

Determination of elliptic curves with everywhere good reduction over certain real quadratic fields

早稲田大学理工学部 加川 貴章 (Takaaki Kagawa)

1 Introduction

代数体 k 上至る所 good reduction を持つ楕円曲線 (の k 上の同型類) を全て決定することは興味深い問題である。

$k = \mathbb{Q}$ の時にそのような楕円曲線が存在しないことはよく知られている。また k が虚二次体の場合は, Stroeker [St] により, k 上至る所 good reduction を持てば global minimal model を持たないこと, k の類数が 6 と素ならばその上には至る所 good reduction を持つ楕円曲線は存在しないことが示されている。従ってこの場合も本質的には解決している。

そこで次は k が実二次体である場合に興味を持つのが自然であるが, この場合に興味を持つもう一つの理由に, 以下のようにして得られる「Shimura の楕円曲線」がある。 $N (> 0)$ を基本判別式とし, χ_N を N に付随する Kronecker 記号とする。 Neben-character χ_N を持つ重さ 2 の newform の空間 $S_2^0(\Gamma_0(N), \chi_N)$ が二次元の \mathbb{Q} -単純な部分空間を持つ時, そこから \mathbb{Q} 上定義された二次元 abel 多様体 A が得られる ([Shim1])。 A は実二次体 $k = \mathbb{Q}(\sqrt{N})$ 上で $B \times B'$ (B は k 上定義された楕円曲線, B' はその共役) と分解する。 B を「Shimura の楕円曲線」と呼ぶ。 B は k 上至る所 good reduction を持つこと (cf. [KM]), 及び B は \mathbb{Q} -curve* であることが知られている ([Shim1])。 逆に, Pinch [Pi1] により, E が実二次体上至る所 good reduction を持つ \mathbb{Q} -curve である時, E は Shimura の楕円曲線と k 上 isogenous であろう, 特に E は modular であろうと予想されている (modular 性に関する話題は, 例えば [Ha], [HHM], 及びその引用文献を参照されたい)。

従って実二次体の場合が特に重要と考えられる。 実二次体上至る所 good reduction を持つ楕円曲線については,

- 例が色々知られている ([Co], [Is], [Set], [Shio] 等),
- 例を作る方法がある ([Um] 等),
- $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{13})$ 上には存在しない ([Is]),
- ある種の条件の下での, 至る所 good reduction を持つ楕円曲線の決定 ([Co],[Ki1] 等)

などといった結果はある。 しかし筆者の知る限り, 実二次体上至る所 good reduction を持つ楕円曲線を全て決定した結果は無いようである。 ここでは $\mathbb{Q}(\sqrt{N})$ ($N = 29, 37$) 上至る所 good reduction を持つ楕円曲線を不定方程式を用いて決定する。 実二次体上で不定方程式を解くのは, 単数群が無限群であることから一般には難しく, 解かれた方程式はあまり多くないことを注意しておく。

* \mathbb{Q} -curve とは, $\overline{\mathbb{Q}}$ 上定義された楕円曲線 E で, 全ての共役 E^σ ($\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) と $\overline{\mathbb{Q}}$ 上 isogenous なものである。 ここでは \mathbb{Q} -curve と言ったら, 共役との isogeny が定義体上定義されているとする。

2 結果

[Shim1]によれば, $N = 29, 37$ の時, $S_2(\Gamma_0(N), \chi_N)$ は二次元 \mathbb{Q} -単純であり, Shimura の abel 多様体 A は N から一意的に定まるので, A_N と書くことにする. η を $\frac{1}{\sqrt{N}} \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$ から引き起こされる $k = \mathbb{Q}(\sqrt{N})$ 上定義された A_N の自己同型とする時, Shimura の楕円曲線は $B_N = (1+\eta)A_N$ で定義される. ここでは便宜上 $C_1 := B_{29}, C_3 := B_{37}$ とおく. 定義方程式は [Shio] において求められており, それを用いて $C_1(\mathbb{Q}(\sqrt{29}))_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z}, C_3(\mathbb{Q}(\sqrt{37}))_{\text{tors}} \cong \mathbb{Z}/5\mathbb{Z}$ が示せる. 従ってこれらの群で割ることと共役を取ることににより, k 上至る所 good reduction を持つ楕円曲線が幾つか得られる (定義方程式は Appendix に載せてある):

$$\begin{aligned} N = 29 : C_1, C'_1, C_2 &:= C_1/C_1(\mathbb{Q}(\sqrt{29}))_{\text{tors}}, C'_2; \\ N = 37 : C_3, C_4 &:= C_3/C_3(\mathbb{Q}(\sqrt{37}))_{\text{tors}}. \end{aligned}$$

ここに ' \prime ' は $\mathbb{Q}(\sqrt{29})$ の共役である. C_3, C_4 の j -invariant はそれぞれ有理整数なので, [Shio], Lemma 1.5 によれば C_3, C_4 はそれぞれの共役と $\mathbb{Q}(\sqrt{37})$ 上同型であることに注意しておく.

