

代数体上良還元をもつ楕円曲線の探索と そのデータベース化

横山 俊一 (東京都立大学)

概要

代数体上良還元 (とくに bad prime が 0 ~ 2 種類程度) をもつ楕円曲線を効率的に探索する手法は, 近年の計算機の発展と共に大きく進展し, さらに UI を意識した統合データベースの開発も並行して行われている. 本稿では, 主にここ 10 年間の (筆者の結果を含む) 進展状況と実装に関する現状について報告する. また基礎体がやや複雑な場合における最新の結果についても紹介する.

1 準備

K を代数体 ($\mathbb{Q}$ の有限次拡大体) とする. 3 次曲線

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K)$$

が K 上で特異点をもたないとき, E は K 上の **楕円曲線** *elliptic curve* とよぶ. E が定まると, 各係数から 判別式 *discriminant* $\Delta(E)$ が求まる (これは容易に計算できる). E が楕円曲線であるとき, 常に $\Delta(E) \neq 0$ になりたつ (逆も成立).

楕円曲線上の点 $P, Q \in E$ に対し, 加法 $P + Q \in E$ 及び整数倍 $nP \in E$ が定義できる. この演算は無限遠点 O を導入する事により閉じている. とくに K -有理点 K -rational point $P = (x, y) \in E$ ($x, y \in K$) のみでも閉じており, その全体は有限生成アーベル群をなす:

$$E(K) \simeq \mathbb{Z}^{\oplus r} \oplus G.$$

これを **Mordell-Weil 群** *Mordell-Weil group* とよぶ. $r \geq 0$ を 階数/ランク *rank* とよび, G は (比較的位数の小さな) 有限群となる.

いま $\mathcal{O}_K$ を K の整数環とし, $\mathcal{P} \in \mathcal{O}_K$ を素イデアルとする. E の各係数を $\text{mod } \mathcal{P}$ して (剰余体の元とみなして) 得られる曲線 $E_{\mathcal{P}}$ を考えたとき, これは剰余体上の楕円曲線とみなせる. $\Delta(E_{\mathcal{P}}) \neq 0$ になりたつとき, E は $\mathcal{P}$ で **良い還元** *good reduction* をもつといい, さらに任意の $\mathcal{P}$ に対して良い還元をもつとき, E は K 上 **至る所良い還元をもつ** *having everywhere good reduction* とよぶ. 楕円曲線には **導手** *conductor* とよばれる不変量が従い, 良い還元をもたない (= **悪い還元** *bad reduction* をもつ) 場合の情報を記述する. よって

$$E \text{ が } K \text{ 上至る所良い還元をもつ} \iff N(E) = (1)$$

になりたつ. このとき, 以下のような問題を考える:

問題. 代数体¹ K を固定したとき, K 上至る所良い還元を持つ楕円曲線 E を (同型類を除いて) すべて決定せよ. また存在しないならばそれを証明せよ.

¹ただし計算限界を考慮し, なるべく次数の小さな体を考える.

このような問題を考える理由はいくつかあるが、例えば次のような動機が考えられる:

- “素性の良い” 楕円曲線 $\iff$ 同じく “素性の良い” 保型形式 *modular form* の対応を考察するための重要なデータとなる.
- 特定の条件を課した「具体的な」楕円曲線を扱う際に有用である. これには例えば E に付随する特別な **Galois 表現** *Galois representation* を扱いたい, などの理由がある.

これについて, 現在知られている結果の一部を列挙すると:

- $K = \mathbb{Q}$ ならば非存在 (Tate)
- K : 類数が 6 と素な虚 2 次体ならば非存在 (Setzer [12])
- $\mathbb{Q}(\sqrt[3]{2})$ ならば非存在 (Bertolini-Canuto [1])
- $K = \mathbb{Q}(\zeta_n)$ (円分体) のとき, 部分的な結果がある.
- K : 低次 (上記を含む) のとき, sporadic だが明示的な結果がある. 例として, Ishii, Bertolini-Canuto, Comalada, Kagawa, Kida, Umegaki, Cremona, Lingham, Fisher, Thongjunthug, etc.

