実二次体上の不定方程式 $X^3 = u + 27v$ について

加川 貴章 (立命館大学理工学部)

1 結果

k を実二次体とする. 以下 $\mathcal{O}_k$ で k の整数環, $\mathcal{O}_k^\times$ で k の単数群, $'$ で $k/\mathbb{Q}$ の共役を表すとする. 次節で見るように, k 上 everywhere good reduction (以降 e.g.r. と略す) を持つ楕円曲線の研究から不定方程式

$$X^3 = u + 27v, \quad X \in \mathcal{O}_k, \quad u, v \in \mathcal{O}_k^\times \tag{1}$$

が生ずる. ここでは (1) に関する次の結果を証明する.

定理 1. p を $p \neq 3$, $p \equiv 3 \pmod 4$ なる素数とし, $k = \mathbb{Q}(\sqrt{6})$ または $k = \mathbb{Q}(\sqrt{3p})$ とする. この時 (1) が解を持つのは $k = \mathbb{Q}(\sqrt{6})$ または $k = \mathbb{Q}(\sqrt{33})$ の時のみで, 解は, $k = \mathbb{Q}(\sqrt{6})$ の時は

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

$k = \mathbb{Q}(\sqrt{33})$ の時は

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

ここで w_1, w_2 はそれぞれ $\mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{33})$ の任意の単数である. ($5 + 2\sqrt{6}$, $23 + 4\sqrt{33}$ はそれぞれの体の基本単数であることを注意しておく.)

2 方程式 (1) の由来

(1) の出所を明らかにしておく. 詳細は [5] を参照されたい.

E_1, E_2 を実二次体 k 上定義された楕円曲線とし, E_1 から E_2 へ k 上定義された 3 次の isogeny が存在するとする. この時それぞれの j 不変量 $j(E_1)$, $j(E_2)$ は

$$j(E_1) = J(t_1), \quad j(E_2) = J(t_2), \quad t_1, t_2 \in k, \quad t_1 t_2 = 3^6 = 729$$

松江数論研究集会 (2001 年 1 月 29 日) で話した内容に若干補足したもの

という形をしている．ここに $J(X) = (X+27)(X+3)^3/X$．E_1, E_2 が k 上 e.g.r. を持つとする．この時 $j(E_1), j(E_2) \in \mathcal{O}_k$ である (cf. [10], Chapter VII, Proposition 5.5) から，$t_1, t_2 \in \mathcal{O}_k$ である．$c_4(E_1), c_6(E_1)$ を E_1 の定義方程式に付随する通常通りのものとし，$\Delta(E_1)$ を E_1 の判別式とすれば，

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

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

単項イデアル $(\Delta(E_1))$ があるイデアルの 12 乗であることと，二次体上 e.g.r. を持つ楕円曲線の j 不変量が 0 でも 1728 でもないこと ([9], Theorem 2 (a)) を用いると，(2) より単項イデアル (t_1) があるイデアルの 3 乗であることが，(3) より (t_1) があるイデアルの 2 乗であることが証明できる．よって

$$(t_1) = \begin{cases} (1),\ (3^6) & (3\text{が惰性している時}), \\ (1),\ (3^3),\ (3^6) & (3\text{が分岐している時}), \\ (1),\ \mathfrak{p}^6,\ \mathfrak{p}'^6,\ (3^6) & ((3) = \mathfrak{p}\mathfrak{p}',\ \mathfrak{p} \neq \mathfrak{p}'\text{ の時}). \end{cases}$$

従って $\Delta(E_1) \in \mathcal{O}_k^\times$ なら (Setzer [8], Theorem 1 の Corollary より，k の類数が 6 と素ならこのようなモデルは必ず存在する)，次のようにして (1) の解が得られる．

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

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

(方程式 (1) の解 (X,u,v) と t_1 の関係は，$(t_1) = (1)$ の時は $t_1 = u/v$，$(t_1) = (3^6)$ の時は $t_1 = 3^6 v/u$.)

