RIMS Kôkyûroku Bessatsu
B72 (2018), 119–133

Mazur-Tateの BSD 型精密化予想について (On the Mazur-Tate refined conjecture of BSD type)

By

太田 和惟 (Kazuto Ota)*

Abstract

This is an expository article of the author's paper [17], where under some assumptions we prove the rank-part of the Mazur-Tate refined conjecture of BSD type. More precisely, we show that the rank of the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$ is less than or equal to the order of zeros of Mazur-Tate elements, which refine the p-adic L function in a sense. In this article, we explain the proof of the main result.

§1. 序論

§1.1. Mazur-Tate の BSD 型精密化予想

BSD 型精密化予想 (refined conjecture of Birch and Swinnerton-Dyer type) は, Mazur-Tate [12] により定式化された予想で, $\mathbb{Q}$ 上の楕円曲線 E の Hasse-Weil L-関数 $L(E,s)$ の代わりに, Mazur-Tate 元を Mordell-Weil 群の階数などの数論的不変量と結びつける予想である. Mazur-Tate 元 θ_S は, Dirichlet 指標 $\chi : (\mathbb{Z}/S\mathbb{Z})^\times \to \mathbb{C}^\times$ によるひねりの特殊値達 $L(E,\chi,1)/\Omega^{\pm}$ を補間する $\mathbb{Q}[G_S]$ の元で ($\zeta_S := e^{2\pi i/S}$, $G_S := \mathrm{Gal}(\mathbb{Q}(\zeta_S)/\mathbb{Q})$), Stickelberger 元の楕円曲線類似ともみなせる. (Mazur-Tate 元の定義については, 第 2 節参照.) また, θ_S の係数の分母が S を動かしたとき有限となることも知られており, 例えば E が強 Weil 曲線であるとき, Manin-Drinfel'd の定理 ([4]) と (2.1) により, 任意の S に対し $(c_E \# E(\mathbb{Q})_{\mathrm{tors}})\,\theta_S \in \mathbb{Z}[G_S]$ となることがわかる. ($c_E \in \mathbb{Z}\setminus\{0\}$ は Manin 定数を表す.)

本稿で扱うのは, [12] の BSD 型精密化予想（以下、精密化予想と略す）の内, BSD 予想の類似の予想であるが, [12] では岩澤主予想 (の片側の包含関係) の類似, つまり θ_S

Received March 31, 2016. Revised December 20, 2016.
2010 Mathematics Subject Classification(s): 11G05, 11G40, 11R34.
This research was conducted as part of the KiPAS program 2013–2018 of the Faculty of Science and Technology at Keio University. This research was supported in part by JSPS KAKENHI (12J04338, 26247004), as well as the JSPS Core-to-Core program "Foundation of a Global Research Cooperative Center in Mathematics focused on Number Theory and Geometry".
*Department of Mathematics, Keio University, Kanagawa, 223-8522, Japan.
e-mail: kazutoota@math.keio.ac.jp

を $E(\mathbb{Q}(\zeta_S))$ と, G_S の群作用込みで結びつける予想も定式化されている ([12, Conjecture 3]). $\{\theta_{p^n}\}_{n\geq 1}$ を適当に変形し逆極限をとることで, E の p 進 L 関数が構成され, 岩澤主予想はその p 進 L 関数と $\cup_n E(\mathbb{Q}(\zeta_{p^n}))$ とを結びつける予想であったことを思い出されたい. 「精密化」という言葉は, p べきとは限らない一般の自然数 S に対し岩澤主予想や p 進 BSD 予想の類似が定式化されているということからきている.

精密化予想の内, 弱 BSD 予想 $\mathrm{ord}_{s=1}(L(E,s)) = \mathrm{rank}(E(\mathbb{Q}))$ の類似である予想を復習する. R を $\mathbb{Q}$ の部分環で $\theta_S \in R[G_S]$ を満たすものとする. また, I_S を $R[G_S]$ の augmentation イデアル, つまり, $I_S = \ker(R[G_S] \to R)$ とおき, $r(E) = \mathrm{rank}(E(\mathbb{Q}))$ とおく.

予想 1.1 (Mazur-Tate)**.** Mazur-Tate 元 θ_S の自明指標における零点の位数は $r(E)$ 以上である, つまり,

$$\theta_S \in I_S^{r(E)}.$$

注意 1.2. BSD 予想とは異なり, $\theta_S \in I_S^{r(E)+1}$ が起こり得る. 例えば次のような場合がある.

- $\#G_S \in R^\times$ なら, $I_S = I_S^2 = \cdots$.
- [12] では, S が E の相異なる split multiplicative prime $p_1, \ldots, p_a$ で割れる場合に, $\theta_S \in I_S^{r(E)+a}$ が予想されている. (このような余分な零点は p が E の split multiplicative prime であるときの p 進 BSD 予想にも現れる.) さらに, θ_S のノルム関係式 (命題 2.2) から, $a_l := l + 1 - \#E(\mathbb{F}_l)$ が 2 になる素数 $l \nmid N$ からも余分な零点が出ることが予想できる. これに対し [17, Theorem 7.1] では, S が平方因子をもたず, S を割る split multiplicative prime の個数を $\mathrm{sp}(S)$, $a_l = 2$ となる素数 $l|S$ の個数を $b_2(S)$ としたときに, 弱い仮定の下で $\theta_S \in I_S^{\mathrm{sp}(S)+b_2(S)}$ となることを示した.

§1.2. 主結果

E が $\mathbb{Q}$ 上の楕円曲線で, CM をもたないと仮定する. 導手を N とおく. 以下の 3 条件を満たす素数 p を, E の**許容素数**とよぶ.

1. $p \nmid 6N\#E(\mathbb{F}_p)\prod_{l|N}[E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)]$,
2. p 進 Tate 加群に付随する Galois 表現 $G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ が全射 ($G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$),
3. $p \geq r(E)$.

ここで, $E_0(\mathbb{Q}_l)$ は素数 l での還元写像 $E(\mathbb{Q}_l) \to E(\mathbb{F}_l)$ における, E の mod l reduction の非特異な有理点の集合 $E^{\mathrm{ns}}(\mathbb{F}_l)$ の逆像である.

以下, R は次の条件を満たすとする.

(1.1) 許容素数でない素数は全て R で可逆.

許容素数の密度は 1 であることに注意する (注意 1.5 参照). このような R に対し, 常に $\theta_S \in R[G_S]$ が成り立つことがわかる (cf. [11, Corollary 4.1]). 次の定理が本稿で解説する [17] の主結果である.

定理 1.3. S を次の条件 $(*)$ を満たす素数 $l \nmid N$ の, 平方因子をもたない積とする.

$(*)$ R で可逆でない任意の素数 p に対し, $E(\mathbb{F}_l)[p] \cong \mathbb{Z}/p\mathbb{Z}, \{0\}$.

