

Determining all elliptic curves with good reduction outside a given set of primes

津田塾大学 後期博士課程 4 年 * 筒石奈央

1. Introduction

楕円曲線の reduction について次が知られている.

定理 1.1. 代数体 K と, 整数環 $\mathcal{O}_K$ の素イデアルの有限集合 S に対して, S に属さない全ての素イデアルで *good reduction* をもつ K 上の楕円曲線の同型類の集合

$$\mathcal{E}_K^S = \left\{ S \text{ の外 good reduction をもつ } K \text{ 上の楕円曲線} \right\}$$

は有限集合.

これを受けて, 次の問題を考える.

問題 1.2. 与えられた K と S に対して, $\mathcal{E}_K^S$ を決定せよ.

本稿では, $\mathcal{E}_K^S$ を決定するアルゴリズムを与える.

2. $\mathcal{E}_K^S$ の決定アルゴリズムの概要

本稿で与えるアルゴリズムの大きな枠組みは次である.

1. S の外 good reduction をもつ K 上の楕円曲線の j 不変量の集合

$$j(\mathcal{E}_K^S) = \{j(E) : E \in \mathcal{E}_K^S\}$$

を含む有限集合 J_K^S を, いくつかの K の拡大体上の S -単数方程式の解を用いて構成する.

2. 各 $j \in J_K^S$ に対して, $j(E) = j$ となる K 上の楕円曲線 E で $E \in \mathcal{E}_K^S$ となるものを全て求める.

*講演時

実は, $\mathcal{E}_K^S$ を決定するアルゴリズムとして, Cremona-Lingham によるもの ([2]) が既に知られている. 彼らの方法では, K 上のある楕円曲線の整数点を全て求めることでステップ 1 のような $j(\mathcal{E}_K^S)$ を含む有限集合が作られる. しかし, そのような整数点を全て求めること自体が難しく, 任意の体 K で求まるわけではない. 一方我々の方法では, K のいくつかの拡大体上の S -単数方程式の解を用いて $j(\mathcal{E}_K^S)$ を含む有限集合 J_K^S を構成する. S -単数方程式を解くアルゴリズムはあり ([7]), これも任意の体で解けるわけではないが, 単数群のランクがある程度小さければ計算可能である. 特に $S = \emptyset$ の場合は単数群のランクが 10 以下のとき, Magma([1]) の既存のコマンド UnitEquation で計算ができる. 4 章で, この場合に我々のアルゴリズムを実装したプログラムを用いた $\mathcal{E}_K^\emptyset$ の決定例をいくつか紹介する.

ステップ 1 については 3 章で詳しく述べるが, ステップ 2 についてはここで簡単に説明する. $j \in K$ に対して, E_j を Weierstrass 方程式

$$\begin{cases} y^2 = x^3 - 3j(j-1728)d^2x - 2j(j-1728)^2d^3 & (\text{if } j \neq 0, 1728), \\ y^2 = x^3 - dx & (\text{if } j = 1728), \\ y^2 = x^3 - d & (\text{if } j = 0) \end{cases} \quad (1)$$

で定義される K 上の楕円曲線とし, $n_j \in \mathbb{Z}$, E_j を次のように定義する.

$$n_j = \begin{cases} 2 & (\text{if } j \neq 0, 1728), \\ 4 & (\text{if } j = 1728), \\ 6 & (\text{if } j = 0). \end{cases}$$

すると, j を j 不変量にもつ楕円曲線は, E_j の n_j 次 twist $E^{(d)}$ ($d \in K^\times / (K^\times)^{n_j}$) になるが (cf. [4, Proposition X.5.3, X.5.4]), $E^{(d)}$ が S の外 good reduction をもつと仮定すると, d として $K^\times / (K^\times)^{n_j}$ のある有限部分集合の元のみを考えれば十分になる (cf. [2]). その有限個の d に対して, $E^{(d)}$ が S の外 good reduction をもつかを調べ, ステップ 2 の楕円曲線を得る.

