Lecture #2

Last time: For $E/\mathbb{Q}$ elliptic curve of cond $= N$,

$p \nmid 2N$ good ordinary prime,

& $K/\mathbb{Q}$ suitable imaginary quadratic field:

(1) Mazur's MC $\Longrightarrow$ p-part of BSD formula in rk 0

(2) Perrin-Riou's MC $\Longrightarrow$ p-converse to Gross-Zagier, Kolyvagin.

(3) BDP IMC $\Longrightarrow$ p-part of BSD formula in rk 1.

if p-part of BSD formula known for $E^K/\mathbb{Q}$ in rk 0.

When $G_{\mathbb{Q}} \circlearrowright E[p]$ has "big image" ($\Rightarrow$ $E[p]$ irreducible $G_{\mathbb{Q}}$-mod.)

these 3 Main Conj. are known under mild ramif. hyp. on $E[p]$ by blending:

(i) Euler/Kolyvagin systems (Kato, Howard)

(ii) Vast generalization of Ribet's method.

(Skinner-Urban, X. Wan)

$GU(2,2)$ $\quad$ $GU(3,1)$

From now on suppose $E[p]$ reducible as $G_{\mathbb{Q}}$-module:

$$E[p]^{ss} \simeq \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$$

where $\phi, \psi : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$, $\phi\psi = \omega$ – Teichmüller character.

Today's goal

Theorem A (C.–Grossi–Skinner).

Supp. $\phi|_{G_{\mathbb{Q}_p}} \neq \mathbb{1}, \omega$, where $G_{\mathbb{Q}_p} \subset G_{\mathbb{Q}}$ a decomp. gp. at p.

Let $K/\mathbb{Q}$ imag. quadratic s.t.

- Heegner hyp. holds.
- $p\mathcal{O}_K = v\bar{v}$ splits.

Then $X_v(E/K_\infty^-)$ is Λ^--torsion, with

$$\mathrm{char}_{\tilde{\Lambda}^-} X_v(E/K_\infty^-) = \left(\mathcal{L}_v^{BDP}(E/K)^2\right).$$

Hence BDP IMC holds.

The proof is in 2 steps:

1. Exploit the congruence $E[p]^{ss} \simeq \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ to show $X_v(E/K_\infty^-)$ & $\mathcal{L}_v^{BDP}(E/K)^2$ have both $\mu = 0$ & the same λ-invariant.

2. $X_v(E/K_\infty^-)$ is Λ^--torsion, with

$$\mathrm{char}_{\tilde{\Lambda}^-} X_v(E/K_\infty^-) \supseteq (\mathcal{L}_v^{BDP}(E/K)^2)$$

in $\tilde{\Lambda}^-[\frac{1}{p}]$.

§2. Anti-cyclotomic Greenberg-Vatsal method.

Let $\Sigma = \{w \mid Np\} \supset S = \{w \mid N\}$,

and consider the S-imprimitive Selmer gp.

$$\mathrm{Sel}_v^S(E/K_\infty^-) := \ker\left[H^1(K^\Sigma/K_\infty^-, E[p^\infty]) \xrightarrow{\mathrm{res}_{\bar{v}}} H^1(K_{\infty,\bar{v}}^-, E[p^\infty]) \right].$$

$$X_v^S(E/K_\infty^-) := \mathrm{Sel}_v^S(E/K_\infty^-)^\vee$$

$$\mathrm{Sel}_v^S(E[p]/K_\infty^-) := \ker\left[H^1(K^\Sigma/K_\infty^-, E[p]) \longrightarrow H^1(K_{\infty,\bar{v}}^-, E[p]) \right]$$

"residual Selmer gp."

$$X_v^S(E[p]/K_\infty^-) := \mathrm{Sel}_v^S(E[p]/K_\infty^-)^\vee.$$

<u>Basic principle</u>:

$$\mathrm{char}_{\tilde{\Lambda}^-} X_v(E/K_\infty^-) = \left(\mathcal{L}_v^{BDP}(E/K)^2\right)$$

$$\Big\Updownarrow$$

$$\mathrm{char}_{\tilde{\Lambda}^-} X_v^S(E/K_\infty^-) = \left(\mathcal{L}_v^{BDP,S}(E/K)^2\right)$$

"remove Euler factors" at $w \in S$.

<u>advantage</u>: better behaved wrt congruences mod p.

Proposition 1 Supp. $\phi|_{G_{\mathbb{Q}_p}} \neq \mathbb{1}, \omega$.

Then $X_v^S(E/K_\infty^-)$ is Λ^--torsion

with $\mu = 0$ & $\lambda = \lambda_\phi + \lambda_\psi$

introduced in the proof.

