楕円曲線の p 進 L 関数と p 等分体のイデアル類群の GALOIS 加群構造について

ON p-ADIC L-FUNCTIONS OF ELLIPTIC CURVES AND THE IDEAL CLASS GROUPS OF THE p-TH DIVISION FIELDS AS GALOIS MODULES

慶應義塾大学 臺信 直人
NAOTO DAINOBU
KEIO UNIVERSITY

1. 導入

整数論における興味深い現象の一つは, Riemann ゼータ関数をはじめとした L 関数と呼ばれる複素関数と, イデアル類群などの代数的な対象とがしばしば深く関係し合っていることである. そのような現象の例として, 円分体のイデアル類群に関する Herbrand と Ribet の結果がある. 以下, p を奇素数とし, ζ_p を $\mathbb{C}$ の中の 1 の原始 p 乗根とする. 円分体 $\mathbb{Q}(\zeta_p)$ のイデアル類群 $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ に対し, $M_p := \mathrm{Cl}(\mathbb{Q}(\zeta_p)) \underset{\mathbb{Z}}{\otimes} \mathbb{F}_p$ とかく. M_p には $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ が作用しており, $p \nmid \#\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = p-1$ なので,

$$M_p = \bigoplus_{i=0}^{p-2} M_p^{(\omega^i)}$$

と M_p を Galois 加群として直和分解できる. ここで, $\omega : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{F}_p^\times$ は Teichmüller 指標で, $M_p^{(\omega^i)}$ は M_p の ω^i 部分である. Herbrand と Ribet は, Riemann ゼータ関数 $\zeta(s)$ の特殊値と, 円分体のイデアル類群の Galois 加群構造とが次の様に深く関わり合っていることを示した.

定理 1.1 (Herbrand-Ribet [3, 4])**.** 任意の正の偶数 n に対して,

$$p \mid \zeta(1-n)\ (\in \mathbb{Q}) \iff M_p^{(\omega^{1-n})} \neq 0.$$

現在では, 他にも様々な代数体の Abel 拡大に対し, そのイデアル類群と代数体の L 関数との間に定理 1.1と同様の現象が知られている. しかし, 代数体の非 Abel 拡大のイデアル類群に対しては, 同様の現象が知られているケースは少ない.

最近, Prasad らによって定理 1.1の, ある非 Abel な設定における類似が研究されている. $\mathbb{Q}$ 上の楕円曲線 E と奇素数 p に対し, E の $\mathbb{Q}$ 上の p 等分体 $K := \mathbb{Q}(E[p])$ が定まる. 以下, E に伴う Galois 表現 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$ は全射であると仮定する. 特に, $E[p]$ は既約 $\mathbb{F}_p[\mathrm{Gal}(K/\mathbb{Q})]$ 加群で, $K/\mathbb{Q}$ は非 Abel 拡大となる. K のイデアル類群 $\mathrm{Cl}(K)$ に対し, $\mathrm{Gal}(K/\mathbb{Q})$ 加群 $M_p(E) := \mathrm{Cl}(K) \underset{\mathbb{Z}}{\otimes} \mathbb{F}_p$ を考え, その $\mathbb{F}_p[\mathrm{Gal}(K/\mathbb{Q})]$ 加群としての半単純化 $M_p(E)^{\mathrm{ss}}$ を

$$M_p(E)^{\mathrm{ss}} = \bigoplus_M M^{\oplus r(M)}$$

と表示する. ここに, 上の直和の M は既約 $\mathbb{F}_p[\mathrm{Gal}(K/\mathbb{Q})]$ 加群全てを走り, $r(M)$ は M 成分の重複度である. Prasad は K を円分体 $\mathbb{Q}(\zeta_p)$ の類似だと見て, $M_p(E)^{\mathrm{ss}}$ の既約成分 $E[p]$ の非自明性を定理 1.1と同様の観点から研究しようとした.

もう少し詳細に彼の研究を述べる. E の Hasse-Weil L 関数を $L(E,s)$, その $s=1$ での Taylor 展開の先頭係数を $L^*(E,1)$ と書き, $L^*(E,1)$ を E の周期とレギュレータで割った値を $L^*(E,1)_{\mathrm{alg}}$ と書く. 一般に $L^*(E,1)_{\mathrm{alg}} \in \mathbb{Q}$ であると予想されており, $\mathrm{ord}_{s=1}L(E,s) \leq 1$ であれば, これは正しい. 以下, この予想を仮定して話を進める. Prasad は次の疑問[1]をモチベーションとして, 一連の研究 [8, 10] を行った.

問 1.2.

$$p \mid L^*(E,1)_{\mathrm{alg}} \overset{???}{\iff} r(E[p]) \neq 0.$$

つまり, L 関数 $L(E,s)$ を定理 1.1のゼータ関数 $\zeta(s)$ に対応するものと見て, $L^*(E,1)_{\mathrm{alg}}$ の値と, 等分体のイデアル類群の“分解”に出てくる既約因子 $E[p]$ の非自明性とが定理 1.1の様に関係しているのではないか?という発想である.

注意 1.3. 問 1.2で期待している L 関数とイデアル類群との関係は, 少々奇妙なものに見えると思う. と言うのも, L 関数と代数的対象物との関係を扱う研究では, モチーフを一つ固定して, そのモチーフの L 関数と Selmer 群との関係を探求するのが一般的である. 一方, ここで考えたいのは 楕円曲線のL 関数と 代数体 K のイデアル類群 (Selmer 群) とのモチーフ横断的な関係である.