k を定理 1 にあるような実二次体とする．この時 t_1，対応する j 不変量 $J(t_1)$ は下の表の通りである．(全て singular modulus なので，CM を持つ整環の判別式も挙げておいた.) ここに $\varepsilon_6 = 5+2\sqrt{6}$，$\varepsilon_{33} = 23+4\sqrt{33}$ はそれぞれ $\mathbb{Q}(\sqrt{6}\,)$，$\mathbb{Q}(\sqrt{33}\,)$ の基本単数である．(以降 ε_m で実二次体 $\mathbb{Q}(\sqrt{m}\,)$ の基本単数で 1 より大きいものを表すとする.)

t_1	$J(t_1)$	整環の判別式
ε_6	8000	-8
ε_6'	8000	-8
$3^6\varepsilon_6$	$64(4\varepsilon_6^4+1)^3/\varepsilon_6^4$	-72
$3^6\varepsilon_6'$	$64(4\varepsilon_6'^4+1)^3/\varepsilon_6'^4$	-72
$-\varepsilon_{33}$	-32768	-11
$-\varepsilon_{33}'$	-32768	-11
$-3^6\varepsilon_{33}$	$-(5+\sqrt{33}\,)^3(243\varepsilon_{33}-1)^3/\varepsilon_{33}$	-99
$-3^6\varepsilon_{33}'$	$-(5-\sqrt{33}\,)^3(243\varepsilon_{33}'-1)^3/\varepsilon_{33}'$	-99

これらを j 不変量とする楕円曲線で e.g.r. を持つものは実際に存在する. (例えば [1], [5] を見よ.)

なお, $(t_1) = (3^3)$ の時は不定方程式 $X^3 = u + v$, $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$ と, $(t_1) = \mathfrak{p}^3$ または $(t_1) = \mathfrak{p}'^3$ で, $\mathfrak{p} = (\pi)$ の時は $X^3 = \pi^3 u + \pi'^3 v$, $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$ と関連する. 前者については若干の結果が得られているが, もう少し整理してから発表する. 後者には k に依存する数 π が現れ, 統一的な扱いは難しいと思われる.

3 定理1の証明

補題 1. (ア) $27Y^2 = X^3 - 676$ を満たす $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$ は存在しない.

(イ) $27Y^2 = X^3 + 784$ を満たす $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$ は存在しない.

(ウ) $27Y^2 = X^3 + 676$ を満たす $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$ は $(X, Y) = (-1, \pm 5), (26, \pm 26)$ のみである.

(エ) $27Y^2 = X^3 - 784$ を満たす $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$ は $(X, Y) = (19, \pm 15), (28, \pm 28)$ のみである.

証明. A を $\pm 676, \pm 784$ のどれかとする. (X, Y) が $27Y^2 = X^3 + A$ の (有理) 整数点ならば, $(3X, 27Y)$ は楕円曲線

$$C_A : y^2 = x^3 + 27A$$

の整数点である. このような楕円曲線の整数点は free のソフトウェア KASH で求めることができる. C_{-676}, C_{784} は整数点を持たない. C_{676} の整数点は

$$(-26, \pm 26), (-3, \pm 135), (13, \pm 143), (22, \pm 170), (78, \pm 702), (1573, \pm 62387)$$

のみであり, x 座標が 3 で, y 座標が 27 で割れるのは $(-3, \pm 135) = (3 \cdot (-1) \ \pm 27 \cdot 5)$, $(78, \pm 702) = (3 \cdot 26\,,\ \pm 27 \cdot 26)$ のみである. C_{-784} の整数点は

$$(28, \pm 28), (57, \pm 405), (84, \pm 756), (1708, \pm 70588)$$

のみであり, x 座標が 3 で, y 座標が 27 で割れるのは $(57, \pm 405) = (3 \cdot 19 \ \pm 27 \cdot 15)$, $(84, \pm 756) = (3 \cdot 28\,,\ \pm 27 \cdot 27)$ のみである. ∎

