二次体上至る所good reductionを持つ楕円曲線について

横山 俊一 (九州大学)

概 要

実二次体および虚二次体上至る所good reductionを持つ楕円曲線の存在 (とその決定), 非存在については多くの先行結果がある. 今回同様の新しい結果を主に実二次体上の場合について得たので報告する.

本研究は大部分が島崎有氏 (九大数理) との共同研究であって, その成果は [21] に纏められているので, 興味を持たれた方はこちらも参照頂きたい. なお, 本研究はこの方面の仕事で先駆的な結果を残されている加川貴章氏 (立命館大) の影響を大きく受けており, 日常的に数多くの助言を頂いている. この場を借りて厚く感謝御礼申し上げたい.

本記事は2011年8月に開催された「第6回福岡数論研究集会」における筆者の講演原稿に修正・加筆を加えたものである. 今回, このような素晴らしい講演の機会を与えて下さった金子昌信先生 (九大数理), 権寧魯先生 (九大数理), そして講演のお誘いを下さった岸康弘先生 (愛知教育大) に, 重ねて厚く感謝御礼申し上げたい.

1 先行結果

まず今までに知られている結果 ([2], [4], [5], [6], [7], [9], [11], [12], [13], [14], [15], [19] and Cremona's table [3]) を述べる. 本稿を通じて K_m は実二次体 $\mathbb{Q}(\sqrt{m})$ (m は square-free) とし, 4章までは $1 < m < 100$ の範囲に限定して考える. また ε を基本単数とする.

定理 1.1. (1) $m = 2, 3, 5, 10, 11, 13, 15, 17, 19, 21, 23, 30, 31, 34, 35, 39, 42, 47, 53, 55, 57, 58, 61, 66, 69, 70, 73, 74, 78, 82, 83, 85, 89, 93, 94, 95, 97$ のとき, K_m 上至る所good reductionを持つ楕円曲線は存在しない.
(2) $m = 6, 7, 14, 22, 29, 33, 37, 38, 41, 65, 77$ のとき, K_m 上至る所good reductionを持つ楕円曲線は全て決定されている.
(3) $m = 26, 79, 86$ のとき, K_m 上至る所good reductionを持つ楕円曲線が発見されている (これで全部か否かは証明されていない).

更に Comalada [1] は $1 < m < 100$ の全ての m に対して admissible な楕円曲線 (=至る所good reductionを持ち位数2の有理点を持つもの) を決定している.

ここからは定理1.1で解決されていない実二次体で**類数が1**のものに限って考え, かつ admissibleでないものに限定する. まず主定理を述べる:

定理 1.2. $m = 43, 46, 59$ のとき K_m 上至る所good reductionを持つ楕円曲線は存在しない.

また, 部分的に解決をみたものもある:

定理 1.3. $m = 62, 67, 71$ のとき K_m 上至る所good reductionを持つ楕円曲線で判別式が3乗数となるようなものは存在しない.

今回の結果により, 未解決なケースは (部分的に解決されたものを除いて) $m = 51, 87, 91$ の3つとなった. これら3つは全て類数2であり, 後述の通り今回の方針は適用出来ない. 以降, **証明の流れと計算結果 (2章, 3章)**, **計算時間の比較 (4章)**, **幾つかの拡張 (5章)** に分けて述べる.

2 証明の流れ

まず Setzer の定理 [16] から出発する.

命題 2.1 (Setzer [16]). E を K_m 上の楕円曲線とする. K_m の類数が 6 と素であれば E は global minimal model を持つ.

以降 E は K_m 上至る所 good reduction を持つ楕円曲線とする. このとき E の global minimal model は

$$E:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

と書ける ($a_i \in \mathcal{O}_{K_m}$ $(i = 1, 2, 3, 4, 6)$). この判別式 $\Delta(E)$ は

$$\Delta(E) = \frac{c_4^3 - c_6^2}{1728}$$

と $c_4, c_6 \in \mathcal{O}_{K_m}$ を用いて表される. この 2 つの値は a_i たちの $\mathbb{Z}$-係数多項式表示で与えられることに注意されたい. ここで次の 2 条件が同値であることを使う:

- E は K_m 上至る所 good reduction を持つ,
- $\Delta(E) \in \mathcal{O}_{K_m}^{\times}$.