3. J_K^S の決定方法

3.1. Admissible 曲線

E が位数 2 の K 有理点を持つとき, つまり $E(K)[2] \neq \{0\}$ が成り立つとき, E を admissible 曲線と呼ぶ. また,

$$\mathcal{E}_K^{S, \text{ad}} = \{E \in \mathcal{E}_K^S : E(K)[2] \neq \{0\}\}$$

とおく.

筆者は, [5] で $\mathcal{E}_K^\emptyset = \emptyset$ となるための 3 次体 K についての条件を与えたが, その証明の中で admissible 曲線について次を示した.

命題 3.1 ([5, Proposition 3.2.]). K を次を満たす 3 次体とする.

(i) 2 は K で不分岐,

(ii) K の狭義類数は 6 と素.

このとき $E \in \mathcal{E}_K^{\emptyset, \text{ad}}$ ならば, K の単数 x, y で

$$x + 16y = 1 \text{ または } x + y = 1$$

を満たし,

$$j(E) \in \left\{ \frac{(x + 2^8 y^2)^3}{x^2 y^2}, \frac{2^4 (x + 2^4 y^2)^3}{x^2 y^2}, \frac{(1 + 2^4 xy)^3}{x^2 y^2}, \frac{2^8 (1 + xy)^3}{x^2 y^2} \right\}$$

となるものが存在する.

K, S が一般の場合でも, 命題 3.1 のように $E \in \mathcal{E}_K^{S, \text{ad}}$ に対応するいくつかの S -単数方程式が取れ, $j(E)$ はその単数解で与えられることが, 次のようにして分かる.

まず, $E \in \mathcal{E}_K^S$ の Weierstrass 方程式の判別式について, 次が成り立つ.

命題 3.2. S -イデアル類群 $C_{K,S}$ の 12 倍写像の核 $C_{K,S}[12]$ の代表系 $\mathcal{C}$ を固定する. $E \in \mathcal{E}_K^S$ とすると, E は判別式 Δ が

$$\Delta \mathcal{O}_{K,S} \in \mathcal{C}^{12} = \{\mathfrak{c}^{12} : \mathfrak{c} \in \mathcal{C}\}$$

を満たす $\mathcal{O}_{K,S}$ 係数の Weierstrass 方程式をもつ. ただし, $\text{ord}_{\mathfrak{p}}(x)$ は $x \in K$ の $\mathfrak{p}$ 指数を表すとし, $\mathcal{O}_{K,S} = \{x \in K : \text{全ての } \mathfrak{p} \notin S \text{ について } \text{ord}_{\mathfrak{p}}(x) \geq 0\}$ とおく.

$C_{K,S}[12]$ の代表系 $\mathcal{C}$ を固定し, $E \in \mathcal{E}_K^{S, \text{ad}}$ とする. 命題 3.2 のように, $\Delta \mathcal{O}_{K,S} \in \mathcal{C}^{12}$ となる E の Weierstrass 方程式をとる. E は admissible より,

$$y^3 = x^3 + Ax^2 + Bx \quad (A, B \in \mathcal{O}_{K,S}) \quad (2)$$

という形の Weierstrass 方程式に変換できる. この変換で判別式は 2^{12} 倍されることより

$$B^2(A^2 - 4B) = 2^8 \Delta \quad (3)$$

が成り立つので, $\alpha_1 = \frac{AB}{\sqrt{\Delta}} + 2^4$, $\alpha_2 = \frac{AB}{\sqrt{\Delta}} - 2^4$ とおくと,

$$\alpha_1 \alpha_2 = \frac{A^2 B^2 - 2^4 \Delta}{\Delta} = \frac{4B^3}{\Delta}, \quad (4)$$

$$\alpha_1 - \alpha_2 = 2^5, \quad (5)$$

$$j(E) = \frac{(2^4(A^2 - 3B))^3}{2^{12}\Delta} = \frac{\left(2^8 + \frac{B^3}{\Delta}\right)^3}{\left(\frac{B^3}{\Delta}\right)^2} = \frac{(2^{10} + \alpha_1 \alpha_2)^3}{(2\alpha_1 \alpha_2)^2} \quad (6)$$

を得る. これらのことから, $j(E)$ を含む集合 $J_K^{S, \text{ad}}$ が次のように定義される.

