$\mathbb{Q}(\sqrt{37})$ 上至る所 good reduction を持つ楕円曲線の決定

立命館大学理工学部　加川貴章　(Takaaki Kagawa)

1　背景, 動機付け

次の定理は有名である.

定理 1 (Tate. 証明は [13] を見よ). $\mathbb{Q}$ 上至る所 good reduction (everywhere good reduction, 以降 "e.g.r." と略す) を持つ楕円曲線は存在しない. □

では有理数体の次に簡単な虚二次体ではどうかというと, 次の結果が知られている：

定理 2 (Stroeker[21]). K を類数が 6 と素な虚二次体とすると, K 上 e.g.r. を持つ楕円曲線は存在しない. □

次に疑問を持つのは実二次体の場合であるが, この場合は Tate が例を見付けている：

$$y^2+xy+\frac{5+\sqrt{29}}{2}y^2=x^3$$

は $\mathbb{Q}(\sqrt{29})$ 上 e.g.r. を持つ. 実際判別式は $-\{(5+\sqrt{29})/2\}^{10}$ で, $(5+\sqrt{29})/2$ は $\mathbb{Q}(\sqrt{29})$ の基本単数である. この例の他に, 色々な実二次体上で例が多く見つかっている.

では, 実二次体 K が与えられた時に, K 上 e.g.r. を持つ楕円曲線がどれくらいあるかを決定する問題を考えるのは自然であろう. 非存在を示す結果としては [4], [11], [14] などがある. 位数 2 の K 有理点をもつという条件下での決定としては [3] がある. また j 不変量が有理整数になる場合に決定した結果がある：

定理 3 (M.Kida [10]). $\mathbb{Q}(\sqrt{37})$ 上 e.g.r. を持つ楕円曲線で j 不変量が有理整数のものは

$$\begin{aligned}
&C1: y^2-\varepsilon y=x^3+\frac{3\varepsilon+1}{2}x^2+\frac{11\varepsilon+1}{2}x,\ \Delta=\varepsilon^6,\ j=2^{12},\\
&C2: y^2-\varepsilon y=x^3+\frac{3\varepsilon+1}{2}x^2-\frac{1669\varepsilon+139}{2}x-7(5449\varepsilon+451),\\
&\qquad \Delta=\varepsilon^6,\ j=3376^3
\end{aligned}$$

のみである. ここで $\varepsilon=6+\sqrt{37}$ は $\mathbb{Q}(\sqrt{37})$ の基本単数である. □

この定理から制限「$j\in\mathbb{Z}$」を除くのが今回の目的である. 実際, 次の定理が得られる：

定理 4. $\mathbb{Q}(\sqrt{37})$ 上 e.g.r. を持つ楕円曲線は $C1, C2$ のみである.

一つ固定された実二次体に対し, その上で e.g.r. を持つ楕円曲線を決定した結果は, この時点では知られていなかった[1].

本稿の目的は, この定理の証明の outline を紹介することである. その過程で幾つかの不定方程式と出会い, それらを解くことによって定理 4 が証明されるわけである. 詳細は [5] を参照のこと[2].

[1] 出版時期の関係で, [11] で $\mathbb{Q}(\sqrt{41})$ 上e.g.r. を持つ楕円曲線を決定したのが publish されたもので初めてのものであるが, 論文を書いた時期は [6] の方が先である.

[2] [6] もあるが, これは "we omit the details" として面倒な所を省いているので, 興味を持たれた方は [5] を読んでください.

2 準備

代数体 K に対し, $\mathcal{O}_K$ で整数環を, $\mathcal{O}_K^\times$ で単数群を, h_K で類数を表すとする.

以降 $k := \mathbb{Q}(\sqrt{37})$ とし, $\varepsilon := 6+\sqrt{37}$ (k の基本単数), $\pi := (7+\sqrt{37})/2$ (3 を割る素元), $\omega := (1+\sqrt{37})/2$ とする. $\mathcal{O}_k = \mathbb{Z}[\omega]$ である.

E/k を楕円曲線とし, $c_4(E), c_6(E), \Delta(E)$ をいつもの通りとすると, 関係式 $c_6(E)^2 = c_4(E)^3 - 1728\Delta(E)$ が成り立つ. また $h_k = 1$ だから, E は global minimal equation で定義される ([17], Chapter VIII, Corollay 8.3.) すなわち $\Delta(E) = \pm\varepsilon^n \in \mathcal{O}_k^\times$ ($n \in \mathbb{Z}$) としてよい. よって楕円曲線

$$E_n^{\pm} : y^2 = x^3 \pm 1728\varepsilon^n \quad \text{(複号同順)}$$

の $\mathcal{O}_k$ 整数点の集合 $E_n^{\pm}(\mathcal{O}_k) = \{(x,y) \in \mathcal{O}_k \times \mathcal{O}_k \mid y^2 = x^3 \pm 1728\varepsilon^n\}$ (複号同順) を決定すればよい. 同型な楕円曲線を変換するごとに, パラメータの 12 乗のずれが生じるから, $-6 \le n < 6$ としてよい.

24 個もの楕円曲線の整数点を求めるのは大変なようだが, 実はかなり数を減らせる. 実際

$$\begin{array}{ccc} E_n^{\pm}(\mathcal{O}_k) & \to & E_{n+6}^{\pm}(\mathcal{O}_k) \quad \text{(複号同順)} \\ \cup & & \cup \\ (x,y) & \mapsto & (\varepsilon^2 x, \varepsilon^3 y) \end{array}$$

は全単射だから, $0 \le n < 6$ としてよい. (これで 12 個になった.)

また次のような規準がある：

補題 5. K を実二次体, η を K の基本単数とする. 以下の 5 条件が成り立つ時, K 上 e.g.r. を持つ楕円曲線の判別式は K の 3 乗数でなくてはならない :

(1) $(h_K, 6) = 1$;
(2) K において 3 は不分岐である;
(3) $3 \nmid h_{K(\sqrt{-3})}$;
(4) $2 \nmid h_{K(\sqrt[3]{\eta})}$;
(5) 3 を割る K の素イデアル $\mathfrak{p}$ に対し, 合同式 $X^3 \equiv \eta \pmod{\mathfrak{p}^3}$ は解 $X \in \mathcal{O}_K$ を持たない. □

証明. [5] の Proposition 2.12. (3 等分点の体を使う. 3 等分点の体には, $\sqrt[3]{\Delta(E)}$, $\sqrt{-3}$ が含まれていることに注意.) □

補題 5 の条件を確認する. $h_k = 1$, $3 \nmid 37$, $h_{k(\sqrt{-3})} = 4$, $h_{k(\sqrt[3]{\varepsilon})} = 1$ であるので, (1), (2), (3), (4) が満たされることがわかる. (5) が満たされることは次の補題からわかる.