二次体の一般論より, $\mathcal{O}_{K_m}^{\times}$ の元は全て K_m の基本単数 ε を用いて $\pm\varepsilon^n$ の形で表される (以降, K_m を一つとるごとに ε を固定して考える). 従って $c_4, c_6 \in \mathcal{O}_{K_m}$ の候補は全て

$$E_n^{\pm}(\mathcal{O}_{K_m}) = \left\{(x, y) \in \mathcal{O}_{K_m} \times \mathcal{O}_{K_m} \mid\ y^2 = x^3 \pm 1728\varepsilon^n\right\},\quad 0 \leq n < 12$$

に含まれることが分かり, このような整数点の集合を決定する問題に帰着される. しかしながら $(c_4, c_6) \in \mathcal{O}_{K_m}^{\oplus 2}$ が見つかったとしても, 元の $(a_1, a_2, a_3, a_4, a_6) \in \mathcal{O}_{K_m}^{\oplus 5}$ が見つかるかどうかは分からない. そのため E と K_m 上同型な楕円曲線

$$E_C:\ y^2 = x^3 - 27c_4x - 54c_6, \tag{1}$$

の導手を計算し, これが自明かどうかを見ることで E が本当に至る所 good reduction を持つかどうかを判定する.

しかし, 24 個の $E_n^{\pm}(\mathcal{O}_{K_m})$ 全てを計算するのは計算機の制約上現実的ではない. そこで幾つかの補題を使って絞り込みをかける. ここでは加川氏 [8] による 2 つの補題を紹介する.

補題 2.2. 次の 5 つの条件を全て満たすならば, K_m 上至る所 good reduction を持つ楕円曲線の判別式は必ず K_m の 3 乗数となる:

1. K_m の類数は 6 と素.
2. 3 は K_m 上不分岐.
3. $K_m(\sqrt{-3})$ の類数は 3 で割れない.
4. $K_m(\sqrt[3]{\varepsilon})$ の類数は 2 で割れない.
5. 3 を割る K_m の素イデアル $\mathfrak{p}$ に対し, $X^3 \equiv \varepsilon \pmod{\mathfrak{p}^3}$ は解 $X \in \mathcal{O}_{K_m}$ を持たない.

補題 2.3. K_m を実二次体, E を K_m 上定義された楕円曲線とする. E が 2 の外で至る所 good reduction を持ち, 更に位数 2 の K_m-有理点を持たなければ, $K_m(E[2])/K_m(\sqrt{\Delta(E)})$ は 2 の外不分岐な巡回 3 次拡大となる. 特に $K_m(\sqrt{\Delta(E)})$ の ray class number mod $\prod_{\mathfrak{p}|2}\mathfrak{p}$ は 3 で割り切れる.

3 計算結果

計算の方針は [9] とほぼ同様である．今回の結果はこれまで $E_n^{\pm}(K_m)$ の height や canonical height が大きく, 計算機的制限から攻略されていなかったものである．計算の流れは大まかには次の 5 ステップに分類される．

1. 計算すべき $E_n^{\pm}$ を決定する．
2. 捩れ部分 $E_n^{\pm}(K_m)_{tors}$ を計算する．
3. 自由部分 $E_n^{\pm}(K_m)_{free}$ を計算する．
4. 整数点の集合 $E_n^{\pm}(\mathcal{O}_{K_m})$ を決定する．
5. (c_4, c_6) の候補に対し E_C が自明な導手を持つかどうか調べる．

1. は先ほどの 2 補題から従う (= 3 乗数の条件を確認し, ray class number が 3 で割り切れるものを抜き出す．例えば $K = K_m(\sqrt{-1})$ は E_0^+ に対応する)．2. は good prime での reduction と等分多項式の分解を見ることで決定され, これについては既に [10] で結果が得られている．3. は infinite descent の適用, 即ち $E_n^{\pm}(K_m)/2E_n^{\pm}(K_m)$ から $E_n^{\pm}(K_m)$ を復元することで計算出来る．rank の評価等は 2-descent 法による．そして elliptic logarithm による評価によって, 整数点を 2. および 3. の生成元の一次結合 (整数係数) で表したときの係数への bound を与え, LLL-reduced algorithm[1]でその bound を極力下げて 4. が実現される．最後の 5. は先述の通りである．

3.1 $m = 46, 59$ の場合

この場合は補題 2.2 の 5 条件を全て満たしている．計算結果は次の通り:

