Lecture # 4

Lemma 1. Let $\ell \in \mathcal{L}_E$ and write $\ell \mathcal{O}_K = \lambda$.

Then

$$H^1_{sing}(K_\lambda, E[p])^{\pm} \cong \mathbb{F}_p.$$

Proof. $\ell \in \mathcal{L}_E \Rightarrow \left(\frac{K(E[p])/\mathbb{Q}}{\ell} \right) \sim \underset{\substack{\uparrow \\ \text{complex conj.}}}{\tau}$ & ℓ is inert in K

$$\Rightarrow \left(\frac{K(E[p])/K}{\lambda} \right) \sim \tau^2 = id$$

$\Rightarrow \lambda$ splits completely in $K(E[p])/K$,

so $E[p] \subset E(K_\lambda)$ & $G_{K_\lambda} \circlearrowright E[p]$ trivially

By inflation-restriction

$$H^1_{sing}(K_\lambda, E[p]) \cong H^1(I_\lambda, E[p])^{G_{K_\lambda}/I_\lambda},$$

$I_\lambda \subset G_{K_\lambda}$ inertia

$$\cong \mathrm{Hom}(I_\lambda, E[p])$$

$$\cong \mathrm{Hom}(\mu_p, E[p])$$

$$\Rightarrow H^1_{sing}(K_\lambda, E[p])^{\pm} \cong \mathrm{Hom}(\mu_p, E[p])^{\pm}$$

$$\cong E[p]^{\mp}$$

$$\cong \mathbb{F}_p \quad \boxtimes.$$

Now we're ready to prove:

<u>Theorem</u> A' (Kolyvagin).

Suppose $y_K \notin E(K)_{tors}$, and let p be a prime s.t.

(a) $p > 2$

(b) $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$

(c) $y_K \notin pE(K)$.

Then

$$\mathrm{Sel}_p(E/K) = \mathbb{F}_p \, \delta(y_K),$$

where $\delta : E(K)/pE(K) \hookrightarrow \mathrm{Sel}_p(E/K)$ Kummer map.

Proof. Suppose we can find $n = \ell_1 \cdots \ell_t \in \mathcal{N}_E$ s.t.

(A) $H^1_{\mathcal{F}_S}(K, E[p]) = \{0\}$,

where $S = \{\lambda_1, \dots, \lambda_t\}$
$(\ell_i \mathcal{O}_K = \lambda_i)$

(B) $y_K \notin pE(K_{\lambda_i}) \quad \forall\, i = 1, \dots, t.$

(C) $(c_{\ell_1})_{\lambda_i} \neq 0 \in H^1(K_{\lambda_i}, E[p])$
$\forall\, i = 2, \dots, t.$

Kolyvagin's derived class

Then

(A) $\Longrightarrow$ $\# \mathrm{Sel}_p(E/K)$

Lecture 2

$$\# \mathrm{Sel}_p(E/K) = \# \mathrm{coker}\left(H^1_{\mathcal{F}^S}(K, E[p]) \xrightarrow[\oplus_i \partial_{\lambda_i}]{\partial_S} \bigoplus_{i=1}^t H^1_{\mathrm{sing}}(K_{\lambda_i}, E[p]) \right)$$

so taking τ-eigenspaces:

$$\# \mathrm{Sel}_p(E/K)^{\pm} = \# \operatorname{coker}(\partial_S^{\pm}). \qquad (\star)$$

• $(-\varepsilon)$-eigenspace: $(\varepsilon = \pm 1 \text{ s.t. } L(E,s) = -\varepsilon L(E,2-s))$

$$(B) \underset{\substack{\text{Prop. 5} \\ \text{in Lecture 3}}}{\Longrightarrow} \underbrace{\partial_{\lambda_i}(c_{\ell_j})}_{= \partial_{\lambda_i}^{-\varepsilon}(c_{\ell_j})} \doteq \delta_{ij} \in H^1_{\mathrm{sing}}(K_{\lambda_i}, E[p])^{-\varepsilon} \cong \mathbb{F}_p.$$

$$\Rightarrow \dim_{\mathbb{F}_p} \operatorname{im}(\partial_S^{-\varepsilon}) \geq t$$

$\Rightarrow$ $\partial_S^{-\varepsilon}$ is surjective,

so $\mathrm{Sel}_p(E/K)^{-\varepsilon} = \{0\}$.