補題 6. $\mathcal{O}_k \to \mathbb{Z}$, $x + y\omega \mapsto x$ ($x, y \in \mathbb{Z}$) は同型 $\mathcal{O}_k/(\pi^2) \cong \mathbb{Z}/9\mathbb{Z}$ を引き起こす. □

よって $n = 0, 3$ としてよい. (これで 4 個になった.) 更に $N_{k/\mathbb{Q}}(\varepsilon) = -1$ に注意すれば, 全単射

$$\begin{array}{ccc} E_3^{+}(\mathcal{O}_k) & \to & E_3^{-}(\mathcal{O}_k) \\ \cup & & \cup \\ (x,y) & \mapsto & (x'\varepsilon^2, y'\varepsilon^3) \end{array}$$

が存在することがわかる. ($'$ は $k/\mathbb{Q}$ の共役を表すとする.)

よって $E_0^{\pm}(\mathcal{O}_k)$, $E_3^{+}(\mathcal{O}_k)$ の 3 個の集合を決定すればよいことになったわけである.

命題 7. $E_0^{+}(k) = \langle(-12, 0)\rangle \cong \mathbb{Z}/2\mathbb{Z}$. 特に $E_0^{+}(\mathcal{O}_k) = \big\{(-12, 0)\big\}$.

命題 8. $E_3^{+}(\mathcal{O}_k) = \big\{(-12\varepsilon, 0), (17640 - 1740\sqrt{37}, \pm(2074464 - 438480\sqrt{37}))\big\}$.

命題 9. $E_0^-(\mathcal{O}_k)$ は以下の 15 個の元からなる：

$$(12,0),\ (16,\pm 8\sqrt{37}),\ (120,\pm 216\sqrt{37}),\ (3376,\pm 32248\sqrt{37}),$$
$$\big(44+4\sqrt{37},\pm(320+40\sqrt{37})\big),\ \big(44-4\sqrt{37},\pm(320-40\sqrt{37})\big),$$
$$\big(572+92\sqrt{37},\pm(19040+3128\sqrt{37})\big),\ \big(572-92\sqrt{37},\pm(19040-3128\sqrt{37})\big).$$

3　命題 7 の証明

よく知られているように, 二次体 $K=\mathbb{Q}(\sqrt{m})$ ($m\in\mathbb{Z}$ は square-free) と, $y^2=f(x)$ ($f(X)\in\mathbb{Q}[X]$ は重根を持たない 3 次式) で定義される楕円曲線 $E/\mathbb{Q}$ に対し,

$$\operatorname{rank} E(K)=\operatorname{rank} E(\mathbb{Q})+\operatorname{rank} E^{(m)}(\mathbb{Q})$$

が成り立つ[3]. 但し $E^{(m)}: my^2=f(x)$.

$E_0^+(\mathbb{Q})$ は 2-descent ([18] の 3 章で解説されている方法) で容易に求まる. 一方 $(E_0^+)^{(37)}(\mathbb{Q})$ は 2-descent では容易には求まらない. なぜなら, 階数を求める時に出てくる 4 次式で至る所 local に解けてしまうが, global な解が中々見つからないものがあるからである. よって Coates–Wiles [2] の定理を使うため, L 関数を使う. $L((E_0^+)^{(37)}/\mathbb{Q},1)=3.1941\cdots$ (Upecs Version 1.4 で計算した) だから, Coates–Wiles の定理より $\operatorname{rank}((E_0^+)^{(37)}(\mathbb{Q}))=0$ である[4]. これらより $\operatorname{rank} E_0^+(\mathbb{Q})+\operatorname{rank}(E_0^+)^{(37)}(\mathbb{Q})=0$ である.

ねじれ部分群は次のよく知られた補題を使って求める[5]：

補題 10. E を代数体 K 上定義された楕円曲線とする. $\mathfrak{p}$ を K の素イデアルとし, p を $\mathfrak{p}\cap\mathbb{Z}=(p)$ を満たす素数とする. $\mathfrak{p}$ が good prime で $K/\mathbb{Q}$ における分岐指数が $p-1$ より大きければ, reduction map $E(K)_{\mathrm{tors}}\longrightarrow E_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p})$ は単射準同型写像である. (ここで $E(K)_{\mathrm{tors}}$ は $E(K)$ のねじれ部分群, $E_{\mathfrak{p}}$ は E の reduction mod $\mathfrak{p}$ である.) □

$$\#(E_0^+)_{\mathfrak{p}}(\mathcal{O}_k/\mathfrak{p})=\begin{cases}2^2 & (\mathfrak{p}\mid 7\text{ の時}),\\ 2\cdot 3\cdot 7 & (\mathfrak{p}\mid 41\text{ の時})\end{cases}$$

だから, $\#E_0^+(k)_{\mathrm{tors}}\le 2$ であるので, $E_0^+(K)_{\mathrm{tors}}=\langle(-12,0)\rangle\cong\mathbb{Z}/2\mathbb{Z}$ である.

4　命題 8 の証明

通常, $y^2=x^3+A$ ($A\in\mathbb{Z}$) (Mordell 方程式と言う) の解 $x,y\in\mathbb{Z}$ を求めるには,

$$x^3=(y-\sqrt{A})(y+\sqrt{A})$$

分解として $\mathbb{Q}(\sqrt{A})$ で考え, いくつかの

$$3\text{ 次斉次式}=\text{定数}$$

[3]「よく知られているように」とは, 書いたが, 筆者の知る限り, 証明が載っている本, 論文は [16] だけである. 他の文献をご存知の方がいらしたら, 教えていただきたい

[4]結局解が中々見つからない 4 次式は, global な解を持たなかったわけである. 言い方を変えれば Tate–Shafarevich 群が nontrivial だったわけである. また当時は CM を持っているから [2] の結果が使えた, というわけであるが, 今では $\mathbb{Q}$ 上の楕円曲線は全て modular であるから, [2] にこだわる必要はない.

[5]これも「よく知られた」と書いたが, 何に出ているんだろうか？ 少なくとも [17] には出ていない.

の形の方程式に帰着させるのが普通である. ここでもそれに習って,

$$x^3 = (y - 24\sqrt{3\varepsilon})(y + 24\sqrt{3\varepsilon})$$

と分解し, $k(\sqrt{3\varepsilon})$ で考える.

まず一つ補題を準備する.

補題 11. u_1, u_2 で k の単数, a で k の整数を表すとする

(a) $64u_1 + u_2 = a^2$ は解を持たない.

(b) $8u_1 + u_2 = a^2$ の解は

$$(u_1, u_2, a) = (w^2, w^2, \pm 3w) \quad (\forall w \in \mathcal{O}_k^\times)$$

のみである.

(c) $16u_1 + 2u_2 = a^2$ は解を持たない.