このとき,

$$\theta_S \in I_S^{r(E)}.$$

定理 1.3 では, (1.1) を満たす R を抽象的に取ったが, 下の注意 1.5 (2) と [1, Theorem 2], [21, Théorème 4′] によって, 次の系 1.4 にあるような明示的な R が (1.1) を満たすことがわかる.

系 1.4. $E(\mathbb{Q})_{\mathrm{tors}} \neq \{0\}$ と仮定する.

$$d = \max\left\{ r(E),\ \frac{4\sqrt{6}}{3} N \prod_{l \mid N} \left(1 + \frac{1}{l}\right)^{\frac{1}{2}} + 1,\ \prod_{\substack{l:\text{split} \\ \text{multiplicative}}} (-\mathrm{ord}_l(j(E))) + 1 \right\}$$

とおき ($j(E)$ は j-不変量を表す),

$$R = \mathbb{Z}\left[p^{-1}; p < d \text{ 素数}\right]$$

ととる. このとき, 定理 1.3 における S に対し $\theta_S \in I_S^{r(E)}$ が成り立つ.

注意 1.5.

1. Chebotarev の密度定理により, $(*)$ を満たす素数 l の密度が 0.997 以上であることがチェックできる. また, よりわかりやすい条件として, $l \nmid N$ が E の supersingular prime のときには $(*)$ が成り立つ.

2. 許容素数に課した条件についてもう少し説明を加える.

   - E が CM をもたないという仮定から, 有限個の素数をのぞいて, 条件 2 は成り立つ ([21]).
   - $p \mid \#E(\mathbb{F}_p)$ を満たす素数 $p \nmid N$ は anomalous prime と呼ばれ, 岩澤理論的な議論をする際にはしばしば除外される素数である. Serre の Chebotarev 密度定理 ([22]) により, anomalous prime の密度が 0 であることがわかる. 特に, 許容素数の密度は 1. また, $E(\mathbb{Q})_{\mathrm{tors}} \neq \{0\}$ なら, anomalous prime は $2, 3, 5$, あるいは, $\#E(\mathbb{Q})_{\mathrm{tors}}$ を割る素数のいずれかであることが知られている ([10, Lemma 8.18]).

- $[E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)]$ は (l での) 玉河数とも呼ばれ, l が split multiplicative なら $[E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)] = -\mathrm{ord}_l(j(E))$, それ以外のときは $[E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)] = 1, 2, 3, 4$ となる (cf. [23, Chapter IV, Corollary 9.2]).

3. 定理 1.3 以前に, 予想 1.1 に関して知られていた結果を述べる. 簡単のため, p は許容素数とする. p が ordinary のとき, $\theta_{p^n} \in \mathbb{Z}_p \otimes I_{p^n}^{r(E)}$ $(n \geq 0)$ が 加藤 [5] の p 進 BSD 予想の半分の不等式から従う. p が supersingular のときは, [5] と 小林 [7], Pollack [19] の結果を組み合わせることで, ordinary のときと同じ主張を示せる. これらは S が p べきのときであるが, 栗原 [9] は, p が ordinary のとき, E の Selmer 群の岩澤 μ-不変量が 0 であるという予想を仮定した上で, 一般の S に対し $\theta_S \in \mathbb{Z}_p \otimes I_S^{r(E)}$ を示している. Tan [24] は, $\mathbb{Q}$ 上の各巡回拡大 $K \subset \mathbb{Q}(\zeta_S)$ に対し $E \otimes_{\mathbb{Q}} K$ の full BSD 予想 (弱 BSD 予想と, L 関数の $s = 1$ での Taylor 展開の主要項を Tate-Shafarevich 群 $Ш(E/K)$ などで記述する公式とを併せた予想) を仮定し, 特別な S に対し $\theta_S \in I_S^{r(E)}$ を示している. [17] の特色は, $\mu = 0$ 予想や BSD 予想といった難しい予想を仮定することなく, 十分一般的な S に対して $\theta_S \in I_S^{r(E)}$ を得た, ということである. 手法の違いを述べると, ([24] を除く) 先行研究で本質的なのは, 加藤 Euler 系 ([5]) に典型的な Euler 系の議論を適用することによって示される岩澤主予想の片側の包含関係であるが, [17] では, 同様に加藤 Euler 系が重要な役割を果たすものの, 典型的な Euler 系の議論で用いられる Kolyvagin 微分でなく, その一般化である「Darmon-Kolyvagin 微分」を加藤 Euler 系に適用し, その合同式を調べることによって定理 1.3 を示した.

定理 1.3 は, 精密化予想の内, 弱 BSD 予想に対応する部分に関する結果であったが, 次に, full BSD 予想に対応する部分に関して得られた結果を述べる. 精密化予想で $\lim_{s\to 1} L(E,s)/(s-1)^{r(E)}$ の役割を果たすのは, θ_S の $I_S^{r(E)}/I_S^{r(E)+1}$ における像 $\tilde{\theta}_S$ である. Mazur-Tate は, $\tilde{\theta}_S$ を $Ш(E/\mathbb{Q})$ や高さ関数, J_S などの数論的不変量で記述する公式を予想した ([12, Conjecture 4]). ここで J_S は, $(S, N) = 1$ なる S に対し次で定義される有限群である.

$$J_S = \mathrm{coker}\left(E(\mathbb{Q}) \to \left(\oplus_{l|S} E(\mathbb{F}_l)\right) \oplus \left(\oplus_{l|N} E(\mathbb{Q}_l)/E_0(\mathbb{Q}_l)\right)\right).$$

次の定理は, その予想された公式を支持する部分的な結果である.

定理 1.6. p を R で可逆でない許容素数とし, S を, $p \mid (l-1)$ かつ $(*)$ を満たす素数 $l \nmid N$ 達の積で, 平方因子をもたないものとする. このとき, $\tilde{\theta}_S \not\equiv 0 \bmod p \left(I_S^{r(E)}/I_S^{r(E)+1}\right)$ ならば,

$$Ш(E/\mathbb{Q})[p] = J_S[p] = \{0\}.$$

注意 1.7.

1. 定理 1.3 より, 定理 1.6 の仮定のもとで $\theta_S \in I_S^{r(E)}$.
2. 条件 $p \mid (l-1)$ は, 記号を簡単にするための仮定である. より一般的な主張については [17, Theorem 6.4] を参照.

記号.

- 以下, CM を持たない $\mathbb{Q}$ 上の楕円曲線 E を固定し, その導手を N とおく.
- $\overline{\mathbb{Q}}$ を $\mathbb{Q}$ の代数閉包とし, 体の埋め込み $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ を固定する.

