

Gross 楕円曲線の二次ツイストの族の中心 L 値の非消滅について

毛塚由佳子
金沢大学

概要

本稿は、研究集会「第 18 回 数論女性の集まり」(WINJ2025) における講演で発表した主要な結果と証明の概要を解説するものである。特に、素数 $q \equiv 7 \pmod{8}$ に対し、虚二次体 $\mathbb{Q}(\sqrt{-q})$ を虚数乗法に持つ Gross 楕円曲線の二次ツイストの中心 L 値に関する非消滅定理を紹介する。この結果は、Coates と Li によって素数 q が $q \equiv 7 \pmod{16}$ の場合に証明されていた定理を、すべての $q \equiv 7 \pmod{8}$ の場合に拡張するものである。この非消滅定理から、これらの楕円曲線のモデル・ヴェイユ群とテイト・シャファレヴィッチ群が有限であることが導かれる。さらに、Birch–Swinnerton-Dyer (BSD) 予想がこの楕円曲線の族に対して完全に成立することも示される。証明の鍵となるのは、岩澤理論と一般化された Zhao の帰納法を組み合わせ、中心 L 値の代数的部分の 2-進付値を精密に決定する点にある。

目次

1	序論	2
1.1	背景：Birch–Swinnerton-Dyer 予想	2
1.2	Gross 楕円曲線	2
1.3	アーベル多様体への変換	3
1.4	主結果	4
2	証明の概略	5
2.1	証明の概略	5
3	基底段階：岩澤理論の応用	5
3.1	特別な素イデアルと岩澤理論の設定	5
3.2	岩澤主予想とセルマー群	5
4	帰納段階：一般化された Zhao の方法	6
4.1	中心的な和公式	6
4.2	帰納法の実行	7

1 序論

1.1 背景：Birch–Swinerton-Dyer 予想

楕円曲線は、数論における中心的対象の一つであり、その整数論的性質は極めて深い構造を持つことが知られている。楕円曲線 E の数体 F 上の有理点全体のなす群 $E(F)$ は、モーデル・ヴェイユの定理により有限生成アーベル群となる：

$$E(F) \cong \mathbb{Z}^r \oplus E(F)_{\text{tors}}.$$

ここで $E(F)$ のねじれ部分群 $E(F)_{\text{tors}}$ は有限群であり、 $E(F)$ の階数 r は E の算術における最も重要な不変量の一つである。

一方、楕円曲線 E/F には、その算術情報を担うハッセ・ヴェイユ L 関数 $L(E/F, s)$ が付随する。Birch–Swinerton-Dyer (BSD) 予想は、 L 関数の解析的な性質と E の算術的な性質を結びつける壮大な予想である。

BSD 予想 楕円曲線 E/F のモーデル・ヴェイユ群の階数 r は、 L 関数 $L(E/F, s)$ の $s = 1$ における零点の位数と一致する：

$$\text{rank}_{\mathbb{Z}}(E(F)) = \text{ord}_{s=1} L(E/F, s).$$

さらに、テイト・シャファレヴィッチ群 $\text{III}(E/F)$ が有限であるという仮定の元、 $L(E/F, s)$ の $s = 1$ におけるテイラー展開に対して、先頭係数は次のように与えられると予想されている：

$$\lim_{s \rightarrow 1} \frac{L(E/F, s)}{(s-1)^r} = \frac{\Omega_E \cdot \text{Reg}(E/F) \cdot \#\text{III}(E/F) \cdot \prod_v c_v}{\sqrt{|\Delta_F|} \#(E(F)_{\text{tors}})^2}.$$

ここで Ω_E は E に付随する複素周期、 $\text{Reg}(E/F)$ はネロン・テイトの高さによるレギュレーター、 $\text{III}(E/F)$ はテイト・シャファレヴィッチ群、 c_v は有限素点 v における玉河数、 Δ_F は F の判別式を表す。