証明したいのは次の定理である:

定理 $\mathbb{Q}(\sqrt{N})$ ($N = 29, 37$) 上至る所 good reduction を持つ楕円曲線は上述のもののみである.

C_1 と C'_1 の間には $\mathbb{Q}(\sqrt{29})$ 上定義された 5 次の isogeny があることが知られているので, 次の系が得られる ([Kil], [Na] も見よ):

系 $k = \mathbb{Q}(\sqrt{N})$ ($N = 29, 37$) 上至る所 good reduction を持つ楕円曲線は全て k 上 isogenous である. 特にこれらの体に対し Pinch の予想は正しい.

注 [Shim1]によれば $S_2^0(\Gamma_0(41), \chi_{41})$ も二次元 \mathbb{Q} -単純であり, $\mathbb{Q}(\sqrt{41})$ 上にも Shimura の楕円曲線 B_{41} が存在する. [Shio] では B_{41} の定義方程式も求められている. 最近筆者は木田雅成氏との共同研究 ([KK]) で, $\mathbb{Q}(\sqrt{41})$ 上至る所 good reduction を持つ楕円曲線を決定した. また我々は $\mathbb{Q}(\sqrt{N})$ ($N = 17, 21, 73, 97, 149, 173, 181$) 上にそのような楕円曲線が存在しないことも示した.

最近木田氏は [Ki2] において, $\mathbb{Q}(\sqrt{m})$ ($m = 2, 3, 47, 94$) 上に存在しないことを示し, $\mathbb{Q}(\sqrt{m})$ ($m = 6, 7, 14$) 上のものを全て尽くした.

以上は全て類数 1 の場合だが, 筆者は類数 2 の場合にも同様の結果を得た. より詳しく言うと, $m = 10, 15, 30, 34, 39, 42, 58, 66, 70, 74, 85$ の場合に非存在を示し, $\mathbb{Q}(\sqrt{65})$ 上のものを全て尽くした.

上記の非存在の場合, $S_2^0(\Gamma_0(N), \chi_N)$ (N は $\mathbb{Q}(\sqrt{m})$ の判別式) が二次元の \mathbb{Q} -単純な部分空間を持たないことも確かめられる ([Shim2], 及び長谷川雄之氏, 日比野剛士氏の計算による). また尽くされた case では, $N = 65$ 以外は $S_2^0(\Gamma_0(N), \chi_N)$ は二次元 \mathbb{Q} -単純部分空間を一つだけ持ち, $N = 65$ の時は丁度二つ持つ (これも長谷川氏, 日比野氏による). よって $\mathbb{Q}(\sqrt{N})$ 上至る所 good reduction を持つ \mathbb{Q} -curve の isogeny class の数は, それぞれの場合 1 または 2 と予想されるが, 実際そうであることを (\mathbb{Q} -curve という条件抜きに) 示すこともできた. 従って, 上記の体全てに対し Pinch の予想は正しいことになる.

3 準備

記号: 代数体 F に対し, $\mathcal{O}_F, \mathcal{O}_F^\times$ と書いたらそれぞれ F の整数環, 単数群を表す. F が二次体の時は, その共役を $'$ で表す.

$k = \mathbb{Q}(\sqrt{N})$ ($N = 29, 37$) とし, E を k 上至る所 good reduction を持つ楕円曲線とする. k の類数は 1 なので, E の model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathcal{O}_k$$

で判別式 Δ が単数であるものが存在する. ε を k の基本単数とし, $\Delta = \pm\varepsilon^n$ ($n \in \mathbb{Z}$) とする. 変数変換の公式を考えると, $-6 \leq n < 6$ としてよい. $c_4, c_6 \in \mathcal{O}_k$ を通常のように定義すると, $c_4^3 - c_6^2 = 1728\Delta$ が成り立つので, k 上至る所 good reduction を持つ楕円曲線を全て決めるには, まず Mordell 型の不定方程式

$$E_n^\pm : y^2 = x^3 \pm 1728\varepsilon^n, \quad -6 \leq n < 6$$

の解 $(x, y) \in \mathcal{O}_k \times \mathcal{O}_k$ を決め, 次に各 x, y が \mathcal{O}_k 係数の Weierstrass 方程式の c_4, c_6 に成れるかどうかを決めればよい.