§2. Mazur-Tate 元

この節では, Mazur-Tate 元の定義及び, 性質を復習する. E の $\mathbb{Z}$ 上の minimal Weierstrass model を一つ固定し, ω を Néron differential とする. このとき, 階数 2 の自由 $\mathbb{Z}$-加群 $\Lambda \subseteq \mathbb{C}$ を次の準同型写像の像で定義する.

$$H_1(E(\mathbb{C}), \mathbb{Z}) \to \mathbb{C}; \quad \gamma \mapsto \int_\gamma \omega.$$

周期 $\Omega^+, -i\Omega^- > 0$ を次を満たす最大の実数として定義する.

$$\Lambda \subseteq \mathbb{Z}\Omega^+ \oplus \mathbb{Z}\Omega^-.$$

(ω が $\mathbb{Q}$ 上, したがって $\mathbb{R}$ 上定義されているため, このような $\Omega^\pm$ をとることができる.) E に対応する重さ 2 の newform $f(\tau) \in \mathscr{S}_2(\Gamma_0(N))$ をとり, q-展開が $f(\tau) = \sum_{n\geq 1} a_n q^n$ で与えられているとする. このとき, $r \in \mathbb{Q}$ に対し, $[r]^\pm \in \mathbb{Q}$ を次で定義する.

$$2\pi \int_0^\infty f(r+it)\, dt = [r]^+ \Omega^+ + [r]^- \Omega^-. \tag{2.1}$$

アプリオリには $[r]^\pm \in \mathbb{R}$ だが, Manin-Drinfel'd の定理 (cf. [4]) により $[r]^\pm \in \mathbb{Q}$ であることがわかる.

定義 2.1. 自然数 $S > 0$ に対し, Mazur-Tate 元 $\theta_S \in \mathbb{Q}[G_S]$ を

$$\theta_S = \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]^+ + \left[\frac{a}{S}\right]^- \right) \sigma_a$$

で定義する. ここで, $a \in (\mathbb{Z}/S\mathbb{Z})^\times$ に対し $\sigma_a \in G_S$ は, 円分指標により定まる同型 $G_S \cong (\mathbb{Z}/S\mathbb{Z})^\times$ のもとで a に対応する元を表す.

$n \mid m$ なる自然数 m, n に対し, 環準同型 $\pi_{m/n} : \mathbb{Q}[G_m] \to \mathbb{Q}[G_n]$ を自然な射影 $G_m \to G_n$ から誘導されるものとし, $\mathbb{Q}$-線形写像 $\nu_{m,n} : \mathbb{Q}[G_n] \to \mathbb{Q}[G_m]$ を, $\sigma \in G_n$ を $\sum_{\tilde{\sigma}\mapsto\sigma} \tilde{\sigma} \in \mathbb{Q}[G_m]$ に送る写像を $\mathbb{Q}$-線形に延長した写像として定義する. ここで, $\tilde{\sigma} \in G_m$ は射影 $G_m \to G_n$ における σ の逆像の元をわたる. 導手 S の Dirichlet 指標 χ に対し, Gauss 和 $\tau(\chi)$ を

$$\tau(\chi) = \sum_{\sigma \in G_S} \chi(\sigma)\zeta_S^\sigma$$

で定義する.

命題 2.2. Mazur-Tate 元の系 $\{\theta_S\}_{S>0}$ は次の 2 つの性質を満たし, これらで特徴付けられる.

1. 素数 l に対し,

$$\pi_{Sl/S}(\theta_{Sl}) = \begin{cases} -\sigma_l^{-1}(1 - a_l\sigma_l + \epsilon(l)\sigma_l^2)\theta_S & (l \nmid S), \\ a_l\theta_S - \epsilon(l)\nu_{S,S/l}(\theta_{S/l}) & (l \mid S). \end{cases}$$

   ここで, $l \nmid N$ なら $\epsilon(l) = 1$, $l \mid N$ なら $\epsilon(l) = 0$.

2. 導手 S の Dirichlet 指標 χ に対し,

$$\chi(\theta_S) = \tau(\chi)\frac{L(E, \overline{\chi}, 1)}{\Omega^{\pm}}.$$

   ここで, $\overline{\chi}$ は χ の複素共役を表し, 符号 $\pm$ は $\chi(-1)$ の符号と同じものとする.

   証明. [13, p. 8, p. 10] を参照. [13] の記号を用いると

$$\lambda(f, 1; -a, S) = \left[\frac{a}{S}\right]^{+}\Omega^{+} + \left[\frac{a}{S}\right]^{-}\Omega^{-}$$

となることに注意する. □

§3. 主結果の証明の概略

この節では, 定理 1.3 の証明を概説する. 大雑把には, 次のように証明を行う.

i) 定理 1.3 を, $\theta_S \in \mathbb{Z}_p \otimes I_S^{r(E)} \subseteq \mathbb{Z}_p[G_S]$ に帰着する (p は許容素数).

ii) 栗原 [8], 小林 [7], 大槻 [18] らの議論を用いて, Mazur-Tate 元と加藤 Euler 系 ([5]) を結びつける.

iii) Darmon [2] による, Heegner 点 (がなす Euler 系) に対する p-可除性の結果の, 定義 3.9 の意味での Euler 系に対する類似物を証明する. これを加藤 Euler 系に対し適用し, ii) と組み合わせることで, $\theta_S \in \mathbb{Z}_p \otimes I_S^{\min\{r_p-1,p\}}$ を得る. ここで, r_p は p-power Selmer 群 $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$ の $\mathbb{Z}_p$-corank を表す. 特に, $r_p \geq r(E)$.

iv) p-parity 予想 $\mathrm{ord}_{s=1}(L(E,s)) \equiv r_p \bmod 2$ ([3],[6],[15],[16] においてすでに証明されている) と θ_S の "関数等式" を用いて, $\theta_S \in \mathbb{Z}_p \otimes I_S^{\min\{r_p,p\}}$ を示す. $p \geq r(E)$ より $\theta_S \in \mathbb{Z}_p \otimes I_S^{r(E)}$ を得る.

以下では各ステップごとにより詳しく説明する. 本稿では特に, 最も大事な三つ目のステップを重点的に解説する.

§3.1. R から $\mathbb{Z}_p$ への帰着

(1.1) を満たす部分環 $R \subsetneq \mathbb{Q}$ を固定する. 有限アーベル群 G に対し, I_G を $R[G]$ の augmentation ideal とおく. まず, 簡単な群環の議論により次がわかる (cf. [2, Lemma 3.2], [17, Lemma 5.2]).

命題 3.1. G を有限アーベル群とし, 各素数 p 毎に有限アーベル群の分解 $G = K_p \times H_p$ $(p \nmid \#H_p)$ が与えられているとする. 整数 $t \geq 1$ と $\alpha \in R[G]$ に対し, 次の二つの条件は同値である:

1. $\alpha \in I_G^t$,
2. 全ての $p \notin R^\times$ なる素数 p に対し, $\alpha_p \in \mathbb{Z}_p \otimes_{\mathbb{Z}} I_{K_p}^t$. ここで, $\alpha_p \in \mathbb{Z}_p[K_p]$ は α の, 射影 $\mathbb{Z}_p[G] \to \mathbb{Z}_p[K_p]$ における像を表す.