2 虚 2 次体の場合

まず虚 2 次体の場合を考える.

- 1978 – 1990: Setzer, Stroeker の定理 / Comalada の規準
- 1980 – 2000 後半: Ishii, Kida, Cremona-Lingham

このうち Comalada の規準 [3] については, 実 2 次体上および純 3 次体上の場合の考察にも用いることができる. 後述する実 2 次体上の場合との違いは, 主として **非存在性** *non-existenceness* の結果が統一的に得られている点にある. 言い方を変えれば, 存在する場合は非存在の場合に比べて圧倒的に少なく, さらに存在する場合には法則性がある. これを保証するのが Setzer の定理である.

定理 (Setzer, 1978 [12]). $K_m = \mathbb{Q}(\sqrt{m})$ ($m < 0$) とおく. このとき次がなりたつ.

- K_m の類数が 6 と素ならば K_m 上至る所良い還元をもつ楕円曲線は存在しない.
- K_{-65} 上に admissible (K_m 上至る所良い還元をもち, かつ位数 2 の K_m -有理点をもつよう) なものが 8 本 存在する.

以上の Setzer の定理のうち「 K_{-65} 上に admissible なものが 8 本存在する」の部分については, j -不変量² j -invariant 等のデータは掲載されているものの, 8 本の曲線の明示的構成はなされていなかった. これに対し Ikawa は, 具体的な 8 本の曲線を明示的に構成した.

命題 (Ikawa, 2024). Setzer によって示唆されていた, K_{-65} 上 admissible な曲線を与えた. 例として

²不変量という語句がついているが, 導手とは異なり一般的には不変量とはならない (が, 特定の代数的所作を施せば不変量的ふるまいを見せる.)

- $y^2 = x^3 + 1310949900x - 1824533802000\sqrt{-65}$
- $y^2 = x^3 + (55512\sqrt{-65} - 340011)x + (-19757304\sqrt{-65} + 30491370)$

などがある³.

Ikawa はさらに, Setzer が示唆した他の場合についても結果を得た. 方針は次の定理による.

定理 (Setzer [12]). K_m ($m < 0$) 上 admissible な曲線が存在するための必要十分条件は, $m = -65m_1$ で次をみたすことである:

- m_1 : square mod 5 and 13
- 65: square mod m_1

例えば $m = -65, -910, -1885, -3315, -3965, \dots$ と続く. Ikawa はこれまでに $|m| \leq 6110$ に対する計算を行った (現在も拡張が進んでいる).

3 実 2 次体 (+ 特定の 3 次体) の場合

前節に対して実の場合を考える. 先行結果としては例えば以下が挙げられる:

- (1) 1990 – 2000 前半: Kagawa [8], Kida (+2 名の共同研究 [9])
2 次体の理論を用いた手法
SIMATH, KANT-KASH, TECC-KASH インターフェース
- (2) 2000 – 2008: Cremona, C.-Lingham [4], C.-Fisher etc.
一般の代数体 K 上のアルゴリズムを提唱 (計算効率の課題)
Pari-GP, Magma インターフェース
- (3) 2011 – 2015: Yokoyama, Yokoyama-Shimasaki [15]
特定の代数体に特化したアルゴリズム (Simon の実装を改良)
Pari-GP, Magma インターフェース
Sage(Python) をグルー言語として用いる
- (4) 2013 – 2015: Cremona-Thongjunthug [5]
代数体上の楕円曲線の canonical height の下限の改善
至る所良い還元をもつ楕円曲線の結果はその応用例
インターフェースは Cremona-Lingham-Fisher と同一

³Ikawa (生川青輝) は筆者の研究室所属の修士 2 年の学生であり, この完全な結果を 2024 年度の修士論文 (2025 年に出版予定) に含める予定であるため, ここではすべての曲線を掲載することを控えた.