[10] で, Prasad と Shekhar は問 1.2に部分的な回答を与えている.

[1]この疑問自体はナイーブなもので, Prasad も [8] でしっかりと予想の形で述べているわけではない. 実際, $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}) \geq 2$ の場合には $\Leftarrow$ の反例が [10] の結果から簡単に作れる. 後に説明する様に, $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}) = 1$ の場合にも本稿の筆者の結果から $\Leftarrow$ の反例が与えられる.

定理 1.4 (Prasad-Shekhar)**.** E の法 p 還元の $\mathbb{F}_p$-有理点の集合を $\tilde{E}(\mathbb{F}_p)$, E の局所玉河数の積を $\mathrm{Tam}(E/\mathbb{Q})$, E の $\mathbb{Q}$ 上の *Tate-Shafarevich* 群を $Ш(E/\mathbb{Q})$ と書く. 二つの条件 $p \nmid \#\tilde{E}(\mathbb{F}_p) \cdot \mathrm{Tam}(E/\mathbb{Q})$ と $\#Ш(E/\mathbb{Q}) < \infty$ を仮定するとき,

$$p \mid \#Ш(E/\mathbb{Q}) \Rightarrow r(E[p]) \neq 0.$$

系 1.5. *Birch–Swinnerton-Dyer* 予想 *(BSD* 予想*)* の p 部分の成立と, 定理 *1.4*の条件 $p \nmid \#\tilde{E}(\mathbb{F}_p) \cdot \mathrm{Tam}(E/\mathbb{Q})$, $\#Ш(E/\mathbb{Q}) < \infty$ を仮定する. このとき,

$$p \mid L^*(E,1)_{\mathrm{alg}} \Rightarrow r(E[p]) \neq 0.$$

Proof. v_p を $v_p(p) = 1$ と正規化された加法的 p 進付値とする. 仮定から,

$$v_p\left(L^*(E,1)_{\mathrm{alg}}\right) = v_p\left(\frac{\mathrm{Tam}(E/\mathbb{Q}) \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}\right) = v_p(\#Ш(E/\mathbb{Q}))$$

が成立する. 一つ目の等号は BSD 予想の p 部分, 二つ目は Theorem 1.4の条件による. よって, 定理 1.4から系 1.5を得る. □

注意 1.6. $\#Ш(E/\mathbb{Q}) < \infty$ のとき, $\#Ш(E/\mathbb{Q})$ は平方数であることが知られている. よって, 系 1.5は「$v_p(L^*(E,1)_{\mathrm{alg}}) \geq 2 \Rightarrow r(E[p]) \neq 0$」とも主張できる.

本稿で紹介したい筆者の結果は, 系 1.5の精密化, 拡張を与えるものである. 筆者は [5] で, E 上の特別な性質を持つ有理点を用いて, 定理 1.4とは異なる観点から $r(E[p])$ の非自明性を考察した. その結果, $\mathrm{ord}_{s=1}L(E,s) = 1$ の場合に, E の円分 p 進 L 関数が定める p 進的な量が $r(E[p])$ の非自明性に寄与することを新たに発見した. その寄与の分だけ系 1.5を精密化したのが一つ目の主結果 (定理 3.2) である. 詳細は 3章で述べるが, 主張は以下である.

定理 A (D., 定理 3.2)**.** 定理 *3.2*の条件 (1) ∼ (5) の下で,

$$v_p(L'(E,1)_{\mathrm{alg}} \cdot \mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)]) \geq 2 \Rightarrow r(E[p]) \neq 0.$$

定理 3.2の条件 (1) より $\mathrm{ord}_{s=1}L(E,s) = 1$ の場合を考えるので, $L^*(E,1) = L'(E,1)$ になることに注意しておく. 上記の $\mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)]$ は E の円分 p 進 L 関数などから定まる値で, 定理 3.2の条件の下で $\mathbb{Z}_p$ の元である. 注意 1.6を踏まえると, この量の分だけ定理 Aは系 1.5を精密化している.

定理 Aでは E の $\mathbb{Q}$ 上の等分体のイデアル類群を考察していたが, 二つ目の主結果 (定理 3.6) では基礎体を虚二次体 F に拡張して, F 上の E の p 等分体 $F(E[p])$ のイデアル類群を考察した. その結果, Bertolini–Darmon–Prasanna らが構成した E の F 上

の反円分 p 進 L 関数と, $F(E[p])$ のイデアル類群の Galois 加群構造との間に定理 A と同様の関係を新たに発見した. 次の章から, 上に述べた二つの筆者の結果について, その詳細を説明する.

以下, $\bar{\mathbb{Q}}$ を $\mathbb{Q}$ の代数閉包とし, 埋め込み $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}, \mathbb{C}_p$ を固定する. ここで, $\mathbb{C}_p$ は $\mathbb{Q}_p$ の代数閉包 $\bar{\mathbb{Q}}_p$ の p 進完備化である. また, 代数体 L に対し, その絶対 Galois 群 $\mathrm{Gal}(\bar{\mathbb{Q}}/L)$ を G_L で表すことにする.

2. 等分体のイデアル類群に関する結果

まず, 楕円曲線の等分体のイデアル類群に関して, これまでに得られていた結果をまとめる. E を $\mathbb{Q}$ 上の楕円曲線, p を奇素数とする. この章では, L を一般の代数体とし, L 上の E の p 等分体 $L(E[p])$ のイデアル類群 $\mathrm{Cl}(L(E[p]))$ を考える. ただし, Galois 表現 $G_L \to \mathrm{Aut}_{\mathbb{F}_p}(E[p])$ は 1章と同様, 全射である場合を考える.

