Iwasawa theory of elliptic curves at Eisenstein primes and arithmetic applications

F. Castella (UCSB)

§1. Statements

$E/\mathbb{Q}$ elliptic curve of conductor N

p prime, good ordinary for E

Descent exact sequence:

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^\infty] \to 0$$

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \subset H^1(G_{\mathbb{Q}}, E[p^\infty])$$

Thm (Gross–Zagier, Kolyvagin, Rubin)
Suppose $\mathrm{ord}_{s=1} L(E,s) = 1$
Then

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 1 \text{ and } \# Ш(E/\mathbb{Q}) < \infty.$$

(In particular, $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = 1$.)

Thm (after Skinner and W. Zhang)
Supp. $p > 2$ and $E[p]$ irreducible as a $G_{\mathbb{Q}}$-module.
(i.e., p is non-Eisenstein).
Then

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = 1 \Longrightarrow \mathrm{ord}_{s=1} L(E,s) = 1.$$

(p-converse to GZK)

Thm (after Jetchev–Skinner–Wan, and W. Zhang).

Supp. $p>2$ and p is non-Eisenstein.

If $\mathrm{ord}_{s=1} L(E,s) = 1$

then $$\mathrm{ord}_p\left(\frac{L'(E,1)}{\Omega_E \cdot \mathrm{Reg}_E}\right) = \mathrm{ord}_p\left(\#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}_E\right).$$

(p-part of BSD formula).

Theorem A (C.–Grossi–Lee–Skinner)

Suppose $p>2$ and $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ with $\phi|_{G_{\mathbb{Q}_p}} \neq \mathbb{1}, \omega$.

Then:

(i) p-converse to GZK holds for E.

(ii) If $\mathrm{ord}_{s=1} L(E,s) = 1$ and

ϕ is either $\begin{cases} p\text{-ramified and odd.} \\ p\text{-unramified and even.} \end{cases}$ ✪

then p-part of BSD formula holds for E.

<u>Corollary</u>. Under the same hyp., we have

$$\mathrm{Sel}_p(E/\mathbb{Q}) \simeq \mathbb{F}_p \implies \mathrm{ord}_{s=1} L(E,s) = 1.$$

$$\left(\text{so } \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 1 \ \& \ \# Ш(E/\mathbb{Q}) < \infty\right)$$

For $p=3$, Corollary + Bhargava–Klagsburn–Lemke Oliver–Shnidman

$\rightsquigarrow$ improved lower bounds on the proportion of quadratic twists E^D with $\mathrm{ord}_{s=1} L(E^D, s) = 1$.

<u>Remark</u>. Allowing $p=2$ and $\phi = \mathbb{1}$ is work in progress.

§2. Anti-cyclotomic Iwasawa theory

$K =$ (auxiliary) imaginary quadratic field s.t.
- $D_K < -3$ odd
- $\exists\, \mathfrak{n} \subset \mathcal{O}_K$ s.t. $\mathcal{O}_K/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$.

$$\begin{tikzcd}
K_\infty = \bigcup_{n \geq 0} K_n \arrow[d, dash, "\Gamma \cong \mathbb{Z}_p"] \arrow[dd, dash, bend right=60, "\Gamma \rtimes \{1,\tau\}"'] \\
K \arrow[d, dash, "\{1,\tau\}"] \\
\mathbb{Q}
\end{tikzcd}$$

anti-cyclotomic $\mathbb{Z}_p$-extension

Kummer images of Heegner points $x_n \in E(K_n)$ give

$$\kappa_\infty \in S = \varprojlim_n \varprojlim_m \mathrm{Sel}_{p^m}(E/K_n)$$

$$\circlearrowleft$$

$$\Lambda := \mathbb{Z}_p[[\Gamma]]$$

Pontryagin dual

Conjecture (Perrin-Riou)

Both S and $X := \mathrm{Sel}_{p^\infty}(E/K_\infty)^\wedge$ have Λ-rank 1, and

$$\mathrm{char}_\Lambda(X_{\Lambda\text{-tors}}) = \mathrm{char}_\Lambda\left(S/(\kappa_\infty)\right)^2.$$

Note. This is roughly a Λ-adic version of

$$\#\text{Ш}(E/K)[p^\infty] \cdot \mathrm{Tam}_E \sim_p [E(K)\otimes\mathbb{Z}_p : \mathbb{Z}_p x_0]^2.$$

Common in the Eisenstein and non-Eisenstein cases:

① PR's conj. (for suitable K) $\Longrightarrow$ p-converse to GZK.

s.t. $L(E^K,1)\neq 0$.

② PR's conj. (for suitable K) $\Longrightarrow$ p-part of BSD formula holds when $\mathrm{ord}_{s=1} L(E,s)=1$.

s.t. $L(E^K,1)\neq 0$ & p-part of BSD formula known for $L(E^K,1)$.

$\leftarrow$ reason for our ✩.