以上 (1)–(4) の計算に共通するのは

$$E_n^\pm : y^2 = x^3 \pm 1728\varepsilon^n$$

を考えたとき (ε は K の基本単数), その Mordell-Weil 群

$$E_n^\pm(K) := \{(x, y) \in K \times K \mid y^2 = x^3 \pm 1728\varepsilon^n\}$$

を計算することがボトルネックとなる点である. $\mathbb{Q}$ 上の場合の実装は Cremona's `mwrnk` (Pari-GP にネイティブ実装がある) などが知られているが, 一般の代数体上での計算に対する実装は 2000 年序盤に実現した. 主として

- Denis Simon's 2-descent (2002 –)
— Pari-GP / Sage インターフェース
- Nils Bruin's 2-descent (2004 –)
— KASH / Magma インターフェース

などがある. なお重要な点として, 以上 2 つの手法は実 2 次体・純 3 次体に限らず 一般の代数体上で利用可能であることに注意する.

以上を用いて, 1 つ目の戦略を概説しよう. この戦略は上述の (1) と (3), および (2) の一部で用いられた. これは基礎体 K を固定し up to isogeny (同種) で楕円曲線を特定・決定する手法である. まず上記 **2-descent** 法 *2-descent method* を用いる. これは完全系列

$$0 \rightarrow E(K)/2E(K) \rightarrow \text{Sel}^{(2)}(K, E) \rightarrow \text{III}(E/K)[2] \rightarrow 0$$

を用いて $E(K)/2E(K)$ を計算する手法である. $\text{Sel}^{(2)}(K, E)$ は E, K から定まる (2-)Selmer 群 *Selmer group*, $\text{III}(E/K)[2]$ は **Shafarevich-Tate** 群 *Shafarevich-Tate group* (の 2-torsion) を表す.

この計算が高確率で成功するのは, この $\text{Sel}^{(2)}(K, E)$ と $\text{III}(E/K)[2]$ との「ずれ」が小さくなるときである. とくに $\text{III}(E/K)[2]$ の計算は極めて困難であることが知られており, この部分が自明 (位数 1) のとき $E(K)/2E(K) \simeq \text{Sel}^{(2)}(K, E)$ になりたつ. したがってこの場合は $\text{Sel}^{(2)}(K, E)$ の計算に帰着される. この群は局所体の理論から来るものであり, 一般的には打ち切り誤差を含む構造を伴うが, これを大域的に計算するアルゴリズムを用いて計算を実現する. また $\text{III}(E/K)[2]$ が非自明であっても, Mordell-Weil 群における有限群パート (前述の G のこと: 捩れ部分 *torsion part* とよばれる) の構造から $E(K)/2E(K)$ を unique に特定できることがある (そして一般に G の計算は容易である). ただし経験則上, $\text{III}(E/K)[2]$ の位数が 4 以上の場合は高確率で失敗する.

$E(K)/2E(K)$ が確定した場合, ここから $E(K)$ を復元するプロセスを行う (これを ∞ -descent 法 *∞ -descent method* とよぶ). その後 $\Delta(E) \in \mathcal{O}_K^\times \simeq \langle -1 \rangle \times \langle \varepsilon \rangle$ (類数 1 の 2 次体の場合) である事から

$$E_n^\pm(K) = \{(x, y) \in K \times K \mid y^2 = x^3 \pm 1728\varepsilon^n\}, \quad 0 \leq n < 6$$

を考える事に帰着させ, さらに類体論的手法 (ray 類群の位数の可除性: 主として 3 の場合に着目する) を用いて計算すべき候補を絞り込む.

最後に isogeny relation を利用する. 例えば

$$E_n^+ \iff y^2 = x^3 - \varepsilon^n \text{ by } (x, y) \mapsto \left(\frac{4x^3 - 16\varepsilon^n}{x^2}, \frac{8x^3y + 64\varepsilon^n y}{x^3} \right)$$

