On Goldfeld Conjecture

Ye Tian

§1 Non-vanishing of quadratic twist L-values

M ell curve $/\mathbb{Q}$. irred cusp self-contragradient autom rep of $GL_2(\mathbb{A}_F)$.

$\rightsquigarrow L(M,s)$ with $\varepsilon(M)=\pm 1$.

<u>Thm</u> (Bump-Frieberg-Hoffstein, FH)

If there exists a quad twist $M\otimes\eta_0$ with sign $(-1)^r$ $(r=0,1)$

then $\exists$ infin many quad twists $\operatorname{ord}_{s=s_0} L(M\otimes\eta_0, s)=r$.

<u>Rem</u> " $\sum_m \frac{L(w, M\otimes\eta_m)}{|m|^s}$ " $\leftarrow \mathbb{Q}(\sqrt{m})$ for $s, w\in\mathbb{C}$.

RS convolution $\rightsquigarrow$ mero conti to $(s,w)\in\mathbb{C}^2$

with poles at $s=1$ & $s=2-2w$.

Res of L-series at $s=1$ for center $w=1/2 \neq 0$.

<u>Q</u> Joint non-vanishing $M_1, \cdots, M_k$.

$\exists \eta_0$, s.t. $\varepsilon(M_i\otimes\eta_0)=(-1)^{r_i}$, $r_i=0,1$

$\overset{?}{\rightsquigarrow}$ $\exists$ infinity many η s.t. $\operatorname{ord}_{s=s_0} L(M\otimes\eta, s)=r_i$ $(1\le i\le k)$.

However. the case is different even when $k=2$.

- Xiannan Li 2022 (Keating-Snaith Conj):

$$\sum L(1/2, f\otimes\eta_m)^k \sim CX(\log X)^{\frac{k(k-1)}{2}} \rightsquigarrow \text{can apply to } k=2.$$

§2 Goldfeld conjecture

<u>Conj</u> $E/\mathbb{Q}: y^2=x^3+ax+b$. Then for $E^{(n)}: ny^2=x^3+ax+b$,

$$\underset{\text{when } n \text{ varies}}{\operatorname{Prob}}\left(\operatorname{ord}_{s=1} L(E^{(n)}/\mathbb{Q}, s)=r\right) = \begin{cases} 1/2, & r=0,1 \\ 0, & r\geq 2. \end{cases}$$

Rem Basically, $\sum_{|D|\le X} \operatorname{ord}_{s=1} L(E^{(D)}/\mathbb{Q}, s) \sim \frac{1}{2}\sum_{|D|\le X} 1$.

- Trivially, LHS has lower bound as RHS.
- Goldfeld proved an upper bound $= (3.25+\varepsilon)\sum_{|D|\le X} 1$.

<u>The joint version of Goldfeld Conj</u>

Σ = a fin set of places of $\mathbb{Q}$, with $2, \infty \in \Sigma$

p prime s.t. all ell curves $\{E^{(n)}\}$ has bad red'ns at p.

$\underbrace{\eta_{n_1} \sim \eta_{n_2}}$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \iff n_2/n_1 \in \mathbb{Q}_v^{\times 2}$, $\forall v \in \Sigma$.

also write $n_1 \sim n_2$.

Conj $\forall$ equiv class $\mathfrak{X}$ in a twist family with sign $(-1)^r$.

$$\operatorname{Prob}(\operatorname{ord}_{s=1} L(E\otimes\eta, s) = r \mid \eta \in \mathfrak{X}) = 1.$$

It implies a $k \ge 2$ result:

Conj $E_1, \cdots, E_k$ ell curves $/\mathbb{Q}$, Σ & $\mathfrak{X}$ as above, sign $\varepsilon(E_i^{(\mathfrak{X})}) = (-1)^{r_i}$.

Then $\operatorname{Prob}(\operatorname{ord}_{s=1} L(E_i\otimes\eta, s) = r_i, 1\le i\le k \mid \eta \in \mathfrak{X}) = 1$.

