実二次体上至る所good reductionを持つ楕円曲線

早稲田大学理工学部　加川 貴章 (Takaaki KAGAWA)

1 Introduction

k を代数体とする. 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を問題とする.

これまでには次のような結果が得られている:

(1) $\mathbb{Q}$ 上至る所 good reduction を持つ楕円曲線は存在しない. (Tate による. 今や彼の Wiles の定理の系である.)

(2) k が類数が 6 と素な虚二次体なら k 上には存在しない ([22]).

(3) 色々な実二次体上に例がある ([3], [4], [9], [14], [21], [23], [25], [29]).

(4) $\mathbb{Q}(\sqrt{5})$ 上には存在しない ([21]).

(5) p が 8 を法として 5 と合同な素数の時, $\mathbb{Q}(\sqrt{p})$ 上非存在かどうかの規準がある. それを用いて, $p = 5, 13$ の時存在しないことが示されている ([9]).

(6) (5) で述べた規準が $\mathbb{Q}(\sqrt{m})$, $m \equiv 1 \pmod 4$ の場合に拡張されている. それを用いて $m = 5, 13, 17, 21, 73, 97, 149, 173, 181$ の場合の非存在の証明と, $m = 41$ 上の全曲線の決定がなされている. ([13])

本稿では実二次体の場合を扱う. この場合至る所 good reduction を持つ楕円曲線としては, 二次指標 χ_N ($N > 1$ は基本判別式) を Neben-type character に持つ保型形式の空間 $S_N := S_2(\Gamma_0(N), \chi_N)$ の二次元 $\mathbb{Q}$-単純部分空間から得られる Shimura's elliptic curve (cf. [24]) もあり興味深い. 証明するのは次のものである:

(1) $m =$ 2, 3, 5, 10, 13, 15, 17, 21, 30, 34, 39, 42, 47, 53, 58, 66, 69, 70, 73, 74, 85, 89, 94, 97 の時, $\mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線は存在しない.

(2) $m =$ 6, 7, 14, 29, 33, 37, 41, 65 の時, $k = \mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線を全て決定した (Appendix 2 の通り). k-isogeny class の数は, $m = 65$ の時だけ 2 で, 他の m の時は 1 である.

このうち一部は [13] で得られているが, 証明はここで与えられるものの方が易しい. また $m = 2, 3, 6, 7, 14, 47, 94$ の場合は電気通信大学の木田雅成氏 ([15], [16]) により独立に得られている.

実二次体 $\mathbb{Q}(\sqrt{m})$ $(1 < m < 100)$ は 60 個ある. ここではそのうち 24 個の体に対し非存在を示し, 8 個の体に対しその上の楕円曲線を全て決定している. ここで扱えなかった場合で

例があるのは $m = 22, 26, 38, 77, 79, 86$ の場合であり, 残りの 22 個の m に対し, $\mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線が存在するかどうかはまだわからない (多分無い).

Shimura's ellptic curve との関係を挙げておこう. $d(m)$ を二次体 $\mathbb{Q}(\sqrt{m})$ の判別式とする. この時 $S_{d(m)}$ の構造が知られている. m が (1) に挙げられているいずれかの値の時, $S_{d(m)}$ は 2 次元の $\mathbb{Q}$-単純部分空間を持たない. $m = 6, 7, 29, 33, 37, 41$ に対しては, $S_{d(m)}$ は 2 次元 $\mathbb{Q}$-単純であり, $S_{d(14)}$ は 2 次元 $\mathbb{Q}$-単純部分空間と 4 次元 $\mathbb{Q}$-単純部分空間の直和, $S_{d(65)}$ は 2 つの 2 次元 $\mathbb{Q}$-単純部分空間の直和である. (上の $S_{d(m)}$ の計算は長谷川雄之氏と日比野剛士氏による.) よって上の 32 個の m に対し, 全ての曲線は Shimura's ellpitic curve, 特に modular である. ($m = 29, 37, 41, 65$ の場合は, どの曲線も虚数乗法を持っていないことに注意.)

記号: 代数体 k に対し, $\mathcal{O}_k$, $\mathcal{O}_k^\times$, h_k でそれぞれ k の整数環, 単数群, 類数を表すとする. $\mathfrak{m}$ が k の因子 (即ち分数 ideal といくつかの無限素点の形式的な積) の時, $h_k(\mathfrak{m})$ を k の ray class number modulo $\mathfrak{m}$ とする. 簡単のため $h_k(\prod_{\mathfrak{p}|2}\mathfrak{p})$ を $h_k^{(2)}$ と書く. また k が実二次体ならば, $k/\mathbb{Q}$ の共役を $'$ で表し, ε (> 1) で基本単数を表すとする. $k = \mathbb{Q}(\sqrt{m})$, $m \equiv 1 \pmod 4$ の時は, $\omega = (1 + \sqrt{m})/2$ とする.

楕円曲線 E に対して, $b_2(E)$, $b_4(E)$, $b_6(E)$, $b_8(E)$, $c_4(E)$, $c_6(E)$, $\Delta(E)$, $j(E)$ を通常通りとする. (定義は [26] を参照. j 以外はモデルに依存するので, $b_2(E)$ 等は一つモデルを決めて考えたものと了解していただきたい). $n \in \mathbb{N}$ に対し $E[n]$ を $nP = O$ なる点 P 全体の成す群とする. E が k 上定義されている時, $k(E[n])$ を $E[n]$ の O でない全ての点の座標を k に添加した体とする.

2 Some criteria

この節では幾つか規準を紹介する.

命題 2.1. k を代数体, E を k 上至る所 good reduction を持つ楕円曲線とする. E が位数 2 の k-有理点を持たなければ, $h^{(2)}_{k(\sqrt{\Delta(E)})}$ は 3 で割れる. □

系 2.2. k を $(h_k, 6) = 1$, または $h_k = 2$ なる実二次体とする. $h_k^{(2)}$, $h^{(2)}_{k(\sqrt{-1})}$, $h^{(2)}_{k(\sqrt{\pm\varepsilon})}$ が全て 3 で割れなければ, k 上至る所 good reduction を持つ楕円曲線は全て admissible である. □

ここで, 代数体 k 上定義された楕円曲線 E が admissible であるとは, E が次を満たすことを言う:

(1) E は k 上至る所 good reduction を持つ;

(2) E は位数 2 の k-有理点を持つ.