定義 3.3. $\mathfrak{D} \in \mathcal{C}^{12}$ に対して

$$\mathcal{F}_{K,\mathfrak{D}} = \left\{ K(\sqrt{\delta}) : \delta \in \mathcal{O}_{K,S} \text{ は } \mathfrak{D} \text{ の生成元} \right\},$$

$F \in \mathcal{F}_{K,\mathfrak{D}}$ に対して

$$B_{F/K,\mathfrak{D}} = \left\{ \mathfrak{B} \in P_S : 0 \leq \text{ord}_{\mathfrak{p}}(\mathfrak{B}) \leq \frac{1}{2} \text{ord}_{\mathfrak{p}}(2^8 \mathfrak{D}) \text{ for all } \mathfrak{p} \notin S \right\}$$

とおく。ただし, P_S は $\mathcal{O}_{K,S}$ の単項イデアル全体を表す。

$F \in \mathcal{F}_{K,\mathfrak{D}}$ に対して

$$S_F = \{ \mathcal{O}_F \text{ のイデアル } \mathfrak{P} : \text{ord}_{\mathfrak{p}}(\mathfrak{P}) > 0, \mathfrak{p} \in S \},$$

$\mathfrak{B} \in B_{F/K,\mathfrak{D}}$ に対して

$$A_{\mathfrak{B}} = \{ (\mathfrak{C}_1 \mathfrak{D}^{-6}, \mathfrak{C}_2 \mathfrak{D}^{-6}) : \mathfrak{C}_i \in P_{S_F} (i=1,2), \mathfrak{C}_1 \mathfrak{C}_2 \mathfrak{D}^{12} = 4 \mathfrak{B}^3 \},$$

$\mathfrak{A}_F = (\mathfrak{A}_1, \mathfrak{A}_2) \in A_{\mathfrak{B}}$ に対して

$$U_{\mathfrak{A}_F} = \{ (\alpha_1, \alpha_2) \in F^2 : \alpha_i \mathcal{O}_{F,S_F} = \mathfrak{A}_i (i=1,2), \alpha_1 - \alpha_2 = 2^5 \},$$

$$J_{K,\mathfrak{A}_F} = \left\{ \frac{(2^{10} + \alpha_1 \alpha_2)^3}{(2 \alpha_1 \alpha_2)^2} : (\alpha_1, \alpha_2) \in U_{\mathfrak{A}_F} \right\} \cap K$$

とおく。そして

$$J_K^{S,\text{ad}} = \bigcup_{\mathfrak{D} \in \mathcal{C}^{12}} \bigcup_{F \in \mathcal{F}_{K,\mathfrak{D}}} \bigcup_{\mathfrak{B} \in B_{F/K,\mathfrak{D}}} \bigcup_{\mathfrak{A}_F \in A_{\mathfrak{B}}} J_{K,\mathfrak{A}_F}$$

とおく。

このとき, 次が成り立つ。

定理 3.4. (i) $J_K^{S,\text{ad}}$ は K と S にのみ依存する有限集合,

(ii) $E \in \mathcal{E}_K^{S,\text{ad}}$ ならば $j(E) \in J_{K,S}^{\text{ad}}$.