$E_n^\pm(\mathcal{O}_k) = \{(x, y) \in \mathcal{O}_k^2 \mid y^2 = x^3 \pm 1728\varepsilon^n\}$ とおく. 写像

$$E_n^\pm(\mathcal{O}_k) \rightarrow E_{n+6}^\pm(\mathcal{O}_k), \quad (x, y) \mapsto (x\varepsilon^2, y\varepsilon^3) \quad (\text{複号同順})$$

は全単射で, 更に, $N_{k/\mathbb{Q}}(\varepsilon) = -1$ なので, 写像

$$E_n^\pm(\mathcal{O}_k) \rightarrow E_{6-n}^\pm(\mathcal{O}_k), \quad (x, y) \mapsto (x'\varepsilon^2, y'\varepsilon^3)$$

(複号は, n が偶数の時は同順, 奇数の時は逆順)

は全単射である. よって

$$E_n^+(\mathcal{O}_k) \quad (n = 0, 1, 2, 3, 5), \quad E_n^-(\mathcal{O}_k) \quad (n = 0, 2)$$

を決定すれば十分である. $N = 37$ の時は, §4 で示すように判別式は三乗数なので, 決定する集合を更に減らせ, 次の三つの集合を決めればよい:

$$E_0^\pm(\mathcal{O}_k), \quad E_3^+(\mathcal{O}_k).$$

本稿では紙数の関係で $\mathbb{Q}(\sqrt{37})$ の場合のみを扱う. 以下 $k = \mathbb{Q}(\sqrt{37})$, $\omega = (1 + \sqrt{37})/2$ とし, $\pi = (7 + \sqrt{37})/2$ を 3 の上にある k の素元とする. また $\varepsilon = 6 + \sqrt{37}$ を k の基本単数とする.

4 判別式は三乗数である ($N = 37$ の場合)

この節では次を証明する:

命題 1 $k = \mathbb{Q}(\sqrt{37})$ 上至る所 good reduction を持つ楕円曲線の判別式は三乗数でなくてはならない.

判別式が三乗数かどうかは model によらないことを注意しておく.

命題 1 を証明するために, 逆に, k 上至る所 good reduction を持ち, 判別式 Δ が三乗数でない楕円曲線 E_1 が存在するとせよ. $L = k(E_1[3])$, $K = k(\sqrt[3]{\Delta}) = \mathbb{Q}(\sqrt[3]{\varepsilon})$, $F = k(\sqrt{-3})$ とおく. $k \subset K \subset FK \subset L$ が成り立ち ([Ser], p. 305, 及び [Si], p. 98 を見よ), Néron–Ogg–Shafarevich の criterion ([Si], p. 184) より L/k は 3 と無限素点の外不分岐である.

補題 1 E_1 は π, π' において ordinary good reduction を持つ.

(証明) (以下の証明の本質的な部分は木田氏による) $\mathfrak{p} = (\pi)$ または $\mathfrak{p} = (\pi')$ とする. \mathfrak{p} は K, F で共に分岐する: $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}_F^2$. E が \mathfrak{p} において supersingular reduction を持つとする. この時 \mathfrak{p} の分解群の位数は 2 の冪である ([Ser], §1.11, §2.2). よって \mathfrak{p} の K における分解は $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_K^2 \mathfrak{P}'_K$ ($\mathfrak{P}_K, \mathfrak{P}'_K$ は K の相異なる素 ideal) であり, FK/M は Galois 拡大だから, FK において \mathfrak{p} は $(\mathfrak{P}\mathfrak{P}'\mathfrak{P}'')^2$ ($\mathfrak{P}, \mathfrak{P}', \mathfrak{P}''$ は FK の相異なる素 ideal) と分解する. よって \mathfrak{P}_F は FK において完全分解する. $FK = F(\sqrt[3]{\varepsilon})$ は F の三次 Kummer 拡大だから, 素数次 Kummer 拡大での分解法則 (例えば [Fu], 4 章, 定理 2.4) を用いて, \mathfrak{P}_F も FK で完全分解することがわかる. 故に FK/F は三次不分岐巡回拡大である. これは F の類数が 4 であることに反する. \square

E_1 が k -rational な位数 3 の部分群を持たないとする. $G = \text{Gal}(L/k)$ を $\text{GL}_2(\mathbb{F}_3)$ の部分群と見る. L は k の三次拡大体 K を含むので, G の位数は 3 で割り切れる. よって [Ser], Proposition 15 より, G は $\text{GL}_2(\mathbb{F}_3)$ のある Borel subgroup に含まれるか, $\text{SL}_2(\mathbb{F}_3)$ を含むかのどちらかである. 前者は仮定により除かれているので, $G \subset \text{SL}_2(\mathbb{F}_3)$ であり, $\det : G \rightarrow \mathbb{F}_3^\times$ は可換図式

$$\begin{array}{ccc} G & \longrightarrow & \text{GL}_2(\mathbb{F}_3) \\ \text{Res} \downarrow & & \downarrow \det \\ \text{Gal}(F/M) & \xrightarrow{\sim} & \mathbb{F}_3^\times \end{array}$$