命題 2.3. k を実二次体とする. $h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)})$ ($\mathfrak{p}_\infty^{(1)}$, $\mathfrak{p}_\infty^{(2)}$ は k の無限素点) が 4 で割れなければ, k 上至る所 good reduction を持つ楕円曲線で判別式が k の 3 乗数のものは k 上定義された 3-isogeny を許す. □

命題 2.4. k を実二次体とする. 12 次体 $k(\sqrt[3]{\varepsilon}, \sqrt{-3})$ の 3 を法とする ray class number が奇数であると仮定する. k 上至る所 good reduction を持つ楕円曲線 E の判別式 $\Delta(E)$ が k の 3 乗数でないならば, $\mathrm{Gal}(k(E[3])/k)$ $(\subset \mathrm{GL}_2(\mathbb{F}_3))$ は

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}, \quad \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

のいずれかと共役である. 特に, E は位数 3 の k-rational subgroup V を持ち, $V \subset E(k)$ である (即ち E が位数 3 の k-有理点を持つ) か, E/V が位数 3 の k-有理点を持つかのどちらかである. □

命題 2.5. 実二次体 k が次を満たす時, k 上至る所 good reduction を持つ楕円曲線の判別式は k の 3 乗数である:

(1) $(h_k, 6) = 1$;
(2) k において 3 は不分岐である;
(3) $h_{k(\sqrt{-3})}$ は 3 で割れない;
(4) $h_{k(\sqrt[3]{\varepsilon})}$ の類数は 2 で割れない;
(5) 3 を割る k の素 ideal $\mathfrak{p}$ に対し, 合同式 $X^3 \equiv \varepsilon \pmod{\mathfrak{p}^2}$ は解 $X \in \mathcal{O}_k$ を持たない. □

証明の方針はいずれも同じである. 即ち

- 代数体 k 上定義された楕円曲線と自然数 n に対し, $\mathrm{Gal}(k(E[n])/k)$ は $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ の部分群に同型である;
- E が代数体 k 上至る所 good reduction を持つとき, $k(E[n])/k$ で分岐する可能性のある有限素点は n の素因子と E の bad prime の素因子のみである,
- $k(E[n])$ $(n = 2, 3)$ は $\sqrt[n]{\Delta(E)}$, 1 の原始 n 乗根を含む

というよく知られた事実を使って, n と無限素点の外不分岐な abel 拡大, あるいは不分岐 abel 拡大を作る, そのような体の存在は類体論により (ray) class number の可除性に帰着される, というわけである. 詳細は [10], [11], [12] を御覧いただきたい ([13], [15], [16] も).

なおいくつかの規準の条件にある "$(h_k, 6) = 1$" は, global minimal model の存在のために使われている. 即ち

補題 2.6 (Setzer [22]). k を代数体, E を k 上至る所 good reduction を持つ楕円曲線とする. $(h_k, 6) = 1$ ならば E は global minimal model を持つ. □

3 Determination

前節の規準を使って, 実二次体上至る所 good reduction を持つ楕円曲線を決定する. 規準の仮定を確認するには ray class number の計算をしなくてはいけないが, その計算は KASH を使えば出来る. (KASH については, 制作者たちの書いた詳しい解説 [6] がある.)

3.1 Admissible curves

$k = \mathbb{Q}(\sqrt{m})$ $(1 < m < 100)$ を類数が 6 と素, または類数が 2 である実二次体とする (k の類数が 3 なのは $m = 79$ の時のみ, 類数が 4 なのは $m = 82$ の時のみで, 他の時は類数 1 か 2 である). $h_K^{(2)}$ $(K = k, k(\sqrt{-1}), k(\sqrt{\pm\varepsilon}))$ を計算すると表 1 のようになる (3 の倍数は太字にした).

m	k	$k(\sqrt{-1})$	$k(\sqrt{\varepsilon})$	$k(\sqrt{-\varepsilon})$	m	k	$k(\sqrt{-1})$	$k(\sqrt{\varepsilon})$	$k(\sqrt{-\varepsilon})$
2	1	1	1	1	47	1	5	1	8
3	1	1	1	2	51	2	**12**	4	8
5	1	1	1	1	53	1	**3**	1	1
6	1	2	1	1	55	2	4	1	**12**
7	1	1	1	4	57	1	2	1	**3**
10	2	2	2	2	58	2	2	2	2
11	1	**3**	1	2	59	1	**9**	1	**6**
13	1	1	1	1	61	1	**3**	1	1
14	1	4	1	1	62	1	8	1	**3**
15	2	2	2	8	65	2	8	2	2
17	1	2	1	1	66	2	16	1	8
19	1	**3**	1	**6**	67	1	**3**	1	14
21	1	2	1	1	69	1	4	1	**3**
22	1	2	1	**3**	70	2	4	1	16
23	1	**3**	1	4	71	1	7	**3**	4
26	2	**6**	2	2	73	1	2	1	1
29	1	**3**	1	1	74	2	10	2	2
30	2	4	1	8	77	1	4	1	**3**
31	1	**3**	1	8	78	2	4	2	**12**
33	1	2	1	**3**	83	1	**9**	1	10
34	2	8	1	8	85	2	4	4	4
35	2	**6**	2	16	86	1	10	1	**3**
37	**3**	**3**	**3**	**3**	87	2	**6**	2	8
38	1	**6**	1	**3**	89	1	**6**	1	1
39	2	4	1	4	91	2	**6**	2	**48**
41	1	4	1	1	93	1	2	1	**3**
42	2	4	2	4	94	1	8	1	5
43	1	**3**	1	10	95	2	8	1	**12**
46	1	4	1	**3**	97	1	2	1	1

表 1: $h_K^{(2)}$ $(K = k, k(\sqrt{-1}), k(\sqrt{\pm\varepsilon}))$

この計算と系 2.2 より次が得られる:

命題 3.1. m が 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 21, 30, 34, 39, 41, 42, 47, 58, 65, 66, 70, 73, 74, 85, 94, 97 のいずれかならば, $\mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線は全て admissible である. □

Comalada [3] は, その上に admissible curve を許すような実二次体の特徴付けを不定方程式を用いて与えている. そして不定方程式を実際に解くことにより, $k = \mathbb{Q}(\sqrt{m})$

$(1 < m < 100)$ 上 admissible な楕円曲線が存在するのは

$$m = 6, 7, 14, 22, 38, 41, 65, 77, 86$$

の場合に限ることを示している. 更にこの時 admissible な楕円曲線の k-isomorphism class が全て求められている. それと命題 3.1 をあわせて次が得られる:

系 3.2. (1) $m = 2$, 3, 5, 10, 13, 15, 17, 21, 30, 34, 39, 42, 47, 58, 66, 70, 73, 74, 85, 94, 97 の時, $\mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線は存在しない.

(2) $m = 6$, 7, 14, 41, 65 の時, $k = \mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線は全て admissible である. 従って Appendix 2 の表にあるものだけである. (Comalada の楕円曲線との対応は Appendix 2 の表に書いておいた.) □

Comalada の結果, 表 1, 命題 2.1, 補題 2.6 をあわせて次も得られる:

系 3.3. E を実二次体 $k = \mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線とする.

(1) m が 33 または 69 の時, E は $\Delta(E) = -\varepsilon^{2n+1}$ $(n \in \mathbb{Z})$ なる global minimal model を持つ.

(2) m が $29, 53, 89$ のいずれかである時, E は $\Delta(E) = -\varepsilon^{2n}$ $(n \in \mathbb{Z})$ なる global minimal model を持つ. □

$\mathbb{Q}(\sqrt{37})$ 上の曲線に対しては, 同じ方法では判別式の符号も指数の偶奇もわからない. というのは, $h_k^{(2)}$, $h_{k(\sqrt{-1})}^{(2)}$, $h_{k(\sqrt{\pm\varepsilon})}^{(2)}$ が全て 3 だからである.

4 $m = 29, 33, 69$ の場合

以下 $k = \mathbb{Q}(\sqrt{m})$, $1 < m < 100$, $(h_k, 6) = 1$ とする. また m は今まで扱われていないものとする. 即ち $m = 11$, 19, 22, 23, 29, 31, 33, 37, 38, 43, 46, 53, 57, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89, 93. この時 $h_k = 1$ である.