命題 3.1. 2-descent 法により次が成り立つ．
(1) $m = 46$ のとき, (c_4, c_6) の候補は $E_3^+(\mathcal{O}_{K_{46}})$ にのみ存在する． E_3^+ の Mordell-Weil 群 $E_3^+(K_{46})$ は $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ に同型であり

- 捩れ部分の生成元は $T = (-12\varepsilon, 0)$ $(\varepsilon = 24335 + 3588\sqrt{46})$
- 自由部分の生成元は
$$P = \left(\frac{1044823225}{6084} + \frac{987505}{39}\sqrt{46}, \frac{116177050458217}{474552} + \frac{73202442649}{2028}\sqrt{46}\right)$$

である．
(2) $m = 59$ のとき, (c_4, c_6) の候補は $E_0^+(\mathcal{O}_{K_{59}})$ または $E_3^-(\mathcal{O}_{K_{59}})$ にのみ存在する．$E_0^+(K_{59})$ および $E_3^-(K_{59})$ はそれぞれ $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/2\mathbb{Z}$ に同型であり

- E_0^+ の捩れ部分の生成元は $T = (-12, 0)$
- E_0^+ の自由部分の生成元は $P = \left(-\frac{133}{16}, \frac{283}{64}\sqrt{59}\right)$
- E_3^- の捩れ部分の生成元は $T = (12\varepsilon, 0)$ $(\varepsilon = -530 + 69\sqrt{59})$

[1] Lenstra-Lenstra-Lovász による．格子基底の reduction アルゴリズムとして良く知られている．

- E_3^- の自由部分の生成元は

$$P_1 = \left(9275 - \frac{2415}{2}\sqrt{59}, -\frac{5810733}{4} + \frac{756493}{4}\sqrt{59}\right)$$

$$P_2 = \left(\frac{50000200}{59} - \frac{6509460}{59}\sqrt{59}, \frac{65094772968}{59} - \frac{500002437752}{3481}\sqrt{59}\right)$$

である．

実際の計算では D. Simon による Pari/GP プログラム (通称 "Simon's 2-descent" と呼ばれている) を用いた．最新版は 2011 年 4 月 6 日付けで update されたものであり, 実はそれ以前のバージョンにはバグが存在する．今回のように $E_0^\pm$ や $E_3^\pm$ の計算だけであれば問題はないが, 代数体によっては $E_1^\pm$ や $E_2^\pm$ の計算をやろうとすると debug error を返して来るため計算が出来ない．W. Stein らによって開発が進んでいる統合ソフトウェア Sage でも Simon's 2-descent が使えるが, 以前のバージョンのものが収録されているため注意が必要である[2].

更に付け加えると, 上述の Pari/GP プログラムをデフォルトのまま実行しても, 上の命題のような生成元 (の一部) は得られない．探せる点の height には bound が定められているため, GP code を手動で変更し幾つかのパラメータを変更する必要がある．だからといって bound を上げ過ぎると計算が終了しなくなるので, うまく調整することが肝要である．

続いて Step.4 を行う．elliptic logarithm を用いて, 全ての整数点を先述の生成元を用いて表したときの係数への bound を与えると, rank 1 のときにはおおよそ $M = 10^{25}$, rank 2 のときにはおおよそ $M = 10^{40}$ 程度となる．そこで LLL-reduced algorithm を適用すると, 新しい bound は $\sqrt{\log M}$ 程度まで下がるので, 2〜3 回 (打ち止めになるまで) 行えば一ケタくらいまで下げることが出来る．後は各個撃破で十分である．

命題 3.2. $m = 46, 59$ の何れの場合も, E_0^+, $E_3^\pm$ の整数点の集合は

$$E_0^+(\mathcal{O}_{K_m}) = \{O, T\} \ \ , \ \ E_3^\pm(\mathcal{O}_{K_m}) = \{O, T\}$$

である．ここに E_0^+ の $T = (-12, 0)$, $E_3^\pm$ の $T = (\mp 12\varepsilon, 0)$ である．

後は Step.5 に移る．結果, 自明な導手を持つ E_C は一つも見つからず, 従って当初の至る所 good reduction を持つ楕円曲線の非存在性が従う．以上, 全ての計算は Magma, Sage, Pari-GP の 3 種のソフトウェアを必要に応じて使い分けて行った．例えば Step.5 の導手の計算は Magma, 2-descent を始めとする numerical な計算は Pari/GP, これらのデータの統合とセットアップには Sage を使う, といった具合である．