Proof. (i) 定義より $\mathcal{C}^{12}$, $B_{F/K,\mathfrak{D}}$, $A_{\mathfrak{B}}$ が有限集合なのは明らか。 $\mathfrak{D} \in \mathcal{C}^{12}$ に対して $\mathfrak{D}$ の生成元 $\delta \in \mathcal{O}_{K,S}$ を固定すると, 各 $F \in \mathcal{F}_{K,\mathfrak{D}}$ は K の単数 u によって $F = K(\sqrt{\delta}u)$ で与えられる。したがって $\mathcal{F}_{K,\mathfrak{D}}$ は $\mathcal{O}_K^\times / (\mathcal{O}_K^\times)^2$ と一対一対応するので, 有限集合。 $\mathfrak{A}_F = (\mathfrak{A}_1, \mathfrak{A}_2) \in A_{\mathfrak{B}}$ に対して $\mathfrak{A}_i$ の生成元 $\gamma_i \in \mathcal{O}_{F,S_F}$ を固定すると, $\mathfrak{A}_i$ のその他の生成元は S_F -単数 $x_i \in \mathcal{O}_{F,S_F}^\times = \{x \in K : \text{全ての } \mathfrak{p} \notin S \text{ に対して } \text{ord}_{\mathfrak{p}}(x) = 0\}$ によって $r_i x_i$ で与えられるので

$$U_{\mathfrak{A}_F} = \{ (\gamma_1 x_1, \gamma_2 x_2) : x_i \in \mathcal{O}_{F,S_F}^\times, \gamma_1 x_1 - \gamma_2 x_2 = 2^5 \}$$

と表せる。ここで, S_F -単数方程式 $\gamma_1 x_1 - \gamma_2 x_2 = 2^5$ は有限個の解しか持たないので ([4, Theorem IX.4.1]), $U_{\mathfrak{A}_F}$ も有限集合。したがって, $J_K^{S,\text{ad}}$ は有限集合。

(ii) 上の説明のように E の Weierstrass 方程式 (2) をとると, $\mathfrak{D} = \Delta \mathcal{O}_{K,S} \in \mathcal{C}^{12}$, $F = K(\sqrt{\Delta}) \in \mathcal{F}_{K,\mathfrak{D}}$ 。また, 式 (3), (4), (5) より, $\mathfrak{B} = B \mathcal{O}_{K,S} \in B_{F/K,\mathfrak{D}}$, $\mathfrak{A}_F = (\alpha_1 \mathcal{O}_{F,S_F}, \alpha_2 \mathcal{O}_{F,S_F}) \in A_{\mathfrak{B}}$, $(a_1, a_2) \in U_{\mathfrak{A}_F}$, $j(E) \in J_{K,\mathfrak{A}_F}$ が成り立つ。したがって, $j(E) \in J_K^{S,\text{ad}}$. $\square$

3.2. Non-admissible 曲線

ここでは, $E \in \mathcal{E}_K^S$ が non-admissible の場合, つまり,

$$E \in \mathcal{E}_K^{S, \text{nad}} = \mathcal{E}_K^S \setminus \mathcal{E}_K^{S, \text{ad}} = \{E \in \mathcal{E}_K^S : E(K)[2] = \{0\}\}$$

となる場合に, $j(E)$ を含むような集合 $J_K^{S, \text{nad}}$ を定義する.

$E \in \mathcal{E}_K^{S, \text{nad}}$ とする. 位数 2 の E 上の点 $P = (p_1, p_2) \in \bar{K} \times \bar{K}$ を取ると, $K(P) = K(p_1, p_2)$ は K 上 3 次拡大体になり, E を $K(P)$ 上の曲線とみなすと明らかに E は $S_{K(P)}$ の外 good reduction をもち, $K(P)$ 上 admissible, つまり $E(K(P))[2] \neq \{0\}$ となる. したがって,

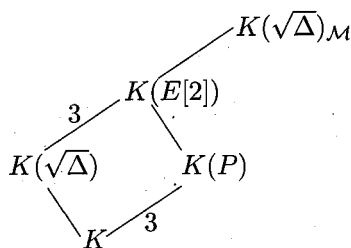
$$j(E) \in J_{K(P)}^{S_{K(P)}, \text{ad}} \cap K$$