この予想の最も基本的な場合は、解析的階数が 0 の場合、すなわち $L(E/F, 1) \neq 0$ の場合である。このとき、モーデル・ヴェイユ群 $E(F)$ は有限群となることが期待される。この方向での進展として、楕円曲線 E が虚二次体 K により虚数乗法 (CM) を持つ場合には Coates–Wiles や Rubin らの研究が、また CM を仮定せずモジュラーである一般的な場合には Gross–Zagier や Kolyvagin らの研究があり、大きな進展が得られている。近年では、Burungale–Flach により Rubin の結果は E が任意の代数体上に定義されている場合にすべての素数 p において一般化された。

本稿は、[4] で得られた CM 楕円曲線に関する結果を報告することを目的とする。

1.2 Gross 楕円曲線

本研究の中心的な対象は、Benedict Gross によって導入された特別な楕円曲線族である。

$q \equiv 7 \pmod{8}$ を素数とする. $K = \mathbb{Q}(\sqrt{-q})$ を虚二次体, $\mathcal{O}_K$ をその整数環とする. 体 K から $\mathbb{C}$ への埋め込みを一つ固定する. Gross 楕円曲線 A は K のヒルベルト類体 H 上で定義される楕円曲線で, 以下の特徴を持つ.

- A は, $\mathcal{O}_K$ による虚数乗法を持つ
- A の minimal discriminant ideal は $\text{disc}(A) = (-q^3)$ で与えられる.
- A は $\mathbb{Q}$ -curve である (A と $\sigma \in \text{Gal}(H/\mathbb{Q})$ のすべての共役 A^σ は isogenous である).

Gross は, 上記を満たす A が存在し, さらに A の H 上のモデル・ヴェイユ階数が 0 であることを自身の 1980 年の博士論文で示した. 続いて 1982 年に, A が H 上で大域的極小モデルを持つことも示した. Rohrlich (1980) はこれに対応して, $L(A/H, 1) \neq 0$ であることを証明し, さらに Rodriguez Villegas (1991) が別の方法によって同様の結果を与えた.

平方因子を持たない整数 R に対し, A の二次ツイスト $A^{(R)}$ は, 二次拡大 $H(\sqrt{R})/H$ に対応するツイストである. (A と $A^{(R)}$ は H 上では同型ではないが, $H(\sqrt{R})$ 上では同型になる.) Yang (1999) は R が q に対して小さい時 (およそ $R < q^{1/4}$), R による二次ツイスト $A^{(R)}$ が $L(A^{(R)}/H, 1) \neq 0$ を満たすことを示した.

本稿では, より広範な二次ツイスト族に対する L 関数の中心値の非消滅性を扱う.

1.3 アーベル多様体への変換

まず, 楕円曲線 A/H の問題を, CM 体 K 上のアーベル多様体の問題に変換する. これは Weil のスカラーの制限を用いる.

定義 1.1. $B = \text{Res}_{H/K}(A)$ を, A の定義体を H から K へ制限して得られるアーベル多様体とする. B は K 上定義された $\dim(B) = [H : K] = h$ 次元のアーベル多様体である. また, $T = \text{End}_K(B) \otimes_{\mathbb{Z}} K$ は K 上次数 h の CM 体である.

この変換により, L 関数の間には以下の関係が成り立つ. A/H の L 関数は, Deuring の定理により, A/H に付随するヘッケ指標 ψ を用いて $L(A/H, s) = L(\psi, s)^2$ と書ける. K の $\mathbb{C}$ への埋め込みを延長する形で, T の $\mathbb{C}$ への埋め込みを一つ固定し, B/K に付随するヘッケ指標を ϕ とする. このような $\alpha : T \hookrightarrow \mathbb{C}$ の選び方は h 通り存在する. A/H のヘッケ指標を ψ と書き, B/K の α に相対するヘッケ指標を ϕ^α と書くと,

$$L(\psi, s) = \prod_{\alpha \in \text{Hom}_K(T, \mathbb{C})} L(\phi^\alpha, s)$$

という積表示を持つ. したがって, $L(A/H, 1) \neq 0$ を示すことは, $L(\phi, 1) \neq 0$ を示すことに帰着される. 同様の関係がツイスト $A^{(R)}$ と $B^{(R)}$ に対しても成り立つ. 証明の目標は, $B^{(R)}/K$ に付随するヘッケ指標 ϕ_R の L 関数 $L(\phi_R, s)$ の $s = 1$ における値の 2-進付値を決定することである.