③ Can choose K where p splits and use:

Thm (after Bertolini–Darmon–Prasanna)
If p splits in K, Perrin-Riou's conj. is equivalent to Iwasawa's Main Conjecture for $\mathcal{L}_{BDP}$:

$$\mathrm{char}_\Lambda(\mathfrak{X}) = (\mathcal{L}_{BDP})^2.$$

§3. Non-Eisenstein case.

One proves IMC for $\mathcal{L}_{BDP}$ by combinings:

- Xin Wan: $\mathrm{char}_\Lambda(\mathfrak{X}) \subset (\mathcal{L}_{BDP})^2$ in $\Lambda[\frac{1}{p}]$.
- Hsieh: $\mu(\mathcal{L}_{BDP}) = 0$.
- Howard: $\mathrm{char}_\Lambda(X_{\Lambda\text{-tors}}) \supset \mathrm{char}_\Lambda(S/(k_\infty))^2$.

$\rightarrow$ all 3 require $E[p]|_{G_K}$ irreducible!

§4. Eisenstein case.

Key principle (after Greenberg–Vatsal):

Let $\Sigma = \{ w \mid N \}$

Then

$$\mathrm{char}_\Lambda(\mathfrak{X}) = (\mathcal{L}_{BDP})^2$$

$$\Updownarrow$$

$$\mathrm{char}_\Lambda(\mathfrak{X}^\Sigma) = (\mathcal{L}^\Sigma_{BDP})^2$$

relaxed local conditions at all $w \in \Sigma$

remove "Euler factors" at all $w \in \Sigma$.

advantage: better behaved wrt congruences mod p.

Theorem B (CGLS).

Supp. $p > 2$ and $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ with $\phi|_{G_{\mathbb{Q}_p}} \neq \mathbb{1}, \omega$.

and K = imag. quadratic field as above where p splits.

Then $\mathfrak{X}$ is Λ-torsion, and $\mathrm{char}_\Lambda(\mathfrak{X}) = (\mathcal{L}_{BDP})^2$.

Sketch of proof:

Given $0 \neq G \in \Lambda \simeq \mathbb{Z}_p[\![T]\!]$

can write $G = u \cdot p^{\mu} \cdot Q$, where

$u \in \Lambda^\times$

$\mu \in \mathbb{Z}_{\geq 0}$

$Q \in \mathbb{Z}_p[T]$ distinguished polynomial

$\deg Q =: \lambda$.

Applied to $\mathcal{F}^\Sigma$ s.t. $\mathrm{char}_\Lambda(\mathcal{X}^\Sigma) = (\mathcal{F}^\Sigma)$

$$\rightsquigarrow \mu(\mathcal{X}^\Sigma),\ \lambda(\mathcal{X}^\Sigma).$$

In our case, we have

$$\underset{\substack{\cap \\ S_2(\Gamma_0(N)) \\ \text{corresp. to } E}}{f_E^\Sigma} \equiv \mathrm{Eis}^\Sigma_{\phi,\psi} \pmod p.$$

(1) If $\phi|_{G_{\mathbb{Q}_p}} \neq \mathbb{1}, \omega$ we show $\exists$ exact seq.

$$0 \to (\mathcal{X}_\phi^\Sigma)^\wedge[p] \longrightarrow (\mathcal{X}^\Sigma)^\wedge[p] \longrightarrow (\mathcal{X}_\psi^\Sigma)^\wedge[p] \to 0$$

$\approx$ anti-cyclotomic class gps.

$$\Longrightarrow \mathfrak{X}^{\Sigma} \text{ is } \Lambda\text{-torsion with } \mu(\mathfrak{X}^{\Sigma}) = 0$$

Rubin + Hida

$$\& \quad \lambda(\mathfrak{X}^{\Sigma}) = \lambda(\mathfrak{X}_{\phi}^{\Sigma}) + \lambda(\mathfrak{X}_{\psi}^{\Sigma}).$$

(2) Kriz's congruence $\left(\mathcal{L}_{BDP}^{\Sigma}\right)^2 \equiv \mathcal{L}_{\phi}^{\Sigma} \cdot \mathcal{L}_{\psi}^{\Sigma} \pmod{p\Lambda}$.

Katz p-adic L-f'ns

$$\Longrightarrow \mathcal{L}_{BDP}^{\Sigma} \neq 0 \text{ with } \mu(\mathcal{L}_{BDP}^{\Sigma}) = 0$$

Hida's work

$$\& \quad \lambda(\mathcal{L}_{BDP}^{\Sigma}) = \lambda(\mathcal{L}_{\phi}^{\Sigma}) + \lambda(\mathcal{L}_{\psi}^{\Sigma}).$$

(3) Kolyvagin's system argument in the p-Eisenstein case:

$$\mathrm{char}_{\Lambda}(\mathfrak{X}^{\Sigma}) \supset \mathrm{char}_{\Lambda}(\mathcal{L}_{BDP}^{\Sigma}) \text{ in } \Lambda[\tfrac{1}{p}].$$

(1) + (2) + (3) + Rubin's proof of IMC for K $\Longrightarrow$ main result.