Proof. Write

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\phi"'] \arrow[rr, bend left, "\tilde{\phi}"] & \mathbb{F}_p^\times \arrow[r, hook] & \mathbb{Z}_p^\times \end{tikzcd}$$

By standard arguments (Greenberg) the Selmer gp.

$$\mathrm{Sel}_v^S(\tilde{\phi}/K_\infty^-) := \ker\left[H^1(K^\Sigma/K_\infty^-, \mathbb{Q}_p/\mathbb{Z}_p(\tilde{\phi})) \xrightarrow{\mathrm{res}_{\bar{v}}} H^1(K_{\infty,\bar{v}}^-, \mathbb{Q}_p/\mathbb{Z}_p(\tilde{\phi})) \right]$$

$$\cong \mathrm{Hom}_{\mathrm{cts}}\left(\mathrm{Gal}\left(\mathcal{M}_\infty / K_\infty \underbrace{K_\phi}_{\overline{\mathbb{Q}}^{\ker(\phi|_{G_K})}}\right), \mathbb{Q}_p/\mathbb{Z}_p\right)$$

max'l ab. pro-p unr outside v & S.

is Λ^--torsion with no proper finite index Λ^--submodules.

By Hida & Rubin, $\mathrm{Sel}_v^S(\tilde{\phi}/K_\infty^-)$ has $\mu_\phi = 0$.

$$\Rightarrow \mathrm{Sel}_v^S(\tilde{\phi}/K_\infty^-) \text{ is divisible, } \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_\phi}$$

$$\Rightarrow \lambda_\phi = \dim_{\mathbb{F}_p} \underbrace{\mathrm{Sel}_v^S(\tilde{\phi}/K_\infty^-)[p]}_{\cong}$$

$$\mathrm{Sel}_v^S(\phi/K_\infty^-) := \ker\left[H^1(K^\Sigma/K_\infty^-, \mathbb{F}_p(\phi)) \xrightarrow{\mathrm{res}_{\bar{v}}} H^1(K_{\infty,\bar{v}}^-, \mathbb{F}_p(\phi)) \right].$$

$\rightsquigarrow$ get the exact sequence

$$0 \to \mathrm{Sel}_v^S(\phi/K_\infty^-) \to \mathrm{Sel}_v^S(E[p]/K_\infty^-) \to \mathrm{Sel}_v^S(\psi/K_\infty^-) \to 0$$

$$\mathrm{Sel}_v^S(E[p]/K_\infty^-) \cong \mathrm{Sel}_v^S(E/K_\infty^-)[p]$$

finite by Hida & Rubin

$$\Rightarrow X_v^S(E/K_\infty^-) \text{ is } \Lambda^- \text{-torsion with } \mu = 0$$

$$\& \ \lambda = \lambda_\phi + \lambda_\psi \quad \boxtimes$$

On the analytic side,

$$E[p]^{ss} \simeq \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$$

$$\Rightarrow \underset{\substack{\uparrow \\ \text{newform} \\ \text{assoc. to } E}}{f} \equiv \underset{\substack{\uparrow \\ \text{wt 2 Eisenstein series}}}{E_{\phi,\psi}} \pmod p$$

$$\underset{\text{Kriz}}{\Rightarrow} \mathcal{L}_v^{BDP,S}(E/K)^2 \equiv \mathcal{L}_v^S(\phi) \cdot \mathcal{L}_v^S(\psi) \pmod{p\tilde{\Lambda}^-}$$

Katz p-adic L-f'ns

$$\Rightarrow \mu\left(\mathcal{L}_v^{BDP,S}(E/K)\right) = 0.$$

$$\& \ \lambda\left(\mathcal{L}_v^{BDP,S}(E/K)\right) = \lambda\left(\mathcal{L}_v^S(\phi)\right) + \lambda\left(\mathcal{L}_v^S(\psi)\right)$$

Rubin

But by Prop. 1, $\lambda\left(X_v^S(E/K_\infty^-)\right) = \lambda_\phi + \lambda_\psi$

$$\mu\left(X_v^S(E/K_\infty^-)\right) = 0.$$

$\therefore$ This concludes Step 1.

§3. Kolyvagin system argument "with error terms"

Prop. 2 Supp. $E(K)[p] = 0$.

Then TFAE:

(1) $X_v(E/K_\infty^-)$ is Λ^--torsion, $\mathcal{L}_v^{BDP}(E/K) \neq 0$ and

$$\mathrm{char}_{\tilde{\Lambda}^-} X_v(E/K_\infty^-) \supseteq \left(\mathcal{L}_v^{BDP}(E/K)^2 \right)$$

in $\tilde{\Lambda}^-[\frac{1}{p}]$.