以下, $M_{p,L}(E) := \mathrm{Cl}(L(E[p])) \underset{\mathbb{Z}}{\otimes} \mathbb{F}_p$ と定め, その $\mathbb{F}_p[\mathrm{Gal}(L(E[p])/L)]$-加群としての半単純化 $M_{p,L}(E)^{\mathrm{ss}}$ を

$$M_{p,L}(E)^{\mathrm{ss}} = \bigoplus_{M} M^{\oplus r_L(M)}$$

と表す. 上の直和で M は既約 $\mathbb{F}_p[\mathrm{Gal}(L(E[p])/L)]$ 加群を全て走り, $r_L(M)$ は M 成分の重複度である. 1章と記号を合わせ, $L = \mathbb{Q}$ のとき $r_{\mathbb{Q}}(M) := r(M)$ と書く.

Galois コホモロジー群 $H^1(L, E[p])$ の不分岐部分を

$$H^1_{\mathrm{ur}}(L, E[p]) := \mathrm{Ker}\left(H^1(L, E[p]) \to \prod_{\mathfrak{p}:\text{素イデアル}} H^1(L^{\mathrm{ur}}_{\mathfrak{p}}, E[p]) \right)$$

と定める. ここに, $L_{\mathfrak{p}}$ は L の素イデアル $\mathfrak{p}$ における L の完備化で, その最大不分岐拡大を $L^{\mathrm{ur}}_{\mathfrak{p}}$ と書いた. $M_{p,L}(E)^{\mathrm{ss}}$ における $E[p]$ 成分の重複度 $r_L(E[p])$ の考察には, 不分岐部分 $H^1_{\mathrm{ur}}(L, E[p])$ が重要である.

命題 2.1.

$$H^1_{\mathrm{ur}}(L, E[p]) \neq 0 \Rightarrow r_L(E[p]) \neq 0$$

Proof. $E[p]$ の $\mathrm{Gal}(L(E[p])/L)$ 加群としての既約性から, 制限写像

$$H^1(L, E[p]) \to H^1(L(E[p]), E[p])^{\mathrm{Gal}(L(E[p])/L)} \simeq \mathrm{Hom}_{\mathrm{Gal}(L(E[p])/L)}(G_{L(E[p])}, E[p])$$

は同型である. 上の同型で, $H^1_{\mathrm{ur}}(L, E[p])$ は部分群

$$\mathrm{Hom}_{\mathrm{Gal}(L(E[p])/L)}(M_{p,L}(E), E[p]) \subset \mathrm{Hom}_{\mathrm{Gal}(L(E[p])/L)}(G_{L(E[p])}, E[p])$$

に移る．ここで, $L(E[p])^{\mathrm{ur}}$ を $L(E[p])$ の最大不分岐 Abel 拡大として, 類体論の同型 $\mathrm{Gal}(L(E[p])^{\mathrm{ur}}/L(E[p])) \simeq \mathrm{Cl}(L(E[p]))$ を用いた．$\mathrm{Hom}_{\mathrm{Gal}(L(E[p])/L)}(M_{p,L}(E), E[p])$ の任意の非自明な元は $E[p]$ の既約性から全射になるので, 主張を得る． □

以下, 二つの観点から $H^1_{\mathrm{ur}}(L, E[p])$ の非自明性を帰結する命題を紹介する．

命題 2.2 ([6, Proposition 2.2])**.** 次の条件を仮定する．

(1) p は E/L の局所玉河数の積 $\mathrm{Tam}(E/L)$ を割らない．
(2) 任意の L の p 進素点 $\mathfrak{p} \mid p$ において, $E(L_{\mathfrak{p}})[p] = 0$.

このとき,

$$\dim_{\mathbb{F}_p}(H^1_{\mathrm{ur}}(L, E[p])) \geq \dim_{\mathbb{F}_p}(\mathrm{Sel}(L, E[p])) - [L : \mathbb{Q}].$$

証明のスケッチ： [1, Lemma 3.4] から, 制限写像 $\mathrm{Sel}(L, E[p]) \to H^1(L^{\mathrm{ur}}_{\mathfrak{q}}, E[p])$ は任意の $\mathfrak{q} \nmid p$ に対して 0-map である．したがって, p 進素点に対する制限写像について

$$\mathrm{Ker}\left(\mathrm{Loc}^{\mathrm{ur}}_p : \mathrm{Sel}(L, E[p]) \to \prod_{\mathfrak{p}|p} H^1(L^{\mathrm{ur}}_{\mathfrak{p}}, E[p])\right) \subset H^1_{\mathrm{ur}}(L, E[p]) \tag{2.1}$$

が成り立つ．一方, 仮定 (2) によって $\dim_{\mathbb{F}_p} \mathrm{Im}(\mathrm{Loc}^{\mathrm{ur}}_p) \leq [L : \mathbb{Q}]$ となることがわかるので, $\mathrm{Loc}^{\mathrm{ur}}_p$ に対する次元定理と包含 (2.1) によって主張を得る． □

注意 2.3. $L = \mathbb{Q}$ の場合, 命題 2.2は [10, Theorem 3.1] で得られており, 命題 2.2はその一般化である．