(d) $u_1 + u_2 = a^2$ の解は

$$(u_1, u_2, a) = (w, -w, 0),\ (w^2\varepsilon^3, w^2\varepsilon'^3, \pm 42w),\ (w^2\varepsilon'^3, w^2\varepsilon^3, \pm 42w) \quad (\forall w \in \mathcal{O}_k^\times)$$

のみである.

証明. (a) (cf, [4]) (u_1, u_2, a) が解なら, どんな $u \in \mathcal{O}_K^\times$ に対し, (u^2u_1, u^2u_1, ua) も解だから, $u_2 = \pm 1, \pm\eta$ としてよい. この時, $\bmod 4$ で考えて, $u_2 = 1$ としてよい $\alpha := (a-1)/2$ とおくと, $\alpha(\alpha+1) = 2^4u_1$ ($\Longrightarrow \alpha \in \mathcal{O}_k$)

$\alpha \notin \mathcal{O}_k^\times$, $1 + \alpha \notin \mathcal{O}_K^\times$ とすると, 2 が k で分解してしまうので, $\alpha \in \mathcal{O}_k^\times$ または $\alpha + 1 \in \mathcal{O}_k^\times$ である. $\alpha + 1 \in \mathcal{O}_k^\times$ としてよい (a と $-a$ を必要なら交換する). よって $\alpha = 2^4u$, $\alpha + 1 = v$ となる $u, v \in \mathcal{O}_k^\times$ が存在する. $2^4u + 1 = \alpha + 1 = v$ なので, norm を取ると, $2^4 N_{k/\mathbb{Q}}(u) + \mathrm{Tr}_{k/\mathbb{Q}}(u) = 0$. これから $u = 8 \pm \sqrt{65}$ が得られるが, これは k の元ではない.

(b) (a) の証明を読むとわかるように, 大事なのは "64" ではなく, "4 | 64" である. 従って (a) の解法と同様にして (b) も解くことができる.

(c) 左辺は 2 で 1 回しか割れないので, 自明である. (2 は k で惰性することに注意.)

(d) $a \neq 0$ とする. この時 [3], Proposition 2 によると $u_1 + u_2 = a^2$ の解は, $u_1 = w^2u_0$, $u_2 = w^2u_0'$, $\mathrm{Tr}_{k/\mathbb{Q}}(u_0) = x^2 \in \mathbb{Z}$ ($u_0, w \in \mathcal{O}_k^\times$, $x \in \mathbb{Z}$) と表せるもののみである. [7] の Theorem 1 によれば, $\mathrm{Tr}(u_0) = x^2$ ($x \in \mathbb{Z}$) $\iff$ $u_0 = \varepsilon^3$ である. □

命題 8 の証明. $x^3 = y^2 - 1728\varepsilon^3$ を $L := k(\sqrt{3\varepsilon})$ で分解して,

$$x^3 = (y + 24\varepsilon\sqrt{3\varepsilon})(y - 24\varepsilon\sqrt{3\varepsilon})$$

を得る.

以下の L に関するデータを使う (KASH を使って得たものを都合のよいように修正した):

(a) $\mathcal{O}_L = \mathcal{O}_k \oplus \mathcal{O}_k\sqrt{3\varepsilon}$.

(b) L の基本単数系は ε, $\varepsilon_1 := \varepsilon + 2\sqrt{3\varepsilon}$. ($N_{L/k}(\varepsilon_1) = 1$ に注意.)

(c) $(2) = \mathfrak{P}_2^2$, $(\pi) = \mathfrak{P}_3^2$, $(\pi') = \mathfrak{P}_3'^2$.

(d) $h_L = 2$.

L/k の共役を $\bar{}$ で表すことにする. L の整イデアル $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ ($\mathfrak{A}, \mathfrak{B}$ は cube-free) を用いて

$$(y + 24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{A}\mathfrak{C}^3, \quad (y - 24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{B}\mathfrak{D}^3$$

とすると, $\mathfrak{A}\mathfrak{B}$ がある整イデアルの 3 乗であること, $\overline{\mathfrak{A}} = \mathfrak{B}$ であることがわかる. L の素イデアル $\mathfrak{P}$ が $\mathfrak{A}$ を割るとすれば, $\mathfrak{P}$ は $(y \pm 24\varepsilon\sqrt{3\varepsilon})$ を, 従って $48\varepsilon\sqrt{3\varepsilon}$ を割る. よって

$$\mathfrak{A} = \mathfrak{P}_2^{a_2}\mathfrak{P}_3^{a_3}\mathfrak{P}_3'^{a_3'},\ 0 \le a_2, a_3, a_3' < 3.$$

と書ける. $\overline{\mathfrak{A}} = \mathfrak{B}$ と (c) より, $\mathfrak{A} = \mathfrak{B}$ がわかる. さらに $\mathfrak{A}\mathfrak{B}$ が cube だから, $a_2 = a_3 = a_3' = 0$ を, 従って

$$(y + 24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{C}^3$$

を得る. (a) と (d) により, $\mathfrak{C} = (a + b\sqrt{3\varepsilon}),\ a, b \in \mathcal{O}_k$ と書けるので, ある $\eta \in \mathcal{O}_L^\times$ を用いて $y + 24\varepsilon\sqrt{3\varepsilon} = \eta(a + b\sqrt{3\varepsilon})^3$ と表せる. $\eta = \varepsilon^l\varepsilon_1^m\ (-1 \le l, m \le 1)$ としてよい. $N_{L/k}$ を取って (b) を考慮に入れれば,

$$x^3 = \varepsilon^{2l}\big\{(a + b\sqrt{3\varepsilon})(a - b\sqrt{3\varepsilon})\big\}^3.$$

となる. よって $l = 0$ で,

$$y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1^m(a + b\sqrt{3\varepsilon})^3,\ m = 0, \pm 1.$$

$m = -1$ の時は, 共役を考えれば

$$-y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1(-a + b\sqrt{3\varepsilon})^3$$

を得る. 故に,

$$\pm y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1^m(a + b\sqrt{3\varepsilon})^3,\ a, b, y \in \mathcal{O}_k,\ m = 0, 1$$

を解けばよい.

Case 1: $m = 1$. $\sqrt{3\varepsilon}$ の係数を比べて

$$2a^3 + 3\varepsilon a^2 b + 18\varepsilon ab^2 + 3\varepsilon^2 b^3 = 24\varepsilon$$

を得る. $3 \mid a$ がすぐわかるので, $A = a/3\ (\in \mathcal{O}_k)$ とおくと $\varepsilon b^3 \equiv -1 \pmod{\pi^2}$ 得られるが, これは補題 6 により不可能である.