まず判別式が 3 乗数の場合を扱う. 最初に次の補題を挙げておく (証明は [12] を参照のこと):

補題 4.1. k を類数が 6 と素な実二次体, E を k 上至る所 good reduction を持つ楕円曲線とする. この時 E が k 上定義された 3-isogeny を許せば, k は $\mathbb{Q}(\sqrt{6})$ か $\mathbb{Q}(\sqrt{33})$ のいずれかで, E は 6A1, 6A1′, 又は 33A1, 33A1′ とそれぞれの体上同型である. □

命題 2.3 を使うために $h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)})$ を求める. その前に, 次を注意しておく. p を素数とする時, k が $\mathbb{Q}(\sqrt{p})$ $(p \equiv 1 \pmod 4)$, $\mathbb{Q}(\sqrt{3p})$ $(p \equiv 3 \pmod 4)$ のいずれでもない実二次体の時は, $h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)})$ は 4 の倍数である. 実際この時 $\tilde{k}$ を k の narrow genus field とすると, $\tilde{k}(\sqrt{-3})/k$ は 3 と無限素点の外不分岐な 4 次以上の abel 拡大である. 他の場合を KASH で求めると

$$h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}) = \begin{cases} 2 & (m = 29, 33, 53, 89 \text{ の時}), \\ 6 & (m = 69 \text{ の時}), \\ 12 & (m = 93 \text{ の時}), \\ 4 & (\text{その他}) \end{cases}$$

が得られる. よって命題 2.3, 補題 4.1 より次が従う.

命題 4.2. (1) $m = 29, 53, 69, 89$ の時, $k = \mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持ち, 判別式が k の 3 乗数である楕円曲線は存在しない.

(2) $k = \mathbb{Q}(\sqrt{33})$ 上至る所 good reduction を持ち, 判別式が k の 3 乗数である楕円曲線は 33A1, 33A1′ のみである. □

次に判別式が 3 乗数でない場合を考える. 命題 2.4 を使うので, 12 次体 $M = k(\sqrt[3]{\varepsilon}, \sqrt{-3})$ の (3) を法とする ray class number $h_M((3))$ を KASH で求めると以下のようになる:

$$h_M((3)) = \begin{cases} 3 & (m = 29 \text{ の時}), \\ 243 & (m = 33 \text{ の時}), \\ 9 & (m = 69 \text{ の時}), \\ 12 & (m = 77 \text{ の時}), \\ 18 & (m = 93 \text{ の時}). \end{cases}$$

計算時間は Sparc station SS4 (CPU 110MHZ) でそれぞれ 1 分, 20 分, 1 分, 8 分, 2 分程度であった. (他の m の場合は, Minkowski bound が大きく, 時間, メモリー共に食いそうなので計算しなかった.) よって命題 2.4 より

命題 4.3. $k = \mathbb{Q}(\sqrt{m})$ $(m = 29, 33, 69)$ とする. 楕円曲線 E が k 上至る所 good reduction を持ち, その判別式が k の 3 乗数でなければ, E は k 上定義された 3-isogeny $f : E \to \bar{E}$ を許し, E か $\bar{E}$ のいずれかが位数 3 の k-有理点を持つ. □

従って命題 4.2, 4.3 を考慮すると, $k = \mathbb{Q}(\sqrt{m})$ $(m = 29, 33, 69)$ 上至る所 good reduction を持つ楕円曲線を決めるには, 位数 3 の k-有理点を持つ楕円曲線で判別式が k の 3 乗数でないものを決めればよい. $m = 29$ の時は, そのような曲線は 29A1, 29A1′ の二つだけであることが [20] で証明されている. $m = 33, 69$ の時はないことがわかる (cf. [12]). よって

定理 4.4. (1) $\mathbb{Q}(\sqrt{29})$ 上至る所 good reduction を持つ楕円曲線は 29A1, 29A1′, 29A2, 29A2′ の 4 本だけである.

(2) $\mathbb{Q}(\sqrt{33})$ 上至る所 good reduction を持つ楕円曲線は 33A1, 33A1′, 33A2, 33A2′, 33A3, 33A3′ の 6 本だけである.

(3) $\mathbb{Q}(\sqrt{69})$ 上至る所 good reduction を持つ楕円曲線は存在しない. □

$\mathbb{Q}(\sqrt{29})$ の場合は [11] も見ていただけると幸いである.

5 $m = 53, 89$ の場合

m を前節の最初に挙げた m のうち $m \neq 29, 33, 69$ なるものとする. この時命題 2.5 の仮定を確かめる.

既述のように, $k = \mathbb{Q}(\sqrt{m})$, $1 < m < 100$, $(h_k, 6) = 1$ なら $h_k = 1$ である. よって (1), (2) は $57, 93$ 以外の m に対しては成立している. $k(\sqrt{-3})$, $k(\sqrt[3]{\varepsilon})$ の類数を計算すれば表 2 のようになる ($k(\sqrt[3]{\varepsilon})$ の類数は数秒で求まる).

m	$k(\sqrt{-3})$	$k(\sqrt[3]{\varepsilon})$	m	$k(\sqrt{-3})$	$k(\sqrt[3]{\varepsilon})$
11	2	1	59	2	1
19	2	1	61	4	1
22	4	1	62	**6**	1
23	4	1	67	**6**	1
31	2	1	71	4	**2**
37	4	1	77	**6**	1
38	4	1	83	**6**	1
43	**6**	1	86	4	1
46	4	1	89	1	1
53	5	1			

表 2: 類数

注. 条件 (3) は $\mathbb{Q}(\sqrt{-3m})$ の類数が 3 で割れないことと同値であり (cf. [17], [18]), このことを使えば計算量を減らすことが出来る.

よって (3), (4) を満たす m は

$$m = 11, 19, 22, 23, 31, 37, 38, 46, 53, 59, 61, 86, 89$$

である. (5) も容易に確認できる: KASH は素数の素 ideal 分解, ideal が単項かどうか, 数が ideal に含まれるかどうか等を確認できるので, ちょっとしたプログラムを書けばよい. しかし (5) の確認くらいは手でも大したことないので, やってしまおう (表 3, 4). $3 = \mathfrak{p}\mathfrak{p}'$ $(\mathfrak{p} \neq \mathfrak{p}')$ の時は, $(\mathcal{O}_k/\mathfrak{p}^2)^\times \cong (\mathbb{Z}/9\mathbb{Z})^\times$ なので, この場合 (5) は $\varepsilon \not\equiv \pm 1 \pmod{\mathfrak{p}^2}$ と同値であることに注意.

m	$\mathfrak{p}$	ε	$\varepsilon \bmod \mathfrak{p}^2$
19	$(4+\sqrt{19})$	$170+39\sqrt{19}$	-4
22	$(5+\sqrt{22})$	$197+42\sqrt{22}$	-4
31	$(11+2\sqrt{31})$	$1520+273\sqrt{31}$	-4
37	$(3+\omega)$	$5+2\omega$	-4
46	$(7+\sqrt{46})$	$24335+3588\sqrt{46}$	2
61	$(3+\omega)$	$17+5\omega$	-4