記号. 以下, 本稿全体を通して E の許容素数 p を固定する. 自然数 S に対し, $\mathbb{Q}(S)$ を $\mathbb{Q}(\zeta_S)$ に含まれる $\mathbb{Q}$ の最大 p-拡大とし, $\Gamma_S = \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$ とおく. 制限写像により自然な射影 $G_S \to \Gamma_S$ があり, また, Γ_S は G_S の直和成分とみなせることに注意する. $I_{S,p}$ を $\mathbb{Z}_p[\Gamma_S]$ の augmentation イデアルとする. $\overline{\mathbb{Q}}_p$ を $\mathbb{Q}_p$ の代数閉包とし, 体の埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ を固定する.

命題 3.1 により, 定理 1.3 を示すには, 次の定理を各許容素数 p 毎に証明すれば十分である.

定理 3.2. S を, $E(\mathbb{F}_l)[p] \cong \mathbb{Z}/p\mathbb{Z}, \{0\}$ なる素数 $l \nmid pN$ 達の, 平方因子をもたない積とする. このとき,

$$\theta_{S,p} \in I_{S,p}^{\min\{r_p,p\}} \subseteq \mathbb{Z}_p[\Gamma_S].$$

ここで, 命題 3.1 のように, $\theta_{S,p}$ は θ_S の $\mathbb{Z}_p[\Gamma_S]$ での像を表す.

§3.2. 加藤 Euler 系と Mazur-Tate 元の関係

$\mathbb{Q}(S)$ の整数環を $\mathscr{O}_S$ とおく. $\hat{E}$ を E の $\mathbb{Z}_p$ 上の形式群則とする. (E の不変微分形式 ω を固定していたことに注意する.) 付随する logarithm を $\log_{\hat{E}}(T) \in \mathbb{Q}_p[[T]]$ とおく.

補題 3.3. $(S,p) = 1$ なる, 平方因子をもたない整数 $S > 0$ に対し, 次を満たす $c_S \in \hat{E}(\mathscr{O}_S \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ がただ一つ存在する ([17, Lemma 5.5]).

$$\left(1 - \frac{a_p}{p}\sigma_p + \frac{1}{p}\sigma_p^2\right) \log_{\hat{E}}(c_S) = \mathrm{tr}_{\mathbb{Q}(\zeta_S)/\mathbb{Q}(S)}(\zeta_S) \in \mathscr{O}_S \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

ここで, $\sigma_p \in \Gamma_S$ は p 乗 Frobenius を表す.

以下, $\{\mathfrak{z}_m\}_m \in \prod_{m\geq 1} H^1(\mathbb{Q}(m), T_p(E))$ を加藤 Euler 系とする. このとき, $\mathfrak{z}_S$ の明示的相互法則 ($\mathfrak{z}_S$ の双対指数写像での像が部分ゼータ関数の特殊値を与える) や, $\{\mathfrak{z}_S\}_S, \{c_S\}_S$ のノルム関係式を用いることで次が示せる[1] ([17, Corollary 5.13]).

[1] 正確には, Mazur-Tate 元の系の関係式 (命題 2.2 (2)) がオリジナルの加藤 Euler 系のノルム関係式と少し異なるため, Euler 系を, 定義 3.9 を満たすように少し修正する必要がある (cf. 注意 3.10).

命題 3.4. $\theta_{S,p} = \sum_{\gamma\in\Gamma_S}(c_S, \mathfrak{z}_S^{\gamma^{-1}})\gamma \in \mathbb{Z}_p[\Gamma_S]$. ここで, $(-,-)$ は次の合成写像を表す:

$$\oplus_{v|p}H^1(\mathbb{Q}(S)_v, T_p(E)) \times \oplus_{v|p}H^1(\mathbb{Q}(S)_v, T_p(E)) \xrightarrow{\oplus_v \cup_v} \oplus_v \mathbb{Z}_p \xrightarrow{(a_v)_v \mapsto \sum a_v} \mathbb{Z}_p.$$

ただし, v は p を割る $\mathbb{Q}(S)$ の素点を走り, $\mathbb{Q}(S)_v$ は $\mathbb{Q}(S)$ の v での完備化を,

$$\cup_v : H^1(\mathbb{Q}(S)_v, T_p(E)) \times H^1(\mathbb{Q}(S)_v, T_p(E)) \to \mathbb{Z}_p$$

はカップ積を表す. また, $c_S \in \hat{E}(\mathscr{O}_S \otimes \mathbb{Z}_p) = \oplus_{v|p}\hat{E}(\mathscr{O}_{S,v})$ を Kummer 写像により, $\mathfrak{z}_S$ を各 v での局所化写像 loc_v の和

$$H^1(\mathbb{Q}(S), T_p(E)) \to \oplus_{v|p}H^1(\mathbb{Q}(S)_v, T_p(E)); \quad x \mapsto (\mathrm{loc}_v(x))_v$$

により, それぞれ $\oplus_{v|p}H^1(\mathbb{Q}(S)_v, T_p(E))$ の元とみなす. ここで, $\mathscr{O}_{S,v}$ は $\mathscr{O}_S$ の v での完備化を表す.

§ 3.3. Euler 系の微分の p-可除性

3.3.1. Darmon-Kolyvagin 微分 各素数 l 毎に, Γ_l の生成元 γ_l を固定する. $k \in \mathbb{Z}$ に対し,

$$D_l^{(k)} = \sum_{j=0}^{\#\Gamma_l - 1} \binom{j}{k} \gamma_l^j \in \mathbb{Z}[\Gamma_l]$$

とおく.

命題 3.5. 上の記号の下, $q \mid (l-1)$ なる p べき $q = p^m$ に対し, $1 \le k < p$ ならば

$$(\gamma_l - 1)D_l^{(k)} \equiv -\gamma_l D_l^{(k-1)} \mod q\mathbb{Z}[\Gamma_l].$$

$k \le 0$ ならば両辺は共に 0 となる.

定義 3.6. 平方因子をもたない整数 $S > 0$ に対し, 次のような形の $D \in \mathbb{Z}[\Gamma_S]$ を Darmon-Kolyvagin 微分という.

$$D = D_{l_1}^{(k_1)} \cdots D_{l_s}^{(k_s)}, \quad 0 \le k_i \le \#\Gamma_{l_i} - 1.$$

ここで, $l_1, \ldots, l_s$ は S を割る相異なる素数で, このような表示は一意的であることに注意する. このとき,

$$\mathrm{ord}(D) = k_1 + \cdots + k_s, \quad \mathrm{Supp}(D) = \prod_i l_i, \quad \mathrm{Cond}(D) = \prod_{i:k_i>0} l_i$$

とおく.

