1/8 楕円曲線の等分体のideal類群のGalois加群の構造について

(臺信直人 / 慶應大)

テーマ: L-関数の特殊値とideal類群の関係.

zeta関数　　　代数体の不変量

Today: Herbrand-Ribetの定理の楕円曲線に対する類似.

§0: 基本的な設定と記号.

- $p \geq 3$: prime
- $E/\mathbb{Q}$: 楕円曲線 $y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z})$
- $L(E,s)$: EのHasse-WeilのL関数
- $r_{an}(E/\mathbb{Q}) := \mathrm{ord}_{s=1} L(E,s)$

  今回は $r_{an}(E/\mathbb{Q}) \leq 1$ となるものだけを考える.
- $r_{alg}(E/\mathbb{Q})$: EのMordell-Weil rank

  (i.e.) $E(\mathbb{Q}) \simeq \mathbb{Z}^{\oplus r_{alg}(E/\mathbb{Q})} \oplus (\mathrm{Tors})$.

Fact [Gross-Zagier-Kolyvagin]

上の設定で以下がわかる.

① $r_{an}(E/\mathbb{Q}) = r_{alg}(E/\mathbb{Q})$

② $\# Ш(E/\mathbb{Q}) < \infty$

§1: Introduction.

- $F := \mathbb{Q}(\zeta_p)$ 円のp分体 $\left(\zeta_p := \exp\left(\frac{2\pi i}{p}\right)\right)$
- $Cl(F)$: Fのideal類群 (有限群)

- $\underset{\substack{\circlearrowright \\ \mathrm{Gal}(F/\mathbb{Q})}}{A(F)} := Cl(F) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ (p-Sylow subgroup)

Theorem [Kummer '50]

$$\exists k \in 2\mathbb{Z}_{>0} \ (\text{s.t.}) \ p \mid \underline{\zeta(1-k)} \overset{\text{iff}}{\Longleftrightarrow} A(F) \neq 0$$

$\left\{ \begin{array}{l} \text{zeta 関数 } \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \\ \zeta(1-k) \in \mathbb{Q} \end{array} \right.$

Remark

$A(F)=0 \overset{\text{Kummer}}{\Longrightarrow} x^p + y^p = z^p$ で $xyz \neq 0$ となる整数解がない.

Example

$k=12$ のとき,

$$\zeta(1-12) = \zeta(-11) = \frac{691}{32760} \leftarrow \text{prime}$$

なので, $A(\mathbb{Q}(\zeta_{691})) \neq 0$.

□ Herbrand - Ribet

$$A(F) = \bigoplus_{i=0}^{p-2} \underbrace{A(F)^{\omega^i}}_{\parallel}$$

$\omega : \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^{\times}$

mod p cyc. char.

$\{ x \in A(F) \mid \forall \sigma \in \mathrm{Gal}(F/\mathbb{Q}),\ \sigma(x) = \omega^i(\sigma) x \}$

Theorem [Herbrand - Ribet]

$k \in 2\mathbb{Z}_{>0}$ に対して

$$p \mid \zeta(1-\underline{\underline{k}}) \overset{\text{iff}}{\Longleftrightarrow} A(F)^{\omega^{1-k}} \neq 0$$

← k の情報がどちらの側にあるのかが重要

これの楕円曲線類似 (due to D. Prasad '20) を考えたい.

- $K := \mathbb{Q}(E[p])$, $E[p] := \{ Q \in E(\overline{\mathbb{Q}}) \mid p \cdot Q = 0 \}$

- $\underset{\substack{\circlearrowright \\ \mathrm{Gal}(K/\mathbb{Q})}}{A(K)} := Cl(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ ← 多くの場合は $\mathrm{Gal}(K/\mathbb{Q}) \simeq GL_2(\mathbb{F}_p)$

$$\underbrace{A(K)^{ss}} = \bigoplus_{M:\text{simple}} M^{\oplus r_M}$$ multiplicity

$A(K)$ の $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-mod としての半単純化

Prasad's Question

(Irr) : $E[p]$ が $\mathrm{Gal}(K/\mathbb{Q})$-mod として既約.

とする.

$$p \mid \underline{\mathcal{L}^*(E,1)_{alg}} \overset{?}{\Longleftrightarrow} r_{E[p]} \neq 0$$

$\mathcal{L}^*(E,1)$: $\mathcal{L}(E,s)$ の $s=1$ の leading term

$$\mathcal{L}^*(E,1)_{alg} := \frac{\mathcal{L}^*(E,1)}{\mathrm{Reg}_\infty(E)\Omega_E} \in \mathbb{Q}.$$

Theorem [Prasad - Shekhar '20]

いくつかの仮定をもとに

$$\dim_{\mathbb{F}_p}(\underline{\mathrm{Sel}(G_\mathbb{Q}, E[p])}) \geq 2 \Rightarrow r_{E[p]} \neq 0$$

$\cap$

$H^1(G_\mathbb{Q}, E[p])$, $G_\mathbb{Q}$ は絶対ガロア群 $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Corollary

BSD予想 の p-部分と上の定理の条件を仮定すると $p \mid \mathcal{L}^*(E,1)_{alg} \Rightarrow r_{E[p]} \neq 0$.