1.4 主結果

本稿では、以下に定義される楕円曲線 A の二次ツイスト族を考察する.

定義 1.2. 集合 $\mathcal{R}$ を、以下の条件を満たす相異なる素数 $r_1, \dots, r_k$ の積で書かれる平方因子を持たない正整数 $R = r_1 \cdots r_k$ ($k \geq 0$) の集合とする.

1. $r_i \equiv 1 \pmod{4}$ for $i = 1, \dots, k$.
2. 各 r_i は K で惰性が残る (inert) .

$R = 1$ の場合は $k = 0$ とみなす.

本稿で紹介する主結果は、このツイスト族の中心 L 値 $L(A^{(R)}/H, 1)$ の非消滅性とその 2-進付値の精密な評価である.

定理 1.3. q を $q \equiv 7 \pmod{8}$ なる素数とし、 $K = \mathbb{Q}(\sqrt{-q})$ とする. H を K のヒルベルト類体、 A を H 上の Gross 楕円曲線とする. $R = r_1 \cdots r_k \in \mathcal{R}$ に対し、 $A^{(R)}$ を A の二次ツイストとする. このとき、中心 L 値は $L(A^{(R)}/H, 1) \neq 0$ を満たす. さらに、 L 値の代数的部分の 2-進付値を評価するにあたり、 K において $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$ と分解し、 T を B の CM 体とする. ここで、 ϕ_R は $B^{(R)}/K$ に付随するヘッケ指標、 Ω_∞ は A の複素周期すると、 $\frac{L(\phi_R, 1)\sqrt{R}}{\Omega_\infty}$ は合成体 TH に属する. さらに、 $\mathcal{P}$ を $\mathfrak{p}$ の上にある TH の特別な素イデアルとすると、

$$\text{ord}_{\mathcal{P}} \left(\frac{L(\phi_R, 1)\sqrt{R}}{\Omega_\infty} \right) = k - 1$$

が成り立つ.

この定理は、 $q \equiv 7 \pmod{16}$ の場合に Coates と Li によって示された結果を、すべての $q \equiv 7 \pmod{8}$ の場合に拡張するものである. 特に、 $q \equiv 15 \pmod{16}$ の場合は、関連する岩澤加群が非自明となり、より深い考察を必要とした.

この主結果の直接的な帰結として、以下の系が得られる.

系 1.4. 上記と同じ仮定の下で、以下が成立する.

1. モーデル・ヴェイユ群 $A^{(R)}(H)$ とテイト・シャファレヴィッチ群 $\text{III}(A^{(R)}/H)$ はともに有限である.
2. $A^{(R)}/H$ に対して、Birch–Swinnerton-Dyer 予想が完全に成立する.
3. 非消滅となるツイストの密度は、fundamental discriminant $D \geq 1$ に対し $N(X) = \#\{D < X \mid L(A^{(D)}/H, 1) \neq 0\}$ と定義すると、

$$N(X) \gg \frac{X}{\log^{\frac{3}{4}} X}$$

を満たす.