補足 3.3. 実は今回のケースでは Step.5 (導手の計算) を行う必要はない．Setzer [17] の「二次体上自明な導手を持つ楕円曲線の j-invariant は 0 でも 1728 でもない」という結果を使えば, 整数点のうち $y = 0$ であるものは直ちに候補から外せる．つまり全ての点が候補から外れてしまうので, 非存在性がすぐに従う．

[2]実は最初に非存在性を攻略しようとしたのは $m = 43$ のときであった．このときは「判別式が 3 乗数」とは限らないため, $E_1^\pm$ や $E_2^\pm$ の計算も必要となり, その過程でこのバグを発見した．この件については木村巌氏 (富山大学) の協力の下, Sage Support なるバグトラッキングシステムに投稿済である．しかしながら, 実際に最新版を使えるようになるのはもう少し先かもしれない．

3.2 $m = 43$ の場合

この場合は補題 2.2 の条件から外れるものが含まれている. 従って補題 2.3 だけを適用し

$$\Delta(E) = -\varepsilon^{2n} \quad (n \in \mathbb{Z})$$

が導かれる. これより $m = 43$ の場合 (c_4, c_6) の候補は $E_n^+(\mathcal{O}_{K_{43}})$ $(n = 0, 2, 4)$ にのみ存在することが分かる. 結果は次の通り:

命題 3.4. $m = 43$ とする. Mordell-Weil 群 $E_n^+(K_{43})$ $(n = 0, 2, 4)$ の構造とその生成元は

- $n = 0$ のとき $E_0^+(K_{43}) \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ で, その生成元は
  - 振れ部分: $T = (-12, 0)$
  - 自由部分: $P = \left(-\frac{104}{9}, -\frac{56}{27}\sqrt{43}\right)$
- $n = 2$ のとき $E_2^+(K_{43}) \simeq \mathbb{Z}$ で, その生成元は

$$P = \left(3200 - 488\sqrt{43}, 294088 - 44848\sqrt{43}\right)$$

- $n = 4$ のとき $E_4^+(K_{43}) \simeq \mathbb{Z}$ で, その生成元は

$$P = \left(-727456 + 110936\sqrt{43}, 496115392 - 75656888\sqrt{43}\right)$$

である.

命題 3.5. $E_n^+(\mathcal{O}_{K_{43}})$ $(n = 0, 2, 4)$ は

- $E_0^+(\mathcal{O}_{K_{43}}) = \{O, T, T \pm P\}$
- $E_2^+(\mathcal{O}_{K_{43}}) = \{O, \pm P, \pm 2P\}$
- $E_4^+(\mathcal{O}_{K_{43}}) = \{O, \pm P, \pm 2P\}$

である. ここに T, P は先述の各 n に対し与えられた点である.

このうち O および T を除く 10 個の整数点に対して Step.5 を行えば, 何れも自明でない導手を持つことが確認出来, 非存在性が従う. 例えば $n = 0$ のときの $T \pm P$ については導手のノルムが 256 となる.

因みに $n = 1, 3, 5$ の場合も $E_n^+(K_{43})$ および $E_n^+(\mathcal{O}_{K_{43}})$ の計算に成功したので, 参考までに載せておく.

命題 3.6. $m = 43$ とする. Mordell-Weil 群 $E_n^+(K_{43})$ $(n = 1, 3, 5)$ の構造とその生成元は

- $n = 1, 5$ のとき $E_n^+(K_{43}) = \{O\}$
- $n = 3$ のとき $E_3^+(K_{43}) \simeq \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/2\mathbb{Z}$ で, その生成元は T (振れ部分), P_1, P_2 (自由部分),
  - $T = (-12\varepsilon, 0)$ $(\varepsilon = -3482 + 531\sqrt{43})$

- $P_1 = (69640 - 10620\sqrt{43}, -23012360 + 3509352\sqrt{43})$
- $P_2 = \left(\frac{126547052}{2601} - \frac{19298206}{2601}\sqrt{43}, -\frac{1218913518550}{132651} + \frac{185882568326}{132651}\sqrt{43}\right)$

である．このとき，整数点の集合は

- $E_1^+(\mathcal{O}_{K_{43}}) = \{O\}$
- $E_3^+(\mathcal{O}_{K_{43}}) = \{O, T, T \pm P_1\}$
- $E_5^+(\mathcal{O}_{K_{43}}) = \{O\}$

