Lecture #3

- <u>Kolyvagin's "derived" classes $c_n \in H^1(K, E[p])$</u>

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

$K = \mathbb{Q}(\sqrt{D})$ imag. quadr. field of discriminant $D \neq -3, -4$ satisfying the Heegner hypothesis.

$p > 2$ prime s.t. $\mathrm{Gal}\left(\mathbb{Q}(E[p])/\mathbb{Q}\right) \cong GL_2(\mathbb{F}_p)$.

<u>Definition</u>. A prime $\ell \nmid N \cdot D \cdot p$ is called a <u>Kolyvagin prime</u> if it satisfies:

(i) ℓ is inert in K.

(ii) $a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$,

where $a_\ell = \ell + 1 - \# \tilde{E}(\mathbb{F}_\ell)$.

<u>Note.</u> Let τ be complex conjugation, and consider the set

$$\mathcal{L}_E := \left\{ \ell \nmid N \cdot D \cdot p \;\middle|\; \left(\frac{K(E[p])/\mathbb{Q}}{\ell}\right) \sim \tau \text{ in } \mathrm{Gal}(K(E[p])/\mathbb{Q}) \right\}$$

Then:

- $\# \mathcal{L}_E = \infty$ by Čebotarev's Density Thm.
- Every $\ell \in \mathcal{L}_E$ is a Kolyvagin prime:

$$\left(\frac{K/\mathbb{Q}}{\ell}\right) \sim \left(\frac{K(E[p])/\mathbb{Q}}{\ell}\right)\Bigg|_K \sim \tau, \text{ order } 2$$

$$\Rightarrow \ell \text{ inert in } K,$$

and by the Eichler-Shimura congruence relation

$$\mathrm{charpol}\left(\left(\frac{K(E[p])/\mathbb{Q}}{\ell}\right) \curvearrowright E[p]\right) = \underset{\underset{\mathbb{F}_p[x]}{\cup}}{\overset{\cap}{x^2 - a_\ell x + \ell}}$$

while $\mathrm{charpol}(\tau \curvearrowright E[p]) = x^2 - 1$

$$\Rightarrow a_\ell \equiv 0 \equiv \ell + 1 \pmod{p}.$$

<u>Definition.</u> Let $\ell \in \mathcal{L}_E$, so we have (since ℓ inert in K)

$$G_\ell := \mathrm{Gal}(H_\ell/H_1) \cong \mathbb{Z}/(\ell+1)\mathbb{Z}$$

Writing $G_\ell = \langle \sigma_\ell \rangle$,

the <u>Kolyvagin derivative operator</u>

is the group ring element

$$D_\ell := \sum_{i=1}^{\ell} i\,\sigma_\ell^i \in \mathbb{Z}[G_\ell] \curvearrowright E(H_\ell)$$

<u>Proposition 3.</u> Let $\ell \in \mathcal{L}_E$ and $y_\ell \in E(H_\ell)$

the Heegner point of conductor ℓ.

Then

$$\underbrace{D_\ell y_\ell \bmod pE(H_\ell)}_{\substack{\| \\ [D_\ell y_\ell]}} \in \left(E(H_\ell)/pE(H_\ell) \right)^{G_\ell}$$

Proof. One immediately checks

$$(\sigma_\ell - 1) D_\ell = \ell + 1 - \mathrm{Norm}_{H_\ell/H_1} \in \mathbb{Z}[G_\ell],$$

where $\mathrm{Norm}_{H_\ell/H_1} = \sum_{\sigma \in G_\ell} \sigma = \sum_{i=1}^{\ell+1} \sigma_\ell^i$.

$$\Rightarrow (\sigma_\ell - 1) D_\ell y_\ell = (\ell+1) y_\ell - \mathrm{Norm}_{H_\ell/H_1}(y_\ell)$$

$$= (\ell+1) y_\ell - a_\ell \cdot y_1$$

norm relations

$$\in pE(H_\ell).$$ ☒.

Definition. Let

$$\mathcal{N}_E := \{ \square\text{-free products of primes } \ell \in \mathcal{L}_E \}$$

(with $1 \in \mathcal{N}_E$ by convention).

and for every $n \in \mathcal{N}_E$ set

$$G_n := \mathrm{Gal}(H_n / H_1) \cong \prod_{\ell \mid n} G_\ell$$

$$D_n := \prod_{\ell \mid n} D_\ell \in \mathbb{Z}[G_n] \quad \text{Kolyvagin's derivative operator.}$$

$$\left(\text{with } G_1 := \mathbb{Z} \ \& \ D_1 = 1 \text{ by convention} \right).$$

The same proof as Proposition 3 shows that

$$[D_n y_n] \in \left(E(H_n) / pE(H_n) \right)^{G_n},$$

where $y_n \in E(H_n)$ is the Heegner point of conductor n.

