楕円曲線に対する栗原の予想について

理化学研究所 革新知能統合研究センター 数理科学チーム　坂本　龍太郎
RYOTARO SAKAMOTO
MATHEMATICAL SCIENCE TEAM,
RIKEN CENTER FOR ADVANCED INTELLIGENCE PROJECT (AIP)

1. Introduction

本稿は論文 [7] に関する概説論文である．著者は論文 [7] において栗原の論文 [3] で提起された予想を肯定的に解決した．まず初めに，この栗原の予想について説明するためにいくつかの記号を導入する．$E/\mathbb{Q}$ を楕円曲線，$S_{\mathrm{bad}}(E)$ を $E/\mathbb{Q}$ が良還元を持たない素数の集合とする．また各素数 ℓ に対して $\mathrm{Tam}_\ell(E)$ を ℓ における $E/\mathbb{Q}$ の玉河因子とする．次の条件を満たす奇素数 p を 1 つ固定する:

(a) E は p で通常良還元を持つ,
(b) $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[p])$ は全射,
(c) $p \nmid \#E(\mathbb{F}_p) \prod \mathrm{Tam}_\ell(E)$.

素数の集合 $\mathcal{P}$ を

$$\mathcal{P} := \{\ell \notin S_{\mathrm{bad}}(E) \mid E(\mathbb{F}_\ell)[p] \cong \mathbb{F}_p \text{ かつ } \ell \equiv 1 \pmod{p}\}$$

と定め，$\mathcal{N}$ を $\mathcal{P}$ の元の積で表される平方因子を持たない自然数全体の集合とする．各素数 $\ell \in \mathcal{P}$ に対して生成元 $h_\ell \in \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ を 1 つとる．$\ell \equiv 1 \pmod{p}$ なので h_ℓ を底とする離散対数から全射

$$\overline{\log}_{h_\ell} \colon \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/(\ell-1) \longrightarrow \mathbb{F}_p;\ h_\ell^a \mapsto a \bmod p$$

が得られる．楕円曲線 $E/\mathbb{Q}$ に付随する重さ 2 の保型形式を f_E と書く．このとき自然数 $d \in \mathcal{N}$ と d と互いに素な整数 a に対して

$$[a/d] := 2\pi\sqrt{-1} \int_{\sqrt{-1}\infty}^{a/d} f(z)\,\mathrm{d}z$$

とおく．

Remark 1.1. 導手 d の Dirichlet 指標 $\chi \colon G_{\mathbb{Q}} \longrightarrow \mathbb{C}^\times$ に対して

$$\frac{\Gamma(s)}{(2\pi)^s} L(E,\chi,s) = \frac{1}{\tau(\overline{\chi})} \sum_{a \in (\mathbb{Z}/d)^\times} \overline{\chi}(\sigma_a) \int_0^\infty f_E(\sqrt{-1}y + a/d) y^{s-1}\,\mathrm{d}y$$

が成り立つ．ただし $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$ は $\sigma_a(\zeta_d) = \zeta_d^a$ を満たす同型写像である．

以上の設定の下で，論文 [3] に従い，解析的な量 $\widetilde{\delta}_d$ を

$$\widetilde{\delta}_d := \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \frac{\mathrm{Re}([a/d])}{\Omega_E^+} \cdot \prod_{\ell \mid d} \overline{\log}_{h_\ell}(\sigma_a) \in \mathbb{F}_p$$

と定義する．ただし Ω_E^+ は E の Néron 周期である．論文 [3] で述べられているように $\widetilde{\delta}_d$ は計算可能な量である．

栗原の論文 [3] に従って用語を 1 つ用意する．

Definition 1.2. 自然数 $d \in \mathcal{N}$ は以下の 2 つの条件を満たすとき δ-極小という:

- $\widetilde{\delta}_d \neq 0$,
- d と異なる d の約数 e に対して $\widetilde{\delta}_e = 0$.