表 3: $\varepsilon \bmod \mathfrak{p}^2$ $(3 = \mathfrak{p}\mathfrak{p}')$

m	$(\mathcal{O}_k/9\mathcal{O}_k)^{\times 3}$	ε	$\varepsilon \bmod 9$
11	$\pm 1, \pm 2\sqrt{11}, \pm(2 \pm 4\sqrt{11})$	$10+3\sqrt{11}$	$1+3\sqrt{11}$
23	$\pm 1, \pm 4\sqrt{23}, \pm(2 \pm \sqrt{23})$	$24+5\sqrt{23}$	$-3-4\sqrt{23}$
38	$\pm 1, \pm 2\sqrt{38}, \pm(2 \pm 4\sqrt{38})$	$37+6\sqrt{38}$	$1-3\sqrt{38}$
53	$\pm 1, \pm 4\omega, \pm(4-4\omega), \pm(1-2\omega)$	$3+\omega$	$3+\omega$
59	$\pm 1, \pm 4\sqrt{59}, \pm(2 \pm \sqrt{59})$	$530+69\sqrt{59}$	$-1-3\sqrt{59}$
86	$\pm 1, \pm 4\sqrt{86}, \pm(2 \pm \sqrt{86})$	$10405+1122\sqrt{86}$	$1-3\sqrt{86}$
89	$\pm 1, \pm(4-4\omega), \pm(1-2\omega), \pm 4\omega$	$447+106\omega$	$-3-2\omega$

表 4: $\varepsilon \bmod 9$ (3 が k で惰性している時)

結局上の 13 個の m は仮定 (1) から (5) を全て満たすので, 次が証明された:

命題 5.1. $m = 11, 19, 22, 23, 31, 37, 38, 46, 53, 59, 61, 86, 89$ の時, $k = \mathbb{Q}(\sqrt{m})$ 上至る所 good reduction を持つ楕円曲線の判別式は k の 3 乗数である. □

$m = 53, 89$ の場合は容易に片付く.

定理 5.2. $\mathbb{Q}(\sqrt{m})$ $(m = 53, 89)$ 上至る所 good reduction を持つ楕円曲線は存在しない.

証明. 命題 4.2, 5.1 より明らかである. □

6 $m = 37$ の場合

$k = \mathbb{Q}(\sqrt{37})$ の場合は [14] において, k 上至る所 good reduction を持ち, しかも j-invariant が有理整数である曲線が決定されている. 条件 "$j \in \mathbb{Z}$" を除きたいので, $\mathbb{Q}(\sqrt{11})$ などよりもあえて $\mathbb{Q}(\sqrt{37})$ を優先した. 他の体に対しては, また別所で発表するつもりである.

E を k 上至る所 good reduction を持つ楕円曲線とする. 補題 2.6, 命題 5.1 と変数変換の公式から $\Delta(E) = \pm\varepsilon^{3n}$ $(-2 \leq n < 2)$ としてよい. $c_4(E)^3 - c_6(E)^2 = 1728\Delta(E)$ だから, $(c_4(E), c_6(E))$ は $E^{\pm}_{3n} : y^2 = x^3 \pm 1728\varepsilon^{3n}$ の $\mathcal{O}_k$-整数点の集合 $E^{\pm}_{3n}(\mathcal{O}_k)$ に含まれる. 前に述べたように, $\Delta(E)$ の符号, n の偶奇は現時点ではわからないから, $E^{\pm}_{3n}(\mathcal{O}_k)$ $(-2 \leq n < 2)$ を全て決める. しかし一対一対応

$$E^{\pm}_{3n}(\mathcal{O}_k) \to E^{\pm}_{3n+6}(\mathcal{O}_k), \quad (x, y) \mapsto (x\varepsilon^2, y\varepsilon^3),$$
$$E^{+}_{3}(\mathcal{O}_k) \to E^{-}_{3}(\mathcal{O}_k), \qquad (x, y) \mapsto (x'\varepsilon^2, y'\varepsilon^3)$$

があるので, $E^{+}_{0}(\mathcal{O}_k)$, $E^{-}_{0}(\mathcal{O}_k)$, $E^{+}_{3}(\mathcal{O}_k)$ の三つだけ決めれば十分である.

命題 6.1. $E^{+}_{0}(O_k) = \big\{(-12, 0)\big\}$.

これは $\operatorname{rank} E^{+}_{0}(k) = \operatorname{rank}(E^{+}_{0})^{(37)}(\mathbb{Q})$ が 0 であることを示せばよい. ここに

$$(E^{+}_{0})^{(37)} : 37y^2 = x^3 + 1728.$$

$\mathbb{Q}$ 上定義された楕円曲線の $\mathbb{Q}$ 上の rank は, 2-descent で大抵の場合求めることができる (cf. [5], [26], [27]). しかし $(E^{+}_{0})^{(37)}$ の場合は, Tate–Shafarevich 群の (予想される) 位数が 4 であるから, 2-descent で rank を求めるのは大変である. しかし $(E^{+}_{0})^{(37)}$ が虚数乗法を持っていて $L((E^{+}_{0})^{(37)}/\mathbb{Q}, 1) = 3.1941\ldots$ であるから, $\operatorname{rank} E^{+}_{0}(k) = 0$ が Coates–Wiles [2] の定理より従う.

注. 2-descent は Cremona によるプログラム mrank (rank だけ求まる), mwrank (Mordell-Weil 群の基底も求まる) で実行できる. SIMATH には 2-descent と, Hasse–Weil 予想, Birch–Swinnerton-Dyer 予想を仮定した Manin のアルゴリズム (cf. [7]) による Mordell-Weil 群の基底を求めるプログラムがある.

注. E が導手がそんなに大きくない modular 楕円曲線の場合, rank を求めるにはまず analytic rank (L 関数の $s=1$ での零点の位数) を計算することが有益である. Analytic rank は SIMATH, UPECS などで求められる. SIMATH には若干 bug があり, いくつかの場合 (一番欲しい $(E_0^+)^{(37)}$ の場合を含む) に対し答が返ってこなかった. PARI/GP では $L(E/\mathbb{Q},s)$ は求められるが, $L^{(n)}(E/\mathbb{Q},s)$ $(n\geq 1)$ は求められない.

以下 $\pi=(7+\sqrt{37})/2$ を 3 を割る素元の一つとする.

命題 6.2.

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

証明 (**概略**). $L:=k(\sqrt{3\varepsilon})$ で分解して考えるので, 必要な L の情報を KASH で求めておく:
(a) $\mathcal{O}_L=\mathcal{O}_k\oplus\mathcal{O}_k\sqrt{3\varepsilon}$.
(b) L の基本単数系は ε, $\varepsilon_1:=\varepsilon+2\sqrt{3\varepsilon}$ である. $N_{L/k}(\varepsilon_1)=1$ に注意.
(c) $2,\pi,\pi'$ は L で $(2)=\mathfrak{P}_2^2$, $(\pi)=\mathfrak{P}_3^2$, $(\pi')=\mathfrak{P}_3'^2$ と分解する.
(d) L の類数は 2 である.

これを使うことにより,

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

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

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

が得られる. 一つ目の式の解は $(a,b)=(0,2),(\pm 84,2\varepsilon^{-2})$ のみであり, 二つ目の式から, $y=0,\pm(2074464-438480\sqrt{37})$ が得られる. □

命題 6.3. $E_0^-(\mathcal{O}_k)$ は次の 15 個の元から成る.

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

証明 (**概略**). 今度は $L:=k(\sqrt{-3})$ で考えるので, L の情報をやはり KASH で求めておく:
(a) $\mathcal{O}_L=\mathcal{O}_k\oplus\mathcal{O}_k\zeta$ $(\zeta=(1+\sqrt{-3})/2)$.
(b) $\mathcal{O}_L^\times=\langle\varepsilon\rangle\times\langle\zeta\rangle\cong\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$.
(c) $2,\pi,\pi'$ は L において $(2)=\mathfrak{P}_2\overline{\mathfrak{P}}_2$ $(\mathfrak{P}_2\neq\overline{\mathfrak{P}}_2)$, $(\pi)=\mathfrak{P}_3^2$, $(\pi')=\mathfrak{P}_3'^2$ と分解する.
(d) L の ideal 類群は $\mathfrak{P}_2$ の類に生成される位数 4 の巡回群である.
(e) $\mathfrak{P}_2^4=(1+\omega-3\zeta)$.