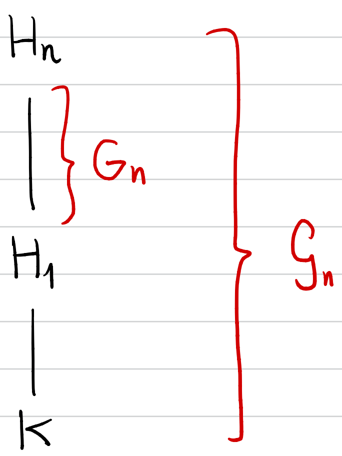
$\Rightarrow$ if $\mathfrak{S}$ = system of representatives for $\mathcal{G}_n / G_n$, $\quad \mathcal{G}_n = \mathrm{Gal}(H_n/K)$

then

$$P_n := \sum_{s \in \mathfrak{S}} s D_n y_n \in E(H_n)$$

satisfies $\quad [P_n] \in \left(E(H_n) / pE(H_n) \right)^{\mathcal{G}_n}$

Picture:



Thus we have

$$\begin{tikzcd}
E(H_n)/pE(H_n) \arrow[r, hook, "\delta"] & H^1(H_n, E[p]) \\
\left(E(H_n)/pE(H_n)\right)^{\mathcal{G}_n} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, hook, "\delta"] \arrow[d, phantom, sloped, "\ni"] & H^1(H_n, E[p])^{\mathcal{G}_n} \arrow[u, phantom, sloped, "\subseteq"] \\
{[P_n]} & H^1(K, E[p]) \arrow[u, "\mathrm{Res}_{H_n}", "\cong"']
\end{tikzcd}$$

follows from the fact that $E(H_n)[p] = \{0\}$ by our hyp. on p.

<u>Definition</u>. (Kolyvagin's derivative classes)

For every $n \in \mathcal{N}_E$ define
$$c_n \in H^1(K, E[p])$$
to be the unique class s.t.
$$\boxed{\mathrm{Res}_{H_n}(c_n) = \delta([P_n])}.$$

<u>Note</u>. For $n=1$,

$$P_1 = \sum_{s \in G} s y_1 = \sum_{\sigma \in Gal(H_1/K)} \sigma y_1$$

$$= Norm_{H_1/K}(y_1) =: y_K$$

$\uparrow$ as in theorem of Th. A'.

so

$$y_K \notin pE(K) \iff c_1 \neq 0.$$

- <u>Properties of the system $\{c_n\}$</u>$_{n \in \mathcal{N}_E}$.

Since $p>2$, the action of $\tau \in Gal(K/\mathbb{Q})$ decomposes

$$H^1(K, E[p]) = H^1(K, E[p])^+ \oplus H^1(K, E[p])^-$$

into $\pm$-eigenspaces.

<u>Proposition 4.</u> Let $n \in \mathcal{N}_E$ and $\varepsilon \in \{\pm 1\}$

s.t. $L(E,s) = -\varepsilon L(E, 2-s)$.

Then

$$c_n \in H^1(K, E[p])^{\varepsilon_n},$$

where $\varepsilon_n = \varepsilon \cdot (-1)^{\#\{\ell | n\}}$.

(Thus if $\ell_1, \ell_2, \ldots \in \mathcal{L}_E$ are different Kolyvagin primes,

we have $c_1 \in H^1(K, E[p])^{\varepsilon}$, $c_{\ell_1} \in H^1(K, E[p])^{-\varepsilon}$

$c_{\ell_1 \ell_2} \in H^1(K, E[p])^{\varepsilon}$, etc.)

<u>Proof.</u> A direct computation using that

$$\tau y_n = \varepsilon \cdot \sigma y_n + \text{torsion} \qquad \text{for some } \sigma \in \mathcal{G}_n.$$

and the relation

$$\tau \sigma = \sigma^{-1} \tau \quad \forall \sigma \in \mathcal{G}_n. \qquad \boxtimes.$$

Proposition 5. Let $\overset{\overset{1}{\#}}{n} \in \mathcal{N}_E$.

Then

$$c_n \in H^1_{\mathcal{F}^S}(K, E[p]),$$

where $S = \{v \mid n\}$.

Moreover, writing $n = \ell \cdot m$ with $\ell \in \mathcal{L}_E$,
$(\text{so } \ell \nmid m)$ $\qquad \ell \mathcal{O}_K = \lambda$

we have

$$\underset{H^1_{sing}(K_\lambda, E[p])}{\underset{\cap}{\partial_\lambda(c_n)}} \neq 0 \iff \underset{\operatorname{im}\delta_\lambda}{\underset{\cap}{(c_m)_\lambda}} \neq 0.$$