この時，論文 [3] で提起された楕円曲線に対する栗原の予想は以下のものである．

Conjecture 1.3 ([3, Conjecture 2])**.** 任意の δ-極小な自然数 $d \in \mathcal{N}$ に対して自然な準同型写像

$$\mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow \bigoplus_{\ell \mid d} E(\mathbb{Q}_\ell) \otimes_{\mathbb{Z}} \mathbb{F}_p \tag{1}$$

は同型である．

Remark 1.4. 素数の集合 $\mathcal{P}$ の定義より各 $\ell \in \mathcal{P}$ に対して

$$\dim_{\mathbb{F}_p} E(\mathbb{Q}_\ell) \otimes_{\mathbb{Z}} \mathbb{F}_p = 1$$

である．従って，d の素因子の数を $\nu(d)$ と書けば Conjecture 1.3 から

$$\dim_{\mathbb{F}_p} \mathrm{Sel}(\mathbb{Q}, E[p]) = \nu(d)$$

が従う．即ち，Conjecture 1.3 を用いることで p-Selmer 群の次元を (計算可能な) 解析的な量で記述できる．

上述したように著者の論文 [7] の主結果はこの栗原による予想 (Conjecture 1.3) の肯定的解決である:

Theorem 1.5 ([7, Theorem 1.5])**.** 任意の δ-極小な自然数 $d \in \mathcal{N}$ に対して準同型写像 (1) は同型である．従って $\dim_{\mathbb{F}_p} \mathrm{Sel}(\mathbb{Q}, E[p]) = \nu(d)$ である．

Remark 1.6. 証明の手法は少し異なるが Chan-Ho Kim も [5] で Theorem 1.5 と同様の結果を示している．

Remark 1.7. Stickelberger 元を用いることで CM 体のイデアル類群に対しても Conjecture 1.3 と同様の予想を考えることができる．しかし [3, §5.4] でその反例が与えられている．

2. Theorem 1.5 の証明の概略

この節では Theorem 1.5 の証明の概略について説明する．Theorem 1.5 の証明では論文 [6] で構成した階数 0 の Kolyvagin 系の理論が中心的な役割を果たすため，まず最初に階数 0 の Kolyvagin 系について説明する．その後，Theorem 1.5 の証明について説明する．

2.1. 階数 0 の Kolyvagin 系.

階数 0 の Kolyvagin 系の定義を述べるために幾つか記号を用意する．

素数 $\ell \in \mathcal{P}$ を 1 つとる．このとき $E[p]$ の基底を上手く選べば

$$\mathrm{Fr}_\ell = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

とできる．従って

$$H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p]) \cong E[p]/(\mathrm{Fr}_\ell - 1)E[p]$$

は 1 次元 $\mathbb{F}_p$-ベクトル空間である．

$$H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p]) := H^1(G_{\mathbb{Q}_\ell}, E[p])/H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p])$$

とおく．このとき

$$H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p]) \cong \mathrm{Hom}(G_{\mathbb{Q}_\ell^{\mathrm{ur}}}, E[p]^{\mathrm{Fr}_\ell = 1})$$

なので固定した生成元 $h_\ell \in \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell)$ を用いれば

$$H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p]) \cong E[p]^{\mathrm{Fr}_\ell = 1}$$

を得る．さらに対応 $x \mapsto (\mathrm{Fr}_\ell - 1)x$ は同型写像 $E[p]/(\mathrm{Fr}_\ell - 1)E[p] \xrightarrow{\sim} E[p]^{\mathrm{Fr}_\ell = 1}$ を定めるので自然な同型

$$H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p]) \xrightarrow{\sim} H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p])$$

を得る．

$$H^1_{/\mathrm{tr}}(G_{\mathbb{Q}_\ell}, E[p]) := H^1(G_{\mathbb{Q}_\ell(\mu_\ell)}, E[p])^{\mathrm{Gal}(\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell)}$$

とおく．このとき自然な準同型写像

$$H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p]) \longrightarrow H^1_{/\mathrm{tr}}(G_{\mathbb{Q}_\ell}, E[p])$$