<u>§3 Main result</u>

<u>Thm</u> (Smith, Pan-Tian)

Let $E_1, \cdots, E_k/\mathbb{Q}$ with $E_i[2] \subseteq E_i(\mathbb{Q})$.

Let $\mathfrak{X}$ be a Σ-equiv class with $\Sigma(E_i^{(\mathfrak{X})}) = (-1)^{r_i}$, $r_i = 0, 1$.

Then $\operatorname{Prob}(\operatorname{corank}_{\mathbb{Z}_2} \operatorname{Sel}_{2^\infty}(E_i^{(n)}/\mathbb{Q}) = r_i \mid n \in \mathfrak{X}) = 1$.

<u>Rem</u> Importance of rk 0 & rk 1: p-converse for $p=2$.

<u>Thm</u> (Burungale-Tian)

Let $m_1, \cdots, m_k$ be positive integers $\equiv 1 \bmod 8$. $E_i: m_i y^2 = x^3 - x$.

$$\mathrm{Prob}\left(\operatorname*{ord}_{s=1} L(E_1^{(n)}, s) = 0 : n>0 \text{ squarefree } \& \ n \equiv 1,2,3 \bmod 8\right) = 1.$$

<u>Cor.</u> rk 1 : p-converse for CM ell curve $/\mathbb{Q}$, $\forall p$.

§4 Selmer groups

F global field.

[BKLPR] gave a distribution model of $\mathrm{Sel}_{p^\infty}(E/F)$

for E running over all ecs $/F$.

$r = 0, 1$. G f.g. $\mathbb{Z}_p$-mod,

$$P_r^{\mathrm{Alt}}(G) := \lim_{n\to\infty} \mathrm{Prob}\left(\mathrm{Coker}\, B \cong G : B \in M_{2k+r}^{\mathrm{Alt}}(\mathbb{Z}_p)\right)$$

<u>Conj</u> (BKLPR) $\mathrm{Prob}\left(\mathrm{Sel}_{p^\infty}(E/F) \cong \widehat{G} : \varepsilon(E/F) = (-1)^r \text{ for } E \text{ ec}/F\right) = P_r^{\mathrm{Alt}}(\widehat{G})$

It also predicts the average order of p-Selmer gp.

<u>Conj</u> Let $P_r^{\mathrm{Alt}}(d \geq 0) = \lim_{n\to\infty} \mathrm{Prob}\left(\mathrm{corank}\, B = d \mid B \in M_{2k+r}^{\mathrm{Alt}}(\mathbb{F}_p)\right)$.

$\Rightarrow$ $\mathrm{Prob}\left(\dim_{\mathbb{F}_p} S_p(E/F) = d \mid \varepsilon(E/F) = (-1)^r\right) = P_r^{\mathrm{Alt}}(d)$

& $\mathrm{Avg}\left(\# S_p(E/F)^{\xi} \mid \varepsilon(E/F) = (-1)^r\right) = \sum_{d=0}^{\infty} P_r^{\mathrm{Alt}}(d) \cdot p^{\xi d} = \prod_{i=1}^{\xi} (1 + p^i)$

<u>Bhagava</u> $F = \mathbb{Q}$, $p \in \{2, 3\}$, $\xi < 1$.

§5 Quadratic twist

- Heath-Brown (1993, 1994): dist of $S_2(E/\mathbb{Q})$, $E : ny^2 = x^3 - x$.
- Swinnerton-Dyer, Kane (2013): dist of $S_2(E/\mathbb{Q})$, E satisfies

  (*) $E[2] \subseteq E(\mathbb{Q})$, E has no rational cyclic order 4 isog.
- Smith proved that the dist of $\mathrm{Sel}_{2^\infty}(E/\mathbb{Q})$ is similar to BKLPR when E satisfies (*).

Removing (*), but still with $E[2] \subseteq E(\mathbb{Q})$.

According to $G_{\mathbb{Q}}$-mod of $E[4]$.