より全射であるから, $G = \text{GL}_2(\mathbb{F}_3)$ である. よって $\text{Gal}(L/K)$ は $\text{GL}_2(\mathbb{F}_3)$ の 2-Sylow 部分群なので, $E_1[3]$ の基底を適当に選ぶことにより,

$$\text{Gal}(L/K) = \langle \sigma, \tau \rangle, \quad \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

としてよい. 補題 1 より E_1 は π, π' において ordinary good reduction を持つから, [BK], Proposition 5.6 の議論を適用することにより, $\langle \sigma, \tau^2 \rangle$ の固定体が K の不分岐二次拡大であることがわかる. しかし, KASH Version 1.7 を用いると, K の類数が 1 であることがわかり (類数の計算は Sparc station SS4 で 10 秒弱で済む), 矛盾である.

従って E_1 は k -rational な位数 3 の部分群を含むが, これが再び矛盾を引き起こすことを示す. 即ち

命題 2 E_1 を k 上至る所 good reduction を持つ楕円曲線とする (判別式は三乗数でもよい). この時 E_1 は k -rational な位数 3 の部分群を含まない.

命題を証明するために, 逆に, k 上定義された 3-isogeny $f: E_1 \rightarrow E_2$ があるとする. この時有理式 $J(x)$ を

$$J(x) = \frac{(x+27)(x+3)^3}{x}$$

で定義すると, Pinch [Pi2] により E_1, E_2 の j -invariant はそれぞれ

$$j(E_1) = J(\tau_1), j(E_2) = J(\tau_2), \tau_1, \tau_2 \in K, \tau_1\tau_2 = 3^6$$

と書ける (これは Fricke による modular curve $X_0(3)$ の parameter 表示と本質的に同じものである. cf. [Ha], [Um]). E_1, E_2 が k 上至る所 good reduction を持つので, $j(E_i) \in \mathcal{O}_k$ で, 単項 ideal $(j(E_i))$ はある ideal の三乗である. これより

$$\tau_1 = \pi^a \pi^{lb} u, \tau_2 = \pi^{6-a} \pi^{6-b} u^{-1}, a, b = 0, 3, 6, u \in \mathcal{O}_k^\times$$

と書ける. 共役, 及び dual isogeny $\hat{f}: E_2 \rightarrow E_1$ を考えて, $(a, b) = (0, 0), (0, 3), (0, 6)$ または $(3, 3)$ としてよい. c_4 を E_1 の定義方程式から通常のように定義すると,

$$j(E_1) = \frac{c_4^3}{\Delta} = \frac{(\tau_1 + 27)(\tau_1 + 3)^3}{\tau_1}$$

Setzer [Set] によれば, 二次体上定義された楕円曲線で j -invariant が 0 のものは bad prime を持つから, $c_4 \neq 0, \tau_1 \neq -27, \tau_1 \neq -3$ である. $(a, b) = (0, 0), (0, 3)$ または $(3, 3)$ ならば, $X = c_4/(\tau_1 + 3) (\neq 0), u_1 = \Delta, u_2 = \Delta/u$ とおくことによりそれぞれ

$$X^3 = u_1 + 27u_2, \tag{1}$$

$$X^3 = u_1 + \pi^3 u_2, \tag{2}$$

$$X^3 = u_1 + u_2 \tag{3}$$

が得られる. $(a, b) = (0, 6)$ ならば, $X = c_4 \pi / (\tau_1 + 3) (\neq 0), u_1 = \Delta, u_2 = \Delta/u$ とおくことにより

$$X^3 = \pi^3 u_1 + \pi^3 u_2 \tag{4}$$

が得られる. $u_1, u_2 \in \mathcal{O}_k^\times$ なので, どの場合でも $X \in \mathcal{O}_k$ である.

補題 2 方程式 (1), (2), (4) は解を持たない. 方程式 (3) は $X \neq 0$ である解を持たない.

(証明) どの場合の証明も大体同じなので, (2) に対してだけ証明しておく.