などの変換写像を用いることで、最終的に至る所良い還元をもつ楕円曲線を明示的に構成できる。

Simon 版と Bruin 版の 2-descent 法の違いは、実装されたプラットフォームの違いだけではなく、制御可能なパラメータの数にある。Bruin 版 (これは後述の別戦略にも採用されている) は、楕円曲線の有理点の探索における 高さ *height* の上限値のみを指定できる。これに対し、Simon 版は有理点に関する 5 種類のパラメータ (高さを含む) を制御できる。詳細は複雑となるため割愛するが、計算機環境に制限のつく場合は Simon 版が有利となる (Bruin 版だと余分な探索を回避できないからである)。しかしながら利用難易度は高く、プロ向けの実装と言える。例として、 $\mathbb{Q}(\sqrt{46})$ 上の曲線の実行例 (画面) は以下の通りである：

```
[E(K):phi'(E'(K))] = 2
#S^(phi')(E'/K) = 2
#III(E'/K)[phi'] = 1

trivial points on E'(K) =
[[0, 0, 1], [0, 0, 1], [1, 1, 0], [0, 0, 1]]

points on E'(K) = [[-202124/3*y - 4112615/9, -389319554/3*y - 23764443157/27],
[0, 0]]
points on E(K) = [[2666689/39*y + 2821472905/6084, 73202442649/2028*y + 1161770
50458217/474552], [0, 0]]

[E'(K):phi(E(K))] = 4
#S^(phi)(E/K) = 4
#III(E/K)[phi] = 1

#III(E/K)[2] = 1
#E(K)[2] = 2
#E(K)/2E(K) = 4
rank = 1

points = [[0, 0], [Mod(2666689/39*y + 2821472905/6084, y^2 - 46), Mod(732024426
49/2028*y + 116177050458217/474552, y^2 - 46)], [0, 0]]
%18 = [1, 2, [[Mod(-43056*y - 292020, y^2 - 46), 0], [Mod(987505/39*y + 10448232
25/6084, y^2 - 46), Mod(73202442649/2028*y + 116177050458217/474552, y^2 - 46)],
[Mod(-43056*y - 292020, y^2 - 46), 0]]]
(05:38) gp >
```

図 1 : Pari-GP ネイティブ環境 [11] における Simon's 2-descent の実行

具体的な構成例 (筆者による結果) も紹介しておく。例えば $\mathbb{Q}(\sqrt{158})$ のとき $E_3^-(K) \simeq \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z}$ となり

- T の生成元は $C = (12\varepsilon, 0)$ ($\varepsilon = 7743 + 616\sqrt{158}$)
- $\mathbb{Z}^2$ の 1 つ目の生成元は $P_1 = (5559122 + 442260\sqrt{158}, 18536310324 + 1474669670\sqrt{158})$
- $\mathbb{Z}^2$ の 2 つ目の生成元は $P_2 = (154860 + 12320\sqrt{158}, 76310080 + 6070904\sqrt{158})$

と計算できる。このとき $P = C - P_1 + P_2 \in E_3^-(\mathcal{O}_K)$ (3 つの線形結合により整数点になるようなもの) となり、しかるべき変数変換を行えば

$$E: y^2 + xy + \sqrt{158}y = x^3 - x^2 + Ax + B$$

- $A = -361817559192191668851 - 28784659475803145415\sqrt{158}$
- $B = 3691288333191863812738417681108 + 293663132146367649175848062813\sqrt{158}$

が容易に求められ, これは K 上至る所良還元をもつ曲線となる.

もう一つ例を挙げる. 純 3 次体 $\mathbb{Q}(\sqrt[3]{46})$ のとき

$$y^2 + \sqrt[3]{46}xy + \frac{\sqrt[3]{46^2} + \sqrt[3]{46} + 1}{3}y$$

$$= x^3 + (\sqrt[3]{46} + 1)x^2 + \frac{C_1\sqrt[3]{46^2} + C_2\sqrt[3]{46} + C_3}{3}x + \frac{C_4\sqrt[3]{46^2} + C_5\sqrt[3]{46} + C_6}{3}$$