$\rightsquigarrow$ 3 types of twist families $\mathcal{E}$.

(A) $\circledast$ & $y^2 = x^3 - x$

(B) E has a rat order 4 isog & $E[4] \not\subseteq E(\mathbb{Q}(i))$, $\forall E \in \mathcal{E}$.

e.g. $X_0(24)$: $y^2 = x(x-1)(x+3)$.

(C) E has a rat order 4 isog & $E[4] \subseteq E(\mathbb{Q}(i))$ for some $E \in \mathcal{E}$.

e.g. $X_0(15)$: $y^2 = x(x-9)(x-25)$ s.t. $25^2 - 9^2 = 4^2$.

It turns out that dist of $\mathrm{Sel}_{2^\infty}(E/\mathbb{Q})$ highly depends on equiv class $\mathfrak{X} \subseteq \mathcal{E}$.

For $r = 0, 1$. $\cdot$ $M_{2k+r}^{Alt}(\mathbb{F}_2)$

$\cdot$ $M_{2k+r, t_1}^{Alt}(\mathbb{F}_2)$: $\begin{pmatrix} 0 & * \\ * & * \end{pmatrix} \in M_{2k+r}^{Alt}(\mathbb{F}_2)$.

$t_1 \equiv r(2)$, size of 0-block is $k + \frac{t_1 + r}{2}$.

$\cdot$ $M_{2k+r, \{t_1, t_2\}}^{Alt}(\mathbb{F}_2)$: $\begin{pmatrix} 0 & * & * \\ * & 0 & * \\ * & * & * \end{pmatrix} \in M_{2k+r}^{Alt}(\mathbb{F}_2)$

$t_i \equiv r(2)$, size of 0-block is $k + \frac{t_i + r}{2}$.

$\forall$ f.g. $\mathbb{Z}_2$-mod G, define

$$P_{r,\underline{t}}^{Alt}(G) := \lim_{k \to \infty} \mathrm{Prob}(\mathrm{coker}\, B \cong G \mid B \in M_{2k+r,\underline{t}}^{Alt}(\mathbb{Z}_2) \xrightarrow{\text{via } \mathbb{Z}_2 \twoheadrightarrow \mathbb{F}_2} M_{2k+r,\underline{t}}^{Alt}(\mathbb{F}_2)\}$$

where $\underline{t} = \phi, \{t_1\}, \{t_1, t_2\}$ for types (A), (B), (C), resp'ly.

<u>Main thm</u> Let $\mathfrak{X}$ be Σ-equiv class in $\mathcal{E}$, $r \in \{0, 1\}$, $\varepsilon(\mathfrak{X}) = (-1)^r$.

Then $\exists$ (i) $t_1 \in \mathbb{Z}$, $t_1 \equiv r(2)$ for type B.

(ii) $t_1, t_2 \in \mathbb{Z}$, $t_i \equiv r(2)$ for type C

s.t. $\forall$ f.g. $\mathbb{Z}_2$-mod G,

$$\mathrm{Prob}(\mathrm{Sel}_{2^\infty}(E/\mathbb{Q}) \cong G \mid E \in \mathfrak{X}) = P_{r,\underline{t}}^{Alt}(G).$$

Rem Average order of $S_2(E/\mathbb{Q})$, $E \in \mathcal{X}$, is $3 + \sum_i 2^{t_i}$

pf. (1) $E \longmapsto S_2(E/\mathbb{Q})$, $E \in \mathcal{X}$.

(2) $\mathrm{Sel}_{2^i}(E/\mathbb{Q})$ $(1 \le i < k)$ $\rightsquigarrow$ $\mathrm{Sel}_{2^k}(E/\mathbb{Q})$.

Thm For any given positive integers $m_1, \cdots, m_k \equiv 1 \bmod 8$,

for almost all square-free positive ints $n \equiv 1, 2, 3 \bmod 8$,

$\forall\, 1 \le i \le k$, the equations $nm_i y^2 = x^3 - x$ has only solution at $y = 0$.