- $\underline{\varepsilon\text{-eigenspace}}$:

$$(c) \Rightarrow \partial_{\lambda_i}(c_{\ell_1 \ell_j}) \doteq \delta_{ij} \in H^1_{sing}(K_{\lambda_i}, E[p])^{\varepsilon}$$

$$\begin{array}{ccc} \partial_{\lambda_i}(c_{\ell_1 \ell_j}) & & H^1_{sing}(K_{\lambda_i}, E[p])^{\varepsilon} \\ \| & & \cong \\ \partial^{\varepsilon}_{\lambda_i}(c_{\ell_1 \ell_j}) & & \mathbb{F}_p \end{array}$$

$$\forall\ 2 \leq i,j \leq t$$

$$\Rightarrow \dim_{\mathbb{F}_p} \operatorname{im}(\partial_S^{\varepsilon}) \geq t-1$$

so $\dim_{\mathbb{F}_p} Sel_p(E/K)^{\varepsilon} \leq 1$ by ✪

But $y_K \notin pE(K) \Rightarrow \delta(y_K) \neq 0 \in Sel_p(E/K)^{\varepsilon}$,

so $Sel_p(E/K) = \mathbb{F}_p\, \delta(y_K)$.

$\therefore$ To conclude, it remains to find $n \in \mathcal{N}_E$ for which (A), (B) & (C) hold.

Lemma 2. Let

$$\begin{array}{c} L := K(E[p]) \\ \Big| \quad \mathcal{G} := \mathrm{Gal}(L/K) \cong GL_2(\mathbb{F}_p). \\ K \end{array}$$

and $C \subset H^1(K, E[p])$ a finite τ-stable subgroup.

Then $\exists\ L_C/L$ finite Galois extension s.t.

$$\boxed{C \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_C/L), E[p])}$$

as $\mathrm{Gal}(K/\mathbb{Q})$-modules.

Proof. The restriction map

$$\mathrm{Res}_L : H^1(K, E[p]) \longrightarrow H^1(L, E[p])^{\mathcal{G}}$$
$$\qquad\qquad\qquad\qquad\qquad\qquad \shortparallel$$
$$\qquad\qquad\qquad\qquad\qquad\qquad \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(\overline{\mathbb{Q}}/L), E[p])$$

is an isomorphism,

since $\operatorname{Ker}(\mathrm{Res}_L) = H^1(\mathcal{G}, E[p])$

$$\cong H^1(GL_2(\mathbb{F}_p), \mathbb{F}_p^2) \underset{p>2}{=} \{0\}$$

& $\operatorname{coker}(\mathrm{Res}_L) \subset H^2(\mathcal{G}, E[p])$

$$\cong H^2(GL_2(\mathbb{F}_p), \mathbb{F}_p^2) = \{0\}$$

The result follows. $\boxtimes$.

Now we take $C = \mathrm{Sel}_p(E/K)$:

$$\begin{tikzcd}
& M := L_C \arrow[dl, dash, "I"'] \arrow[dd, dash, "H := \mathrm{Gal}(M/L)"] \\
L(\tfrac{1}{p} y_K) \arrow[dr, dash, "\cong E[p]"'] & \\
& L = K(E[p]) \arrow[d, dash, "\mathcal{G}"] \\
& K
\end{tikzcd}$$

By Lemma 2,

$$\boxed{\mathrm{Sel}_p(E/K) \cong \mathrm{Hom}_{\mathcal{G}}(H, E[p])}$$

as $\mathrm{Gal}(K/\mathbb{Q})$-modules.