が至る所良い還元をもつ楕円曲線となる. ここで C_k ($1 \leq k \leq 6$) は以下で与えられる:

$$C_1 = 94219593757433390681493864706,$$

$$C_2 = 1081334709186632184731947617604,$$

$$C_3 = 5084087035543830437128808550119,$$

$$C_4 = 23258423334479295709473275474986025640457867,$$

$$C_5 = 827892116462926667504946133778759990377913857,$$

$$C_6 = 3264974121115333449055262059201401614426686175.$$

この曲線が自明な導手をもつことを検証するためには, 現在では約 3 時間程度⁴を要する. 一般に導手の計算は高負荷であるため, 別の検証方法として判別式の基本単数によるべき表示を探索することも考えられる. 実際, この例では

$$\Delta(E) = -379398439773458170089051719617891293880506387970110968885$$

$$9069841240872146001465208442236960\sqrt[3]{46^2}$$

$$+ 38266373510239702375947834653456075318013469606118717466$$

$$402223327610129260665089286586642440\sqrt[3]{46}$$

$$- 88402196060375965791126700381485837764341711498964900463$$

$$229074317241483287536740383170905601$$

$$= -\varepsilon^{24} \in \mathcal{O}_K^\times \simeq \langle -1 \rangle \times \langle \varepsilon \rangle$$

と確かめられる (べき演算の計算は容易である). ここで $\varepsilon = 309\sqrt[3]{46^2} + 48\sqrt[3]{46} - 4139$ は $\mathbb{Q}(\sqrt[3]{46})$ の基本単数を表す (従って, 上記曲線は大域極小モデルではない).

4 EllipticCurveSearch アルゴリズム

前節で述べた戦略に対して, やや異なる (が根本的には同じ) 戦略を紹介する. 簡潔に述べると, 各種不変量 – とくに j -不変量に注目することで楕円曲線の族を特定するアルゴリズムである. 2-descent の別表記として

$$1 \rightarrow \mathcal{O}_{K,S}^* / \mathcal{O}_{K,S}^{*m} \rightarrow K(S, m) \rightarrow \mathcal{C}_{K,S}[m] \rightarrow 1$$

を考え, 楕円曲線の候補の絞り込みを j -不変量によって行い, それを次のような問題として解釈する:

1. 前節の戦略とほぼ同一の楕円曲線 E/K の **整数点** *integral point* を特定する.

⁴計算機環境: Magma ver. 2.28-2 on Mac OS Sonoma 14.5 / M3 processor / 24GB Memory.

2. K を少し拡大させて, その上の 1 次方程式の 単数解 *unit / fundamental solution* を特定する.

このうち Magma [2] には 2 つ目の手法を補助する関数 `UnitEquation` が存在するが, 永らくバグが解消されていなかったことがある (v2.20-5 で修正).

以上を統一的に計算できるプロトコルとして誕生したのが `EllipticCurveSearch` アルゴリズムである. 実装のベースは Cremona-Thongjunthug の探索法 [5] に基づく. これは数論統合データベース LMFDB [10] の開発の一環として行われたものである. この核となる実装コードを紹介する:

```
ECGrS(FldNum, [RngOrdIdl], {RngOrdIdl})
> intrinsic ECGrS(K::FldNum, S::[RngOrdIdl])→SeqEnum5
> vprint egrosNF, 1: "S=", S;
> jlist:=ECGrS.getjlist(K, S);
> vprint egrosNF, 1:
> "List of", #jlist, "possible j-invariants:", jlist;
> Elist:=ECGrS.fromjlist(K, S, jlist);
```

ここでは m -Selmer 群 (とくに $m = 2$ を考える) のかわりに有限集合

$$K(S, m) := \{x \in K^*/K^{*m} \mid \text{ord}_{\mathcal{P}}(x) \equiv 0 \pmod{m} \text{ for all } \mathcal{P} \notin S\}$$

を考えて, j -不変量 ($\neq 0, 1728$) の候補を絞って楕円曲線を探査する.

まず `ECGrS.getjlist(K, S)` について解説する. K を代数体, S を有限個の素点の集合 (空集合でもよい) としたとき, $(x, y) \in K \times K$ が S -整数点 *S -integral point* であるとは, 任意の $\mathcal{P} \notin S$ に対して $\text{ord}_{\mathcal{P}}(x) \geq 0$ かつ $\text{ord}_{\mathcal{P}}(y) \geq 0$ をみたすことと定義する. この関数では, K 上の楕円曲線

$$E_w : y^2 = x^3 - 1728w \quad (w \in K)$$

の S -整数点を効率的に求めることが要求される. ここで

$$K(S, 6) \ni w \equiv j^2(j - 1728)^3 \pmod{(K^*)^6}$$

となり, ある S -整数点 $(x, y) \in E_w$ に対して

$$j = \frac{x^3}{w} = 1728 + \frac{y^2}{w}$$

がなりたつ.