となる. ここで $K(P)$ が満たす条件をみていくと, まず, $K(P)$ は E の位数 2 の点の座標を全て K に添加した体 $K(E[2])$ の K 上 3 次部分体であり, $K(E[2])$ は $K(P)/K$ の Galois closure になっている. また, $K(E[2])/K(\sqrt{\Delta})$ (Δ は E を定める任意の Weierstrass 方程式の判別式) の分岐は次のように制限される.

命題 3.5 (cf. [4, Proposition VII.4.1]). $E \in \mathcal{E}_K^{S, \text{ad}}$ とし, E の Weierstrass 方程式の判別式を Δ とおく. この時, $K(E[2])/K(\sqrt{\Delta})$ は $S' = S_{K(\sqrt{\Delta})} \cup \{\mathfrak{p} : \text{ord}_{\mathfrak{p}}(2) > 0\}$ の外不分岐な 3 次巡回拡大. したがって, $K(E[2])$ は $K(\sqrt{\Delta})$ の $\text{mod } \mathcal{M} = \prod \mathfrak{p}^{e_{\mathfrak{p}}}$ ($\mathfrak{p} \in S'_{K(\sqrt{\Delta})}$) の ray class field $K(\sqrt{\Delta})_{\mathcal{M}}$ の $K(\sqrt{\Delta})$ 上 3 次部分体. ただし,

$$e_{\mathfrak{p}} = \begin{cases} \left\lfloor \frac{3 \text{ord}_{\mathfrak{p}}(3)}{2} \right\rfloor + 1 & \text{if } \text{ord}_{\mathfrak{p}}(3) > 0, \\ 1 & \text{otherwise.} \end{cases} \quad (7)$$

特に, $K(\sqrt{\Delta})$ の $\text{mod } \mathcal{M}$ の ray class group $C_{K(\sqrt{\Delta})}^{\mathcal{M}}$ の位数は 3 の倍数.



定義 3.6. $\mathfrak{D} \in \mathcal{C}^{12}$ に対して

$$\mathcal{F}'_{K, \mathfrak{D}} = \{F \in F_{K, \mathfrak{D}} : C_F^{\mathcal{M}} \text{ の位数は 3 で割り切れる } \},$$

$F \in \mathcal{F}'_{K, \mathfrak{D}}$ に対して

$$\mathcal{L}_{F/K} = \{L : K \subset L \subset F_{\mathcal{M}}, \deg(L/K) = 3, FL \text{ は } L/K \text{ の Galois closure}\}$$

とおく.

このとき、命題 3.5 より

$$K(P) \in \bigcup_{\mathfrak{D} \in \mathcal{C}^{12}} \bigcup_{F \in \mathcal{F}'_{K, \mathfrak{D}}} \mathcal{L}_{F/K}$$

となるので、 $J_K^{S, \text{nad}}$ は次のように定義できる.

定理 3.7.

$$J_K^{S, \text{nad}} = \bigcup_{\mathfrak{D} \in \mathcal{C}^{12}} \bigcup_{F \in \mathcal{F}'_{K, \mathfrak{D}}} \bigcup_{L \in \mathcal{L}_{F/K}} J_L^{S, \text{ad}} \cap K$$

とおく.

(i) $J_K^{S, \text{nad}}$ は K と S にのみ依存する有限集合,

(ii) $E \in \mathcal{E}_K^{S, \text{nad}}$ ならば $j(E) \in J_K^{S, \text{nad}}$.

定理 3.4 と 3.7 より、 $j(\mathcal{E}_K^S)$ を含む有限集合 J_K^S を得る.

系 3.8. $J_K^S = J_K^{S, \text{ad}} \cup J_K^{S, \text{nad}}$ とおく.