注意 3.7. $D_{l_1}^{(1)}\cdots D_{l_s}^{(1)}$ は Kolyvagin 微分とよばれ, [20] などにおける Euler 系の議論でも用いられている.

$S=l_1\cdots l_s$ のとき, 命題 3.4 を用いて Taylor 展開の類似を考えることで, 次を得られる (cf. [17, Proposition 3.3][2]).

$$\theta_{S,p}=\sum_{\boldsymbol{k}=(k_1,\dots,k_s)\in\mathbb{Z}_{\geq 0}^{\oplus s}}(c_S,D^{(\boldsymbol{k})}(\mathfrak{z}_S))(\gamma_{l_1}^{-1}-1)^{k_1}\cdots(\gamma_{l_s}^{-1}-1)^{k_s}. \tag{3.1}$$

ここで, $D^{(\boldsymbol{k})}=D_{l_1}^{(k_1)}\cdots D_{l_s}^{(k_s)}$ とおいた. また, $k_i>\#\Gamma_{l_i}-1$ なら $D_{l_i}^{(k_i)}=0$ となるので, 上の和は有限和であることに注意する. ここで, 次を思い出す (cf. [2, Lemma 3.5]).

命題 3.8. 各素数 l に対し,

$$\#\Gamma_l\cdot(\gamma_l-1)\in I_{l,p}^p.$$

この命題と (3.1) により, $D^{(\boldsymbol{k})}(\mathfrak{z}_S)$ の p-可除性を調べて定理 3.2 にアプローチするのが基本的なアイディアである.

3.3.2. p-可除性

p べき $q=p^m$ $(m\geq 0)$ に対し,

$$\mathscr{R}_q=\{l\nmid pN:\text{素数}\mid\ l-1\equiv 0 \bmod q\},\quad \mathscr{R}_{E,q}=\{l\in\mathscr{R}_q\mid\ \#E(\mathbb{F}_l)\equiv 0 \bmod q\}$$

とおき, $\mathscr{N}_q$ を相異なる $l\in\mathscr{R}_q$ 達の積と 1 からなる集合とする. $\mathscr{N}_{E,q}$ も同様に定義する.

定義 3.9. $\{z_{mp^n}\}_{m,n}\in\prod_{m\in\mathscr{N}_1,n\geq 0}H^1(\mathbb{Q}(mp^n),T_p(E))$ が Euler 系であるとは, 次の条件が成り立つ時をいう. $S=mp^n$ $(m\in\mathscr{N}_1,n\geq 0)$ と素数 $l\nmid N$ に対し,

$$\mathrm{Cor}_{Sl/S}(z_{Sl})=\begin{cases}(1-a_l\sigma_l^{-1}+\sigma_l^{-2})z_S & (l\nmid pS)\\ z_S & (l=p).\end{cases}$$

ここで, $\mathrm{Cor}_{Sl/S}:H^1(\mathbb{Q}(Sl),T_p(E))\to H^1(\mathbb{Q}(S),T_p(E))$ は corestriction map を表し, $\sigma_l\in\Gamma_S$ は l 乗 Frobenius を表す.

注意 3.10.

1. この定義は, [20] などで用いられている, よく知られた ($T_p(E)$ に対する) Euler 系の定義とはほんの少し異なる. しかし, [20, Lemma 9.6.1] によって, [20] の意味での Euler 系から定義 3.9 の意味での Euler 系を構成することができ, 逆の構成もまたできる (cf. [17, Remark 3.12]).
2. 本稿で考えている加藤 Euler 系 $\{\mathfrak{z}_S\}$ は, [5] で構成された Euler 系に [20, Lemma 9.6.1] を適用してできる, 定義 3.9 の意味での Euler 系のことを指す.

[2]本稿の γ_l は, [17] では σ_l であることに注意.

3. 定義から, $S \in \mathscr{N}_1$ を止めるごとに, 系 $\{z_{Sp^n}\}_n$ はノルム系をなす. つまり, $\{z_{Sp^n}\}_n \in \varprojlim_n H^1(\mathbb{Q}(Sp^n), T_p(E))$. これにより, p を割らない $\mathbb{Q}(S)$ の任意の素イデアル v で, z_S が不分岐, つまり, $\mathrm{loc}_v(z_S) \in H^1_{\mathrm{ur}}(\mathbb{Q}(S)_v, T_p(E))$ となることがわかる (cf. [20, Corollary B.3.4]). 本稿における $\{z_{Sp^n}\}_n$ の役割は, z_S の不分岐性の保証だけである. (したがって, $\{z_S\}_{S\in\mathscr{N}_1}$ の不分岐性を初めから仮定しておけば, 添え字が p べきで割れる元を考える必要はない.)

次が, p-可除性に関する重要な定理である ([17, Theorem 4.9] の特殊な場合).

定理 3.11. $\{z_m\}_m$ を Euler 系とする. q を p べき, D を Darmon-Kolyvagin 微分とし, $S = \mathrm{Supp}(D)$ とおく. $S \in \mathscr{N}_q$, かつ全ての素数 $l \mid S$ が, $E(\mathbb{F}_l)[p] \cong \mathbb{Z}/p\mathbb{Z}, \{0\}$ を満たすと仮定する. このとき, もし $\mathrm{ord}(D) < \min\{r_p - 1, p\}$ なら,

$$D(z_S) \equiv 0 \bmod qH^1(\mathbb{Q}(S), T_p(E)).$$

この定理の証明を概説する前に, これから得られる系を述べておく.

系 3.12. S を定理 3.2 のようにとる. このとき, $\theta_{S,p} \in I_{S,p}^{\min\{r_p-1,p\}}$.