2 証明の概略

定理 1.3 の証明は、基底段階 (base case) と帰納段階 (inductive step) の 2 つの部分から構成される。基底段階を示す過程では A のスカラー制限 $B = \text{Res}_{H/K}(A)$ に対して、素数 2 における岩澤理論を用いる。帰納段階では一般化した Zhao の方法を用いる。

2.1 証明の概略

証明は R の素因数の数 k に関する帰納法で行われる。

基底段階 ($k = 0, R = 1$): ツイストのない場合、 $L(\phi, 1) \neq 0$ を示す。これは岩澤理論を用いて達成される。具体的には、 B に付随する岩澤主予想を利用し、 $L(\phi, 1)$ の代数的部分の $\mathfrak{P}$ -進付値が -1 であることを示す。これが帰納法の出発点となる。

帰納段階 ($k \geq 1$): R の素因数の数が $k - 1$ 以下の場合に定理が成立すると仮定し、 k の場合に証明する。ここでは、Zhao によって開発された帰納的な手法をアーベル多様体の場合に一般化して用いる。異なるツイストの L 値を関係付ける和公式を使い、帰納法の仮定と基底段階の結果から、 $L(\phi_R, 1)$ の $\mathfrak{P}$ -進付値を求める。

3 基底段階：岩澤理論の応用

基底段階である $R = 1$ の場合の証明は、岩澤理論の深い応用にに基づいている。

3.1 特別な素イデアルと岩澤理論の設定

$K = \mathbb{Q}(\sqrt{-q})$ で $q \equiv 7 \pmod{8}$ であるから、素数 2 は K で分解する: $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. B の自己準同型環から生成される CM 体を T とする。このとき、 T の素イデアルで $\mathfrak{p}$ の上にある特別なもの $\mathfrak{P}$ を一つ選ぶ。この $\mathfrak{P}$ が岩澤理論を展開する上での「素数」の役割を果たす。

$F_\infty = K(B_{\mathfrak{P}^\infty})$ を、 B の $\mathfrak{P}$ -べき捻れ点すべてを K に添加した体とする。この拡大 F_∞/K は $\mathbb{Z}_2$ 拡大を部分拡大に持つ。この拡大に付随する岩澤加群を $X(F_\infty)$ とする。これは、 F_∞ の最大不分岐アーベル pro-2 拡大のガロア群である。

3.2 岩澤主予想とセルマー群

岩澤理論の主定理（主予想）は、 L 関数の p -進的な類似物（ p -進 L 関数）と、算術的な対象である岩澤加群（あるいはセルマー群）とを結びつけるものである。

命題 3.1. B/K に対する岩澤主予想は成立する（[10] で証明済み）。これは、解析的に定義される

$\mathfrak{P}$ -進 L 関数が、代数的に定義される岩澤加群 $X(F_\infty)$ の特性イデアルを生成することを主張する.

セルマー群と岩澤加群は双対的な関係にある. 有限レベルでの降下理論 (finite-level descent) と無限レベルでの岩澤理論 (infinite-level descent) を組み合わせることで, セルマー群の位数を計算することができる.

論文 [4] では, これらの降下理論の計算を組み合わせることで, $\text{Gal}(F_\infty/K_\infty)$ の作用で不変なセルマー群の部分群の位数を決定する. K_∞ は F_∞/K に含まれる $\mathbb{Z}_2$ 拡大である. この計算結果を岩澤主予想と結びつけることで, $\mathfrak{P}$ -進 L 関数の特殊値が非零であることが示され, その値が具体的に計算される.

最終的に, この一連の議論から次の結論が得られる.

系 3.2. $L(\phi, 1) \neq 0$ であり, その代数的部分の $\mathfrak{P}$ -進付値は

$$\text{ord}_{\mathfrak{P}} \left(\frac{L(\phi, 1)}{\Omega_\infty} \right) = -1$$

となる.

これは主定理の $k = 0$ の場合に相当し, 帰納法の基盤となる.

4 帰納段階：一般化された Zhao の方法

基底段階の結果を元に, R の素因数の数 k に関する帰納法で主定理を証明する. 中心的な役割を果たすのは, 異なるツイストの L 値を関係付ける和の公式である.

4.1 中心的な和公式

命題 4.1. $R = r_1 \cdots r_k \in \mathcal{R}$ とする. このとき, $H_R = H(\sqrt{r_1}, \dots, \sqrt{r_k})$ の元 V_R で, 2 の上の素点で整なものが存在し, 以下の等式を満たす.

$$\sum_{d|R} \mathcal{L}_R(\phi_d, 1) = 2^k V_R.$$

ここで $\mathcal{L}_R$ は R と q 以外の素点でのオイラー因子を取り除いた非原始的 (*imprimitive*) L 関数である.