(2) $X(E/K_\infty^-)$ has Λ^--rank 1, $\kappa_\infty^{Hg} \neq \Lambda^-\text{-tors}$ and

$$\mathrm{char}_{\Lambda^-}\left(X(E/K_\infty^-)_{tors} \right) \supseteq \mathrm{char}_{\Lambda^-} \left(\frac{\check{S}(E/K_\infty^-)}{(\kappa_\infty^{Hg})} \right)^2$$

in $\Lambda^-[\frac{1}{p}]$

The same holds for the divisibilities "$\subseteq$".

Proof. By the Λ^--adic BDP formula (C.–Hsieh)

$\exists$ big logarith map

$$\mathrm{Col}_v : \varprojlim_n H^1_{ord}(K^-_{n,v}, T_pE) \hookrightarrow \tilde{\Lambda}^- \quad \text{with finite coker}$$

sending $\mathrm{res}_v(\kappa_\infty^{Hg}) \longmapsto \mathcal{L}_v^{BDP}(E/K)$.

Then use Poitou–Tate duality. $\boxtimes$

Proposition 3. Supp. $E(K)[p] = 0$.

Then $X(E/K_\infty^-)$ has Λ^--rk 1, and

$$\mathrm{char}_{\Lambda^-}\left(X(E/K_\infty^-)_{tors}\right) \supseteq \mathrm{char}_{\Lambda^-}\left(\frac{\check{S}(E/K_\infty^-)}{(\kappa_\infty^{Hg})}\right)^2$$

in $\Lambda^-[\frac{1}{p}]$.

Proof. A refinement of Kolyvagin's methods.

difficulty: no "big image" hypothesis.

Standard arguments (Howard) give

$$X(E/K_\infty^-) \sim \Lambda^- \oplus M \oplus M,$$

with $M = $ f.g. Λ^--tors.

Let $\mathfrak{P} \neq p\Lambda^-$ ht 1 prime, & take $\mathfrak{P}_m \xrightarrow{m\to\infty} \mathfrak{P}$

$$\updownarrow$$

$$\alpha_m : \Gamma^- \longrightarrow R^\times$$

$\uparrow$ finite $/\mathbb{Z}_p^\times$

From a Čebotarev argument (to inductively choose a seq. of "Kolyvagin primes" of depth k, $k \gg 0$)

get
$$\mathrm{length}_{\mathfrak{P}_m}(M_{\mathfrak{P}_m}) \leq \mathrm{length}_{\mathfrak{P}_m}\left(\check{S}_{\mathfrak{P}_m} \big/ (\kappa_{\infty,\mathfrak{P}_m}^{\mathrm{Hg}}) \right)$$
$$+ E_m$$

with "error term" $E_m \left(\approx v_p(\alpha_m(\gamma) - \alpha_m^{-1}(\gamma))\right) = O(1)$ as $m \to \infty$

unless $\mathfrak{P} = (\gamma - 1)$.

$$\overset{\text{control thm.}}{\Longrightarrow} \ \text{length}_\beta(M) \leq \text{length}_\beta\left(\check{S}/(K_\infty^{H_g})\right),$$

$$\beta \neq (\gamma - 1).$$

To handle $\beta = (\gamma-1)$, take $\beta_m = (T + p^m)$

$$\beta = (\gamma - 1) \updownarrow (T)$$

$$\beta_m = (T+p^m) \updownarrow \alpha_m : \Gamma \longrightarrow \mathbb{Z}_p^\times,$$

$$\alpha_m \equiv 1 \pmod{p^m}.$$

Choose depth κ, $\kappa \gg 0$ Kolyvagin primes by working over

$$(T_pE \otimes \alpha_m)/p^m \circlearrowleft \tau$$

and do a new induction argument

$$\rightsquigarrow \text{get } \text{length}_{\mathbb{Z}_p}(M_{\beta_m}) \leq \text{length}_{\mathbb{Z}_p}\left(\check{S}_{\beta_m}/(K_\infty^{H_G}, \beta_m)\right)$$

$$+ E$$

E indep. of m.

$\boxed{}$

Prop 1–3 $\Rightarrow$ Thm. A.

joint with Grossi-Lee-Skinner

Remark Equality in $\tilde{\Lambda}^-[\frac{1}{T}]$ enough for arithmetic applications to p-conv of GZK & p-part of BSD in rk 1,

but equality in $\tilde{\Lambda}^-$ will be essential to the proof of Mazur's MC (next time)