である．ここに T, P_1 は各 n に対して先に与えた点を表す．

一方，E_n^- については何一つ成功しなかった．2-descent を用いた計算法では，これ以上の計算は困難だと思われる．

3.3 $m = 62, 67, 71$ の場合 (定理 1.3)

先程と同様にして，$m = 62, 71$ のときは $E_3^-(\mathcal{O}_{K_m})$ を，$m = 67$ のときは $E_0^+(\mathcal{O}_{K_m})$ を決定すれば十分であることが分かる．結果は以下の通り．

命題 3.7. (1) $m = 62$ のとき，Mordell-Weil 群 $E_3^-(K_{62})$ は $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ に同型であり

- 捩れ部分の生成元は $T = (12\varepsilon, 0)$ $(\varepsilon = -63 + 8\sqrt{62})$
- 自由部分の生成元は $P = \left(\frac{30492}{25} - \frac{3872}{25}\sqrt{62}, -\frac{8377936}{125} + 8512\sqrt{62}\right)$

である．
(2) $m = 67$ のとき，Mordell-Weil 群 $E_0^+(K_{67})$ は $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ に同型であり

- 捩れ部分の生成元は $T = (-12, 0)$
- 自由部分の生成元は $P = \left(-\frac{584}{49}, \frac{248}{343}\sqrt{67}\right)$

である．
(3) $m = 71$ のとき，Mordell-Weil 群 $E_3^-(K_{71})$ は $\mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/2\mathbb{Z}$ に同型であり

- 捩れ部分の生成元は $T = (12\varepsilon, 0)$ $(\varepsilon = 3480 + 413\sqrt{71})$
- 自由部分の生成元は

  $P_1 = \left(165300 + \frac{39235}{2}\sqrt{71}, \frac{377098253}{4} + \frac{44753329}{4}\sqrt{71}\right)$

  $P_2 = \left(\frac{1560462848}{3025} + \frac{185192868}{3025}\sqrt{71}, -\frac{87152513410872}{166375} - \frac{10343100438152}{166375}\sqrt{71}\right)$

である．

命題 3.8. $m = 62, 67, 71$ のとき，整数点の集合は

- $E_3^-(\mathcal{O}_{K_{62}}) = \{O, T\}$

- $E_0^+(\mathcal{O}_{K_{67}}) = \{O, T, T \pm P\}$
- $E_3^-(\mathcal{O}_{K_{71}}) = \{O, T, \pm P1 \mp P2, T \pm P1 \mp P2\}$ (複号同順)

となる．これら (c_4, c_6) の候補は全て Step.5 において自明な導手を与えず, 定理 1.3 が従う．

$m = 62, 67, 71$ に関しては, ここで調べた n 以外のものについては何一つ自由部分の生成元を求めることが出来なかった．実際には $m = 62, 71$ の場合は $n = 1, 3, 5$ のときを (但し rank 0 のときを除く), $m = 67, 83$ の場合は $n = 0, 2, 4$ のときを決定すれば良いことが分かる．そこでこれらの生成元を求めようと試みたが, $m = 62$ の場合は $n = 5$ のとき rank は 1 ($n = 1$ のときは rank は 0), $m = 67$ の場合は $n = 2, 4$ のとき何れも rank は 1, $m = 71$ の場合は $n = 1, 5$ のとき何れも rank は 1 以上 3 以下である, という所までは判明したものの, それより先の見通しは立っていない (analytic rank は求まる).

補足 3.9 (計算機に関する補足)**.** 計算代数システム Magma には, 代数体上の楕円曲線に関するコマンドが多数用意されており, そのうちの幾つかは主定理の証明に大いに役立った．例えば Mordell-Weil 群の rank の上限と下限は Pari/GP では一致しないことがあったが, `RankBound` コマンドを用いて上限の精密な評価を行うことで, 下限と一致させるのに成功している．

一般に代数体 K 上定義された楕円曲線 E に対し, Mordell-Weil 群 $E(K)$ を計算することは困難である．捩れ部分だけならばそれほど労力はかからないが, 自由部分を決定するのは例え K が今回のケースのように二次体であっても難しい．そこで Magma にはこの困難を回避するために, `MordellWeilSubgroup` 乃至 `PseudoMordellWeilGroup` というコマンドが用意されているのだが, これは楕円曲線の選び方に依存しており, 今回のケースでは役に立たなかった．残る手法としては, 2-covering と呼ばれる超楕円曲線を経由して求めるテクニック (4-descent) が考えられるが, うまくいくかどうかの問題以前に, 有理数体上の楕円曲線についてしか実装されていないことが分かった．