この公式を, 通常 (原始的) L 関数を用いて書き直すと,

$$\sum_{d|R} \frac{L(\phi_d, 1)}{\Omega_\infty} \prod_{r|R/d} \left(1 - \frac{\phi_d(r\mathcal{O}_K)}{r^2} \right) = 2^k V_R$$

となる. ここで r は素数を表す.

4.2 帰納法の実行

記法を簡潔にするため, $\mathcal{L}(d) = \frac{L(\phi_d, 1)\sqrt{d}}{\Omega_\infty}$ とおく. 目標は $\text{ord}_{\mathfrak{P}}(\mathcal{L}(R)) = k - 1$ を示すことである.

Step 1: ($k = 1, R = r$) の場合 和公式は $d = 1, r$ の和となり,

$$\frac{\mathcal{L}(r)}{\sqrt{r}} + \mathcal{L}(1) \left(1 - \frac{\phi(r\mathcal{O}_K)}{r^2} \right) = 2V_r$$

と書き直せる. ヘッケ指標の性質から $\phi(r\mathcal{O}_K) = -r$ であることがわかる. 基底段階の結果より $\text{ord}_{\mathfrak{P}}(\mathcal{L}(1)) = -1$ である. 一方,

$$\text{ord}_{\mathfrak{P}} \left(1 - \frac{-r}{r^2} \right) = \text{ord}_{\mathfrak{P}} \left(1 + \frac{1}{r} \right) = \text{ord}_{\mathfrak{P}} \left(\frac{r+1}{r} \right)$$

$r \equiv 1 \pmod{4}$ より, $\text{ord}_2(r+1) = 1$ である. よって $\text{ord}_{\mathfrak{P}}(r+1) \geq 1$ となる. したがって, 第2項の付値は $\text{ord}_{\mathfrak{P}}(\mathcal{L}(1)) + \text{ord}_{\mathfrak{P}}(r+1) \geq -1 + 1 = 0$ となる. 右辺は $\text{ord}_{\mathfrak{P}}(2V_r) \geq 1$ である. 非アルキメデス付値の性質から, 和の付値は最小の付値に等しい. もし $\text{ord}_{\mathfrak{P}}(\mathcal{L}(r)/\sqrt{r}) \neq \text{ord}_{\mathfrak{P}}(\text{第2項})$ であれば, いずれかが全体の付値を決定する. 論文での精密な議論により, $\text{ord}_{\mathfrak{P}}(\mathcal{L}(r)/\sqrt{r}) = 0$ が結論付けられる. これは $k = 1$ の場合の主張 $k - 1 = 0$ と一致する.

Step 2: ($k \geq 2$) の場合 和公式を $\mathcal{L}(1)$ で割り,

$$\frac{\mathcal{L}(R)/\mathcal{L}(1)}{\sqrt{R}} + \sum_{d|R, d \neq R} \frac{\mathcal{L}(d)/\mathcal{L}(1)}{\sqrt{d}} \prod_{r|R/d} (\dots) = \frac{2^k V_R}{\mathcal{L}(1)}$$

という形に変形する. 帰納法の仮定により, $d|R, d \neq R$ なる項 $\mathcal{L}(d)$ の $\mathfrak{P}$ -進付値は分かっている. ここでの困難は, 各項が異なる体の中に値を持つことである. しかし, [4, Proposition 6.5] により, 比 $\mathcal{L}(d)/\mathcal{L}(1)$ は常に CM 体 T に属することが示される. これにより, 全ての項を T の $\mathfrak{P}$ -進完備化 $T_{\mathfrak{P}}$ で評価することが可能になる.