以上の結果を `ECGrS.fromjlist(K, S, jlist)` に移す. このとき $(3u_0)^6 w \in K(S, 12)$ をみたす $u_0 \in K^*$ に対して

$$E_{u_0}/K : y^2 = x^3 - 3xu_0^2x - 2yu_0^3$$

は $j(E_{u_0}) = j$ かつ S の外で至る所良い還元をもつ. 最後に E_{u_0} の 2 次捻り *quadratic twist* $E_{u_0}^{(u)}$ ($u \in K(S, 2)$) を列挙する. $K(S, m)$ の決定には先述の完全系列を用いる:

$$1 \rightarrow \mathcal{O}_{K,S}^*/\mathcal{O}_{K,S}^{*m} \rightarrow K(S, m) \rightarrow \mathcal{C}_{K,S}[m] \rightarrow 1$$

⁵代数体 K の素イデアルの集合 (リスト) S が与えられたとき, K 上 S の外で良い還元をもつ (= S のみで悪還元をもつ) 楕円曲線のリストを返す. つまり $S = \{\}$ (empty) の場合, K 上至る所良い還元をもつ楕円曲線を探査していることになる.

これを *K-Kummer* 系列 *K-Kummer sequence* とよぶ.

具体的な計算例を一つ挙げる:

```
> P<x>:=PolynomialRing(Rationals());
> N<a>:=NumberField(x^2-5);
> I2:=ideal<MaximalOrder(N)|31>; I2;
Principal Ideal
Generator:
[31, 0]
> ECS:=EllipticCurveSearch(I2,10);
> ECS;
[
  Elliptic Curve defined by y^2 + y = x^3 + 1/2*(-a + 1)*x^2
    + 2*x + 1/2*(-a-3) over N,
  Elliptic Curve defined by y^2 + y = x^3 + 1/2*(a + 1)*x^2
    + 2*x + 1/2*(a-3) over N
]
> E:=ECS[1]; Conductor(E);
Principal Ideal
Generator:
[31, 0]
```

これは $\mathbb{Q}(\sqrt{5})$ 上 $S = \{(31)\}$ の外で至る所良い還元をもつ楕円曲線の探索を行ったものであり, 結果として 2 本見つかった. なお $\mathbb{Q}(\sqrt{5})$ 上至る所良い還元をもつ楕円曲線は存在しないことが証明されており, 上記曲線が導手ノルム最小であることが知られている. なお `EllipticCurveSearch` 関数の第 2 成分はエフォート値であり, 探索範囲を線形に指定するパラメータ (Bruin's 2-descent に協働するデータ) である.

最後に S -整数点の計算アルゴリズムに関してだが, その実装例は Herrmann-Pethö の論文 [6] および Herrmann の学位論文 [7] に示されているのみである. 実装そのものは 2003 年に完成していると記載があるが, 現時点でもその実装は公開されていない模様である. しかし現在では Magma の内部関数を用いて実装され, 上述の関数に実装された.

以上の戦略, とくに 1 次方程式の単数解に着目した結果として Takeshi による結果がある. このケースでは基礎体を固定するのではなく, 基礎体の定義多項式を楕円曲線の係数でパラメトライズすることで, 至る所良い還元をもつ楕円曲線の無限族を構成するものである.

定理 (Takeshi, 2012 [13]). 基礎体 K_b を, 多項式

$$f_b(X) = X^3 - 16(b-16)X^2 + bX - 1 \quad (b \in \mathbb{Q})$$

で定義される 3 次体とする. この時 $f_b(X)$ の根を β とすれば

$$y^2 + xy = x^3 - 8\beta x^2 - \beta(1 - 16\beta)x$$

は K_b 上至る所良い還元をもつ⁶.

⁶ K_b は無限個走るので, 楕円曲線も無限個構成される.