これを使えば

$$(\pm y+24\sqrt{-3})=\mathfrak{P}_2^{a_2}\overline{\mathfrak{P}}_2^{\overline{a}_2}\mathfrak{C}^3,\quad y\in\mathcal{O}_k,\ (a_2,\overline{a}_2)=(0,0),(2,1),\ \mathfrak{C}\text{ は }L\text{ の整 ideal}$$

を解けばよいことがわかる.

Case 1: $(a_2,\overline{a}_2)=(0,0)$. L の類数が 3 と素なことから $\mathfrak{C}$ が単項であることがわかり,

$$\pm y+24\sqrt{-3}=\varepsilon^m\zeta^n(a+b\zeta)^3,\ a,b,y\in\mathcal{O}_k,\ m=0,\pm1,\ n=0,1$$

を解けばよいことがわかる. $n=1$ の時は解がないことがわかる.

$n=0$ の時は

$$16=ab(a+b), \tag{1}$$

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

を解くことになる. (1) の解は $(a,b)=(2,2),(2,-4),(-4,2)$ のみであり, (2) よりいずれの場合も $y=0$ であることがわかる.

Case 2:$(a_2,\overline{a}_2)=(2,1)$. 両辺に $(4)=(\mathfrak{P}_2\overline{\mathfrak{P}}_2)^2$ を掛け, (d), (e) を用いれば

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

が得られ, L の類数が 3 と素であることより,

$$4(\pm y+24\sqrt{-3})=\zeta^n(1+\omega-3\zeta)(a+b\zeta)^3,\ a,b,y\in\mathcal{O}_k,\ n=0,\pm1$$

を解けばよいことがわかる.

$n=\pm1$ 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,

$$-64=a^3-(\omega-2)a^2b-(\omega+1)ab^2-b^3, \tag{3}$$

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

が得られ, 後で見るように (3) の解は次の 21 個のみである:

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

これらを (4) 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. □

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.

これで $E_{3n}^{\pm}(\mathcal{O}_k)$ $(-2 \leq n < 2)$ が全て決まった. 即ち k 上至る所 good reduction を持つ楕円曲線の c_4, c_6 の候補が出揃ったわけである. $(x, y) \in E_{3n}^{\pm}(\mathcal{O}_k)$ が k 上至る所 good reduction を持つ楕円曲線の global minimal model の c_4, c_6 に成れることと, $Y^2 = X^3 - 27xX - 54y$ の k 上の導手が (1) であることは同値である. 実際に導手を計算することにより, c_4, c_6 に成れるのは

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

の二つのみであることがわかる. j-invariant を比較すれば, 前者が 37A1 に, 後者が 37A2 に対応することがわかる. よって次が得られた:

定理 6.4. $\mathbb{Q}(\sqrt{37})$ 上至る所 good reduction を持つ楕円曲線は 37A1, 37A2 のみである. □

二次体上の楕円曲線の導手は SIMATH で求まる (最新の version 4.1 にも若干 bug がある). 任意の代数体上の楕円曲線の導手は梅垣氏が PARI/GP で作成したプログラムで求まる (cf. [30]).

7 $\mathbb{Q}(\sqrt{37})$ 上の Thue 方程式

この節では (3) を解く. $k = \mathbb{Q}(\sqrt{37})$ とする.

$a, b \in \mathcal{O}_k$ を (3) の解とする. $A = -a - (\omega + 2)b$ が 4 で割れることと b が 2 で割れることは直ちにわかる. $A = 4X$, $b = 2Y$, $X, Y \in \mathcal{O}_k$ とおくと,

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

が得られる. (5) のような二次体上の Thue 方程式は de Weger が [32] において解いたものが (筆者の知る限り) 唯一である. そこでの証明と同様の方法で次を示す:

命題 7.1. (5) を満たす $(X, Y) \in \mathcal{O}_k \times \mathcal{O}_k$ は以下の 21 個のみである:

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

証明 (概略). $F(X, Y)$ を (5) の左辺, θ を多項式 $F(X, 1)$ の根の一つとし, $L = \mathbb{Q}(\theta)$ とおく. すると $k \subset L$ であり, $[L : \mathbb{Q}] = 6$, $\mathcal{O}_L = \mathbb{Z}[\xi]$ である. ここに $\xi = (12 + 18\theta - 4\theta^3 - \theta^4)/20$. $L/\mathbb{Q}$ は Galois 拡大で, Galois 群は $\langle \sigma, \tau \rangle$,

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

である. σ, τ は $\sigma^3 = 1$, $\tau^2 = 1$, $\sigma\tau = \tau\sigma^2$ を満たす. 即ち $\mathrm{Gal}(L/\mathbb{Q})$ は 3 次対称群である. L の 1 組の基本単数系は次で与えられる:

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

$N_{L/k}(\varepsilon_i) = 1$ $(i = 1, 2, 3, 4)$, $N_{L/k}(\varepsilon_5) = \varepsilon$ がわかる. (KASH を用いて得られた基本単数系を用いてこうなるようにしたのである.)

(5) は $N_{L/k}(X - Y\theta) = 1$ と同値であるから, $\eta := X - Y\theta = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_4^{a_4}$ $(a_1, \ldots, a_4 \in \mathbb{Z})$ である. X, Y を消去して

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

よって

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

これは次と同値である:

$$-\varepsilon_1^{b_1}\varepsilon_2^{b_2}\varepsilon_3^{b_3}\varepsilon_4^{b_4} - 1 = \varepsilon_1^{d_1}\varepsilon_2^{d_2}\varepsilon_3^{d_3}\varepsilon_4^{d_4}. \tag{6}$$

ここに

$$\begin{aligned}
&b_1 = a_1 + 2a_3,\ b_2 = a_2 + 2a_4 - 1,\ b_3 = -2a_1 - a_3 + 1,\ b_4 = -2a_2 - a_4,\\
&d_1 = -b_3,\ d_2 = -b_4,\ d_3 = b_1 + b_3,\ d_4 = b_2 + b_4.
\end{aligned}$$

Thue 方程式を解く時にいつもやるように (cf. [14], [28], [32]), linear forms in the logarithms

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

を評価する. $i_0 \in \{1, \ldots, 6\}$ を $|\eta^{(i_0)}| = \min\limits_{1 \le i \le 6}\{|\eta^{(i)}|\}$ で決める. [32] の議論と同様にして, $B \ge 100$ なら

$$|\Lambda_{i_0}| < 4.1069 \exp(-0.24457B) \tag{7}$$

が成り立つことがわかる. これを得るのに θ, ε_i $(i = 1, 2, 3, 4)$ の共役の近似値を使うが, それは KASH で求められる.

次に, Baker 理論を用いて $|\Lambda_{i_0}|$ の lower bound を求める. [32] の場合と同じく, $i_0 = 1$ として一般性を失わない. [1] の定理より

$$\log|\Lambda_1| > -4.1810 \times 10^{18}\log(B) \tag{8}$$

が得られる. この時に ε_i $(i = 1, 2, 3, 4)$ の height が必要になるが, それも KASH で求められる.