帰納法の仮定から, 和の中の各項 $\frac{\mathcal{L}(d)}{\mathcal{L}(1)\sqrt{d}}$ の付値は $\text{ord}_{\mathfrak{P}}(\mathcal{L}(d)) - \text{ord}_{\mathfrak{P}}(\mathcal{L}(1)) = (\text{val}(d) - 1) - (-1) = \text{val}(d)$ となる. ここで $\text{val}(d)$ は d の素因数の数. 右辺の付値は $\text{ord}_{\mathfrak{P}}(2^k V_R/\mathcal{L}(1)) \geq k - (-1) = k + 1$ となる. 和の部分 $\sum_{d|R, d \neq 1, R} (\dots)$ を $\mathfrak{P}$ のべき剰余で評価する議論により, この和全体の付値が $k + 1$ 以上であることが示される. 最終的に, 付値が最も小さい項が $\frac{\mathcal{L}(1)}{\mathcal{L}(1)} \prod (\dots) = \prod (\dots)$ の項と $\frac{\mathcal{L}(R)/\mathcal{L}(1)}{\sqrt{R}}$ の項となり, 全体の付値の関係から

$$\text{ord}_{\mathfrak{P}} \left(\frac{\mathcal{L}(R)}{\mathcal{L}(1)} \right) = k$$

が導かれる. これより,

$$\text{ord}_{\mathfrak{P}}(\mathcal{L}(R)) = k + \text{ord}_{\mathfrak{P}}(\mathcal{L}(1)) = k - 1$$

が得られ, 帰納法が完遂される.

これにより、素数 $q \equiv 7 \pmod{8}$ に付随する Gross 楕円曲線 A の、 $\mathcal{R}$ に属する整数 R による二次ツイスト $A^{(R)}$ の族に対して、以下の結果が得られた。

1. 中心 L 値は消滅しない: $L(A^{(R)}/H, 1) \neq 0$.
2. L 値の代数的部分の 2-進付値が精密に決定された: $\text{ord}_{\mathfrak{p}}(\dots) = k - 1$.

本研究の意義は、単に非消滅定理を証明しただけでなく、岩澤理論と降下法を駆使して L 値の p -進的性質を深く解明し、それを帰納的な手法と組み合わせることで、数体上の楕円曲線の無限ツイスト族に対する BSD 予想に打ち立てた点にある。証明は、 $q \equiv 7 \pmod{16}$ という技術的な制約を取り払い、より自然な数論的条件下で定理を確立したものである。

系 1.4, 1. を示すには、Gross–Zagier と Kolyvagin の定理を用いる。系 1.4, 2. は Burungale–Flach [1] の結果と合わせることでにより得られる。系 1.4, 3. における密度結果の証明は、Serre [6] の着想に密接に従うものであり、その基盤には Delange, Wintner らによる池原のタウバー型定理の一般化 および Landau [5] の方法がある。

謝辞

著者は、研究集会「第 18 回 数論女性の集まり」(WINJ2025) において本研究を発表する機会を与えてくださった主催者の皆様に感謝申し上げます。本稿は JSPS 科研費 JP25K17227 の助成を受けたものです。

参考文献

- [1] A. Burungale and M. Flach, *The conjecture of Birch and Swinnerton-Dyer for certain elliptic curves with complex multiplication*, Camb. J. Math. 12, No. 2, pp. 357–415 (2024).
- [2] J. Coates and Y. Li, *Non-vanishing theorems for central L -values of some elliptic curves with complex multiplication*, Proc. Lond. Math. Soc. (3) 121 (2020), no. 6, pp. 1531–1578.
- [3] B. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics 776, Springer, Berlin, 1980.
- [4] Y. Kezuka and Y. Li, *Non-vanishing of central L -values of the Gross family of elliptic curves*, J. Lond. Math. Soc., Vol. 111, Issue 6 (2025)
- [5] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. der Math. und Phys., (3) 13 (1908), pp. 305–312.
- [6] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Séminaire Delange–Pisot–Poitou. Théorie des nombres 16.1 (1974–1975), pp. 1–28.