$u_1 = 1, \varepsilon$ または ε^{-1} としてよい. この時, π^2 を法として考えると $u_1 = 1$ でなくてはならないことがわかる. (2) を

$$\pi^3 u_2 = X^3 - 1 = (X - 1)(X^2 + X + 1)$$

と書くことにより,

$$\pi^{2a}u_3^2 + 3\pi^a u_3 + 3 = \pi^{3-a}u_4, \quad u_3, u_4 \in \mathcal{O}_k^\times, \quad 0 \leq a \leq 3$$

が得られる. $a = 0, 1$ 及び 3 の時は直ちに矛盾が出る. $a = 2$ の時は次のようにして矛盾が出る. 両辺の norm を考えて,

$$N_{k/\mathbb{Q}}(u_4) = \text{Tr}_{k/\mathbb{Q}}(\pi^2 u_3)^2 + (3 + 9N_{k/\mathbb{Q}}(u_3)) \text{Tr}_{k/\mathbb{Q}}(\pi^2 u_3) + (30 + 9N_{k/\mathbb{Q}}(u_3))$$

が得られるが, $N_{k/\mathbb{Q}}(u_3), N_{k/\mathbb{Q}}(u_4) = \pm 1$ の 4 通りの組合せのいずれでも $\text{Tr}_{k/\mathbb{Q}}(\pi^2 u_3)$ が有理数になり得ない. \square

よって再び矛盾である. これで命題 2 の, 従って命題 1 の証明が完結した.

5 $\mathbb{Q}(\sqrt{37})$ 上の Mordell 方程式

以下 $E_n^\pm(\mathcal{O}_k)$ を決定する.

命題 3 $E_0^+(\mathcal{O}_k) = \{(-12, 0)\}$.

これは $\text{rank } E_0^+(k) = 0$ を公式

$$\text{rank } E_0^+(k) = \text{rank } E_0^+(\mathbb{Q}) + \text{rank } (E_0^+)^{(37)}(\mathbb{Q})$$

($(E_0^+)^{(37)}$ は 37 による quadratic twist) を用いて示せばよく, $\text{rank } E_0^+(\mathbb{Q}) = 0$ は 2-descent で容易に求まるが, $\text{rank } (E_0^+)^{(37)}(\mathbb{Q})$ を 2-descent で求めるのは容易ではない. というのは $(E_0^+)^{(37)}$ の Shafarevich-Tate 群 III の (予想される) 位数は 4 だからである. しかし, $(E_0^+)^{(37)}$ は $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ に虚数乗法を持ち, また

$$L((E_0^+)^{(37)}/\mathbb{Q}, 1) = 3.1941\dots$$

(これは SIMATH Version 3.10, PARI/GP Version 1.39, UPECS Version 1.4 等で求まる) なので, Coates-Wiles [CW] の定理から $\text{rank } E_0^+(\mathbb{Q}) = 0$ がわかる.

注 Liverance 氏は, Satgé [Sa] の方法 (三次の isogeny を使う descent) で $\text{rank } E_0^+(\mathbb{Q}) = 0$ が従うことを指摘してくれた. 同論文の結果を用いると III[3] は trivial であることも示せる. また 2-descent をきちんと行なえば, III[2] の位数が 4 であることは実際確かめられる. 従って Rubin [Ru] の結果をあわせれば, III の位数は (予想抜きに) 4 であることがわかる.

補題 3 u_1, u_2 で k の単数を, A で k の整数を表すとする. この時

(a) 方程式 $64u_1 + u_2 = A^2$ は解を持たない.

(b) 方程式 $8u_1 + u_2 = A^2$ の解は

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

のみである.

(c) 方程式 $16u_1 + 2u_2 = A^2$ は解を持たない.

(d) 方程式 $u_1 + u_2 = A^2$ の解は

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

のみである.

(証明) (a) は [Is], Lemma 2.1 の特別な場合である. (b) は (a) と同様に示せる. (c) は明らかである.

(d) $A \neq 0$ とすると [Co], Proposition 2 より

$$u_1 = w^2 u_0, \quad u_2 = w^2 u'_0, \quad w, u_0 \in \mathcal{O}_k^\times, \quad \text{Tr}_{k/\mathbb{Q}}(u_0) = x^2, \quad x \in \mathbb{Z}$$

となる. $u_1 > 0$ として, 従って $u_0 = \varepsilon^n$ ($n \in \mathbb{Z}$) としてよい. [KT], Theorem 1 より, $\text{Tr}_{k/\mathbb{Q}}(\varepsilon^n) = x^2$ を満たす有理整数 x, n は $n = 3, x = \pm 42$ のみである. \square

命題 4 $E_3^+(\mathcal{O}_k) = \{ (-12\varepsilon, 0), (12(588 - \varepsilon^{-3}), \pm 3024(196 + \varepsilon^{-3})) \}$.