系 *3.12* の証明. (3.1) を使う. $k_1 + \cdots + k_s < \min\{r_p - 1, p\}$ なる $\boldsymbol{k} = (k_1, \ldots, k_s)$ を任意にとる. つまり, $\mathrm{ord}(D^{(\boldsymbol{k})}) < \min\{r_p - 1, p\}$. $k_1 = k_2 = \cdots = k_s = 0$ ならば $r_p \geq 2$ となり, したがって $\mathcal{S}_{\Sigma_p}(\mathbb{Q}, E[p^\infty]) := \ker\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \to \varinjlim_n \left(E(\mathbb{Q}_p) \otimes \frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p\right)\right)$ が無限群となる. よって, [20, Theorem 2.3] により $z_1 = 0 \in H^1(\mathbb{Q}, T_p(E))$ なので,

$$D^{(\boldsymbol{k})} z_S = \mathrm{Cor}_{S/1} z_S = \prod_{l|S}(1 - a_l + 1) z_1 = 0 \in H^1(\mathbb{Q}, T_p(E)).$$

以下, $\boldsymbol{k} \neq (0, \ldots, 0)$ とする. $q = \min_{1\leq i\leq s}\{\#\Gamma_{l_i} |\ k_i > 0\}$ とおく. $q > 1$ ならば, 定理 3.11 より,

$$(c_S, D^{(\boldsymbol{k})}(\mathfrak{z}_S)) \equiv 0 \mod q$$

を得る. したがって, 命題 3.8 より

$$(c_S, D^{(\boldsymbol{k})}(\mathfrak{z}_S)) \prod_{0\leq i\leq s} (\gamma_{l_i}^{-1} - 1)^{k_i} \in I_{S,p}^p. \tag{3.2}$$

$q = 1$ のときは, ある i で, $k_i > 0$ かつ $\#\Gamma_{l_i} = 1$ なので, $(\gamma_{l_i}^{-1} - 1)^{k_i} = 0$. よって, $q = 1$ のときも (3.2) が成り立つ. これより, 系を得る. □

3.3.3. 定理 3.11 の証明の概略

p べき q を固定する.

定義 3.13. $\mathrm{Supp}(D) \in \mathscr{N}_q$ なる Darmon-Kolyvagin 微分 D をとり, $S = \mathrm{Supp}(D)$ とおく. 重さ $w(D) \in \mathbb{Z}$ を

$$w(D) = \mathrm{ord}(D) - \#\{l : S \text{ を割る素数} \mid l \in \mathscr{R}_{E,q}\}$$

で定義する.

$\mathrm{Supp}(D)$ の素因子の個数に関する帰納法により, 次が示せる.

命題 3.14. 定義 3.13 の記号の下, もし, $\mathrm{ord}(D) < p$ かつ $w(D) < 0$ ならば,

$$D(z_S) \equiv 0 \mod qH^1(\mathbb{Q}(S), T_p(E)).$$

証明 ($\mathrm{Supp}(D)$ の素因子が一つの場合). 素因子が一つ, つまり $S = l$ (素数) と仮定すると, $w(D) < 0$ より, $l \in \mathscr{R}_{E,q}$ かつ $D = D_l^{(0)} = \sum_{g\in\Gamma_l} g$. よって, Euler 系の定義より,

$$D(z_l) = \sum_{g\in\Gamma_l} gz_l = (1 - a_l\sigma_l^{-1} + \sigma_l^{-2})z_1 = (1 - a_l + 1)z_1 \equiv \#E(\mathbb{F}_l)z_1 \equiv 0 \mod q.$$

ここで, 最初の合同式は $l \in \mathscr{R}_q$, 二つ目の合同式は $l \in \mathscr{R}_{E,q}$ から従う.

一般の場合については, [17, Proposition 4.7] を参照されたい. □

q-Selmer 群 $\mathrm{Sel}(\mathbb{Q}, E[q]) \subseteq H^1(\mathbb{Q}(S), E[q])$ は次で定義されることを思い出す.

$$\mathrm{Sel}(\mathbb{Q}, E[q]) = \ker\left(H^1(\mathbb{Q}, E[q]) \to \prod_{l:\text{素数}} \frac{H^1(\mathbb{Q}_l, E[q])}{E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)}\right).$$

ここで, 記号の乱用であるが, $E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)$ は Kummer 写像

$$E(\mathbb{Q}_l)/qE(\mathbb{Q}_l) \hookrightarrow H^1(\mathbb{Q}_l, E[q])$$

の像を表す. 自然数 S に対し,

$$\mathscr{S}^{(S)}(\mathbb{Q}, E[q]) = \ker\left(H^1(\mathbb{Q}, E[q]) \to \prod_{l\nmid S} \frac{H^1(\mathbb{Q}_l, E[q])}{E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)}\right),$$
$$H^1_{f,S}(\mathbb{Q}, E[q]) = \ker\left(\mathrm{Sel}(\mathbb{Q}, E[q]) \to \oplus_{l|S} H^1(\mathbb{Q}_l, E[q])\right)$$

とおく. $H^1_{f,S}(\mathbb{Q}, E[q]) \subseteq \mathrm{Sel}(\mathbb{Q}, E[q]) \subseteq \mathscr{S}^{(S)}(\mathbb{Q}, E[q])$ に注意する.

定理 3.11 の証明の概略. q, D, S を定理 3.11 のようにとる. 証明は $w(D)$ の帰納法による. $w(D) < 0$ ならば, 命題 3.14 により定理 3.11 は成り立つ. したがって, $w(D) \geq 0$ とし, $w(D') < w(D)$ なる D' に対しては定理 3.11 が成り立っていると仮定する.

$$D(z_S) \not\equiv 0 \mod q$$

と仮定する. $S' = \mathrm{Cond}(D)$ とおくと次の完全系列があることに注意する.

$$0 \to H^1_{f,pS'}(\mathbb{Q}, E[q]) \to \mathrm{Sel}(\mathbb{Q}, E[q]) \to \oplus_{l|pS'} E(\mathbb{Q}_l)/qE(\mathbb{Q}_l). \tag{3.3}$$

まず,

$$\text{位数 } q \text{ の元 } \eta \in H^1_{f,pS'}(\mathbb{Q}, E[q]) \text{ が存在する}$$

ことを示す.

自然な写像 $\mathrm{Sel}(\mathbb{Q}, E[q]) \to \mathrm{Sel}(\mathbb{Q}, E[p^\infty])[q]$ が全射であることから (cf. [20, Lemma 1.5.4]), (non-canonical な) 単射

$$(\mathbb{Z}/q\mathbb{Z})^{\oplus r_p} \hookrightarrow \mathrm{Sel}(\mathbb{Q}, E[q]) \tag{3.4}$$

がある. S の仮定と $p \nmid \#E(\mathbb{F}_p)$ より, 任意の素数 $l \mid pS'$ に対し, $E(\mathbb{Q}_l)/pE(\mathbb{Q}_l) \cong \mathbb{Z}/p\mathbb{Z}, \{0\}$. よって,

$$\dim_{\mathbb{F}_p}(\oplus_{l|pS'} E(\mathbb{Q}_l)/pE(\mathbb{Q}_l)) \leq \#\{pS' \text{を割る素数 }\} \leq \mathrm{ord}(D) + 1 < r_p.$$

(最後の不等号は, $\mathrm{ord}(D) < \min\{r_p - 1, p\} \leq r_p - 1$ による.) これと, (3.3), (3.4) より, 位数 q の元 $\eta \in H^1_{f,pS'}(\mathbb{Q}, E[q])$ が存在することがわかる.