補題 2. k を実二次体とする. (1) の解で uv または $-uv$ が k の平方数であるものが存在するのは $k = \mathbb{Q}(\sqrt{29}\,)$ の時のみで, この時解は

$$(X, u, v) = (\pm\varepsilon_{29}^{n-1}, \mp\varepsilon_{29}^{3n+1}, \pm\varepsilon_{29}^{3n-1}), (\pm\varepsilon_{29}^{n+1}, \mp\varepsilon_{29}^{3n-1}, \pm\varepsilon_{29}^{3n+1}).$$

ここで n は任意の有理整数.

証明. (X, u, v) が (1) の解ならば, $(uX, u^4, u^3 v)$ も (1) の解である. よって $N_{k/\mathbb{Q}}(u) = N_{k/\mathbb{Q}}(v) = 1$ と仮定してよい. この時 (1) のノルムを考えて,

$$N_{k/\mathbb{Q}}(X)^3 = 730 + 27\,\mathrm{Tr}_{k/\mathbb{Q}}(uv') = 730 + 27\,\mathrm{Tr}_{k/\mathbb{Q}}(uv^{-1}). \tag{4}$$

仮定より $uv^{-1}=\pm w^2$ なる $w\in\mathcal{O}_k^\times$ が存在するので, (4) より

$$N_{k/\mathbb{Q}}(X)^3=730\pm 27\,\mathrm{Tr}_{k/\mathbb{Q}}(w^2)=730\pm 27\big\{\mathrm{Tr}_{k/\mathbb{Q}}(w)^2-2N_{k/\mathbb{Q}}(w)\big\}.$$

(複号は $uv^{-1}=\pm w^2$ と同順である.)

$uv^{-1}=w^2$ の時,

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

補題 1 より $N_{k/\mathbb{Q}}(w)=-1$ で, $\mathrm{Tr}_{k/\mathbb{Q}}(w)=\pm15,\pm28$, 即ち $w=\pm(15\pm\sqrt{229}\,)/2$, $\pm(14\pm\sqrt{197}\,)$ である. $w=\pm(15\pm\sqrt{229}\,)/2$ とすると, $(u+27v)=(w^2+27)=\mathfrak{p}^3$. ($\mathfrak{p}$ は $\mathbb{Q}(\sqrt{229}\,)$ の素イデアルで 19 の上にあるもの.) $\mathfrak{p}$ は単項イデアルではないから, $u+27v$ は $\mathbb{Q}(\sqrt{229}\,)$ の 3 乗数ではない. ($\mathbb{Q}(\sqrt{229}\,)$ の類数が 3 であることに注意.) $w=\pm(14\pm\sqrt{197}\,)$ の時は, $(u+27v)=(w^2+27)=(2)^3\mathfrak{p}_7^2\mathfrak{p}_7'$ ($(7)=\mathfrak{p}_7\mathfrak{p}_7'$, $\mathfrak{p}_7\neq\mathfrak{p}_7'$) と分解するから, $u+27v$ は $\mathbb{Q}(\sqrt{197}\,)$ の 3 乗数ではない.