は同型である (cf. [4, Lemma 1.2.4])．従って，同型 $H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p]) \cong \mathbb{F}_p$ を 1 つ固定すると 2 つの $\mathbb{F}_p$ への準同型写像

$$\begin{aligned} v_\ell &\colon H^1(G_{\mathbb{Q}}, E[p]) \longrightarrow H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p]) = \mathbb{F}_p, \\ \varphi_\ell &\colon H^1(G_{\mathbb{Q}}, E[p]) \longrightarrow H^1_{/\mathrm{tr}}(G_{\mathbb{Q}_\ell}, E[p]) = \mathbb{F}_p \end{aligned}$$

を得る．

Definition 2.1. 自然数 $n \in \mathcal{N}$ に対して

$$H^1_{\mathcal{F}^n}(G_{\mathbb{Q}}, E[p]) := \ker\left(H^1(G_{\mathbb{Q}}, E[p]) \longrightarrow \bigoplus_{\ell \nmid n} H^1(G_{\mathbb{Q}_\ell}, E)[p] \right)$$

とおく．さらに $n = dm$ のとき

$$H^1_{\mathcal{F}^d(m)}(G_{\mathbb{Q}}, E[p]) := \ker\left(H^1_{\mathcal{F}^n}(G_{\mathbb{Q}}, E[p]) \xrightarrow{\oplus_{\ell \mid m} \varphi_\ell} \bigoplus_{\ell \mid m} \mathbb{F}_p \right)$$

とおく．特に $d = 1$ の場合には $H^1_{\mathcal{F}(m)}(G_{\mathbb{Q}}, E[p]) := H^1_{\mathcal{F}^1(m)}(G_{\mathbb{Q}}, E[p])$ と書くことにする．

Remark 2.2. $\mathrm{Sel}(\mathbb{Q}, E[p]) = H^1_{\mathcal{F}^1}(G_{\mathbb{Q}}, E[p])$ である．

以上の準備の下で階数 0 の Kolyvagin 系を定義する．

Definition 2.3. $\mathcal{M} := \{(d, \ell) \in \mathcal{N} \times \mathcal{P} \mid \gcd(d, \ell) = 1\}$ とおく．以下の条件を満たすコホモロジー群の元の族

$$(\kappa_{d,\ell})_{(d,\ell) \in \mathcal{M}} \in \prod_{(d,\ell) \in \mathcal{M}} H^1_{\mathcal{F}^\ell(d)}(G_{\mathbb{Q}}, E[p])$$

を階数 0 の Kolyvagin 系と呼ぶ:

$$\begin{aligned} v_\ell(\kappa_{d\ell,q}) &= \varphi_\ell(\kappa_{d,q}), \\ v_\ell(\kappa_{1,\ell}) &= v_q(\kappa_{1,q}), \\ v_q(\kappa_{d\ell,q}) &= -\varphi_\ell(\kappa_{d,\ell}). \end{aligned} \tag{2}$$

さらに (階数 0 の) Kolyvagin 系の集合を $\mathrm{KS}_0(E[p])$ と書く．Kolyvagin 系 $\kappa \in \mathrm{KS}_0(E[p])$ と $(d, \ell) \in \mathcal{M}$ に対して

$$\delta(\kappa)_d := v_\ell(\kappa_{d,\ell}) \in \mathbb{F}_p$$

とおく．Kolyvagin 系の持つ関係式から $\delta(\kappa)_d$ は ℓ に依らないことが分かる．

Remark 2.4. 階数 0 の Kolyvagin 系が満たす関係式 (2) は栗原による論文 [1, 2] で最初に現れた．

次の定理は [6] の主結果 ([6, Proposition 5.6, Theorem 5.8]) から直ちに従う．

Theorem 2.5.

(1) $\dim_{\mathbb{F}_p} \mathrm{KS}_0(E[p]) = 1$.
(2) 非自明な *Kolyvagin* 系 $\kappa \in \mathrm{KS}_0(E[p])$ と自然数 $d \in \mathcal{N}$ に対して以下は同値である．
  (a) $\delta(\kappa)_d \neq 0$.
  (b) $H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, E[p]) = 0$.