Galois 表現 $G_\mathbb{Q} \to \mathrm{Aut}(T_p(E))$ の全射性より, 任意のアーベル拡大 $K/\mathbb{Q}$ に対し, $E(K)[p] = 0$ がわかる. したがって, $H^1(\mathbb{Q}(S), T_p(E)) \otimes \mathbb{Z}/q\mathbb{Z} \to H^1(\mathbb{Q}(S), E[q])$ は単射であり $D(z_S) \bmod q \neq 0 \in H^1(\mathbb{Q}(S), E[q])$. また, 帰納法の仮定と命題 3.5 により,

$$D(z_S) \bmod q \in H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), E[q])\right) \tag{3.5}$$

を示せる. 実際, $S = l_1 \cdots l_s$ (素因数分解), $D = D_{l_1}^{(k_1)} \cdots D_{l_s}^{(k_s)}$ とすると, 命題 3.5 より

$$(\gamma_{l_1} - 1)D(z_S) \equiv -\gamma_{l_1} D_{l_1}^{(k_1-1)} D_{l_2}^{(k_2)} \cdots D_{l_s}^{(k_s)}(z_S) \mod q \tag{3.6}$$

となり, 右辺は, $k_1 = 0$ なら零元, $k_1 \geq 1$ なら $w\left(D_{l_1}^{(k_1-1)} D_{l_2}^{(k_2)} \cdots D_{l_s}^{(k_s)}\right) = w(D) - 1$ と帰納法の仮定により modulo q で零元となる. この議論を各 $1 \leq i \leq s$ に対して行い, $(\gamma_{l_i} - 1)Dz_S \equiv 0 \bmod q$ を示すことで, (3.5) を得る. (γ_{l_i} は Γ_{l_i} の生成元であることを思い出す).

$E(\mathbb{Q}(S))[p] = 0$ より, 制限写像

$$H^1(\mathbb{Q}, E[q]) \to H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), E[q])\right)$$

は同型である. この同型における $D(z_S) \bmod q$ の逆像を $\kappa \in H^1(\mathbb{Q}, E[q])$ とおく. $\kappa \neq 0$ に注意する.

Chebotarev の密度定理を用いると次の (1), (2), (3) を満たす素数 $l \in \mathscr{R}_q$ が存在することが示せる (cf. [17, Lemma 4.10]).

(1) l は $\mathbb{Q}(S)$ で完全分解し, $E(\mathbb{Q}_l)/qE(\mathbb{Q}_l) \cong \mathbb{Z}/q\mathbb{Z}$. 特に, $l \in \mathscr{R}_{E,q}$.

(2) $\mathrm{loc}_l(\kappa) \neq 0 \in H^1(\mathbb{Q}_l, E[q])$, ここで, loc_l は局所化写像 $H^1(\mathbb{Q}, E[q]) \to H^1(\mathbb{Q}_l, E[q])$ を表す.

(3) $\mathrm{loc}_l(\eta) \in E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)$ の位数は q. 特に, $H^1_{f,pS'}(\mathbb{Q}, E[q]) \to E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)$ は全射.

(3.5) のように, 帰納法の仮定と命題 3.5 を用いて

$$DD_l^{(1)}(z_{Sl}) \bmod q \in H^0\left(\Gamma_{Sl}, H^1(\mathbb{Q}(Sl), E[q])\right) \tag{3.7}$$

がわかり, この元の, 同型

$$H^1(\mathbb{Q}, E[q]) \xrightarrow{\sim} H^0\left(\Gamma_{Sl}, H^1(\mathbb{Q}(Sl), E[q])\right)$$

における逆像を $\kappa_l \in H^1(\mathbb{Q}, E[q])$ とおく. これは次の (4), (5) の性質を満たす.

(4) $\kappa_l \in \mathscr{S}^{(pS'l)}(\mathbb{Q}, E[q])$.[3]

(5) $\mathrm{loc}_l(\kappa_l) \notin E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)$.[4]

次の完全系列を思い出す (cf. [14, Chapter I, Theorem 4.10]).

$$0 \to \mathscr{S}^{(pS')}(\mathbb{Q}, E[q]) \to \mathscr{S}^{(pS'l)}(\mathbb{Q}, E[q]) \to \frac{H^1(\mathbb{Q}_l, E[q])}{E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)} \to H^1_{f,pS'}(\mathbb{Q}, E[q])^\vee. \tag{3.8}$$

ここで, $\vee$ は Pontryagin 双対 $\mathrm{Hom}(-, \mathbb{Z}/q\mathbb{Z})$ を表す. $\frac{H^1(\mathbb{Q}_l, E[q])}{E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)} = (E(\mathbb{Q}_l)/qE(\mathbb{Q}_l))^\vee$ と (3) に注意すると, $\mathscr{S}^{(pS'l)}(\mathbb{Q}, E[q]) \to \frac{H^1(\mathbb{Q}_l, E[q])}{E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)}$ は 0-写像. これは条件 (5) に矛盾する. この矛盾は $D(z_S) \not\equiv 0 \mod q$ を仮定したことからきた. □

注意 3.15.

1. $\theta_S \in I_S^{r(E)}$ を証明するために, $\mathrm{ord}(D) < \min\{r_p, p\}$ を仮定して p-可除性を示したいというのが自然かもしれないが, 残念ながら上手くいかない. 必ずしも $\mathrm{loc}_p(\kappa_l) \in E(\mathbb{Q}_p)/qE(\mathbb{Q}_p)$ が成り立たないということが, $\mathrm{ord}(D) < \min\{r_p - 1, p\}$ と仮定する必要がある理由である. [2] の Heegner 点の場合には, loc_p での像が局所有理点からくることが我々との大きな違いである.

2. 本稿の主定理である定理 1.3 を, S が平方因子を持つ場合に一般化するためには, 各 p べき q に対し, $D(\mathfrak{z}_{mp^n})$ $(m \in \mathscr{N}_{E,q},\ q|p^n)$ という形の微分全てに対し定理 3.11 を証明する必要がある. これは, $w(D)$ の定義を少し修正し, 加藤 [5] によって示された岩澤主予想の片側の包含関係を応用することで, やはり $w(D)$ の帰納法により証明できるのではないかと著者は期待している. 現在, 詳細を研究中である.

§3.4. p-parity 予想の適用

まず, θ_S の "関数等式" を思い出す. w_N を $g \mapsto \frac{1}{N\tau^2} g\left(\frac{-1}{N\tau}\right)$ で定義される $\mathscr{S}_2(\Gamma_0(N))$ 上の作用素とする. このとき, §2 のように $f \in \mathscr{S}_2(\Gamma_0(N))$ を E に対応する newform とすると, $\varepsilon_f \in \{\pm 1\}$ が存在し $w_N(f) = -\varepsilon_f f$. よく知られているように,

$$\varepsilon_f = (-1)^{\mathrm{ord}_{s=1}(L(E,s))}. \tag{3.9}$$

[3] これを示すには, まず Kolyvagin 微分の場合と同様に, 注意 3.10(3) より素数 $v \nmid pS'l$ に対し $\mathrm{loc}_v(\kappa_l) \in H^1_{\mathrm{ur}}(\mathbb{Q}_v, E[q])$ を示し. $v \mid N$ のときは, さらに [14, Chapter I, Proposition 3.8] と $p \nmid [E(\mathbb{Q}_v) : E_0(\mathbb{Q}_v)]$ という仮定から, $\mathrm{loc}_v(\kappa_l) \in E(\mathbb{Q}_l)/qE(\mathbb{Q}_l)$ が示せる.