命題 2.2から, Selmer 群の次元が大きい場合には $H^1_{\mathrm{ur}}(L, E[p]) \neq 0$ が帰結できることがわかった．次に, E 上に特別な条件を満たす有理点がある場合にも, 同様の非自明性が帰結できることを述べる．以下, L の素点 $\mathfrak{p} \mid p$ を任意に一つ固定する．そして, E は $E/L_{\mathfrak{p}}$ の minimal model を与える $\mathcal{O}_L$ 上の Weierstrass 方程式で定義されていると仮定する．non-singular reduction を持つ点のなす $E(L_{\mathfrak{p}})$ の部分群を $E_0(L_{\mathfrak{p}})$, reduction $E_0(L_{\mathfrak{p}}) \to \tilde{E}(\mathbb{F})$ の核を $E_1(L_{\mathfrak{p}})$ と書く．ここで, $\mathbb{F}$ は $L_{\mathfrak{p}}$ の剰余体である．

命題 2.4 ([6, Proposition 2.5])**.** 次の条件を仮定する．

(1) $L/\mathbb{Q}$ は *Galois* 拡大．
(2) p は E/L の局所玉河数の積 $\mathrm{Tam}(E/L)$ を割らない．
(3) $L_{\mathfrak{p}}/\mathbb{Q}_p$ の分岐指数 $e := e(L_{\mathfrak{p}}/\mathbb{Q}_p)$ に対し, $e(L_{\mathfrak{p}}/\mathbb{Q}_p) < p - 1$ が成立する．

このとき, E の L-有理点 $Q \in (E(L) \cap E_1(L_{\mathfrak{p}})) \setminus pE(L)$ で,

$$v_p(\log_\omega(Q)) \geq \frac{e+1}{e}$$

なるものがあれば $H^1_{\mathrm{ur}}(L, E[p]) \neq 0$ である. ここで, $\mathfrak{m}_\mathfrak{p}$ を $L_\mathfrak{p}$ の極大イデアルとして, $\log_\omega : E_1(L_\mathfrak{p}) \to \mathfrak{m}_\mathfrak{p}$ は固定した $E/L_\mathfrak{p}$ の *minimal model* に対する *Néron* 微分 ω から定まる *formal logarithm* である.

証明のスケッチ : Kummer 写像 $\kappa : E(L)/pE(L) \to H^1(L, E[p])$ による点 Q の像 $\kappa(Q) \in \mathrm{Sel}(L, E[p])$ が $H^1_{\mathrm{ur}}(L, E[p])$ の元となることを示す. 仮定 (2) と [1, Lemma 3.4] によって, 任意の $\mathfrak{q} \nmid p$ に対して $\mathrm{Sel}(L, E[p]) \subset \mathrm{Ker}(H^1(L, E[p]) \to H^1(L^{\mathrm{ur}}_\mathfrak{q}, E[p]))$ である. 仮定 (1) から, 後は固定した L の素点 $\mathfrak{p} \mid p$ に対して

$$\kappa(Q) \in \mathrm{Ker}(H^1(L, E[p]) \to H^1(L^{\mathrm{ur}}_\mathfrak{p}, E[p]))$$

を示せば良いが, これには $Q \in pE(L_\mathfrak{p})$ を示せばよい. 仮定 (3) によって, $\log_\omega$ は同型 $E_1(L_\mathfrak{p}) \simeq \mathfrak{m}_\mathfrak{p}$ を与えるが, $\log_\omega(Q)$ に課された付値の条件は $\log_\omega(Q) \in p\mathfrak{m}_\mathfrak{p} \subset \mathfrak{m}_\mathfrak{p}$ であることを導く. つまり, $Q \in pE_1(L_\mathfrak{p}) \subset pE(L_\mathfrak{p})$ である. □

注意 2.5. $E_1(L_\mathfrak{p})$ は命題 2.4の条件 (3) から torsion-free となり, 点 Q は必然的に位数無限大となる. 特に, 命題 2.4は $\mathrm{rank}_\mathbb{Z}(E(L)) > 0$ のときにしか使えない.

$H^1_{\mathrm{ur}}(L, E[p])$ の非自明性を帰結する道具として命題 2.2, 2.4を紹介した. 命題 2.1より, これらは $r_L(E[p])$ の非自明性を帰結するのだった. ここで強調したいのは, 命題 2.4によってのみ $H^1_{\mathrm{ur}}(L, E[p]) \neq 0$ が帰結できる例が, $\mathrm{rank}_\mathbb{Z}(E(L)) = 1$ の場合に多く存在することである.

例 2.6. $L = \mathbb{Q}$ とし, E を方程式 $y^2 + y = x^3 + x$ で定義される楕円曲線とする (Cremona label は 43a1). このとき, 命題 2.4の仮定 (1), (3) は自明に成立している. (2) の成立も具体的計算によって確かめられる.

この例の Mordell-Weil 群は $E(\mathbb{Q}) \simeq \mathbb{Z}$ であり, その生成元として $Q := (0, 0)$ が取れる. $\#\tilde{E}(\mathbb{F}_{13}) = 19$ なので, $19 \cdot Q \in E_1(\mathbb{Q}_{13})$ であり, 計算機によって $v_{13}(\log_\omega(19 \cdot Q)) = 3$ が確かめられる. ゆえに, 命題 2.4から $r(E[13]) \neq 0$ である. BSD 予想の 13 部分を認めると (この例では正しいことが示せるが), $13 \nmid \#Ш(E/\mathbb{Q})$ が示せるので, 命題 2.2からは $r(E[13]) \neq 0$ を帰結できない.