Case 2: $m = 0$. 係数を比較して

$$8\varepsilon = b(a^2 + \varepsilon b^2), \quad \pm y = a(a^2 + 9\varepsilon b^2) \tag{1}$$

を得る. (1) の一つ目の式より, $b = u, 2u, 4u$ または $8u$ となる k の正の単数 u がある. (2 は k で惰性することに注意.) $b = 8u$ なら $a^2 = \varepsilon u^{-1} - 64\varepsilon u^2$ で, これは補題 11, (a) により不可能. $b = u$ なら $a^2 = 8\varepsilon u^{-1} - \varepsilon u^2$ で, 補題 11, (b) より $u^3 = -1$ が得られるが, $u > 0$ に反する. $b = 4u$ なら, $a^2 = -16\varepsilon u^2 + 2\varepsilon u^{-1}$ で, これは補題 11, (c) より不可能. $b = 2u$ の時は,

$$\left(\frac{a}{2}\right)^2 = \varepsilon u^{-1} - \varepsilon u^2. \tag{2}$$

補題 11, (d) より, (2)が成り立つのは $u = 1, \varepsilon^{-2}$ の時だけである. これより $(a, b) = (0, 2), (\pm 84, 2\varepsilon^{-2})$. (1) の 2 つ目の式より, $\pm y = 0,\ 2074464 - 438480\sqrt{37}$ が得られる. □

5　命題 9 の証明

先程と同様に, $L := k(\sqrt{-3})$ で

$$x^3 = (y + 24\sqrt{-3})(y - 24\sqrt{-3})$$

と分解する.

以下の L に関するデータを使う (やはり KASH で得たものを修正した):

(a) $\mathcal{O}_L = \mathcal{O}_k \oplus \mathcal{O}_k\zeta \quad (\zeta := (1+\sqrt{-3})/2.)$

(b) $\mathcal{O}_L^\times = \langle\varepsilon\rangle \times \langle\zeta\rangle \cong \mathbb{Z} \times (\mathbb{Z}/6\mathbb{Z})$.

(c) $(2) = \mathfrak{P}_2\overline{\mathfrak{P}}_2$ $(\mathfrak{P}_2 \neq \overline{\mathfrak{P}}_2)$, $(\pi) = \mathfrak{P}_3^2$, $(\pi') = \mathfrak{P}_3'^2$

(d) $Cl_L = \langle cl(\mathfrak{P}_2)\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

(e) $\mathfrak{P}_2^4 = (1 + \omega - 3\zeta)$.

これらのデータを使って命題 8 の場合と同様の議論をやると,

$$(\pm y + 24\sqrt{-3}) = \mathfrak{P}_2^{a_2}\overline{\mathfrak{P}}_2^{\overline{a}_2}\mathfrak{C}^3,$$

$(a_2, \overline{a}_2) = (0,0), (2,1)$, $\mathfrak{C}$ は L の整イデアル, となる.

Case 1 : $(a_2, \overline{a}_2) = (0,0)$.

$(\pm y + 24\sqrt{-3}) = \mathfrak{C}^3$ で, (d) より $(h_L, 3) = 1$ なので, $\mathfrak{C}$ は単項イデアルである. よって, $\pm y + 24\sqrt{-3} = \varepsilon^m\zeta^n(a + b\zeta)^3$, $a, b \in \mathcal{O}_k$, $m = 0, \pm 1$, $n = 0, \pm 1$. $N_{L/k}$ を考えると $m = 0$ が得られる. 共役を考えて $n = 0, 1$ としてよい.

$n = 0$ の時, 係数を比較して

$$\pm y = \frac{1}{2}(a-b)(2a+b)(a+2b), \tag{3}$$

$$16 = ab(a+b). \tag{4}$$

(4) より, $(a+b, ab)$ は, ある $u \in \mathcal{O}_k^\times$ を用いて, $(a+b, ab) = (u, 16u^{-1})$, $(2u, 8u^{-1})$, $(4u, 4u^{-1})$, $(8u, 2u^{-1})$, $(16u, u^{-1})$ と表せる.

$(a+b, ab) = (4u, 4u^{-1})$ なら, a, b は 2 次式

$$X^2 - 4uX + 4u^{-1}$$

の根である. よってこの 2 次式の判別式 $16(u^2 - u^{-1}) = \square_k$ $(= k$ の平方元) となるので, 補題 11, (d) より, $(u^2, -u^{-1}) = (w, -w), (w^2\varepsilon^3, w^2\varepsilon'^3)$. $(w \in \mathcal{O}_k^\times.)$ $(u^2, -u^{-1}) = (w, -w)$ から $u = 1$, $a = b = 2$, $y = 0$ が得られる.

$(u^2, -u^{-1}) = (w^2\varepsilon^3, w^2\varepsilon'^3)$ なら $w^2 = \varepsilon$ となり, これは矛盾である.

$(a+b, ab) = (2u, 8u^{-1})$ なら, a, b は 2 次式

$$X^2 - 2uX + 8u^{-1}$$

の根である. よって判別式は $4(u^2 - 8u^{-1}) = \square_k$. 補題 11, (b) より $u = -1$, $(a, b) = (2, -4), (-4, 2)$, よって (3) により $y = 0$.

$(a, b) = (u, 16u^{-1})$, $(8u, 2u^{-1})$, $(16u, u^{-1})$ の時は a, b の満たす 2 次式の判別式はそれぞれ

$$u^2 + 64u^{-1}, \quad 4(16u^2 - 2u^{-1}), \quad 4(64u^2 - u^{-1}).$$

これらは補題 11, (a), (c) によりいずれも $\square_k$ でない.

$n=1$ の時は

$$a^3+3a^2b-b^3=48.$$

$a\equiv b \pmod 3$ がわかる. $a=3A+b, A\in\mathcal{O}_k$ として mod π^2 とすれば矛盾が出る.

Case 2 : $(a_2,\overline{a}_2)=(2,1)$.

$4(\pm y+24\sqrt{-3})=\zeta^n(1+\omega-3\zeta)(a+b\zeta)^3$, $a,b\in\mathcal{O}_k$, $n=0,\pm1$ を得る. $n=1$, $n=-1$ の時はそれぞれ,

$$192=(-2+\omega)a^3+3(1+\omega)a^2b+9ab^2+(2-\omega)b^3,$$
$$-192=(1+\omega)a^3+9a^2b+3(1+\omega)ab^2-(2-\omega)b^3$$

を得るが, これが不可能であることは, Case 1, $n=1$ の時と同様にしてわかる.