(i) J_K^S は K と S にのみ依存する有限集合,

(ii) $E \in \mathcal{E}_K^S$ ならば $j(E) \in J_K^S$.

4. 例

$\mathcal{E}_K^\emptyset$ に属する楕円曲線、つまり全ての素イデアルで good reduction をもつ楕円曲線を、 K 上の EGR 曲線と呼ぶ.

ここでは、Magma に用意されている単数方程式を解く既存のコマンド (UnitEquation) を用いて決定された EGR 曲線の例をいくつか紹介する. なお、ここでの計算は Magma Ver.2.21-4 を用いている.

4.1. $\mathbb{Q}(\sqrt{-2} + \sqrt{-6})$

$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-2} + \sqrt{-6})$ とおく (α は $x^4 + 16x^2 + 16$ の根). K の 3 つの 2 次部分体 $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-6})$, $\mathbb{Q}(\sqrt{3})$ 上, EGR 曲線は存在しないが、 K 上は EGR 曲線が存在することが示される.

命題 4.1. K 上の EGR 曲線は同型を除いて 2 曲線存在し、それは j 不変量が 8000 の Weierstrass 方程式

$$y^2 = x^3 - 120\alpha^2 x \pm 448\alpha^3$$

で与えられる.

K の類数は 2 で, イデアル類群は 2 の上の素イデアル $\mathfrak{p}$ ($2\mathcal{O}_K = \mathfrak{p}^4$) で生成される. $\mathcal{C}^{12} = \{\mathcal{O}_K, 8\mathcal{O}_K\}$ とおくと, $\mathcal{F}_{K,\mathcal{O}_K} = \{K, K(\sqrt{-1}), K(\sqrt{\pm 2\alpha})\}$, $\mathcal{F}_{K,8\mathcal{O}_K} = \mathcal{F}_{K,\mathcal{O}_K} \cup \{K(\sqrt{\pm 2}), K(\sqrt{\pm \alpha})\}$ となる. $F \in \mathcal{F}_{K,8\mathcal{O}_K}$ の modulo 2 の ray class number を計算すると, どれも 3 で割れないので, $\mathcal{F}'_{K,\mathcal{O}_K} = \mathcal{F}'_{K,8\mathcal{O}_K} = \emptyset$ となる. したがって, K 上の EGR 曲線は admissible である. つまり $\mathcal{E}_K^\emptyset = \mathcal{E}_K^{\emptyset, \text{ad}}$ が成り立つ. $j = 8000$ は, $F = K(\sqrt{-1})$ 上の単数方程式 $x - y = 2$ (解は 35 個存在) の解から構成される.

4.2. $\mathbb{Q}(\sqrt[3]{46})$

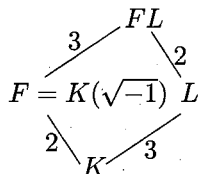
横山氏は [8] で $\mathbb{Q}(\sqrt[3]{46})$ 上の EGR 曲線として $j(E) = -9936$ であるものを見つけているが, $\mathbb{Q}(\sqrt[3]{46})$ 上の EGR 曲線はその曲線のみであることが示される.

命題 4.2. $\mathbb{Q}(\sqrt[3]{46})$ 上の EGR 曲線は同型を除いてただ一つで, その楕円曲線は j 不変量 -9936 を持ち, Weierstrass 方程式

$$y^2 = x^3 - 2\sqrt[3]{46}x - 8$$

で定義される.

上の曲線は non-admissible 曲線で, $F = K(\sqrt{-1})$ の mod 2 の ray class field の K 上 3 次部分体 L 上の admissible EGR 曲線になっており, j 不変量は 18 次体 FL (単数群のランク 8) の単数方程式の解から計算される.



4.3. EGR 曲線の族

[6] で任意の次数 ≥ 3 の体上定義される次の EGR 曲線の無限族が構成されている.