(7), (8) をあわせて, $B \leq 1.5142 \times 10^{21}$ が得られる.

この upper bound は大きすぎるので, 適当な大きさまで下げる必要がある. そのために次の補題 ([28] の Proposition 3.1) を使う

補題 7.2. $\mu_1, \ldots, \mu_n$ を与えられた実数とする. $b_1, \ldots, b_n \in \mathbb{Z}$ を変数とし, $\Lambda = \sum_{i=1}^{n} b_i\mu_i$ とおく. K_1, K_2, K_3 を与えられた正の実数とし, $b_1, \ldots, b_n$ が

$$|\Lambda| < K_1\exp(-K_2B),\ B := \max\Big\{|b_1|, \ldots, |b_n|\Big\} < K_3 \tag{9}$$

を満たすとする. 十分大きな実数 c_0 に対し,

$$\mathcal{A} = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ [c_0\mu_1] & \cdots & [c_0\mu_{n-1}] & [c_0\mu_n] \end{pmatrix}.$$

の列で生成される lattice Γ を考える. ここに

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

即ち $[\cdot]$ は 0 に向かっての切り捨てである. $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ を Γ の LLL-reduced basis とする. もし $|\boldsymbol{b}_1| > \sqrt{(n^2+n-1)2^{n-1}}K_3$ が成り立つならば, (9) の全ての解は

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

を満たす. □

$c_0 = 10^{100}$ とし行列 $\mathcal{A}$ に LLL-reduction algorithm を適用する (ここでは PARI/GP を使った) と,

$$\mathcal{B} = \Big(\boldsymbol{b}_1\ \boldsymbol{b}_2\ \boldsymbol{b}_3\ \boldsymbol{b}_4\Big),$$

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

$$\boldsymbol{b}_3 = \begin{pmatrix} 407267427999956449527312 7 \\ 269244207052729576352184 4 \\ 782025387667325633997448 6 \\ -285101950383064823043109 4 \end{pmatrix},\ \boldsymbol{b}_4 = \begin{pmatrix} -782540284530375014759499 4 \\ -154731239896422989358345 9 \\ -529196120215387679117837 \\ -106205987118553569141892 51 \end{pmatrix}$$

が得られる. $|\boldsymbol{b}_1| = 4.096\cdots\times 10^{24} > \sqrt{(n^2+n-1)2^{n-1}}K_3 = 1.866\times 10^{22}$ であるから, 補題 7.2 より $B \le 719$ がわかる.

$c_0 = 10^{18}$ と取る. 再び $\mathcal{A}$ に LLL-reduction algorithm を適用すると,

$$(\boldsymbol{b}_1\ \boldsymbol{b}_2\ \boldsymbol{b}_3\ \boldsymbol{b}_4) = \begin{pmatrix} -291 & -1300 & 23101 & 13586 \\ 2046 & 2852 & 6305 & -24467 \\ 19892 & 7913 & 5062 & -1315 \\ 285 & -18603 & -7284 & -5310 \end{pmatrix}.$$

$|\boldsymbol{b}_1| = 2.000\cdots\times 10^4 > \sqrt{(n^2+n-1)2^{n-1}}K_3 = 8.874\times 10^3$, であるから, $B \le 141$ が得られる.

残っているのは, $B \le 141$ の範囲で (6) の解を探すことである. 正直にやると時間がかかるので, [32] と同様の工夫をする. そうすれば, C 言語で書いた program を Sparc station SS4 で走らせれば, 全 21 個の解が 15 分で見つかる. 各解 (a_1,a_2,a_3,a_4) に対し, $\varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_4^{a_4}$ が $X - Y\theta$ の形をしていることがやはり KASH で確かめられる (KASH は relative extension も扱えるのである). 全ての解は次の表の通りである:

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	$-8+\omega$	$-2+\omega$

表 5: (5), (6) の全ての解

8 Appendix 1: Free-ware

本文中に出てきた free-ware は, その後に書いた URL から入手可能.

KASH	ftp://math.tu-berlin.de/pub/algebra/Kant/Kash
mrank, mwrank	ftp://euclid.ex.ac.uk/pub/cremona
PARI/GP	ftp://megrez.math.u-bordeaux.fr/pub/pari
SIMATH	ftp://ftp.math.uni-sb.de/pub/simath
Upecs	ftp://math.mcgill.ca/pub/upecs

Upecs は memory 640KB のパソコンでも動くので, 出来ることは限られているが, つい最近まで 10 年以上前のパソコンを使っていた筆者にとっては重宝であった.

9 Appendix 2: Table

ここでは $k = \mathbb{Q}(\sqrt{m})$ $(m = 6, 7, 14, 29, 33, 37, 41, 65)$ 上至る所 good reduction を持つ全楕円曲線の表を与える. k-isogeny classes にも分けてある. 表には各曲線のデータが次のように与えられている:

(1) mXi の形の code. m は曲線が $k = \mathbb{Q}(\sqrt{m})$ 上定義されていることを意味する. $X = A, B$ は k-isogeny class を表す. (isogeny class が二つあるのは $m = 65$ の時だけだが.) i は単なる順番である. $m = 6, 7, 14, 41, 65$ の時は, Comalada [3] の code も書いておいた.
(2) 定義方程式の係数 a_1, a_2, a_3, a_4, a_6.
(3) 判別式.
(4) j-invariant.
(5) Torsion subgroup の構造. C_n は位数 n の巡回群のこととする.
(6) Isogeny graph. k 上定義された楕円曲線 E, $\bar{E}$, 及び素数 p に対し,

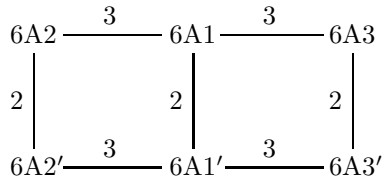
$$E \overset{p}{\text{---}} \bar{E}$$

は E と $\bar{E}$ が k 上 p-isogenous であることを意味する.

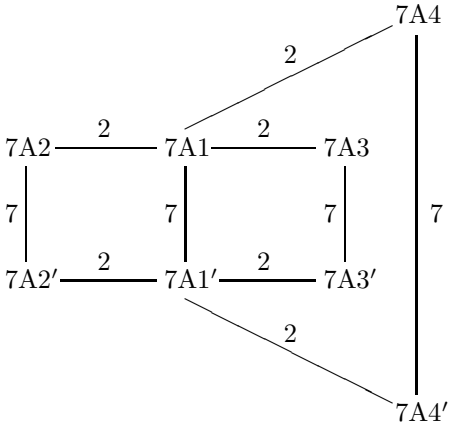
Torsion subgroup の構造は, $E(k)_{\text{tors}}$ から good prime $\mathfrak{p}$ での reduction の $\mathcal{O}_k/\mathfrak{p}$-有理点の群 $E_{\mathfrak{p}}(\mathcal{O}_k/\mathfrak{p})$ への単射準同型があることを用いればある程度しぼれる. しかし同じ k-isogeny class に属する E, $\bar{E}$ に対しては, $E_{\mathfrak{p}}(\mathcal{O}_k/\mathfrak{p}) = \bar{E}_{\mathfrak{p}}(\mathcal{O}_k/\mathfrak{p})$ が全ての good prime $\mathfrak{p}$ に対して成り立つので, これだけではだめである. 最終結果を出すには, n 等分多項式 ψ_n の k での分解を用いる, [19] の表 (二次体 k 上定義された楕円曲線 E で, $j(E) \in \mathcal{O}_k$ であり $E(k)_{\text{tors}}$ が $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ でないものは有限個しかなく, その表が与えられている) の中から導手 (1) のものを見つけだすなどすればよい.

k-isogeny class に分けるには, torsion point を求める, ψ_n の分解を求める, などをしたのち Vélu の公式 ([31]) を使えばよい. そうはいっても ψ_7, ψ_{11} などの分解は時間がかかるので, $\mathbb{Q}$-curve に関する結果 ([8]) を使う, $j \in \mathbb{Z}$ の時は [5] の表の曲線の twist になっているかどうか確かめる, などをする. この方法により, 表中の 7-isogeny と 11-isogeny の存在を確かめた.