2.2. **Theorem 1.5 の証明の概略.** 加藤の Euler 系と modular symbol の関係を利用することで $(\widetilde{\delta}_d)_{d\in\mathcal{N}}$ と関係する階数 0 の Kolyvagin 系を構成することができる:

Proposition 2.6 ([7, Theorem 3.14])**.**

$$(\tilde{\delta}_d)_{d\in\mathcal{N}} \in \mathrm{im}\left(\delta\colon \mathrm{KS}_0(E[p]) \longrightarrow \prod_{d\in\mathcal{N}} \mathbb{F}_p\right).$$

自然数 $d \in \mathcal{N}$ に対して

$$\lambda(d) := \dim_{\mathbb{F}_p} H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, E[p])$$

とおく．Theorem 2.5 と Proposition 2.6 を用いて δ-極小という性質から $\lambda(d)$ に関する情報を得ることができる:

Corollary 2.7. δ-極小な自然数 $d \in \mathcal{N}$ に対して次が成り立つ．

(1) $\lambda(d) = 0$.
(2) d と異なる d の約数 e に対して $\lambda(e) > 0$.

Corollary 2.8. δ-極小な自然数 $d \in \mathcal{N}$ に対して準同型写像 (1) は単射である．特に *Conjecture 1.3* は $\lambda(1) = \nu(d)$ と同値である．

Proof. Corollary 2.7 と定義より

$$\ker\left(\mathrm{Sel}(\mathbb{Q}, E[p]) \xrightarrow{(1)} \bigoplus_{\ell|d} E(\mathbb{Q}_\ell)\otimes\mathbb{F}_p\right) \subset H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, E[p]) = 0$$

である． □

以上の結果から Conjecture 1.3 を証明するためには d を動かした時の $\lambda(d)$ の挙動を理解すればよい．Poitou–Tate の完全列を利用することで次の補題を証明することができる．

Lemma 2.9 ([6, Proposition 4.7])**.** $\lambda(d) = 0$ を満たす $d \in \mathcal{N}$ 対して，ある d の約数 e が存在して $\nu(e) = \lambda(1)$ かつ $\lambda(e) = 0$ が成り立つ．

Remark 2.10. Lemma 2.9 の証明では Galois 表現 $E[p]$ と Selmer 構造が持つ対称性が重要な役割を果たす．また，それこそが CM 体のイデアル類群に対して Conjecture 1.3 の類似が成立しない理由である．

以上の結果を用いることで Theorem 1.5 が証明できる．

proof of Theorem 1.5. δ-極小な自然数 $d \in \mathcal{N}$ に対して Corollary 2.7 と Lemma 2.9 より $\lambda(d) = \nu(d)$ が成り立つ．従って Corollary 2.8 より準同型写像 (1) は同型である． □

References

[1] M. Kurihara, Refined Iwasawa theory and Kolyvagin systems of Gauss sum type, Proc. Lond. Math. Soc. (3) 104 (2012), no. 4, 728–769.
[2] Kurihara, Masato. Refined Iwasawa theory for p-adic representations and the structure of Selmer groups, Münster J. Math. 7 (2014), no. 1, 149–223.
[3] Kurihara, Masato. The structure of Selmer groups of elliptic curves and modular symbols, Iwasawa theory 2012, 317–356, Contrib. Math. Comput. Sci., 7, Springer, Heidelberg, 2014.
[4] Mazur, Barry; Rubin, Karl. Kolyvagin systems, Mem. Amer. Math. Soc. **799** (2004).
[5] Kim, Chan-Ho. Refined applications of Kato's Euler systems for modular forms. preprint, arXiv:2203.12157.
[6] Sakamoto, Ryotaro. On the theory of Kolyvagin systems of rank 0. to appear in Journal de Théorie des Nombres.
[7] Sakamoto, Ryotaro. p-Selmer group and Modular symbols. preprint, arXiv:2106.03370.

RIKEN Center for Advanced Intelligence Project, Nihonbashi 1-chome Mitsui Building, 15th floor, 1-4-1 Nihonbashi, Chuo-ku, Tokyo 103-0027, Japan
Email address: ryotaro.sakamoto@riken.jp