4 計算時間の比較

それでは, 実際に Simon's 2-descent を実行するのにどれくらいの CPU time を要したのかを示しておこう．まず始めに, 本プログラムは主に 4 つのパラメータで調整されていることを断わっておく:

- `lim1`: limit on trivial points on binary quartic forms ("quartics" for short),
- `lim3`: limit on points on ELS (everywhere locally solvable) quartics,
- `limtriv`: limit on trivial points on elliptic curve,
- `limbigprime`: distinguish between small and large prime numbers to use probabilistic tests for large primes.

他に幾つかの補助パラメータも用意されている (`maxprob`,`bigint`,`nbideaux`, etc.).

ここでは例として (`lim1`,`lim3`,`limtriv`,`limbigprime`) $= (40, 60, 40, 30)$ と主パラメータを固定してみる．これは $m = 43$ の場合に適用したパラメータであって, 以下に示すように他のケースに関しては適していない場合もあることに注目されたい．

m	$E_n^{\pm}$	desired	actual	CPU time (sec.)	S/F
43	E_0^+	1	1	570.168	success
	E_2^+	1	1	120.916	success
	E_4^+	1	1	112.554	success
46	E_3^+	1	1	670.117	success
59	E_0^+	1	1	195.500	success
	E_3^-	2	1	300.582	failure
62	E_3^-	1	1	317.216	success
67	E_0^+	1	0	976.785	failure
71	E_3^-	2	2	279.413	success

$E_n^{\pm}(K_m)$ **の rank と実際に得られた生成元の個数, および CPU time の比較**

残る failure となっているケースは, 改めてパラメータを取りかえて計算を行う. 例えば $m = 67$ に関してはほぼ全てのパラメータを変更し, 2 時間弱を費やして計算した.

以上, 全ての計算は OS Windows 7 32bit 版, Intel$^{\mathrm{TM}}$ Core-i5 3.30GHz CPU と 4.00GB メモリを搭載した環境で行っている.

5　幾つかの拡張

5.1　実二次体上の場合

$1 < m < 100$ の範囲で本稿で取り扱ったケースを除き, 現在未解決なものは

$$m = 51, 87, 91$$

の 3 つであるが, これらは全て類数が 2 であって類数 1 の場合の手法が使えない. 恐らくここからは至る所 good reduction を持つようなものは見つからないと予想している.

一方, 類数 1 であるものを少し拡張して 200 以下の m についてはどのようになっているかを考察してみた. 次ページの表は, 先行研究で得られていた結果に個人的に計算を進めて新たに得た結果を追加したものである. 現在進行中につき, データは正確ではないかもしれないので注意されたい.

5.2　虚二次体上の場合

この方面での最たる結果は, 1980 年代の Stroeker [18] および Setzer [16], [17] の定理である.

定理 5.1. K_m が類数が 6 と素な虚二次体であるとき, K_m 上至る所 good reduction を持つような楕円曲線は存在しない.

$|m|$ を 100 以下に限定すれば, [16] に挙げられている次の例が唯一の存在定理である.

定理 5.2. K_{-65} 上至る所 good reduction を持つ楕円曲線は同型を除いて 8 個存在する. 加えてこれらは admissible (至る所 good reduction を持ち, 更に 2-division point を持つ) である.

更に [16] には admissible な曲線が存在するための必要十分条件が与えられている. この条件は初等整数論的に与えられたものであり, 比較的容易に admissible な楕円曲線の族が求まる.