$n=0$ の時は

$$-64=a^3-(\omega-2)a^2b-(\omega+1)ab^2-b^3, \tag{5}$$
$$\pm4y-96=(\omega+1)a^3+9a^2b-3(\omega-2)ab^2-(\omega+1)b^3. \tag{6}$$

$(a,b)\in\mathcal{O}_k\times\mathcal{O}_k$ を (5) の解とする. $A=-a-(\omega+2)b$ とおけば,

$$A^3+(4\omega+4)A^2b+(16\omega+48)Ab^2+(32\omega+80)b^3=64.$$

$4\mid A$, $2\mid b$ が容易にわかるので, $A=4X, b=2Y$ $(X,Y\in\mathcal{O}_k)$ とすれば,

$$X^3+2(\omega+1)X^2Y+4(\omega+3)XY^2+2(2\omega+5)Y^3=1. \tag{7}$$

命題 12. (7) を満たす $(X,Y)\in\mathcal{O}_k\times\mathcal{O}_k$ は

$(-2-9\omega,22-4\omega)$, $(-23-8\omega,-4+8\omega)$, $(25+17\omega,-18-4\omega)$, $(21+8\omega,-8-3\omega)$,
$(-9-3\omega,1+\omega)$, $(-12-5\omega,7+2\omega)$, $(9+2\omega,1-2\omega)$, $(-3-\omega,-2+\omega)$,
$(-6-\omega,1+\omega)$, $(-5-2\omega,1+\omega)$, $(1+\omega,-1)$, $(4+\omega,-\omega)$,
$(-2-\omega,2)$, $(1,0)$, $(1+\omega,-2)$, $(3+\omega,1-\omega)$, $(-\omega,1)$,
$(-3,-2+\omega)$, $(7-2\omega,11-3\omega)$, $(1+\omega,-9+2\omega)$, $(-8+\omega,-2+\omega)$.

の 21 個のみである. □

(6) に代入すれば, $E_0^-(\mathcal{O}_k)$ が決定できる. □

次のセクションで命題 12 の証明の概略を与える.

6 命題 12 の証明

de Weger [24] は 2 次体上の Thue 方程式

$$x^3+(9+2\sqrt{13})x^2y-(12+\sqrt{13})xy^2-\frac{11+3\sqrt{13}}{2}y^3=\left(\frac{3+\sqrt{13}}{2}\right)^n$$
$$(x,y\in\mathcal{O}_{\mathbb{Q}(\sqrt{13})},\quad n\in\mathbb{Z})$$

を解いている. この解法を参照にして (7) を解く.

命題 12 の証明. $F(X,Y)$ を (7) の左辺, θ を $F(X,1)$ の根の一つとし, $L=\mathbb{Q}(\theta)$ とおく. この時 $k\subset L$, $[L:\mathbb{Q}]=6$, $\mathcal{O}_L=\mathbb{Z}[\xi]$ が成り立つことがわかる. 但し $\xi=(12+18\theta-4\theta^3-\theta^4)/20$. 特に, $\theta=4\xi-5\xi^2-4\xi^3+4\xi^4+\xi^5$, $\sqrt{37}=3-12\xi-8\xi^2+8\xi^3+2\xi^4$ である. $L/\mathbb{Q}$ はガロア拡大で, $\mathrm{Gal}(L/\mathbb{Q})=\langle\sigma,\tau\rangle$. 但し σ, τ は

$$\begin{aligned}\sigma(\xi)&=-14-6\xi+49\xi^2+9\xi^3-28\xi^4-6\xi^5,\\ \tau(\xi)&=-1-3\xi+5\xi^2+4\xi^3-4\xi^4-\xi^5\end{aligned}$$

で与えられ, $\sigma^3=1,\tau^2=1$, $\sigma\tau=\tau\sigma^2$ が成り立つ. よって $\mathrm{Gal}(L/\mathbb{Q})\cong S_3$ である. ξ の L における共役を以下の様に番号を付けておく：

$$\begin{aligned}\xi^{(1)}&=\quad\xi&&=-4.6017164\ldots,\\ \xi^{(2)}&=\quad\sigma(\xi)&&=-0.5284180\ldots,\\ \xi^{(3)}&=\quad\sigma^2(\xi)&&=-0.4112467\ldots,\\ \xi^{(4)}&=\quad\tau(\xi)&&=-1.2776453\ldots,\\ \xi^{(5)}&=\quad\tau\sigma(\xi)&&=\quad0.6985045\ldots,\\ \xi^{(6)}&=\quad\tau\sigma^2(\xi)&&=\quad1.1205221\ldots.\end{aligned}$$

L の基本単数系を KASH で求めて, それを少し修正することで次の基本単数系を得る.

$$\begin{aligned}\varepsilon_1&=-\xi,\\ \varepsilon_2&=-5-4\xi+18\xi^2+5\xi^3-9\xi^4-2\xi^5,\\ \varepsilon_3&=-6-8\xi+23\xi^2+9\xi^3-13\xi^4-3\xi^5,\\ \varepsilon_4&=1+3\xi-5\xi^2-4\xi^3+4\xi^4+\xi^5,\\ \varepsilon_5&=-16-15\xi+63\xi^2+18\xi^3-36\xi^4-8\xi^5.\end{aligned}$$

σ, τ の $\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4,\varepsilon_5$ への作用は以下のようになる:

$$\sigma(\varepsilon_i)=\begin{cases}\varepsilon_3^{-1} & (i=1\text{ の時}),\\ \varepsilon_4^{-1} & (i=2\text{ の時}),\\ \varepsilon_1\varepsilon_3^{-1} & (i=3\text{ の時}),\\ \varepsilon_2\varepsilon_4^{-1} & (i=4\text{ の時}),\\ \varepsilon_1\varepsilon_2^{-1}\varepsilon_3^{-1}\varepsilon_4\varepsilon_5 & (i=5\text{ の時}),\end{cases}\quad \tau(\varepsilon_i)=\begin{cases}\varepsilon_4 & (i=1\text{ の時}),\\ \varepsilon_3 & (i=2\text{ の時}),\\ \varepsilon_2 & (i=3\text{ の時}),\\ \varepsilon_1 & (i=4\text{ の時}),\\ -\varepsilon_1^{-1}\varepsilon_2\varepsilon_3\varepsilon_4^{-1}\varepsilon_5^{-1} & (i=5\text{ の時}).\end{cases}$$

$N_{L/k}(\varepsilon_i)=1$ $(i=1,2,3,4)$, $N_{L/k}(\varepsilon_5)=\varepsilon_1\varepsilon_2^{-1}\varepsilon_3^{-2}\varepsilon_4^2\varepsilon_5^3=\varepsilon$ がわかる.