L が $\mathbb{Q}$ や虚二次体の場合に, 命題 2.4による $r_L(E[p])$ の非自明性への寄与を E の p 進 L 関数の言葉で読み替え, 系 1.5へ加えたのが次に述べる本稿の主結果である.

3. 主結果

3.1. $\mathbb{Q}$ 上の等分体に関する結果. まず, 楕円曲線の円分 p 進 L 関数に関する記号について必要な限りでまとめる. $\mathbb{Q}$ 上の楕円曲線 E と奇素数 p を固定し, E は p で良還

元を持ち, $E[p]$ は $G_{\mathbb{Q}}$ の $\mathbb{F}_p$ 上の表現として既約であるとする. E の p 進 Tate 加群を $T := T_pE$ で表し, $V := T \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p$ とおく.

$a_p(E) := p+1-\#\tilde{E}(\mathbb{F}_p)$ と定め, Hecke 多項式 $x^2 - a_p(E)x + p$ の二つの根 $\alpha, \beta \in \bar{\mathbb{Q}}_p$ を $v_p(\alpha) \leq v_p(\beta)$ となるように並べておく.

岩澤コホモロジー類 $\mathbf{z}^{\mathrm{BK}} \in H^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, T) := \varprojlim H^1(\mathbb{Q}_n, T)$ を [7] で導入された E に伴う Beilinson–Kato 元のなす類とし, その局所化による $H^1_{\mathrm{Iw}}(\mathbb{Q}_{\infty,p}, T) := \varprojlim H^1(\mathbb{Q}_{n,p}, T)$ での像も同じ記号で書く. ここで, $\mathbb{Q}_\infty$ は $\mathbb{Q}$ の円分 $\mathbb{Z}_p$ 拡大, $\mathbb{Q}_n$ は $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$ となる唯一の $\mathbb{Q}_\infty/\mathbb{Q}$ の中間体である.

$* \in \{\alpha, \beta\}$ に対し, Perrin-Riou の big logarithm map による $\mathbf{z}^{\mathrm{BK}}$ の像を用いて E の $*$-p 進 L 関数 $\mathcal{L}_{p,*}(E, X)$ $(\in \mathbb{Q}_p(\alpha)[[X]])$ を定める. ここで, X はべき級数環 $\mathbb{Q}_p(\alpha)[[X]]$ の変数である. $\mathcal{L}_{p,*}(E, X)$ の定義の詳細は [9, Section 3] を参照されたい. $*$-p 進 L 関数は, その特殊値が導手 p べきの Dirichlet 指標 χ で捻られた L 関数 $L(E, \chi, s)$ の特殊値を $*$ に応じた補完公式によって捉えるものである.

以下, $r_{\mathrm{an}}(E/\mathbb{Q}) := \mathrm{ord}_{s=1}L(E, s) = 1$ であると仮定する. これは, 命題 2.4が使える状況, 及び (p 進) BSD 予想の p 部分の成立が知られている場合を考えたい事情による. この状況で, 1章で触れた p 進的な量 $\mathcal{S}_{\alpha,\beta}$ を以下の様に定義する.

定義 3.1.

$$\mathcal{S}_{\alpha,\beta} := \left(1 - \frac{1}{\alpha}\right)^{-2} \mathcal{L}'_{p,\alpha}(E, 0) - \left(1 - \frac{1}{\beta}\right)^{-2} \mathcal{L}'_{p,\beta}(E, 0) \ (\in \mathbb{Q}_p(\alpha))$$

本稿の一つ目の主結果は次である.

定理 3.2 (D. [6, Theorem 4.1])**.** 以下の条件を仮定する.

(1) E は p で良還元とし, $r_{\mathrm{an}}(E/\mathbb{Q}) = 1$.
(2) *Galois* 表現 $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_p}(E[p])$ は全射.
(3) E と p に対する円分岩澤主予想が正しい.
(4) $p \nmid a_p(E)$ のときは, α-p 進 *height pairing* が非自明.
(5) $p \nmid \#\tilde{E}(\mathbb{F}_p) \cdot \mathrm{Tam}(E/\mathbb{Q})$.

このとき,

$$v_p(L'(E, 1)_{\mathrm{alg}} \cdot \mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)]) \geq 2 \Rightarrow r(E[p]) \neq 0.$$

ここで, ω は E の *Néron* 微分を比較同型で $\mathbf{D}_{\mathrm{crys}}(V)$ の元と見たもの, φ は $\mathbf{D}_{\mathrm{crys}}(V)$ の *Frobenius*, *pairing* $[,] : \mathbf{D}_{\mathrm{crys}}(V) \times \mathbf{D}_{\mathrm{crys}}(V) \to \mathbb{Q}_p$ は *cup* 積である.

注意 3.3. 仮定 (1), (3), (4) の下では, $\mathcal{L}'_{p,\alpha}(E,0)$ の特殊値公式である p 進 BSD 予想の p 部分, 及び BSD 予想の p 部分の正当性が Schneider, Perrin-Riou, Kobayashi らの結果によって知られている. (2), (5) の仮定は命題 2.2, 2.4を使うためのものである. いずれの仮定もそこまで強いものではない. (2) で仮定した円分岩澤主予想は, 例えば $p \nmid a_p(E)$ であれば Kato–Skinner–Urban によって緩い条件の下で証明されている.