$uv^{-1}=-w^2$ の時

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

よって補題 1 より, $N_{k/\mathbb{Q}}(w)=-1$ で $\mathrm{Tr}_{k/\mathbb{Q}}(w)=\pm5,\pm26$, 即ち $w=\pm(13\pm\sqrt{170}\,)$, $\pm(5\pm\sqrt{29}\,)/2$ である. $w=\pm(13\pm\sqrt{170}\,)$ の時, $(u+27v)=\mathfrak{p}_2^3\mathfrak{p}_{13}^2\mathfrak{p}_{13}'$ ($(2)=\mathfrak{p}_2^3$, $(13)=\mathfrak{p}_{13}\mathfrak{p}_{13}'$, $\mathfrak{p}_{13}\neq\mathfrak{p}_{13}'$) と分解するから, $u+27v$ は $\mathbb{Q}(\sqrt{170}\,)$ の 3 乗数ではない. $w=\pm(5\pm\sqrt{29}\,)/2$ の時は, $u+27v=v\varepsilon_{29}^{\pm2}$ となる. よって $v=\pm\varepsilon_{29}^{3n-1}$, $X=\pm\varepsilon_{29}^{n-1}$, または $v=\pm\varepsilon_{29}^{3n+1}$, $X=\pm\varepsilon_{29}^{n+1}$ となる $n\in\mathbb{Z}$ が存在する. ∎

注意. [7] において, $X^3=\varepsilon_{29}^{4+12m}-27\varepsilon_{29}^2$ を満たす $m\in\mathbb{Z}$, $X\in\mathcal{O}_{\mathbb{Q}(\sqrt{29})}$ は $m=0$, $X=-1$ のみであることが証明されている. 補題 2 はこの結果の一般化になっている.

次の補題もやはり KASH を使って確認した.

補題 3. (ア) $Y^2=X^3+676$ を満たす $(X,Y)\in\mathbb{Z}\times\mathbb{Z}$ は $(X,Y)=(0,\pm26)$ のみである.

(イ) $Y^2=X^3-784$ を満たす $(X,Y)\in\mathbb{Z}\times\mathbb{Z}$ は存在しない.

(ウ) $Y^2=X^3-676$ を満たす $(X,Y)\in\mathbb{Z}\times\mathbb{Z}$ は $(X,Y)=(10,\pm18)$, $(13,\pm39)$, $(26,\pm130)$, $(130,\pm1482)$, $(338,\pm6214)$, $(901,\pm27045)$ のみである.

(エ) $Y^2=X^3+784$ を満たす $(X,Y)\in\mathbb{Z}\times\mathbb{Z}$ は $(X,Y)=(-7,\pm21)$, $(0,\pm28)$, $(8,\pm36)$, $(56,\pm420)$ のみである.

補題 4. k を定理 1 の通りとし, ε (>1) を k の基本単数とする. この時 $\sqrt{3\varepsilon}\in k$.

証明. k で 3 が分岐していて, k の類数は奇数である (例えば [2] を見よ) から, $\pi^2 = 3w$ なる $\pi \in \mathcal{O}_k$, $w \in \mathcal{O}_k^\times$ が存在する. $w = \pi^2/3 > 0$, $k \neq \mathbb{Q}(\sqrt{3}\,)$ であるから, $w = \varepsilon^{2n+1}$ となる $n \in \mathbb{Z}$ が存在し, $3\varepsilon = (\pi/\varepsilon^n)^2$. ∎

注意. k の類数が奇数であることは, [3] の Theorem 39 の Corollary 1 から従う, と言いたいところだが, この Corollary は間違っている.

定理 1 を証明する. $\varepsilon\ (>1)$ を k の基本単数とする. k で 3 が分岐しているので, k の全ての単数のノルムは 1 である.

(X, u, v) を (1) の解とする. (1) のノルムを考えるとやはり (4) が得られる. uv^{-1}, $-uv^{-1}$ の一方が k の平方数の時は解が無い (補題 2) から, $uv^{-1} = \pm\varepsilon w^2$ となる $w \in \mathcal{O}_k^\times$ が存在する. 補題 4 より $\sqrt{3\varepsilon} \in k$ であるから,

$$27\,\mathrm{Tr}_{k/\mathbb{Q}}(uv^{-1}) = \pm 9\,\mathrm{Tr}_{k/\mathbb{Q}}((\sqrt{3\varepsilon}\,w)^2) = \pm 9\big\{\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)^2 - 2N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,)\big\}. \qquad (5)$$

$N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,) = -3$ の時, (4), (5) より

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

よって補題 3 よりこの場合は解無しである.