5 最近の進展

先述の Ikawa による結果に関連して、その基盤となったものを紹介する。それが Yoshimura⁷ [16] によるものである。Yoshimura は、 $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-65})$ と特定の 2 次体との合成体 (CM-type 4 次拡大体) を基礎体とした場合を考察した。例として

- $K = \mathbb{Q}(\sqrt{-1}, \sqrt{n})$ ($2 \leq n \leq 100$)
- $K = \mathbb{Q}(\sqrt{-65}, \sqrt{n})$ ($2 \leq n \leq 100$)

の場合を考察している。その結果、後述する整数論統合オンラインデータベース LMFDB に未記載の曲線を多く構成した。例として $K = \mathbb{Q}(\sqrt{-1}, \sqrt{7})$ 上で

- $a_1 = \frac{1}{16}(3\varphi_7^3 - 44\varphi_7^2 + 172\varphi_7 - 224)$
- $a_2 = \frac{1}{16}(-99\varphi_7^3 - 24\varphi_7^2 + 2100\varphi_7 + 4368)$
- $a_3 = \frac{1}{16}(-135\varphi_7^3 + 532\varphi_7^2 - 116\varphi_7 - 1456)$
- $a_4 = \frac{1}{16}(-3453\varphi_7^3 + 12600\varphi_7^2 + 2388\varphi_7 + 45376)$
- $a_6 = \frac{1}{16}(14933\varphi_7^3 - 47176\varphi_7^2 - 49028\varphi_7 + 254736)$
- $\Delta(E) = 193545\varphi_7^3 - 3870900\varphi_7 + 8193151$
- $j(E) = 16581375$

(ただし、 $\varphi_7 = \sqrt{-1} + \sqrt{7}$) などがある。 $K = \mathbb{Q}(\sqrt{-1}, \sqrt{n})$ ($2 \leq n \leq 100$) 上で探索成功した、 K 上至る所良い還元をもつ曲線は合計 19 本である⁸。その内訳は $n = 14, 31, 77$ で各 1 本、 $n = 41$ で 4 本、残りは各 2 本である。

n	2	3	5	6	7	10	11	13	14	15	17	19
Found	×	×	×	○	○	×	×	×	○	×	×	×
n	21	22	23	26	29	30	31	33	34	35	37	38
Found	×	×	×	○	○	×	×	○	×	×	○	×
n	39	41	42	43	46	47	51	53	55	57	58	59
Found	×	○	×	×	×	×	×	×	×	×	×	×
n	61	62	65	66	67	69	70	71	73	74	77	78
Found	×	×	○	×	×	×	×	×	×	×	○	×
n	79	82	83	85	86	87	89	91	93	94	95	97
Found	×	×	×	×	×	×	×	×	×	×	×	×

表 1 : $K = \mathbb{Q}(\sqrt{-1}, \sqrt{n})$ ($2 \leq n \leq 100$) 上の探索結果⁹

⁷Yoshimura (吉村隼人) は筆者の研究室に所属していた学生であり、2024 年 3 月に本研究により修士号を取得した。

⁸その後 Ikawa によって、存在性のデータが更新された。本稿執筆時 (2024 年 10 月現在) では、加えて $n = 22, 38, 42, 55, 57, 79, 86, 91, 95$ の場合が追加されている。

⁹ただし ○ は「1 本以上見つかった」、× は「探索の結果見つからなかった」という意味であり、完全な存在性 (= すべての曲線を探索し尽くすこと) ・非存在性 (= 1 本も存在しないこと) を保証しない点に注意である。

Yoshimura はこれらの計算機実験をもとに、特定の条件下¹⁰において次のような性質を予想した:

予想 (Yoshimura, 2024 [16]). $K_1 = \mathbb{Q}(\sqrt{-1}), K_2 = \mathbb{Q}(\sqrt{n})$ とする. このとき $(1) \implies (2)$ が成り立つ.

(1) K_2 上至る所良い還元をもつ楕円曲線が存在する.

(2) K_1 と K_2 の合成体 M 上至る所良い還元をもつ楕円曲線が存在する.

とくに, M 上至る所良い還元をもつ楕円曲線 E に対し, その j -不変量が整数値であるとき, K_2 上でも至る所良い還元をもつ楕円曲線 E' が存在して, 2 本の j -不変量是一致的.