注意 3.4. 定理 3.2は, 定理の条件の下で系 1.5の精密化を与えている. 実際, 定理 3.2の条件 (5) において $p \nmid \#\tilde{E}(\mathbb{F}_p)$ を仮定したので, 任意の点 $Q \in E(\mathbb{Q}_p)$ に対して $\log_\omega(Q) \in p\mathbb{Z}_p$ である. 定理 3.2の条件の下で証明される命題 4.1 (後述) によると, このとき $v_p(\mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)]) \geq 1$ が証明できる. 従って, 定理 3.2から系 1.5が導かれる.

例 3.5. $p = 13$ とし, E を $y^2 + y = x^3 + x$ で定義される楕円曲線とする (例 2.6で扱ったもの). このとき, 定理の条件 (1), (2), (4), (5) の成立が計算により確認できる. また, $13 \nmid a_{13}(E)$ であり, Kato–Skinner–Urban の結果から条件 (3) の成立も確認できる.

今, $v_{13}(L'(E,1)_{\mathrm{alg}}) = 0$ であり, 系 1.5からは $r(E[13]) \neq 0$ を帰結できない. 一方, 命題 4.1の等式と例 2.6の点 $Q = (0,0) \in E(\mathbb{Q})$ に対する計算を合わせることで, $v_{13}(\mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)]) = 5$ がわかる. 従って, 定理 3.2から $r(E[13]) \neq 0$ が帰結できる.

例 3.5の様に, p 進的な量 $\mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)]$ を考慮して初めて $r(E[p]) \neq 0$ が帰結される例は大変多く観察できる. このことから, $r_{\mathrm{an}}(E/\mathbb{Q}) = 1$ の場合に限定されるが, 定理 3.2は系 1.5を強く精密化したものだと筆者は考えている.

3.2. **虚二次体上の等分体に関する結果.** 引き続き E を $\mathbb{Q}$ 上の楕円曲線で, 奇素数 p で良還元を持つものとする. 今度は虚二次体 F 上の E の p 等分体 $F(E[p])$ のイデアル類群を, 定理 3.2と同様の観点から考察してみる.

定理 3.2と同様に, E の F 上の Hasse-Weil L 関数 $L(E/F,s)$ に対し, $r_{\mathrm{an}}(E/F) := \mathrm{ord}_{s=1}L(E/F,s) = 1$ の場合を考える. このとき, 微分値 $L'(E/F,1)$ を周期とレギュレータで割った値 $L'(E/F,1)_{\mathrm{alg}}$ について, $L'(E/F,1)_{\mathrm{alg}} \in \mathbb{Q}$ が知られている. さらに, 虚二次体 F に対して以下の条件を仮定する.

- (a) Galois 表現 $G_F \to \mathrm{Aut}_{\mathbb{F}_p}(E[p])$ は全射.
- (b) F の判別式は p と E の導手 $\mathrm{Cond}(E)$ と素.
- (c) $\mathrm{Cond}(E)$ を割る任意の素数は F で分解する (Heegner 条件).
- (d) p は F で分解する.

以下, p の上にある F の素イデアル $\mathfrak{p}$ を一つ取り, $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ と書く. 以上の状況で, Bertolini–Darmon–Prasanna, Brakočević, Castella-Hsieh らによって構成された E の

F 上の反円分 p 進 L 関数を, $\mathcal{L}_{\mathfrak{p}}^{\mathrm{BDP-B}}(X) \in \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[X]]$ と書く. ここで, $\hat{\mathbb{Z}}_p^{\mathrm{ur}}$ は $\mathbb{Q}_p^{\mathrm{ur}}$ の完備化の付値環である. また, $L_{\mathfrak{p}}^{\mathrm{BDP-B}}(X) := (\mathcal{L}_{\mathfrak{p}}^{\mathrm{BDP-B}}(X))^2$ とおく. $L_{\mathfrak{p}}^{\mathrm{BDP-B}}(X)$ は, その特殊値が反円分 Hecke 指標で捻られた E の F 上の L 関数の値を捉えるものである.

以上の設定において, $L_{\mathfrak{p}}^{\mathrm{BDP-B}}(X)$ の特殊値が定理 3.2と同様に, そしてより率直な形で $r_F(E[p])$ の非自明性へ寄与することがわかった.

定理 3.6 (D. [6, Theorem 4.7])**.** 以下の条件を仮定する.

(1) E は p で良還元とし, $r_{\mathrm{an}}(E/F) = 1$.
(2) 前ページの条件 $(a) \sim (d)$ が成り立つ.
(3) E と $\mathfrak{p}$ に対する反円分岩澤主予想が正しい.
(4) $p \nmid \#\tilde{E}(\mathbb{F}_p) \cdot \mathrm{Tam}(E/\mathbb{Q})$.

このとき,

$$v_p(L'(E/F,1)_{\mathrm{alg}} \cdot L_{\mathfrak{p}}^{\mathrm{BDP-B}}(0)) \geq 1 \Rightarrow r_F(E[p]) \neq 0.$$

注意 3.7. 定理 3.2では E の円分 p 進 L 関数の微分値を扱っていたが, ここでは特殊値 $L_{\mathfrak{p}}^{\mathrm{BDP-B}}(0)$ を考えていることに注意する. $r_{\mathrm{an}}(E/F) = 1$ のとき, $L_{\mathfrak{p}}^{\mathrm{BDP-B}}(0) \neq 0$ であることが Bertolini–Darmon–Prasanna の結果により知られている.