$\Rightarrow$ have a non-degerate pairing

$$[\ ,\ ] : \mathrm{Sel}_p(E/K) \times H \longrightarrow E[p]$$
$$(s\ ,\ g) \longmapsto \mathrm{Res}_L(s)(g)$$

and for any $s \in \mathrm{Sel}_p(E/K)$

& $\lambda \nmid Np$ prime of K that splits completely in L

we have

$$\underset{\substack{\cap \\ H^1(K_\lambda, E[p])}}{s_\lambda} = 0 \iff \left[s, \left(\frac{M/L}{\lambda''}\right)\right] = 0$$

for some (equiv., any) $\lambda'' | \lambda$ in M.

Lemma 3. Let $s \in \mathrm{Sel}_p(E/K)^{\pm}$,

and suppose $[s, h] = 0 \;\; \forall h \in H^{+} \setminus I^{+}$

$(\Leftrightarrow [s, h] = 0 \;\; \forall h \in H^{+})$

since $I^{+} \neq H^{+}$ & $\mathrm{Res}_L(s)$ is gp. hom.

Then $s = 0$.

Proof. Enough to show $s(H) = 0$.

Since $\mathrm{Res}_L(s) \in \mathrm{Hom}_{\mathcal{G}}(H, E[p])^{\pm}$,

it maps
$$H^{+} \longrightarrow E[p]^{\pm}$$
$$H^{-} \longrightarrow E[p]^{\mp}$$
$\mathcal{G}$-equivariantly.

Thus
$$s(H^{+}) = 0 \Rightarrow s(H) \subset E[p]^{\mp}$$
proper G-inv. subspace of $E[p]$.

$$\Rightarrow s(H) = 0 \quad \blacksquare.$$

$\boxed{\text{Proof of (A)}}$: $\exists\ n = \ell_1 \cdots \ell_t \in \mathcal{N}_E$

s.t. $H^1_{\mathcal{F}_S}(K, E[p]) = \{0\}$.

Let $H^+ \setminus I^+ = \{\gamma_1, \dots, \gamma_t\}$.

write $\gamma_i = (\tau h_i)^2$ with $h_i \in H$ (use $p > 2$)

& pick $\ell_i \nmid N \cdot D \cdot p$ s.t.

possible by Čebotarev's Density Thm.

$$\left(\frac{M/\mathbb{Q}}{\ell_i}\right) \sim \tau h_i \quad (i = 1, \dots, t).$$

Then $$\left(\frac{L/\mathbb{Q}}{\ell_i}\right) \sim \left(\frac{M/\mathbb{Q}}{\ell_i}\right)\Big|_L \sim \tau h_i\Big|_L = \tau$$

$$\Longrightarrow \ell_i \in \mathcal{L}_E.$$

seen in Lecture 3.

Write $l_i \mathcal{O}_K = \lambda_i$ and put $S = \{\lambda_1, \dots, \lambda_t\}$.

Let $s \in H^1_{\mathcal{F}_S}(K, E[p])$.

WTS $s = 0$.

image in $H^1_{\mathcal{F}_S}(K, E[p])^{\pm}$

By Lemma 3, enough to show $[s^{\pm}, h] = 0 \quad \forall h \in H^+ \setminus I^+$.

$$\Leftrightarrow [s^{\pm}, \gamma_i] = 0 \quad \forall i = 1, \dots, t$$

use choice of l_i

$$\Leftrightarrow \left[s^{\pm}, \left(\frac{M/L}{\lambda_i''}\right)\right] = 0 \quad \forall i,$$

where $\lambda_i'' \mid \lambda_i$ in M.

$$\Leftrightarrow (s^{\pm})_{\lambda_i} = 0 \quad \forall i$$

$\checkmark$, since $s \in H^1_{\mathcal{F}_S}(K, E[p])$.

$\therefore$ (A) holds.