上記予想の一般化も考察しており, $K_1 = \mathbb{Q}(\sqrt{m}), K_2 = \mathbb{Q}(\sqrt{n})$ かつ最後の結論が K_1, K_2 上いずれに対しても成立すると予想している. ただし一般に逆は不成立であり, 必要十分となる場合の条件などについて, 現在考察を進めている.

謝辞

今回このような素晴らしい研究集会において講演の機会をいただき, 世話人である金子昌信氏 (九州大学), 権寧魯氏 (九州大学), 岸康弘氏 (愛知教育大学), および松坂俊輝氏 (九州大学) に深く感謝いたします. また, 13 年前 (筆者は第 6 回福岡数論研究集会で講演の機会をいただいた) と同じ研究をここまで続けてこられたのは, 加川貴章氏 (立命館大学) の寄与なしでは達成し得ませんでした. ここに心からの感謝を申し上げます. 加えて, 本研究をふたたび interesting なものとしてくれた吉村隼人氏と生川青輝氏にも感謝いたします.

最後に, 至る所良い還元をもつ楕円曲線の文献表 [14] を快く提供・配布の許可をくださった山村健氏 (防衛大学校: 2024 年 3 月ご退職) に深謝いたします.

なお本研究は日本学術振興会・基盤研究 (C)20K03537 「Julia 言語を用いた新しい計算機数論システムの開発とその応用」の援助を得ています.

参考文献

- [1] M. Bertolini and G. Canuto, Good reduction of elliptic curves defined over $\mathbb{Q}(\sqrt[3]{2})$, Arch. Math. (Basel) **50** (1988), no. 1, 42–50.
- [2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I: The user language, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.
- [3] S. Comalada, Elliptic curves with trivial conductor over quadratic fields, Pacific J. Math. **144** (1990), no. 2, 237–258.
- [4] J. Cremona and M. Lingham, Finding all elliptic curves with good reduction outside a given set of primes, Experiment. Math. **16** (2007), no. 3, 303–312.
- [5] J. Cremona and T. Thongjunthug, The complex AGM, periods of elliptic curves over $\mathbb{C}$ and complex elliptic logarithms, J. Number Theory **133** (2013), no. 8, 2813–2841.

¹⁰詳細は込み入るので割愛するが, 基礎体および楕円曲線に条件がつく.

- [6] E. Herrmann and A. Pethö, S -integral points on elliptic curves. Notes on a paper of B. M. M. de Weger: “ S -integral solutions to a Weierstrass equation”, J. Théor. Nombres Bordeaux **13** (2001), no. 2, 443–451.
- [7] E. Herrmann, Bestimmung aller S -ganzen Lösungen auf elliptischen Kurven, Ph.D. Thesis, Universität des Saarlandes, 2002.
- [8] T. Kagawa, Elliptic curves with everywhere good reduction over real quadratic fields, Ph.D. Thesis, Waseda University, 1998.
- [9] M. Kida and T. Kagawa, Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields, J. Number Theory **66** (1997), no. 2, 201–210.
- [10] LMFDB, The L -functions and modular forms database, <https://www.lmfdb.org>.
- [11] The PARI Group, A computer algebra system designed for fast computations in number theory, <http://pari.math.u-bordeaux.fr/>.
- [12] B. Setzer, Elliptic curves over complex quadratic fields, Pacific J. Math. **74** (1978), no. 1, 235–250.
- [13] N. Takeshi, On elliptic curves having everywhere good reduction over cubic fields, Master’s Thesis, Tsuda College, 2012.
- [14] 山村健, Everywhere good reduction をもつ楕円曲線に関する文献 (2024 年 3 月更新版), 6pp.
- [15] S. Yokoyama and Y. Shimasaki, Non-existence of elliptic curves with everywhere good reduction over some real quadratic fields, J. Math-for-Ind. **3B** (2011), 113–117.
- [16] 吉村隼人, $\mathbb{Q}(\sqrt{-1})$ と 2 次体の合成体における楕円曲線の everywhere good reduction について, Master’s Thesis, Tokyo Metropolitan University, 2024.