(7) は $N_{L/k}(X-Y\theta)=1$ と同値だから, $\eta:=X-Y\theta=\varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_4^{a_4}$ となる $a_1,a_2,a_3,a_4\in\mathbb{Z}$ が存在する. X,Y を消去することにより

$$\big(\sigma(\theta)-\sigma^2(\theta)\big)\eta+\big(\sigma^2(\theta)-\theta\big)\sigma(\eta)+\big(\theta-\sigma(\theta)\big)\sigma^2(\eta)=0$$

が得られ,

$$\frac{\theta-\sigma^2(\theta)}{\theta-\sigma(\theta)}\cdot\frac{\sigma(\eta)}{\sigma^2(\eta)}-1=-\frac{\sigma(\theta)-\sigma^2(\theta)}{\sigma(\theta)-\theta}\cdot\frac{\eta}{\sigma^2(\eta)}$$

が, 即ち

$$-\varepsilon_1^{b_1}\varepsilon_2^{b_2}\varepsilon_3^{b_3}\varepsilon_4^{b_4}-1=\varepsilon_1^{d_1}\varepsilon_2^{d_2}\varepsilon_3^{d_3}\varepsilon_4^{d_4}\tag{8}$$

が得られる. 但し

$$b_1 = a_1 + 2a_3, \quad b_2 = a_2 + 2a_4 - 1, \quad b_3 = -2a_1 - a_3 + 1, \quad b_4 = -2a_2 - a_4,$$
$$d_1 = -b_3, \quad d_2 = -b_4, \quad d_3 = b_1 + b_3, \quad d_4 = b_2 + b_4.$$

Thue 方程式の通常の解法 ([20], [22], [24] 参照) に習って, 対数一次形式

$$\Lambda_i = \sum_{j=1}^{4} b_j \log|\varepsilon_j^{(i)}| = \begin{cases} \log\left|\dfrac{\theta^{(i)} - \sigma^2(\theta^{(i)})}{\theta^{(i)} - \sigma(\theta^{(i)})} \cdot \dfrac{\sigma(\eta^{(i)})}{\sigma^2(\eta^{(i)})}\right| & (1 \le i \le 3), \\ \log\left|\dfrac{\theta^{(i)} - \sigma(\theta^{(i)})}{\theta^{(i)} - \sigma^2(\theta^{(i)})} \cdot \dfrac{\sigma^2(\eta^{(i)})}{\sigma(\eta^{(i)})}\right| & (4 \le i \le 6). \end{cases}$$

の評価をする.

$i_0 \in \{1, \dots, 6\}$ を $|\eta^{(i_0)}| = \min_{1 \le i \le 6} |\eta^{(i)}|$ で定める. ここで $L/\mathbb{Q}$ がガロア拡大であることなどが効いて, $i_0 = 1$ としてよいことがわかる. (cf. [23].)

やや初等的な, やや面倒な計算 ([5] で言うと, 36 ページの後半から 38 ページの最後の方) をすることにより,

$$B := \max\{b_1, b_2, b_3, b_4\} \ge 100 \quad \Longrightarrow \quad |\Lambda_1| < 4.1069 \exp(-0.24457B) \tag{9}$$

が得られる.

$|\Lambda_1|$ の lower bound を得るために, Baker–Wüstholz [1] の主結果を使う：

補題 13. $\alpha_1, \dots, \alpha_n$ を 0 でない代数的数とし, $b_1, \dots, b_n$ をどれかが 0 でない有理整数とする. また $d := [\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}]$, $h'(\alpha_i) := \max\{h(\alpha_i), |\log \alpha_i|/d, 1/d\}$ とする. (但し $h(\alpha_i)$ は α_i の absolute logarithmic height で, log は一つ枝を決めておく.) $\Lambda := b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n \ne 0$ で $B := \max\{|b_1|, \dots, |b_n|\}$ とする. この時

$$\log|\Lambda| > -18(n+1)!\, n^{n+1} (32d)^{n+2} \log(2nd) h'(\alpha_1) \dots h'(\alpha_n) \log B$$

が成り立つ. □

$\Lambda_1 \ne 0$ である. 実際 $\Lambda_1 = 0$ とすると, $b_1 = \cdots = b_4 = 0$ となり, これから $a_1 = 2/3$ となってしまい矛盾である. よって補題 13 を $\alpha_i = |\varepsilon_j^{(i)}|$ に適用出来る. 今の場合は, $\mathbb{Q}(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = L$ であるから, $d = [\mathbb{Q}(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) : \mathbb{Q}] = 6$ である. また $\varepsilon_4 = \varepsilon_1^{(4)}$, $\varepsilon_2 = 1/\varepsilon_1^{(5)}$, $\varepsilon_3 = 1/\varepsilon_1^{(2)}$ で, ε_1 は $x^6 - 5x^5 + 9x^3 - 2x^2 - 3x + 1$ の根であるから, $h(\varepsilon_i) = 0.314207\dots$ $(i = 1, 2, 3, 4)$ が得られる. $1/d = 0.166\dots$ で,

$$\frac{\left|\log|\varepsilon^{(i)}|\right|}{d} = \begin{cases} 0.22544\dots & (i = 1 \text{ の時}), \\ 0.05980\dots & (i = 2 \text{ の時}), \\ 0.10631\dots & (i = 3 \text{ の時}), \\ 0.04083\dots & (i = 4 \text{ の時}) \end{cases}$$

だから, $h'(\varepsilon_i) = 0.314207\cdots < 0.31421$ $(i = 1, 2, 3, 4)$. よって補題 13 より, lower bound

$$\log|\Lambda_1| > -4.1810 \times 10^{18} \log(B) \tag{10}$$

が得られる. (9), (10) により, $B \le 1.5142 \times 10^{21}$ が得られる.

この範囲で解を求めようと思って, 出来ないことはないだろうが, 時間がどれくらい掛かるかわからない. (恐らく筆者の生きているうちには結果は出ないであろう.) よって upper bound を下げなければならない. そのために LLL-reduced basis が必要となる：

定義 (LLL-reduced basis). $\Gamma = \mathbb{Z}\mathbf{b}_1 \oplus \cdots \oplus \mathbb{Z}\mathbf{b}_n$ $(\subset \mathbb{R}^n)$ を格子とする. $\mathbf{b}_i^*$ $(1 \le i \le n)$ と $\mu_{i,j}$ $(1 \le j < i \le n)$ を帰納的に以下の様に定義する ((,) は $\mathbb{R}^n$ の標準的な内積)：

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*, \quad \mu_{i,j} = \frac{(\mathbf{b}_i, \mathbf{b}_j*)}{(\mathbf{b}_j^*, \mathbf{b}_j^*)}.$$

(この時 $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ は $\mathbb{R}^n$ の直交基底になっている.)

$$|\mu_{i,j}| \le \frac{1}{2} \quad (1 \le j < i \le n), \quad |\mathbf{b}_i^* + \mu_{i,i-1}|^2 \ge \frac{3}{4} \quad (1 < i \le n)$$

が成り立っている時, $\mathbf{b}_1, \ldots, \mathbf{b}_n$ を Γ の LLL-reduced basis という.

