varepsilon^{6n+2}$.
- $\varepsilon^{6n+1}=(a+b\sqrt{3p})/2$ ($a,b\in\mathbb{N}$), $c=N_{k/\mathbb{Q}}(X)$ とすると, $c^3=2-a=-3\square$ が成り立ち, c は奇数である.
- $3pb^2=c^6-4c^3=a^2-4$, $c^3-4=-p\square$ が成り立つ.
- $p\equiv 7 \pmod 8$ である.

(b) $p\equiv 2 \pmod 3$ ならば,

- $\exists n\in\mathbb{Z}$ s.t. $v=\varepsilon^{6n+2}$.
- $\varepsilon^{6n+1}=(a+b\sqrt{3p})/2$ ($a,b\in\mathbb{N}$), $c=N_{k/\mathbb{Q}}(X)$ とすると, $c^3=a+2=3\square$, $3pb^2=c^6-4c^3=a^2-4$, $c^3-4=p\square$ が成り立つ.
- $p\equiv 7 \pmod 8$ である.

証明. (a) $v=\varepsilon^{6n+2}$ と仮定する. $X^3=\varepsilon+\varepsilon^{6n+2}$ のノルムを考えて,

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

$a^2-3pb^2=4$ だから, $3pb^2=c^6-4c^3$ である. 補題 7 より, $c^3-4=a-2=3\square$ が成り立つが, $\{(x,y)\in\mathbb{Z}\times\mathbb{Z}\mid 3y^2=x^3-4\}=\emptyset$ なので不可能である. よって $v=-\varepsilon^{6n+2}$ であり, 補題 7 より, $c^3=2-a=-3\square$, $c^3-4=-2-a=-p\square$ である. c を偶数と仮定する. この時もちろん $a=2-c^3$ も偶数である. $c^3=-3\square$ より, $c=-3\square$. よって $-p\square=c^3-4\equiv -4 \pmod{64}$, $-p\square/4=c^3/4-1\equiv 3 \pmod 4$ となってしまい, $p\equiv 1 \pmod 4$ が得られるが, これは不可能である. ゆえに c は奇数である. $a=\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon^{6n+1})$ は奇数なので, 補題 8 より $p\equiv 7 \pmod 8$ である.

(b) (a) と同様の議論により, $v=\varepsilon^{6n+2}$, $a=c^3-2$, $c^3=3\square$, $c^3-4=p\square$, (a,b,c は主張にある通り) が得られる. c が奇数なら a も奇数なので, 補題 8 より $p\equiv 7 \pmod 8$ である. c を偶数とする. $c^3=3\square$ より, $c=3\square$ である. よって $p\square=c^3-4\equiv -4 \pmod{64}$ であり, $p\square/4=c^3/4-1\equiv 7 \pmod 8$, $p\equiv 7 \pmod 8$ が得られる. ∎

系 10. $p\equiv 3 \pmod 8$, $p\neq 3$ ならば, 方程式 (1) は解を持たない.

定理 9 より方程式 (4) の解き方がわかる. 例で見てみよう.

例. $p=23$ ($\equiv 2 \pmod 3$)
定理 9 より, $v=\varepsilon^{6n+2}$ ($n\in\mathbb{Z}$) であり, a,b,c, を定理にあるような整数とすると,

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

が成り立つことがわかる. KASH を用いると, $\{(x,y)\in\mathbb{Z}\times\mathbb{Z}\mid 23y^2=x^3-4\}=\{(3,\pm 1)\}$ であることがわかるので, $c=3, a=c^3-2=25, b^2=(25^2-4)/69=3^2$ である. よって $\varepsilon^{6n+1}=(25+3\sqrt{69})/2=\varepsilon$ であるので, $n=0$, $X^3=\varepsilon+\varepsilon^2=((9+\sqrt{69})/2)^3$. よって解は $(X,v)=((9+\sqrt{69})/2,\varepsilon^2)$ のみである.

コンピューターで計算すると, 以下のような結果が得られる. $p\equiv 7 \pmod 8$, $7\le p\le 500$ の範囲で,
(a) (4) が解を持つ $\iff$ $p=23,31,431,439$.
(b) 上述の p に対し, 解の個数は一つである. (前の表にあるもののみ.)
いずれも解が一つだけであることは興味深い. もう少し数値実験を進めてみようと思っている.

3. 至る所 good reduction を持つ楕円曲線への応用を挙げておく：

定理 11. p を $p \equiv 3 \pmod 8$, $p \neq 3, 11$ なる素数とし, $k := \mathbb{Q}(\sqrt{3p})$ とおく. $\varepsilon\ (>1)$ を k の基本単数とし, $\mathfrak{P}_\infty^{(1)}, \mathfrak{P}_\infty^{(2)}$ を $k(\sqrt[3]{\varepsilon})$ の実無限素点とする. 次の 2 条件が成り立てば, k 上至る所 good reduction を持つ楕円曲線は存在しない

(a) $3 \nmid h_k$,

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

(但し代数体 K と K の divisor $\mathfrak{m}$ に対し, $h_K(\mathfrak{m})$ を $\mathfrak{m}$ を法とする K の ray class number とする.)

証明. E を k 上至る所 good reduction を持つ楕円曲線とする. 類数が奇数であることと条件 (a) をあわせると, E は global minimal equation で定義される. 条件 (b) より, E から他の曲線への k 上定義された 3 次の isogeny が存在する ([2], [3]). すると前に見たとおり, $X^3 = u + 27v$ または $X^3 = u + v$ を満たす $X \in \mathcal{O}_k - \{0\}$, $u, v \in \mathcal{O}_k^\times$ が存在するが, それは定理 1, 系 10 より不可能である. よってそのような楕円曲線は存在しない. ∎

系 12. $m = 129, 177, 201$ または 249 ならば, $\mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線は存在しない.

証明. KASH を使うと, 定理 11 で現れた ray class number が次のように計算される：

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	$\mathbf{2 \cdot 3}$	

よって定理 11 より主張が従う. ∎

参考文献

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

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

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

[4] T. Kagawa, The Diophantine equation $X^3 = u + 27v$ over real quadratic fields, to appear in *Tokyo J. Math.*

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

[6] J. H. Silverman, *The Arithmetic of Elliptic Curves*, G. T. M. **106**, Springer, 1986.

〒 525-8577 滋賀県草津市野路東 1-1-1
立命館大学数理科学科
e-mail : kagawa@se.ritsumei.ac.jp