(証明) $L = k(\sqrt{3\varepsilon})$ で分解して考えることにより,

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

を解けばよいことがわかる. $m = 1$ の時に解が無いことは, π^2 を法として考えるなどすれば容易にわかる.

$m = 0$ の時, 係数を比較して

$$8\varepsilon = b(a^2 + \varepsilon b^2), \quad \pm y = a(a^2 + 9\varepsilon b^2) \quad (5)$$

が得られる. (5) の一つ目の式より, k の単数 $u > 0$ を用いて $b = u, 2u, 4u$ または $8u$ と書ける. $b = u, 4u, 8u$ の時はそれぞれ補題 3 (b), (c), (a) より解が無いことがわかる. $b = 2u$ の時は

$$\left(\frac{a}{2}\right)^2 = \varepsilon u^{-1} - \varepsilon u^2 \quad (6)$$

なので, 補題 3 (d) より, (6) が成り立つのは $u = 1$ または $u = \varepsilon^{-2}$ の場合に限ることがわかる. これより $(a, b) = (0, 2), (\pm 84, 2\varepsilon^{-2})$ であり, (5) の二つ目の式から, 対応する y の値はそれぞれ $y = 0, \pm 3024(196 + \varepsilon^{-3})$ である. \square

命題 5 $E_0^-(\mathcal{O}_k)$ は次の 15 個の元から成る:

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

(証明) $L = k(\sqrt{-3})$ で考えることにより,

$$(\pm y + 24\sqrt{-3}) = \mathfrak{P}_2^{a_2} \bar{\mathfrak{P}}_2^{\bar{a}_2} \mathfrak{C}^3, \quad (a_2, \bar{a}_2) = (0, 0), (2, 1)$$

を解けばよいことがわかる. 但し, $(2) = \mathfrak{P}_2 \bar{\mathfrak{P}}_2$, $\mathfrak{P}_2, \bar{\mathfrak{P}}_2$ は L の相異なる素 ideal.

$(a_2, \bar{a}_2) = (0, 0)$ の時は, 補題 3 などにより, $y = 0$ 以外に解が無いことがわかる.

$(a_2, \bar{a}_2) = (2, 1)$ の時. 両辺に $(4) = (\mathfrak{P}_2 \bar{\mathfrak{P}}_2)^2$ を掛け, \mathfrak{P}_2 の ideal 類の位数が 4 で, $\mathfrak{P}_2^4 = (1 + \omega - 3\zeta)$ ($\zeta = (1 + \sqrt{-3})/2$) であることに注意すれば

$$(4)(\pm y + 24\sqrt{-3}) = \mathfrak{P}_2^4 (\bar{\mathfrak{P}}_2 \mathfrak{C})^3 = (1 + \omega - 3\zeta) (\bar{\mathfrak{P}}_2 \mathfrak{C})^3$$

が得られ, L の類数が 4 であることより,

$$4(\pm y + 24\sqrt{-3}) = \zeta^n(1 + \omega - 3\zeta)(a + b\zeta)^3, \quad a, b \in \mathcal{O}_k, \quad n = 0, \pm 1$$

を解けばよいことがわかる.

$n = \pm 1$ の時は解が無いことが示せる. $n = 0$ の時は, 係数を比較することにより,

$$-64 = a^3 - (\omega - 2)a^2b - (\omega + 1)ab^2 - b^3, \quad (7)$$

$$\pm 4y - 96 = (\omega + 1)a^3 + 9a^2b - 3(\omega - 2)ab^2 - (\omega + 1)b^3 \quad (8)$$

が得られ, [dW] の議論を真似て, (7) の解は次の 21 個のみであることがわかる:

$$\begin{aligned} & (4, -4), (0, 4), (-4, 0), \\ & (-3 + \sqrt{37}, -2\sqrt{37}), (-2\sqrt{37}, 3 + \sqrt{37}), (3 + \sqrt{37}, -3 + \sqrt{37}), \\ & (-40 - 4\sqrt{37}, 8\sqrt{37}), (8\sqrt{37}, 40 - 4\sqrt{37}), (40 - 4\sqrt{37}, -40 - 4\sqrt{37}), \\ & (-2, 3 + \sqrt{37}), (-1 - \sqrt{37}, -2), (3 + \sqrt{37}, -1 - \sqrt{37}), \\ & (-3 + \sqrt{37}, 2), (1 - \sqrt{37}, -3 + \sqrt{37}), (2, 1 - \sqrt{37}), \\ & (-19 - 3\sqrt{37}, 16 + 2\sqrt{37}), (16 + 2\sqrt{37}, 3 + \sqrt{37}), (3 + \sqrt{37}, -19 - 3\sqrt{37}), \\ & (-16 + 2\sqrt{37}, 19 - 3\sqrt{37}), (-3 + \sqrt{37}, -16 + 2\sqrt{37}), (19 - 3\sqrt{37}, -3 + \sqrt{37}). \end{aligned}$$

これらを (8) に代入して, 命題に述べたもののうち $y = 0$ 以外の全ての値が得られる. \square

注 $E_0^-(k) = (E_0^-)^{(37)}(\mathbb{Q})$ の rank は 2 で, これは 2-descent で簡単に求まる.