補題 14. $\nu_1, \ldots, \nu_n$ を与えられた実数とする. $b_1, \ldots, b_n \in \mathbb{Z}$ とし, $\Lambda := \sum_{i=1}^{n} b_i\nu_i$ とおく. K_1, K_2, K_3 を与えられた正の整数とし, $b_1, \ldots, b_n$ を

$$|\Lambda| < K_1 \exp(-K_2 B), \quad B := \max\bigl\{|b_1|, \ldots, |b_n|\bigr\} < K_3. \tag{11}$$

の解とする. 十分大きな $c_0 \in \mathbb{R}$ に対し,

$$\mathcal{A} = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ [c_0\nu_1] & \ldots & [c_0\nu_{n-1}] & [c_0\nu_n] \end{bmatrix},$$

の各列を基底とする格子 Γ を考える. ここで

$$[x] = \begin{cases} \lfloor x \rfloor & \text{if } x \ge 0, \\ \lceil x \rceil & \text{if } x < 0, \end{cases}$$

即ち言い換えれば, $[\cdot]$ は 0 へ向かっての切り捨てである. (例えば $[-0.5] = 0$). $\mathbf{b}_1, \ldots, \mathbf{b}_n$ を Γ の LLL-reduced basis とする. $|\mathbf{b}_1| > \sqrt{(n^2+n-1)2^{n-1}}K_3$ が成り立つとすると, (11) の解は

$$B < \frac{\log(c_0K_1) - \log(\sqrt{2^{1-n}|\mathbf{b}_1|^2 - (n-1)K_3^2} - nK_3)}{K_2}$$

を満たす.

証明. [22], Proposition 3.1. □

PARI/GP や KASH などに, 与えられた格子の基底から, LLL-reduced basis を一組求めるアルゴリズムが実装されている. (ここでは仮に LLL-reduction と呼ぶことにする.)

我々の case では, $n = 4$, $\nu_i = \log|\varepsilon_i^{(1)}|$ $(i = 1, \ldots, 4)$, $K_1 = 4.1069$, $K_2 = 0.24457$, $K_3 = 1.5142 \times 10^{21}$ である. $c_0 = 10^{100}$ と取る. LLL-reduction を $\mathcal{A}$ に PARI/GP を用いて適用すると, 下記の LLL-reduced basis $\mathbf{b}_1$, $\mathbf{b}_2$, $\mathbf{b}_3$, $\mathbf{b}_4$ が得られる：

$$\mathbf{b}_1 = \begin{bmatrix} 525766899856084740716174 \\ 384638986832445610427342 7 \\ -124418666451172811371813 1 \\ -395108746616005504770747 \end{bmatrix}, \ \mathbf{b}_2 = \begin{bmatrix} -358052285081368813529910 4 \\ -341447815688279270973156 \\ 172781386077326034251467 5 \\ 324672105193753478335587 3 \end{bmatrix},$$

$$\mathbf{b}_3 = \begin{bmatrix} 407267427999956449527312 7 \\ 269244207052729576352184 4 \\ 782025387667325633997448 6 \\ -285101950383064823043109 4 \end{bmatrix}, \ \mathbf{b}_4 = \begin{bmatrix} -782540284530375014759499 4 \\ -154731239896422989358345 9 \\ -52919612021538767911783 7 \\ -106205987118553569141892 51 \end{bmatrix}.$$

$|\mathbf{b}_1| = 4.096\cdots\times 10^{24} > \sqrt{(n^2+n-1)2^{n-1}}K_3 = 1.866\times 10^{22}$, だから, 補題 14 により, より新しい B の upper bound K_3 として 719 が得られる.

更に $c_0 = 10^{18}$ として $\mathcal{A}$ に再び LLL-reduction を適用すると,

$$\mathbf{b}_1 = \begin{bmatrix} -291 \\ 2046 \\ 19892 \\ 285 \end{bmatrix}, \mathbf{b}_2 = \begin{bmatrix} -1300 \\ 2852 \\ 7913 \\ -18603 \end{bmatrix}, \mathbf{b}_3 = \begin{bmatrix} 23101 \\ 6305 \\ 5062 \\ -7284 \end{bmatrix}, \mathbf{b}_4 = \begin{bmatrix} 13586 \\ -24467 \\ -1315 \\ -5310 \end{bmatrix}$$

が得られる. $|\mathbf{b}_1| = 2.000\cdots\times 10^4 > \sqrt{(n^2+n-1)2^{n-1}}K_3 = 8.874\times 10^3$ だから, 補題 14 より, より小さな upper bound $B \leq 141$ が得られる.

後は $B \leq 141$ の範囲で (8) の解を探す[6]. (8) の解が 39 個見つかるが, その内の 21 個が $(a_1,a_2,a_3,a_4) \in \mathbb{Z}^4$ を満たす. 各 (a_1,a_2,a_3,a_4) に対し, KASH を使って単数 $\varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_4^{a_4}$ が $X - Y\theta$ $(X, Y \in k)$ の形をしているかどうか確認する. 解を表にしておく.

a_1	a_2	a_3	a_4	b_1	b_2	b_3	b_4	X	Y
-3	-4	-1	5	-5	5	8	3	$-2-9\omega$	$22-4\omega$
0	4	4	0	8	3	-3	-8	$-23-8\omega$	$-4+8\omega$
5	-1	-4	-3	-3	-8	-5	5	$25+17\omega$	$-18-4\omega$
4	-1	-4	1	-4	0	-3	1	$21+8\omega$	$-8-3\omega$
-3	0	0	1	-3	1	7	-1	$-9-3\omega$	$1+\omega$
1	0	3	0	7	-1	-4	0	$-12-5\omega$	$7+2\omega$
3	-3	-3	3	-3	2	-2	3	$9+2\omega$	$1-2\omega$
-2	2	0	1	-2	3	5	-5	$-3-\omega$	$-2+\omega$
1	0	2	-2	5	-5	-3	2	$-6-\omega$	$1+\omega$
2	0	-2	1	-2	1	-1	-1	$-5-2\omega$	$1+\omega$
-1	0	0	0	-1	-1	3	0	$1+\omega$	-1
1	-1	1	1	3	0	-2	1	$4+\omega$	$-\omega$
1	0	-1	1	-1	1	0	-1	$-2-\omega$	2
0	0	0	0	0	-1	1	0	1	0
1	-1	0	1	1	0	-1	1	$1+\omega$	-2
1	1	-1	1	-1	2	0	-3	$3+\omega$	$1-\omega$
0	0	0	-1	0	-3	1	1	$-\omega$	1
1	-2	0	2	1	1	-1	2	-3	$-2+\omega$
1	-4	-1	4	-1	3	0	4	$7-2\omega$	$11-3\omega$
0	3	0	1	0	4	1	-7	$1+\omega$	$-9+2\omega$
1	0	0	-3	1	-7	-1	3	$-8+\omega$	$-2+\omega$

7 Q.E.D.

これで $E_{-6}^{\pm}(\mathcal{O}_k), E_{-3}^{\pm}(\mathcal{O}_k), E_0^{\pm}(\mathcal{O}_k), E_3^{\pm}(\mathcal{O}_k)$ が決定され, c_4, c_6 の候補が出揃った. どれが Weierstrass 方程式の c_4, c_6 に成るか判定するために, 次の Kraus [12] の結果を使う:

[6] $B \leq 141$ といっても, そのまま検索するのは大変である. よって若干工夫をする. 詳細は [24], [5] を参照のこと.