$\boxed{\text{Proof of (B)}}$: $y_K \notin pE(K_{\lambda_i}) \quad \forall i = 1, \dots, t.$

For any i, if $\lambda_i' \mid \lambda_i$ in L:

$$\left(\frac{L(\frac{1}{p}y_K)/L}{\lambda_i'}\right) \sim \left(\frac{M/L}{\lambda_i'}\right)\Big|_{L(\frac{1}{p}y_K)}$$

$$\sim \left(\frac{M/K}{\lambda_i}\right)\Big|_{L(\frac{1}{p}y_K)}$$

λ_i splits completely in L/K

$$\sim \left(\frac{M/\mathbb{Q}}{\ell_i}\right)^2\Big|_{L(\frac{1}{p}y_K)}$$

ℓ_i inert in $K/\mathbb{Q}$

$$\overset{\text{def}}{\sim} (\tau h_i)^2\Big|_{L(\frac{1}{p}y_K)}$$

$$= \gamma_i\Big|_{L(\frac{1}{p}y_K)} \neq id,$$

since $\gamma_i \notin I$

$\Rightarrow$ λ_i' doesn't split completely in $L(\frac{1}{p}y_K)/L$

$\Rightarrow$ λ_i doesn't split completely in $L(\frac{1}{p}y_K)/K$

$\Rightarrow$ $y_K \notin pE(K_{\lambda_i})$ $\quad \forall\, i = 1, \dots, t.$

$\boxed{\text{Proof of (c)}}$: $(c_{\ell_1})_{\lambda_i} \neq 0 \in H^1(K_{\lambda_i}, E[p])$
$\forall\, i = 2, \dots, t.$

Let L'/L = smallest Galois extension s.t.

$$\begin{tikzcd}
\mathrm{Res}_L(c_{\ell_1}) : \mathrm{Gal}(\overline{\mathbb{Q}}/L) \arrow[rr] \arrow[dr, two heads] & & E[p] \\
& \mathrm{Gal}(L'/L) \arrow[ur, hook, dashed] &
\end{tikzcd}$$

Lemma 4. $\mathrm{Gal}(L'/L) \cong E[p]$ and $\mathrm{Gal}(L'/L)^{\pm} \cong \mathbb{F}_p$.

Proof. $\mathrm{Res}_L(c_{\ell_1}) : \mathrm{Gal}(L'/L) \hookrightarrow E[p]$

is $\neq 0$ and $\mathcal{G}$-equivariant,

hence surjective. (since $\mathcal{G} \curvearrowright E[p]$ transitively)

The second claim follows from

$c_{\ell_1} = \tau$-eigenvector. $\boxtimes$.

Finally,

$$y_K \notin pE(K_{\lambda_1}) \Rightarrow \partial_{\lambda_1}(c_{\ell_1}) \neq 0$$

(by (B))

$$\Rightarrow c_{\ell_1} \notin \mathrm{Sel}_p(E/K)$$

$$\Rightarrow L' \cap M = L.$$

$\therefore$ WLOG, may assume the above $\lambda_2, \dots, \lambda_t$ are s.t.

$$\left(\frac{M/\mathbb{Q}}{\ell_i}\right) \sim \tau h_i \in \mathrm{Gal}(M/\mathbb{Q})$$

with $(\tau h_i)^2 \in H^+ \setminus I^+$

as before

and

$$\left(\frac{L'/\mathbb{Q}}{\ell_i}\right) \sim \tau h_i' \in \mathrm{Gal}(L'/\mathbb{Q})$$

with $\underset{\mathrm{id}}{(\tau h_i')^2} \in \underset{(\cong \mathbb{F}_p)}{\mathrm{Gal}(L'/L)^+}$

$\Rightarrow$ λ_i doesn't split completely in L'/K

$\forall i = 2, \dots, t$

(indeed, $\left(\frac{L'/K}{\lambda_i}\right) \sim \left(\frac{L'/\mathbb{Q}}{\ell_i}\right)^2 \sim (\tau h_i')^2 \neq \mathrm{id}$.)

$\Rightarrow$ $(c_{\ell_1})_{\lambda_i} \neq 0 \quad \forall i = 2, \dots, t.$

$\therefore$ Kolyvagin's Thm. A' $\square$.