命題 4.3. $n, a \in \mathbb{Z} (n \geq 2)$ とし, ϵ を

$$g_{n,a}(x) = x^n - 16^{n-2}(a-16)x^{n-1} + ax - 1$$

の根とする. このとき, $g_{n,a}(x)$ は $\mathbb{Q}$ 上既約で, 楕円曲線

$$E_1: y^2 + xy = x^3 + 16\epsilon x^2 + 8\epsilon x + \epsilon,$$

$$E_2: y^2 + xy = x^3 - 8\epsilon x^2 + 2\epsilon(8\epsilon - 3)x + \epsilon(4\epsilon - 1),$$

$$E_3: y^2 + xy = x^3 - 8\epsilon x^2 + \epsilon(16\epsilon - 1)x,$$

$$E_4: y^2 + xy = x^3 - 2\epsilon x^2 + \epsilon^2 x$$

は $\mathbb{Q}(\epsilon)$ 上の EGR 曲線.

証明の概略 $g_{n,a}(x)$ の既約性は, Perron の既約性定理 ([3, Theorem 2]) から従う. $g_{n,a}(x)$ の定数項が単数より, ϵ は明らかに単数だが, $1 - 16\epsilon$ の絶対ノルムを計算すると 1 となり $1 - 16\epsilon$ も単数であることが分かる. したがって, Weierstrass 方程式の判別式は上から $\epsilon(1 - 16\epsilon), \epsilon(1 - 16\epsilon)^4, \epsilon^2(1 - 16\epsilon)^2, \epsilon^4(1 - 16\epsilon)$ となり, どれも単数なので $E_i (i = 1, 2, 3, 4)$ は EGR 曲線. $\square$

類数が 1 で, 比較的判別式の絶対値が小さい $(n, a) = (3, 19), (4, 16)$ の場合に, EGR 曲線を決定した.

命題 4.4. 多項式

$$g_{3,19}(x) = x^3 - 48x^2 + 19x - 1,$$

$$g_{4,16}(x) = x^4 + 16x - 1$$

で定義される体 K 上, EGR 曲線はちょうど 8 曲線ずつ存在し, 上の多項式の根を $\epsilon \in K$ とおくと, EGR 曲線 $E_i, E'_i (i = 1, 2, 3, 4)$ の j 不変量は

$$j(E_1) = j(E'_1) = 4124\epsilon^2 - 197943\epsilon + 66391,$$

$$j(E_2) = j(E'_2) = 218300419\epsilon^2 - 10461642895\epsilon + 3492807433,$$

$$j(E_3) = j(E'_3) = 9788250386431\epsilon^2 - 3902514659536\epsilon + 205621494493,$$

$$j(E_4) = j(E'_4) = 619787628373344257\epsilon^2 - 29711081063503953712\epsilon \\ + 9919579807195071219$$

で与えられる.

参考文献

- [1] W. Bosma, J. Cannon, and C. Playoust: *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.
- [2] J. Cremona and M. Lingham: *Finding all elliptic curves with good reduction outside a given set of primes*, Exp. Math. 16 No.3 (2007), 303–312.
- [3] O. Perron: *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*, J. Reine Angew. Math., 132 (1907), 288–307.
- [4] J. H. Silverman: *The Arithmetic of Elliptic Curves* (2nd edition), Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 2009.
- [5] N. Takeshi: *Elliptic curves with good reduction everywhere over cubic fields*, Int. J. Number Theory, vol. 11, no. 04 (2015), 1149–1164.
- [6] N. Takeshi: *Family of elliptic curves with good reduction everywhere over number fields of given degree*, preprint.

- [7] K. Wildanger: *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern* (*On the solution of units and index form equations in algebraic number fields*), J. Number Theory 82 (2000), no. 2, 188–224.
- [8] S. Yokoyama: *On elliptic curves with everywhere good reduction over certain number fields*, American J. Comput. Math (2012), vol. 2, no. 4, 358–366.