補題 15. K を $\mathbb{Q}_2$ の有限次不分岐拡大, $\mathcal{O}_K$ を K の付値環とする. $C_4,\ C_6 \in \mathcal{O}_K$ が $(C_4^3 - C_6^2)/1728 \in \mathcal{O}_K - \{0\}$ を満たすとする. この時 Weierstrass 方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathcal{O}_K\ (i = 1, 2, 3, 4, 6)$$

で $c_4 = C_4$, $c_6 = C_6$ を満たすものが存在することと, 以下の (1) または (2) が成立することが同値である：

(1) $C_4 \in \mathcal{O}_K^\times$ で, $-C_6 \equiv x^2 \pmod 4$ を満たす $x \in \mathcal{O}_K$ が存在する；

(2) $C_4 \equiv 0 \pmod{16}$ で, $C_6 \equiv 8x^2 \pmod{32}$ を満たす $x \in \mathcal{O}_K$ が存在する. □

補題 15 の条件を満たすのは $(16\varepsilon^{-2}, -8\sqrt{37}\varepsilon^{-3}), (3376\varepsilon^{-2}, 32248\sqrt{37}\varepsilon^{-3}) \in E^-_{-6}(\mathcal{O}_k)$ だけで, 前者が $C1$ に, 後者が $C2$ に対応している.

8 最後に

$\mathbb{Q}(\sqrt{37})$ 以外の実二次体はどうかと言うと, その後色々非存在を証明したり, 決定をしたりしている. (もっぱら筆者と木田雅成氏による.) ただし, 本稿からわかるように, 体の特性によって証明方法は変えざるを得ない. 一々文献を挙げるとページ数が増えそうなので, [8] の文献表を御覧頂きたい.

結局今回は何をやったかというと, e.g.r を持つ楕円曲線の決定をすることを, 楕円曲線の整数点を求める問題に帰着させたわけである. 楕円曲線の整数点を求めるには, 今回のように Thue 方程式に帰着させる方法の他に, elliptic logarithm の評価を使う方法が知られている (cf. [19], [20]). [8] ではその方法で, いくつかの実二次体上 e.g.r. を持つ楕円曲線の決定をしている. 興味があれば御覧頂きたい.

なお, 実二次体上で導手が非自明な楕円曲線を決定した結果は少ない. $\mathbb{Q}(\sqrt{5})$ 上導手が 2 の冪の楕円曲線を決定した結果 [15] と, $\mathbb{Q}(\sqrt{2})$ 上導手が $\sqrt{2}$ の冪の楕円曲線を決定した結果 [9] ぐらいであろう. (ただし同型類の数は共に異様に多く, それぞれ 368, 400 である.)

また当日 modular 性に関する質問があったが, そのことを説明するには若干筆者は能力不足なので, ここでは省略する. 興味がある方は [14] を取り寄せて, 読んでいただきたい.

参考文献

[1] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine angew. Math.* **442** (1993), 19–62.

[2] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251.

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

[4] H. Ishii, The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields, *Japan. J. Math.* **12** (1986), 45–52.

[5] T. Kagawa, *Elliptic curves with everywhere good reduction over real quadratic fields*, dissertation, Waseda University, 1998 (`http://www.ritsumei.ac.jp/se/~kagawa/proj.html` より入手可能).

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

[7] T. Kagawa and N. Terai, Squares in Lucas sequences and some Diophantine equations, *Manuscripta Math.* **96** (1998), 195–202.

[8] 加川貴章「実二次体上の楕円曲線の整数点の計算，および自明な導手を持つ楕円曲線の決定」整数論シンポジウム，研究集会報告集 X －整数論－，早大理工総研 (1999)，32-41.（`http://www.ritsumei.ac.jp/se/~kagawa/papers.html` より入手可能.）

[9] T. Kagawa, Elliptic curves over $\mathbb{Q}(\sqrt{2})$ with good reduction outside $\sqrt{2}$, *Mem. Inst. Sci. Engrg. Ritsumeikan Univ.* **59**, (2000), 63–79 (2001).

[10] M. Kida, On a characterization of Shimura's elliptic curve over $\mathbb{Q}(\sqrt{37})$, *Acta Arith.* **77** (1996), 157–171.

[11] M. Kida and T. Kagawa, Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields, *J. Number Theory* **66** (1997), 201–210.

[12] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique, *Acta Arith.* **54** (1989), 75–80.

[13] A. P. Ogg, Abelian curves of 2-power conductor, *Proc. Camb. Phil. Soc.*, **62** (1966), 143–148.

[14] R. G. E. Pinch, *Elliptic curves over number fields*, Ph. D. thesis, Oxford, 1982.

[15] R. G. E. Pinch, Elliptic curves with good reduction away from 2: III, `http://arxiv.org/PS_cache/math/pdf/9803/9803012.pdf` より入手可能

[16] M. I. Rosen, Some confirming instances of the Birch–Swinnerton-Dyer conjecture over biquadratic fields, *Number Theory* (R. A. Mollin ed.) 493–499, de Gruyter.

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

[18] J. H. シルヴァーマン, J. テイト (足立恒雄, 小松啓一, 木田雅成, 田谷久雄訳)「楕円曲線論入門」シュプリンガー, 1995.

[19] N. P. Smart and N. M. Stephens, Integral points on elliptic curves over number fields, *Math. Proc. Camb. Phil. Soc.* **122** (1997), 9–16.

[20] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Text **41**, 1998.

[21] R. J. Stroeker, Reduction of elliptic curves over imaginary quadratic number fields, *Pacific J. Math.* **108** (1983), 451–463.

[22] N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equation, *J. Number Theory* **31** (1989), 99–132.

[23] B. M. M. de Weger, A hyperelliptic diophantine equation related to imaginary quadratic number fields with class number 2, *J. Reine angew. Math.* **427** (1992), 137–156; Correction, ibid. **441** (1993), 217–218.

[24] B. M. M. de Weger, A Thue equation with quadratic integers as variables, *Math. Comp.* **64** (1995), 855–861.

加川貴章
立命館大学理工学部
〒 525-8577 滋賀県草津市野路東 1-1-1
email: kagawa@se.ritsumei.ac.jp

Takaaki Kagawa
Ritsumeikan University
Faculty of Engineering and Science
Kusatsu, Shiga, 525-8577, JAPAN
http://www.ritsumei.ac.jp/se/~kagawa/