[4] これは, [20, Theorem 4.5.4] の証明と同様の方法を用いて, $\mathrm{loc}_l(\kappa) \neq 0$ から示せる.

$S>0$ を $(S,N)=1$ なる自然数とすると, [13, Chapter 1, §6] より, $(a,S)=1$ なる $a\in\mathbb{Z}$ に対し

$$[a/S]_E^{\pm}=\varepsilon_f\,[a'/S]_E^{\pm}.$$

ここで, a' は $a'aN\equiv -1 \mod S$ を満たす任意の整数. したがって, $\iota:\mathbb{Q}[G_S]\to\mathbb{Q}[G_S]$ を $\sigma\in G_S$ を σ^{-1} に送る写像から誘導される準同型とすると, 次の "関数等式" を得る.

$$\theta_S=\varepsilon_f\sigma_{-N}^{-1}\iota(\theta_S). \tag{3.10}$$

ここで, $\sigma_{-N}\in G_S$ は, 円分指標 $G_S\cong(\mathbb{Z}/S\mathbb{Z})^\times$ のもとで $-N\in(\mathbb{Z}/S\mathbb{Z})^\times$ に対応する元であったことを思い出す.

定理 3.2 の証明. S を定理 3.2 のようにとる. 系 3.12 より, $\theta_{S,p}\in I_{S,p}^{\min\{r_p-1,p\}}$. $p\le r_p-1$, あるいは $r_p=0$ なら何も示すことがないので, $1\le r_p\le p$ と仮定してよい. このとき, $\theta_{S,p}\in I_{S,p}^{r_p-1}$. 関数等式 (3.10) より, イデアル商 $I_{S,p}^{r_p-1}/I_{S,p}^{r_p}$ において

$$\theta_{S,p}\equiv\varepsilon_f\delta_{-N}^{-1}\iota(\theta_{S,p})\equiv\varepsilon_f\delta_{-N}^{-1}(-1)^{r_p-1}\theta_{S,p}\equiv\varepsilon_f(-1)^{r_p-1}\theta_{S,p}\mod I_{S,p}^{r_p}. \tag{3.11}$$

p-parity 予想より $(-1)^{\mathrm{ord}_{s=1}(L(E,s))}=(-1)^{r_p}$. これと (3.9), (3.11) より,

$$2\theta_{S,p}\equiv 0 \mod I_{S,p}^{r_p}.$$

したがって, $p\nmid 2$ より, $\theta_{S,p}\in I_{S,p}^{r_p}$. □

謝辞

[17] の元になった著者の博士論文の執筆を指導し, また, 研究集会「代数的整数論とその周辺 2015」における著者の講演を推薦してくださった小林真一先生に感謝申し上げます. 講演の機会をくださった, 高橋浩樹先生, 大野泰生先生, 津嶋貴弘先生にお礼申し上げます. また, 講演に際して有益なコメントをくださった, 栗原将人先生, 山内卓也先生に感謝いたします. 最後に, 本原稿を注意深く読み, 数多くのご指摘・コメントをくださった査読者に感謝申し上げます。

References

[1] Cojocaru, A. C., On the surjectivity of the Galois representations associated to non-CM elliptic curves, *Canad. Math. Bull.,* **48** (2005), 16–31.
[2] Darmon, H., A refined conjecture of Mazur-Tate type for Heegner points, *Invent. Math.,* **110** (1992), 123–146.
[3] Dokchitser, T. and Dokchitser, V., On the Birch-Swinnerton-Dyer quotients modulo squares, *Ann. of Math.* (2), **172** (2010), 567–596.
[4] Drinfel'd, V. G., Two theorems on modular curves, *Funkcional. Anal. i Prilož en.,* **7** (1973), 83–84.

[5] Kato, K., p-adic Hodge theory and values of zeta functions of modular forms, *Astérisque,* **295** (2004), ix, 117–290.
[6] Kim, B. D., The parity conjecture for elliptic curves at supersingular reduction primes, *Compos. Math.,* **143** (2007), 47–72.
[7] Kobayashi, S., Iwasawa theory for elliptic curves at supersingular primes, *Invent. Math.,* **152** (2003), 1–36.
[8] Kurihara, M., On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I, *Invent. Math.,* **149** (2002), 195–224.
[9] Kurihara, M., The structure of Selmer groups of elliptic curves and modular symbols, *Iwasawa Theory 2012*, *Contrib. Math. Comput. Sci.,* Springer, Heidelberg, **7** (2014), 317–356.
[10] Mazur, B., Rational points of abelian varieties with values in towers of number fields, *Invent. Math.*, **18** (1972), 183–266.
[11] Mazur, B., Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.*, **44** (1978), 129–162.
[12] Mazur, B. and Tate, J., Refined conjectures of the "Birch and Swinnerton-Dyer type", *Duke Math. J.*, **54** (1987), 711–750.
[13] Mazur, B., Tate, J. and Teitelbaum, J., On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.*, **84** (1986), 1–48.
[14] Milne, J. S., *Arithmetic duality theorems*, BookSurge, LLC, Charleston, SC, second ed., 2006.
[15] Monsky, P., Generalizing the Birch-Stephens theorem. I. Modular curves, *Math. Z.,* **221** (1996), 415–420.
[16] Nekovář, J., Selmer complexes, *Astérisque*, **310** (2006), viii+559.
[17] Ota, K., Kato's Euler system and the Mazur-Tate refined conjecture of BSD type, *Amer. J. Math.*, **140** (2018), 495–542.
[18] Otsuki, R., Construction of a homomorphism concerning Euler systems for an elliptic curve, *Tokyo J. Math.*, **32** (2009), 253–278.
[19] Pollack, R., On the p-adic L-function of a modular form at a supersingular prime, *Duke Math. J.,* **118** (2003), 523–558.
[20] Rubin, K., *Euler systems*, Annals of Mathematics Studies **147**, Princeton University Press, Princeton, NJ, 2000.
[21] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, **15** (1972), 259–331.
[22] Serre, J.-P., Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.*, **54** (1981), 323–401.
[23] Silverman, J. H., *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.
[24] Tan, K.-S., Refined theorems of the Birch and Swinnerton-Dyer type, *Ann. Inst. Fourier* (*Grenoble*), **45** (1995), 317–374.