以上で $E_n^\pm(\mathcal{O}_k)$ ($n = 0, 3, 6, 9$) が決まった.

6 Q. E. D.

Kraus [Kr] は, 各 $(x, y) \in E_n^\pm(\mathcal{O}_k)$ に対し, $(c_4, c_6) = (x, y)$ なる Weierstrass 方程式が存在するかどうかの local な条件を与えている. Kraus の結果の条件を満足するのは

$$(16\epsilon^{-2}, -8\sqrt{37}\epsilon^{-3}), (3376\epsilon^{-2}, 32248\sqrt{37}\epsilon^{-3}) \in E_{-6}^-(\mathcal{O}_k)$$

のみで, 前者が Shimura の楕円曲線 C_3 に, 後者が C_4 に対応することがわかる.

Kraus の結果を使う代わりに, 楕円曲線 $Y^2 = X^3 - 27xX - 54y$ の k における導手を Tate の algorithm を用いて計算しても結果が得られる. 上記二つ以外の各 (x, y) に対する楕円曲線は, 2 のみが bad prime であることが確かめられる. 二次体上の Tate の algorithm は, 梅垣敦紀氏が PARI/GP Version 1.39 を用いて作ったプログラムがあるので利用させていただいた. 同様のものは SIMATH Version 3.10 にもあるが, bug があるようで, 役に立たなかった.

7 $N = 29$ の場合について

$N = 37$ の時に §4 のような考察をしたのは, $E_1^+(\mathcal{O}_k)$ 等決定するのが大変で, しかも役に立たないものが幾つかあったからである.

他方 $N = 29$ の場合は, 役に立たないものは空集合であるか, 比較的容易に決定できるかのどちらかだったので, 全部決めてしまった. 結果は次の通りである.

$$\begin{aligned} E_0^\pm(\mathcal{O}_k) &= \{(\mp 12, 0)\} \text{ (複号同順)}, \\ E_3^+(\mathcal{O}_k) &= \{(-12\varepsilon, 0)\}, \\ E_1^+(\mathcal{O}_k), E_5^+(\mathcal{O}_k), E_2^-(\mathcal{O}_k) &= \emptyset \end{aligned}$$

であり, $E_2^+(\mathcal{O}_k)$ は次のもののみからなる:

$$\begin{aligned} &(-4, \pm 8\varepsilon^2), (12\varepsilon^2, \pm 8(1 + \varepsilon^4)), (-1 + 3\varepsilon^2, \pm(9 - 28\varepsilon^2)), \\ &(-1 + 243\varepsilon^{-2}, \pm(513 - 19684\varepsilon^{-2})) \end{aligned}$$

(このうち, 求めるのが大変なのは $E_2^+(\mathcal{O}_k)$ のみである). こうして, $E_n^\pm(\mathcal{O}_k)$ ($-6 \leq n < 6$) が全て決まり,

$$(-1 + 3\varepsilon^{-2}, -9 + 28\varepsilon^{-2}) \in E_{-2}^+(\mathcal{O}_k)$$

が Shimura の楕円曲線 C_1 に対応し,

$$(-1 + 243\varepsilon^{-2}, -513 + 19684\varepsilon^{-2}) \in E_2^+(\mathcal{O}_k)$$

が C_2 に対応することがわかり, 証明が終る.

もともと [Na] をよく読むと, その中で $N = 29$ の場合の決定は殆ど済んでいることがわかるので, その計算を活かした証明を与えるのが望ましく, 現在考慮中である.