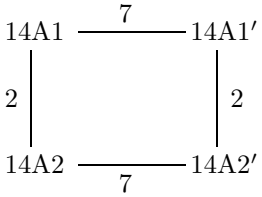
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
6A1 (E_1)	$\sqrt{6}$	$-2-\sqrt{6}$	-1	0	0	ε^3	8000	C_6
6A1′ (E_2)	$-\sqrt{6}$	$-2+\sqrt{6}$	-1	0	0	ε'^3	8000	C_6
6A2 (E_3)	$\sqrt{6}$	$1-\sqrt{6}$	$1+\sqrt{6}$	$9-34\varepsilon$	$-1122-459\sqrt{6}$	ε	$64(4\varepsilon^4+1)^3\varepsilon'^4$	C_2
6A2′ (E_4)	$-\sqrt{6}$	$1+\sqrt{6}$	$1-\sqrt{6}$	$9-34\varepsilon'$	$-1122+459\sqrt{6}$	ε'	$64(4\varepsilon'^4+1)^3\varepsilon^4$	C_2
6A3 (E_5)	$\sqrt{6}$	$2+\varepsilon'$	$3-\sqrt{6}$	$-7+3\sqrt{6}$	0	ε'^5	$64(4\varepsilon^4+1)^3\varepsilon'^4$	C_6
6A3′ (E_6)	$-\sqrt{6}$	$2+\varepsilon$	$3+\sqrt{6}$	$-7-3\sqrt{6}$	0	ε^5	$64(4\varepsilon'^4+1)^3\varepsilon^4$	C_6



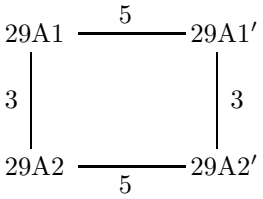
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
7A1 (E_7)	1	4ε	0	ε	0	ε^6	255^3	$C_2\times C_2$
7A1′ (E_8)	1	$4\varepsilon'$	0	ε'	0	ε'^6	255^3	$C_2\times C_2$
7A2 (E_9)	1	4ε	0	$6\varepsilon-80\varepsilon^2$	$-3044+48513\varepsilon$	ε^3	$(256\varepsilon^2+\varepsilon')^3$	C_4
7A2′ (E_{10})	1	$4\varepsilon'$	0	$6\varepsilon'-80\varepsilon'^2$	$-3044+48513\varepsilon'$	ε^{-3}	$(256\varepsilon'^2+\varepsilon)^3$	C_4
7A3 (E_{14})	ε'	$-2\varepsilon'$	0	ε'^2	0	$-\varepsilon'^6$	-15^3	C_4
7A3′ (E_{13})	ε	-2ε	0	ε^2	0	$-\varepsilon^6$	-15^3	C_4
7A4 (E_{12})	1	4ε	0	-4ε	$-\varepsilon^3-2\varepsilon$	ε'^9	$(256\varepsilon'^2+\varepsilon)^3$	C_2
7A4′ (E_{11})	1	$4\varepsilon'$	0	$-4\varepsilon'$	$-\varepsilon'^3-2\varepsilon'$	ε^9	$(256\varepsilon^2+\varepsilon')^3$	C_2



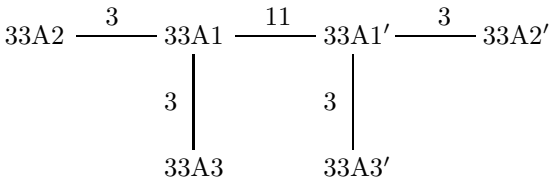
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
14A1 (E_{15})	$1+\sqrt{14}$	$-9-2\sqrt{14}$	0	ε	0	$-\varepsilon^3$	-15^3	C_2
14A1′ (E_{16})	$1-\sqrt{14}$	$-9+2\sqrt{14}$	0	ε'	0	$-\varepsilon'^3$	-15^3	C_2
14A2 (E_{17})	$1+\sqrt{14}$	$-9-2\sqrt{14}$	0	-4ε	$651+174\sqrt{14}$	ε^3	255^3	C_2
14A2′ (E_{18})	$1-\sqrt{14}$	$-9+2\sqrt{14}$	0	$-4\varepsilon'$	$651-174\sqrt{14}$	ε'^3	255^3	C_2



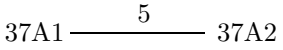
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
29A1	1	0	ε^2	0	0	$-\varepsilon^{10}$	$(5\varepsilon-2)^3\varepsilon'^4$	C_3
29A1′	1	0	ε^{-2}	0	0	$-\varepsilon'^{10}$	$(5\varepsilon'-2)^3\varepsilon^4$	C_3
29A2	1	0	ε^2	$-5\varepsilon^2$	$-(\varepsilon^2+7\varepsilon^4)$	$-\varepsilon^{14}$	$-(1+216\varepsilon^2)^3\varepsilon'^{14}$	1
29A2′	1	0	ε'^2	$-5\varepsilon'^2$	$-(\varepsilon'^2+7\varepsilon'^4)$	$-\varepsilon'^{14}$	$-(1+216\varepsilon'^2)^3\varepsilon^{14}$	1



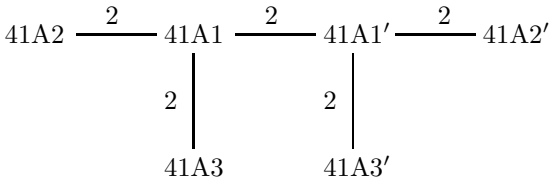
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
33A1	$(\varepsilon-3)/4$	0	ε	0	0	$-\varepsilon^3$	-2^{15}	C_3
33A1′	$(\varepsilon'-3)/4$	0	ε'	0	0	$-\varepsilon'^3$	-2^{15}	C_3
33A2	$(\varepsilon-3)/4$	0	ε	$(5-215\varepsilon)/4$	$34-1563\varepsilon$	$-\varepsilon$	$-(5+\sqrt{33})^3(243\varepsilon-1)^3\varepsilon'$	1
33A2′	$(\varepsilon'-3)/4$	0	ε'	$(5-215\varepsilon')/4$	$34-1563\varepsilon'$	$-\varepsilon'$	$-(5-\sqrt{33})^3(243\varepsilon'-1)^3\varepsilon$	1
33A3	$(\varepsilon-3)/4$	0	ε	$(15\varepsilon-5)/4$	$(127\varepsilon-1)/4$	$-\varepsilon^5$	$-(5-\sqrt{33})^3(243\varepsilon'-1)^3\varepsilon$	1
33A3′	$(\varepsilon'-3)/4$	0	ε'	$(15\varepsilon'-5)/4$	$(127\varepsilon'-1)/4$	$-\varepsilon'^5$	$-(5+\sqrt{33})^3(243\varepsilon-1)^3\varepsilon'$	1