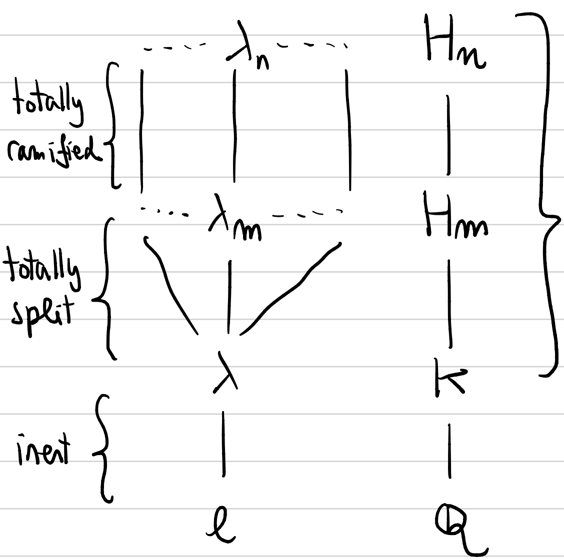
Proof. That $(c_n)_\lambda \in \operatorname{im}\delta_\lambda \ \forall \lambda \in S$ follows easily from the definitions, so we just prove the second claim.

By the explicit description of the Kummer map δ_λ,

$$\partial_\lambda(c_n) \neq 0 \iff \left[\sigma \mapsto \frac{(\sigma-1)P_n}{p}\right] \neq 0$$

$$\in H^1\big((\mathcal{G}_n)_\lambda, E((H_n)_{\lambda_n})\big)[p].$$

Recall the picture



$$\mathcal{G}_n \supset (\mathcal{G}_n)_\lambda = \mathrm{Gal}(H_n/H_m)$$
$$\cong \mathrm{Gal}(H_\ell/H_1)$$
$$= G_\ell$$
$$= \langle \sigma_\ell \rangle$$

$$\therefore\ \partial_\lambda(c_n) \neq 0 \iff Q_n := \frac{(\sigma_\ell - 1)P_n}{p}$$

$$\notin \ker\left(\mathrm{red}_{\lambda_n} : E((H_n)_{\lambda_n}) \to \tilde{E}(\mathbb{F}_{\ell^2})\right).$$

Now we compute:

$$P_n = \sum_{s \in G} s \underbrace{D_n}_{= D_\ell \cdot D_m} y_n$$

$$\Rightarrow Q_n \underset{(\sigma_\ell - 1)D_\ell = \ell+1-\mathrm{Norm}}{=} \sum_{s \in G} s D_m \left(\frac{\ell+1}{p} y_n - \frac{a_\ell}{p} y_m \right)$$

by Norm relations

$$\equiv \frac{(\ell+1)\left(\frac{H_m/\mathbb{Q}}{\lambda_m}\right) - a_\ell}{p} \underbrace{\sum_{s \in G} s D_m y_m}_{= P_m} \pmod{\lambda_n}$$

by the congruence relation.

$$\therefore \ \mathrm{red}_{\lambda_n}(Q_n) = \mathrm{red}_{\lambda_m}\left(\frac{(\ell+1)\left(\frac{H_m/\mathbb{Q}}{\lambda_m}\right) - a_\ell}{p} \cdot P_m \right)$$

$$\overset{\left(\frac{H_m/\mathbb{Q}}{\lambda_m}\right) = \tau \ + \text{Prop. 4.}}{=} \frac{(\ell+1)\varepsilon_m - a_\ell}{p} \cdot \underbrace{\mathrm{red}_{\lambda_m}(P_m)}_{\in\, \tilde{E}(\mathbb{F}_{\ell^2})^{\varepsilon_m}}$$

$$\overset{(\ell+1)\varepsilon_m - a_\ell \text{ annihilates } E(\mathbb{F}_{\ell^2})^{\varepsilon_m}}{\Longrightarrow} \quad \mathrm{red}_{\lambda_n}(Q_n) \neq 0$$

$$\Updownarrow$$

$$\mathrm{red}_{\lambda_m}(P_m) \notin p\tilde{E}(\mathbb{F}_{\ell^2})$$

$$\Updownarrow$$

$$P_m \notin p\, E((H_m)_{\lambda_m})$$

$$\Updownarrow$$

$$(c_m)_\lambda \neq 0. \qquad \blacksquare$$

Remarks. (1) Proposition 5 shows that

$$\mathcal{C}_\infty := \{ c_n \in H^1(K, E[p]) \}_{n \in \mathcal{N}_E}$$

forms a "mod p" Kolyvagin system for T_pE.

(2) In particular, taking $m=1$ in Prop. 5 we get:

For any $\ell \in \mathcal{L}_E$, writing $\ell\mathcal{O}_K = \lambda$ we have

$$\partial_\lambda(c_\ell) \neq 0 \iff (c_1)_\lambda \neq 0$$

$$\iff \underset{\substack{\| \\ y_K}}{P_1} \notin pE(K_\lambda).$$

including classes mod p^N, $N \geq 1$

(an enlargement of)

(3) [Aside].

Kolyvagin (1991) conjectured that $\mathcal{C}_\infty$ is always $\neq \{0\}$.

This was proved by W. Zhang (2014) et al. under mild hypotheses on $E[p]$ (& $p \geq 5$ good ordinary).