$N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,) = 3$ の時,

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

よって $uv^{-1} = \varepsilon w^2$ ならば補題 3 より $\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w) = \pm 6, \pm 9015$. ($N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w) = 3$ であり, $\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)^2 - 4N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)$ は平方数の $3p$ 倍だから, $\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)$ は 3 の倍数でなくてはならない.) $N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w) = N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,) = 3$ であるから,

$$\sqrt{3\varepsilon}\,w = \begin{cases} 3 \pm \sqrt{6} & (\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w) = 6 \text{ の時}), \\ -3 \pm \sqrt{6} & (\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w) = -6 \text{ の時}), \\ (\pm 9015 \pm \sqrt{3 \cdot 503 \cdot 53857})/2 & (\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w) = \pm 9015 \text{ の時}). \end{cases}$$

よって $k = \mathbb{Q}(\sqrt{6}\,)$, $\varepsilon = \varepsilon_6 = 5 + 2\sqrt{6}$ である. $\sqrt{3\varepsilon} = 3 + \sqrt{6}$, $\sqrt{3\varepsilon}\,\varepsilon' = 3 - \sqrt{6}$ であるから,

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

である. ($\sqrt{3\varepsilon}$ の求め方は証明後の注意参照.) $uv^{-1} = \varepsilon$ の時は $u + 27v = v(\varepsilon + 27) = v\varepsilon(4 - \sqrt{6})^3$ なので, $v = w_1^3\varepsilon'$, $u = w_1^3$, $X = w_1(4 - \sqrt{6}\,)$ となる $w_1 \in \mathcal{O}_k^\times$ が存在する. $uv^{-1} = \varepsilon'$ の時は $u + 27v = v(\varepsilon' + 27) = v\varepsilon'(4 + \sqrt{6}\,)^3$ なので $v = w_1^3\varepsilon$, $u = w_1^3$, $X = w_1(4 + \sqrt{6}\,)$ となる $w_1 \in \mathcal{O}_k^\times$ が存在する.

$uv^{-1}=-\varepsilon w^2$ の時は, 補題 3 より $\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)=\pm 12$ であり,

$$\sqrt{3\varepsilon}\,w=\begin{cases}6\pm\sqrt{33} & (\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)=12\text{ の時}),\\ -6\pm\sqrt{33} & (\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)=-12\text{ の時}),\end{cases}$$

よって $k=\mathbb{Q}(\sqrt{33}\,)$, $\varepsilon=\varepsilon_{33}=23+4\sqrt{33}$ である. $\sqrt{3\varepsilon}=6+\sqrt{33}$, $\sqrt{3\varepsilon}\,\varepsilon'=6-\sqrt{33}$ であるから,

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

である. $uv^{-1}=-\varepsilon$ の時は $u+27v=v\varepsilon(5-\sqrt{33}\,)^3$ であるから, $u=-w_2^3$, $v=w_2^3\varepsilon'$, $X=w_2(5-\sqrt{33}\,)$ となる $w_2\in\mathcal{O}_k^\times$ がある. $uv^{-1}=-\varepsilon'$ の時は $u+27v=v\varepsilon'(5+\sqrt{33}\,)^3$ なので, $u=-w_2^3$, $v=w_2^3\varepsilon$, $X=w_2(5+\sqrt{33}\,)$ となる $w_2\in\mathcal{O}_k^\times$ がある.

これで定理 1 の証明が終わった.