§ Main - Results

① Prasad - Shekhar's work の部分的 改善

("全素点不分岐 な有理点" の導入)

Remark

先の Cor の "$\Leftarrow$" が 成り立たない.

$$\exists E. \ r_{an}(E/\mathbb{Q}) = 1 \quad \text{(s.t.)} \quad p \nmid \mathcal{L}^*_{alg}(E,1) \ \text{ and } \ r_{E[p]} \neq 0.$$

② p進L値の p-可除性から $r_{E[p]} \neq 0$ を示した.

§2 Everywhere unramified points

Definition

- $E(\mathbb{Q})_{ur,p} := \ker\left(E(\mathbb{Q}) \longrightarrow \prod_{\ell:\text{prime}} \dfrac{E(\mathbb{Q}_\ell^{ur})}{pE(\mathbb{Q}_\ell^{ur})} \right)$

$$\begin{array}{c} \mathbb{Q}_\ell^{ur} \\ | \\ \mathbb{Q}_\ell \end{array}$$

$$\begin{array}{c} E(\mathbb{Q})_{ur,p} \\ \cup \\ pE(\mathbb{Q}) \end{array}$$

- $r_{ur,p}(E) := \dim_{\mathbb{F}_p}\left(E(\mathbb{Q})_{ur,p} / pE(\mathbb{Q})\right)$

Proposition 1

$r_{E[p]} \geq r_{ur,p}(E)$ が (Irr) の仮定の下で成り立つ.

Proposition 2

(Tam) : $p \nmid \mathrm{Tam}_E$ $(\in \mathbb{Z}_{>0})$ を仮定.

このとき,

$$E(\mathbb{Q})_{ur,p} = \ker\left(E(\mathbb{Q}) \to E(\mathbb{Q}_p^{ur}) / pE(\mathbb{Q}_p^{ur}) \right)$$

Theorem [D]

(Irr), (Tam) を仮定する.

p進付値

$$\exists Q \in E(\mathbb{Q}) \cap E_1(\mathbb{Q}_p) \setminus pE(\mathbb{Q}) \quad (\text{s.t.}) \quad 2 \leq v_p(\log_E(Q)) \rightsquigarrow Q \in E(\mathbb{Q})_{ur,p}$$

(X, Y) $/\!/$ 　$r_{an}(E/\mathbb{Q}) = 1$ ならば.....

$\log_E(Q) \in \mathbb{Z}_p$, $\quad v_p(\log_E(Q)) = v_p\left(\frac{X}{Y}\right)$

$$\Rightarrow \quad r_{ur,p}(E) > 0$$

特に (prop 1) より $r_{E[p]} \neq 0$.

Remark

$r_{an}(E/\mathbb{Q}) = 1$ かつ $p \nmid \#Ш(E/\mathbb{Q})$ の場合,

Thm 1 $\Rightarrow$ Prasad - Shekher 's result

//

§3 p-adic L-values and non-vanishing of $r_{E[p]}$.

以下, $r_{an}(E/\mathbb{Q})=1$ & E は p で good とする.

α, β : $X^2 - a_p(E)X + p = 0$ の 2解 $\quad (a_p(E) := (1+p) - \#E(\mathbb{F}_p))$

ただし, $v_p(\alpha) \leq v_p(\beta)$ とする.

- $* \in \{\alpha, \beta\}$ に対して

$L_{p,*}(E,s)$: E の $*$-p進 L関数 $\quad (s \in \mathbb{C}_p)$
(cyclotomic)

Theorem 2 [D]

次を仮定する : (Tam), (Irr), (Cond), (non-anom), (SS), (ord)

(Cond) : Cond(E) は 平方因子なし. 素因子 2つ以上.

(non-anom) : $p \nmid \#E(\mathbb{F}_p)$.

(SS) : E が p で SS のとき $a_p(E) = 0$

(ord) : E が p で good ordinary のとき, α-p進高さ関数が 非自明.

このとき,

$$v_p\left((1-\tfrac{1}{\alpha})^{-2} L'_{p,\alpha}(E,1) - (1-\tfrac{1}{\beta})^{-2} L'_{p,\beta}(E,1) \right) \geq 2 - v_p([\omega, \varphi(\omega)])$$

$\Rightarrow r_{E[p]} \neq 0$.

Remark

Thm 2の 仮定 + BSD 予想 の p部分の 仮定 の下で

Thm 2 $\Rightarrow$ 「$p \mid L^*(E,1)_{alg} \Rightarrow r_{E[p]} \neq 0$」

//