m	決定すべき $E_n^{\pm}$	admissible	それ以外	進捗状況
101	24 個全て (実質 12 個)	×	×	非存在
103	無し	×	×	非存在
107	E_0^+, E_3^+	×	?	?
109	$E_0^+, E_1^+, E_2^+, E_3^+, E_4^+, E_5^+$	×	○	存在性のみ
113	無し	×	×	非存在
118	E_0^+, E_3^+	≥ 2	×	存在性のみ
127	E_3^-	×	?	?
129	$E_0^+, E_1^+, E_2^+, E_3^+, E_4^+, E_5^+$	×	×	非存在
131	$E_0^+, E_2^+, E_4^+, E_1^-, E_3^-, E_5^-$	×	?	?
133	E_1^-, E_3^-, E_5^-	×	2	完全決定
134	E_1^-, E_3^-, E_5^-	≥ 2	?	?
137	無し	×	×	非存在
139	E_0^+, E_2^+, E_4^+	×	?	?
141	24 個全て (実質 12 個)	×	×	非存在
149	無し	×	×	非存在
151	E_1^-, E_3^-, E_5^-	×	?	?
157	E_0^+, E_2^+, E_4^+	×	1	完全決定
158	E_1^-, E_3^-, E_5^-	×	○	存在性のみ
161	E_3^-	○	○	存在性のみ
163	$E_0^+, E_1^+, E_2^+, E_3^+, E_4^+, E_5^+$	×	?	?
166	E_3^-	≥ 2	?	?
167	E_1^-, E_3^-, E_5^-	×	×	非存在
173	無し	×	×	非存在
177	E_1^+, E_3^+, E_5^+	×	×	非存在
179	$E_0^+, E_1^+, E_2^+, E_3^+, E_4^+, E_5^+$	×	?	?
181	無し	×	×	非存在
191	無し	×	×	非存在
193	E_3^+, E_3^-	?	?	?
197	24 個全て (実質 12 個)	×	×	非存在
199	E_0^+, E_2^+, E_4^+	×	?	?

実二次体 $\mathbb{Q}(\sqrt{m})$ 上 e.g.r. な楕円曲線の存在・非存在 ($100 \leq m \leq 200$)

補足

今回の筆者の講演では補助資料を配布した．ひとつは山村健氏 (防衛大) による e.g.r. な楕円曲線を扱った論文, 書籍の文献表である．2011 年 11 月現在, e.g.r. な楕円曲線に関する文献は 60 を超えているようである．資料を快く提供下さった山村氏にこの場を借りて感謝御礼申し上げたい．もうひとつは筆者のウェブページ

`http://www2.math.kyushu-u.ac.jp/~s-yokoyama/ECtable.html`

でも公開・随時更新している, 幾つかの代数体上 e.g.r. な楕円曲線の存在・非存在リストである．データの誤り等, 何かお気付きの点があれば横山までご連絡を頂ければ幸甚である．

また, 本講演で扱った題材における別のアプローチとその計算効率比較について [20] に簡潔に記した．出版にはもう暫くの時間を要するが, こちらも筆者のウェブページにて記事を公開している．興味を持たれた方はこちらもご覧頂ければ幸いである．

参考文献

[1] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. **144** (1990), 233–258.

[2] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Exp. Math. **16** (2007), 303–312.

[3] J. E. Cremona (compiled), *Elliptic Curves with Everywhere Good Reduction over Quadratic Fields*, available from his website: `http://www.warwick.ac.uk/staff/J.E.Cremona/ecegr/ecegrqf.html`.

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

[6] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields*, Arch. Math. **73** (1999), 25–32.

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

[8] T. Kagawa, *Elliptic curves with everywhere good reduction over real quadratic fields*, Ph. D. Thesis, Waseda University, 1998.

[9] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields, II*, preprint.

[10] 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, 加川氏のウェブページより入手可能.

[11] M. Kida, *Reduction of elliptic curves over certain real quadratic number fields*, Math. Comp. **68** (1999), 1679–1685.

[12] M. Kida, *Nonexistence of elliptic curves having good reduction everywhere over certain quadratic fields*, Arch. Math. **76** (2001), 436–440.

[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] 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.

[15] R. G. E. Pinch, *Elliptic curves over number fields*, Ph. D. Thesis, The University of Oxford, 1982.

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

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

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

[19] T. Thongjunthug, *Heights on elliptic curves over number fields, period lattices, and complex elliptic logarithms*, Ph. D. Thesis, The University of Warwick, 2011.

[20] 横山俊一, 至る所良い還元を持つ楕円曲線について, 計算機的手法とその最近の進展, 第 9 回「代数学と計算」研究集会 (AC2011) 報告集, 2012.

[21] S. Yokoyama and Y. Shimasaki, *Non-existence of elliptic curves with everywhere good reduction over some real quadratic fields*, J. Math-for-Industry **3** (2011), 113–117.