注意. (ア) 実二次体 k の基本単数 ε (>1) のノルムが 1 の時,

$$\frac{\sqrt{\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon)+2}\ +\sqrt{\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon)-2}}{2}$$

は ε の平方根である. これを使えば $\sqrt{3\varepsilon}$ を求めることは容易である. 例えば $k=\mathbb{Q}(\sqrt{6}\,)$ なら $\varepsilon=\varepsilon_6=5+2\sqrt{6}$ なので, $\sqrt{\varepsilon}=\sqrt{3}+\sqrt{2}$, $\sqrt{3\varepsilon}=3+\sqrt{6}$, $k=\mathbb{Q}(\sqrt{93}\,)$ なら $\varepsilon=\varepsilon_{93}=(29+3\sqrt{93}\,)/2$ なので, $\sqrt{\varepsilon}=(3\sqrt{3}+\sqrt{31}\,)/2$, $\sqrt{3\varepsilon}=(9+\sqrt{93}\,)/2$.

(イ) $N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,)=\pm 3$ であるが, $N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,)=3$, $N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,)=-3$ どちらの場合も起こる. 実際 (ア) からわかるように, $N_{\mathbb{Q}(\sqrt{6})/\mathbb{Q}}(\sqrt{3\varepsilon_6}\,)=3$, $N_{\mathbb{Q}(\sqrt{93})/\mathbb{Q}}(\sqrt{3\varepsilon_{93}}\,)=-3$.

(ウ) $k=\mathbb{Q}(\sqrt{3\cdot 503\cdot 53857}\,)$ の時は (1) は解を持たない. 実際 k の基本単数 ε は $\varepsilon=(27090073+3005\sqrt{3\cdot 503\cdot 53857}\,)/2$ なので, 上の式から $\sqrt{3\varepsilon}=(9015+\sqrt{3\cdot 503\cdot 53857}\,)/2$. 上と同様にして $u+27v=v(\varepsilon+27)$ または $u=v(\varepsilon'+27)$ が得られるが, 単項イデアル $(\varepsilon+27)$, $(\varepsilon'+27)$ は単項でないイデアルの 3 乗であることが確かめられる. (k のイデアル類群は $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/36\mathbb{Z}$ と同型である.)

4 e.g.r. を持つ楕円曲線への応用

定理 2. p を $p\equiv 3\pmod 4$, $p\neq 3,11$ なる素数とし, $k=\mathbb{Q}(\sqrt{3p}\,)$ とおく. ε 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. この時次の 3 条件が成り立てば, k 上 e.g.r. を持つ楕円曲線は存在しない.

(ア) k の類数 h_k は 3 と素である.

(イ) $k(\sqrt[3]{\varepsilon}\,)$ の $(3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)}$ を法とする ray class number $h_k((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)})$ か $k(\sqrt[3]{\varepsilon},\sqrt{-3}\,)$ の (3) を法とする ray class number $h_{k(\sqrt[3]{\varepsilon},\sqrt{-3}\,)}((3))$ は 4 で割れない.

(ウ) $X^3=u+v$ を満たす $X\in\mathcal{O}_k\backslash\{0\}$, $u,v\in\mathcal{O}_k^\times$ は存在しない.

証明. E を k 上 e.g.r. を持つ楕円曲線とする. 補題 4 の証明中で注意したように, h_k は奇数である. よって条件 (ア) は $(h_k, 6) = 1$ と同値であるので, [8], Theorem 1 の Corollary より E は global minimal equation で定義される. (イ) より E から他の曲線へ k 上定義された 3 次の isogeny がある ([5], Propositions 11, 12, [4], Lemma 2 の Corollary 1). 従って 2 節で説明した通り (1) または $X^3 = u + v$ を満たす $X \in \mathcal{O}_k \backslash \{0\}$, $u, v \in \mathcal{O}_k^\times$ が存在するが, これは条件 (ウ) と定理 1 より不可能である. (元々は (1) が解を持たないことも仮定の一部だったわけだが, それが定理 1 で除けたのである.) ∎

$p = 43, 47, 59, 67, 71, 83$ $(3p = 129, 141, 177, 201, 213, 249)$ の時は, 定理 2 の仮定 (ア), (イ) が満たされる. (下の表参照. Ray class number で 4 の倍数であるものは太字にしておいた. また必要ない所は計算しておらず, 空欄にしてある.)