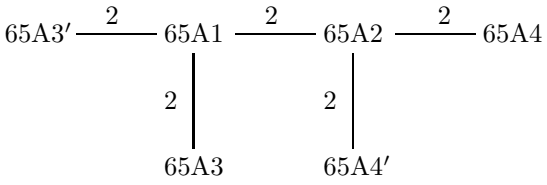
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
37A1	0	$(3\varepsilon+1)/2$	$-\varepsilon$	$(11\varepsilon+1)/2$	0	ε^6	2^{12}	C_5
37A2	0	$(3\varepsilon+1)/2$	$-\varepsilon$	$-(1669\varepsilon+139)/2$	$-7(5449\varepsilon+451)$	ε^6	3376^3	1



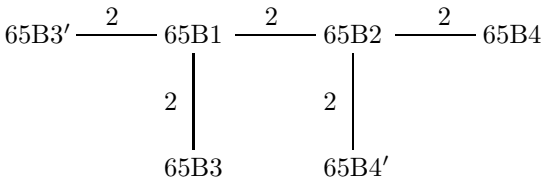
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
41A1 (E_{23})	1	0	0	$-\varepsilon$	0	ε^4	$-(\varepsilon-16)^3\varepsilon'$	$C_2\times C_2$
41A1′ (E_{24})	1	0	0	$-\varepsilon'$	0	ε'^4	$-(\varepsilon'-16)^3\varepsilon$	$C_2\times C_2$
41A2 (E_{26})	1	$(7-\sqrt{41})/2$	$(7-\sqrt{41})/2$	$6-\sqrt{41}$	0	$-\varepsilon'$	$17^3\varepsilon$	C_4
41A2′ (E_{25})	1	$(7+\sqrt{41})/2$	$(7+\sqrt{41})/2$	$6+\sqrt{41}$	0	$-\varepsilon$	$17^3\varepsilon'$	C_4
41A3 (E_{28})	1	0	0	4ε	ε	$-\varepsilon^5$	$-(256\varepsilon'+1)^3\varepsilon$	C_2
41A3′ (E_{27})	1	0	0	$4\varepsilon'$	ε'	$-\varepsilon'^5$	$-(256\varepsilon+1)^3\varepsilon'$	C_2



Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
65A1 (E_{29})	1	-4ε	0	$-\varepsilon$	0	ε^6	257^3	$C_2 \times C_2$
65A2 (E_{31})	1	2ε	0	ε^2	0	ε^6	17^3	$C_4 \times C_2$
65A3 (E_{38})	1	-4ε	0	4ε	$2\varepsilon - \varepsilon^3$	ε'^3	$(256\varepsilon'^2 - \varepsilon)^3$	C_2
65A3′ (E_{37})	1	$-4\varepsilon'$	0	$4\varepsilon'$	$2\varepsilon' - \varepsilon'^3$	ε^3	$(256\varepsilon^2 - \varepsilon')^3$	C_2
65A4 (E_{35})	1	$-\omega$	ω	$6 + 4\varepsilon$	$-(431 + 53\sqrt{65})/2$	$-5^6\varepsilon^3$	$(8 + \varepsilon')^3$	C_4
65A4′ (E_{36})	1	$-\omega'$	ω'	$6 + 4\varepsilon'$	$-(431 - 53\sqrt{65})/2$	$-5^6\varepsilon'^3$	$(8 + \varepsilon)^3$	C_4



Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
65B1 (E_{30})	1	$1 - 20\varepsilon$	0	-25ε	0	$(5\varepsilon)^6$	257^3	$C_2 \times C_2$
65B2 (E_{32})	1	$1 + 10\varepsilon$	0	$25\varepsilon^2$	0	$(5\varepsilon)^6$	17^3	$C_2 \times C_2$
65B3 (E_{40})	1	$1 - 20\varepsilon$	0	100ε	$-125(2\varepsilon - \varepsilon^3)$	$-5^6\varepsilon^9$	$(256\varepsilon'^2 - \varepsilon)^3$	C_2
65B3′ (E_{39})	1	$1 - 20\varepsilon'$	0	$100\varepsilon'$	$-125(2\varepsilon' - \varepsilon'^3)$	$-5^6\varepsilon'^9$	$(256\varepsilon^2 - \varepsilon')^3$	C_2
65B4 (E_{33})	1	$1 + \omega$	ω	$7 + \omega$	ω	$-\varepsilon^3$	$(8 + \varepsilon')^3$	C_2
65B4′ (E_{34})	1	$1 + \omega'$	ω'	$7 + \omega'$	ω'	$-\varepsilon'^3$	$(8 + \varepsilon)^3$	C_2



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), 233–258.

[4] J. E. Cremona, Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction, *Math. Proc. Cambridge Phil. Soc.* **111** (1992), 199–218.

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

[6] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig and K. Wildanger, KANT V4, *J. Symbolic Computation* **24** (1997), 267–283.

[7] J. Gebel and H. G. Zimmer, Computing the Mordell–Weil group of an elliptic curve over $\mathbb{Q}$, in *Elliptic Curves and Related Topics*, H. Kisilevsky and M. Ram Murty (eds.), CRM Proceedings and Lecture Notes, Amer. Math. Soc., Providence, RI, 1994, 61–83.

[8] Y. Hasegawa, $\mathbb{Q}$-curves over quadratic fields, *Manuscripta Math.* **94** (1997), 347–364.

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

[10] T. Kagawa, Determination of elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{37})$, *Acta. Arith.*, to appear.

[11] ———, Determination of elliptic curves with everywhere good reduction over real quadratic fields, *submitted*.

[12] ———, Determination of elliptic curves with everywhere good reduction over real quadratic fields, II, *preprint*.

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

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

[15] ———, Reduction of elliptic curves over real quadratic number fields, *preprint*.

[16] 木田 雅成「実二次体上で定義された楕円曲線の reduction について」, 研究集会報告集 VIII –整数論–, 早大理工総研 (1997), 103–107.

[17] T. Kubota, Über den bizyklischen biquadratischen Zahlkörper, *Nagoya J. Math.* **10** (1956), 65–85.

[18] J. M. Masley, Solution of small class number problems for cyclotomic fields, *Compositio Math.* **33** (1976), 179–186.

[19] H. H. Müller, H. Ströher and H. G. Zimmer, Torsion groups of elliptic curves with integral j-invariant over quadratic fields, *J. Reine angew. Math.* **397** (1989), 100–161.

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

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

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

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

[24] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan, no. 11, Iwanami Shoten, Publishers and Princeton University Press, 1971.

[25] K. Shiota, On the explicit models of Shimura's elliptic curves, *J. Math. Soc. Japan* **38** (1986), 649–659.

[26] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer, 1986.

[27] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, UTM, Springer, 1992.

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

[29] A. Umegaki, A construction of everywhere good $\mathbb{Q}$-curves with p-isogeny, *preprint*.

[30] 梅垣敦紀「代数体上の楕円曲線の計算」, 本集会.

[31] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sc. Paris* **273** (1971), 238–241.

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

加川 貴章 (Takaaki KAGAWA)
〒 169–8555 早稲田大学理工学部情報学科
E-mail: kagawa@mn.waseda.ac.jp