Appendix : 定義方程式

楕円曲線 C_i ($i = 1, 2, 3, 4$) の定義方程式を書いておく.

$$N = 29 \quad C_1 : y^2 + xy + \varepsilon^2 y = x^3, \quad \Delta = -\varepsilon^{10}, \quad j = (5\varepsilon - 2)^3 \varepsilon^{-4},$$

$$\begin{aligned} C_2 : y^2 + xy + \varepsilon^2 y &= x^3 - 5\varepsilon^2 x - (\varepsilon^2 + 7\varepsilon^4), \\ \Delta &= -\varepsilon^{14}, \quad j = -(1 + 216\varepsilon^2)^3 \varepsilon^{-14}, \end{aligned}$$

$$N = 37 \quad C_3 : y^2 - \varepsilon y = x^3 + \frac{3\varepsilon + 1}{2} x^2 + \frac{11\varepsilon + 1}{2} x, \quad \Delta = \varepsilon^6, \quad j = 2^{12},$$

$$\begin{aligned} C_4 : y^2 - \varepsilon y &= x^3 + \frac{3\varepsilon + 1}{2} x^2 - \frac{1669\varepsilon + 139}{2} x - 7(5449\varepsilon + 451), \\ \Delta &= \varepsilon^6, \quad j = 3376^3. \end{aligned}$$

本文中に述べたように, $C_1(\mathbb{Q}(\sqrt{29}))_{\text{tors}} = \langle(0, 0)\rangle \cong \mathbb{Z}/3\mathbb{Z}$, $C_3(\mathbb{Q}(\sqrt{37}))_{\text{tors}} = \langle(0, 0)\rangle \cong \mathbb{Z}/5\mathbb{Z}$ であり, また $C_2(\mathbb{Q}(\sqrt{29}))_{\text{tors}}$, $C_4(\mathbb{Q}(\sqrt{37}))_{\text{tors}}$ は共に $\{O\}$ である (cf. [Na], [Shio]).

参考文献

- [BK] A. Brumer and K. Kramer, The rank of elliptic curves, *Duke Math. J.* **44** (1977), 715–743.
- [CW] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251.
- [Co] S. Comalada, Elliptic curves with trivial conductor over quadratic fields, *Pacific J. Math.* **144** (1990), 233–258.
- [Fu] 藤崎源二郎「代数の整数論入門(下)」裳華房, 1974.
- [Ha] Y. Hasegawa, \mathbb{Q} -curves over quadratic fields, *preprint*.
- [HHM] Y. Hasegawa, K. Hashimoto and F. Momose, Modular conjecture for \mathbb{Q} -curves and QM-curves, *preprint*.
- [Is] H. Ishii, The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields, *Japanese J. Math.* **12** (1986), 45–52.
- [KT] T. Kagawa and N. Terai, Squares in Lucas sequences and some Diophantine equations, *preprint*.
- [KM] N. Katz and B. Mazur, *The Arithmetic Moduli of Elliptic Curves*, Princeton University Press, 1985.
- [Ki1] M. Kida, On a characterization of Shimura's elliptic curve over $\mathbb{Q}(\sqrt{37})$, *Acta Arith.* **77** (1996), 157–171.
- [Ki2] M. Kida, Reduction of elliptic curves over real quadratic number fields, *preprint*.
- [KK] M. Kida and T. Kagawa, Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields, *J. Number Theory*, to appear.
- [Kr] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique, *Acta Arith.* **54** (1989), 75–80.
- [Na] T. Nakamura, On Shimura's elliptic curve over $\mathbb{Q}(\sqrt{29})$, *J. Math. Soc. Japan* **36** (1984), 701–707.
- [Pi1] R. G. E. Pinch, Elliptic curves over number fields, Ph. D. thesis, Oxford university, 1982.
- [Pi2] R. G. E. Pinch, Elliptic curves with good reduction away from 3, *Math. Proc. Camb. Phil. Soc.* **101** (1987), 451–459.
- [Ru] K. Rubin, The “main conjectures” of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1991), 25–68.
- [Sa] P. Satgé, Groupes de Selmer et corps cubiques, *J. Number Theory* **23** (1986), 294–317.
- [Ser] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

- [Set] B. Setzer, Elliptic curves with good reduction everywhere over quadratic fields and having rational j -invariant, *Illinois J. Math.* **25** (1981), 233–245.
- [Shim1] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan, no. 11, Iwanami Shoten and Princeton university press, 1971.
- [Shim2] G. Shimura, Class fields over real quadratic fields and Hecke operators, *Ann. of Math.* **95** (1972), 130–190.
- [Shio] K. Shiota, On the explicit models of Shimura's elliptic curves, *J. Math. Soc. Japan* **38** (1986), 649–659.
- [Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer, 1986.
- [St] R. J. Stroeker, Reduction of elliptic curves over imaginary quadratic number fields, *Pacific J. Math.* **108** (1983), 451–463.
- [Um] A. Umegaki, A construction of everywhere good \mathbb{Q} -curves with p -isogeny, *preprint*.
- [dW] B. M. M. de Weger, A Thue equation with quadratic integers as variables, *Math. Comp.* **64** (1995), 855–861.

Department of Information and Computer Science
School of Science and Engineering
Waseda University
3-4-1, Ohkubo Shinjuku-ku, Tokyo 169, Japan