注意 3.8. Castella らの preprint [2] によると, 定理 3.6の仮定 (1), (3) と (2) の (a) の下では, $L_{\mathfrak{p}}^{\mathrm{BDP-B}}(0)$ の特殊値公式である p 進 BSD 予想の p 部分, 及び $L'(E/F,1)_{\mathrm{alg}}$ の特殊値公式である BSD 予想の p 部分が正しい. (4) の仮定は命題 2.2, 2.4を使うためのものである. いずれの仮定もそこまで強いものではない. (3) で仮定した反円分岩澤主予想は, $p \nmid a_p(E)$ の場合には, Burungale–Castella–Kim によって緩い条件の下で証明されている. $p \mid a_p(E)$ の場合にも, 特に $a_p(E) = 0$ であれば, [2, Corollary 7.2] において緩い条件の下で証明されている.

4. 証明のあらすじ

最後に, 定理 3.2, 3.6の証明のあらすじを述べる. いずれも, 命題 2.4で見られた有理点の log の値による重複度 $r_L(E[p])$ ($L = \mathbb{Q}$, 虚二次体 F) の非自明性への寄与を, p 進 L 関数の言葉に読み替えるのがポイントとなる.

4.1. **定理 3.2の証明のスケッチ.** 定理の条件 (1) で $r_{\mathrm{an}}(E/\mathbb{Q}) = 1$ としたので, Gross–Zagier–Kolyvagin の結果によって, $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 1$ かつ $\#Ш(E/\mathbb{Q}) < \infty$ である. そこで, $Q \in E(\mathbb{Q})$ を $E(\mathbb{Q})$ の自由部分の生成元とする. 定理 1.4と命題 2.4から,

$$v_p(\#Ш(E/\mathbb{Q}) \cdot \log_\omega(Q)) \geq 2 \Rightarrow r(E[p]) \neq 0$$

である. 実際, $v_p(\#Ш(E/\mathbb{Q})) > 0$ であれば $v_p(\#Ш(E/\mathbb{Q})) \geq 2$ であり, 定理 1.4から $r(E[p]) \neq 0$ がいえる. $v_p(\#Ш(E/\mathbb{Q})) = 0$ ならば, $v_p(\log_\omega(Q)) \geq 2$ であり, $\#\tilde{E}(\mathbb{F}_p)\cdot Q$ が命題 2.4の条件を満たし $r(E[p]) \neq 0$ が帰結される. そこで,

$$v_p(L'(E,1)_{\mathrm{alg}} \cdot \mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)]) \geq 2 \Rightarrow v_p(\#Ш(E/\mathbb{Q}) \cdot \log_\omega(Q)) \geq 2 \tag{4.1}$$

が証明できれば定理 3.2が示される. (4.1) の証明は次の付値の等式に帰着される.

命題 4.1. 定理 *3.2*の仮定の下で,

$$v_p(\mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)]) = v_p(\#Ш(E/\mathbb{Q}) \cdot \log_\omega(Q)^2) + v_p(\alpha - \beta) - 1.$$

注意 3.3より, 今 BSD 予想の p 部分が正しく, その帰結として $v_p(L'(E,1)_{\mathrm{alg}}) = v_p(\#Ш(E/\mathbb{Q}))$ が成り立つ. この等式と命題 4.1から (4.1) が証明できる.

最後に命題 4.1の証明の流れを述べる. $\mathcal{S}_{\alpha,\beta}$ を $Ш(E/\mathbb{Q})$ や $\log_\omega(Q)$ と結びつけるにあたり, 両者の間に $\mathbf{z}^{\mathrm{BK}}$ の Bottom layer $z^{\mathrm{BK}} \in \mathrm{Sel}(\mathbb{Q}, T)(\subset H^1(\mathbb{Q}, T))$ を仲介させる. まず, E の α, β-p 進 L 関数の定義と, Perrin-Riou の big logarithm が Bloch-Kato の log を補完していることから, $\mathcal{S}_{\alpha,\beta}$ は z^{BK} を用いて

$$\mathcal{S}_{\alpha,\beta} \cdot [\omega, \varphi(\omega)] = \log_\omega(z^{\mathrm{BK}}) \cdot \frac{\alpha - \beta}{(1-\alpha)(1-\beta)} \tag{4.2}$$

と表すことができる. さらに, Perrin-Riou による一般化 Rubin 公式 [9, Proposition 2.2.4, 2.3.4] の帰結として, $\log_\omega(z^{\mathrm{BK}})$ は次のように表せる.

$$\log_\omega(z^{\mathrm{BK}}) = \left(1 - \frac{1}{\alpha}\right)^{-1} \left(1 - \frac{1}{\beta}\right) \mathcal{L}'_{p,\alpha}(E,0) \cdot \log_p(\chi_{\mathrm{cyc}}(\gamma)) \cdot \frac{\log_\omega(Q)^2}{\langle Q, Q\rangle_{p,\alpha}} \tag{4.3}$$

ここで, χ_{cyc} は円分指標, γ は $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ の位相的生成元, $\langle , \rangle_{p,\alpha}$ は α に付随する p 進 height pairing である. 注意 3.3で述べた様に, $\mathcal{L}'_{p,\alpha}(E,0)$ の特殊値公式である p 進 BSD 予想の p 部分が今正しい. その帰結として, p 進付値の等式

$$v_p(\mathcal{L}'_{p,\alpha}(E,0)) = v_p\left(\#Ш(E/\mathbb{Q}) \cdot \langle Q, Q\rangle_{p,\alpha}\right) \tag{4.4}$$