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	1	$\mathbf{2^2 \cdot 3}$	$2 \cdot 3^3$
47	141	1	$2 \cdot 3^3$	
59	177	1	$2 \cdot 3$	
67	201	1	$\mathbf{2^2 \cdot 3}$	$2 \cdot 3^3$
71	213	1	$\mathbf{2^2 \cdot 3}$	$2 \cdot 3^2$
79	237	1	$\mathbf{2^3 \cdot 3}$	$\mathbf{2^3 \cdot 3^3 \cdot 5}$
83	249	1	$2 \cdot 3$	

(ウ) が満たされることも証明できる (略) ので, 次が得られたことになる.

定理 3. $m = 129, 141, 177, 201, 213, 249$ の時, $\mathbb{Q}(\sqrt{m})$ 上 e.g.r. を持つ楕円曲線は存在しない.

なお $\mathbb{Q}(\sqrt{33})$ 上 e.g.r. を持つ楕円曲線は決定済みで, $\mathbb{Q}(\sqrt{m})$ $(m = 57, 69, 93)$ 上 e.g.r. を持つ楕円曲線が存在しないことは証明されている. ([5] を見よ.)

5 Appendix

(1) に関する他の結果も紹介しておく.

定理 4 ([4]). k を二次体とする. (1) の解で u が 3 乗数であるものが存在するのは $k = \mathbb{Q}(\sqrt{6})$ または $k = \mathbb{Q}(\sqrt{33})$ の時のみで, 解は定理 1 にあるもののみである.

定理 5 ([6]). k を二次体とする. (1) の解で v が k の 3 乗数であるものは存在しない.

定理 6 ([6]). k を二次体とする. (1) の解で $X \in \mathcal{O}_k^\times$ であるものが存在するのは $k = \mathbb{Q}(\sqrt{29})$ または $k = \mathbb{Q}(\sqrt{733})$ の時のみであり, $k = \mathbb{Q}(\sqrt{29})$ の時は解は

$$(X, u, v) = (\pm\varepsilon_{29}^{n+1}, \mp\varepsilon_{29}^{3n-1}, \pm\varepsilon_{29}^{3n+1}), (\pm\varepsilon_{29}^{n-1}, \mp\varepsilon_{29}^{3n+1}, \pm\varepsilon_{29}^{3n-1}),$$

$k = \mathbb{Q}(\sqrt{733}\,)$ の時は解は

$$(X, u, v) = (\pm\varepsilon_{733}^{n}, \mp\varepsilon_{733}^{3n+2}, \mp\varepsilon_{733}^{3n+1}), (\pm\varepsilon_{733}^{-n}, \mp\varepsilon_{733}^{-3n-1}, \mp\varepsilon_{733}^{-3n-1}).$$

ここに n は任意の有理整数.

これから $\mathbb{Q}(\sqrt{733}\,)$ 上 e.g.r. を持つ楕円曲線の例が得られている. (cf. [6].)

参考文献

[1] S. Comalada, Elliptic curves with trivial conductor over quadratic fields, *Pacific J. Math.* **144** (1990), 237–258.

[2] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemp. Math. 24, 1983.

[3] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge studies in advanced mathematics 27, Cambridge University Press, Cambridge, 1991.

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

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

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

[7] T. Nakamura, On Shimura's elliptic curve over $\mathbb{Q}(\sqrt{29}\,)$, *J. Math. Soc. Japan* **36** (1984), 701–707.

[8] B. Setzer, Elliptic curves over complex quadratic fields, *Pacific J. Math.* **74** (1978), 235–250.

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

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

〒 525–8577　滋賀県草津市野路東 1–1–1
立命館大学理工学部数理科学科
E-mail: kagawa@se.ritsumei.ac.jp