を得る. 以上の (4.2), (4.3), (4.4) を組み合わせることで, 命題 4.1を得る. □

4.2. **定理 3.6の証明のスケッチ.** 定理 3.6は, 定理 3.2よりもずっとスッキリ証明できる. まず, 定理の条件 (1) の $r_{\mathrm{an}}(E/F) = 1$ から, Gross–Zagier–Kolyvagin の結果により, $\#Ш(E/F) < \infty$ かつ $\mathrm{rank}_{\mathbb{Z}}(E(F)) = 1$ である. そこで, $Q \in E(F)$ を $E(F)$ の自由部分の生成元とする. このとき, 命題 2.2, 2.4から,

$$v_p(\#Ш(E/F) \cdot \log_\omega(Q)) \geq 2 \Rightarrow r_F(E[p]) \neq 0$$

が示せる. 実際, $v_p(\#Ш(E/F)) > 0$ であれば $\dim_{\mathbb{F}_p}(\#Ш(E/F)[p]) \geq 2$ である. ここで, 単完全列

$$0 \to E(F)/pE(F) \to \mathrm{Sel}(F, E[p]) \to Ш(E/F)[p] \to 0$$

を考えると, $\mathrm{rank}_{\mathbb{Z}}(E(F)) = 1$ から $\dim_{\mathbb{F}_p}(\mathrm{Sel}(F, E[p])) \geq 3$ が従う. よって命題 2.2から $r_F(E[p]) \neq 0$ である. $v_p(\#Ш(E/F)) = 0$ ならば, $v_p(\log_\omega(Q)) \geq 2$ であり, $\#\tilde{E}(\mathbb{F}_p) \cdot Q$ が命題 2.4の条件を満たし $r_F(E[p]) \neq 0$ が帰結される. そこで,

$$v_p(L'(E/F, 1)_{\mathrm{alg}} \cdot L_{\mathfrak{p}}^{\mathrm{BDP-B}}(0)) \geq 1 \Rightarrow v_p(\#Ш(E/F) \cdot \log_\omega(Q)) \geq 2 \tag{4.5}$$

が証明できれば定理 3.6が示される. 注意 3.8で述べたように, 定理 3.6の仮定の下では, $L'(E/F, 1)_{\mathrm{alg}}$ に対する BSD 予想の p 部分, 及び $L_{\mathfrak{p}}^{\mathrm{BDP-B}}(0)$ に対する p 進 BSD 予想の p 部分が正しい. p 進 BSD 予想の p 部分の帰結として,

$$v_p(L_{\mathfrak{p}}^{\mathrm{BDP-B}}(0)) = v_p(\#Ш(E/F) \cdot \log_\omega(Q)^2) - 2 \tag{4.6}$$

が得られる. 一方, BSD 予想の p 部分の帰結として,

$$v_p(L'(E/F, 1)_{\mathrm{alg}}) = v_p(\#Ш(E/F)) \tag{4.7}$$

が成立する. これらの p 進付値の等式 (4.6), (4.7) から, (4.5) は直ちに導かれる. □

(4.6) で用いた p 進 BSD 予想によると, 反円分 p 進 L 関数の特殊値 $L_{\mathfrak{p}}^{\mathrm{BDP-B}}(0)$ は有理点の log の値と直結する. 命題 2.4で見たように, この log の値が $r_F(E[p])$ の非自明性に寄与する. 一方, 定理 3.2で扱った E の円分 p 進 L 関数の微分値 $\mathcal{L}'_{p,\alpha}(E, 0)$ は, p 進 BSD 予想の下で有理点の p 進 height pairing の値と結びついた. p 進 height pairing の値と有理点の log の値とを結びつけるために, 定理 3.2の証明では定理 3.6よりも色々な計算の工夫が必要となった.

謝辞

「代数的整数論とその周辺 2024」での貴重な講演機会を与えてくださったオーガナイザーの三枝洋一先生, 中村健太郎先生, 杉山真吾先生に感謝いたします. また, 講演を推薦してくださった栗原将人先生に感謝いたします.

References

[1] A. Agashe and W. Stein. Visibility of Shafarevich-Tate groups of abelian varieties. Journal of Number Theory, **97**(1):171-185, 2002.

[2] F. Castella, C. Y. Hsu, D. Kundu, Y. S. Lee, and Z. Liu. Derived p-adic heights and the leading coefficient of the Bertolini–Darmon–Prasanna p-adic L-function. 2023, arXiv:2308.10474.

[3] J. Herbrand. Sur les classes des corps circulaires. Journal de Mathématiques Pures et Appliquées, **11**:417-441, 1932.

[4] K. A. Ribet. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. Invent. Math., **34**(3):151-162, 1976.

[5] N. Dainobu. Ideal class groups of division fields of elliptic curves and everywhere unramified rational points. Journal of Number Theory, **264**:211-232, 2024.

[6] N. Dainobu. On p-adic L-functions of elliptic curves and the ideal class groups of the division fields. 2024, arXiv:2405.19142

[7] K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. Astérisque, (**295**):ix, 117-290, 2004. Cohomologies p-adiques et applications arithmétiques. III.

[8] D. Prasad. A proposal for non-abelian Herbrand-Ribet. 2017. http://www.math.iitb.ac.in/ dprasad/ribet1.pdf.

[9] B. Perrin-Riou. Fonctions L p-adiques d' une courbe elliptique et points rationnels. Annales de l' Institut Fourier, **43**(4):945-995, 1993.

[10] D. Prasad and S. Shekhar. Relating the Tate-Shafarevich group of an elliptic curve with the class group. Pacific J. Math., **312**(1):203-218, 2021.

Department of Mathematics, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa 223-8522 Japan

Email address: dainobu@keio.jp