Euler Systems

1 Heegner points (and BSD)

1.1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$, $[F:\mathbb{Q}] < \infty \Rightarrow E(F) \cong E(F)_{\text{tor}} \otimes \mathbb{Z}^{r(E,F)}$.

Given E, we have an L-function, $L(E,s) = \prod_{p|N}(1-a_p p^{-s})^{-1} \prod_{p\nmid N}(1-a_p p^{-s}+p^{1-2s})^{-1}$ with $\mathrm{Re}(s) > 3/2$ and $a_p = \begin{cases} p+1-\#E(\mathbb{F}_p) & p \nmid N \\ 0 & E\,\text{additive at}\,p \\ 1 & \text{split multi at}\,p \\ -1 & \text{non split multi at}\,p \end{cases}$, $N = \mathrm{cond}(E)$.

Note. $L(E,1)$ " = " $\prod_{p|N}(\,)\cdot\prod_{p\nmid N}\frac{p}{p-a_p+1} = \prod_p \frac{p}{N_p}$ where $N_p = \#E(\mathbb{F}_p)_{\text{ns}}$.

Conjecture (Birch-Swinnerton-Dyer). *Let $E/\mathbb{Q}$ be an elliptic curve*

1. $\mathrm{ord}_{s=1}L(E,s) = \mathrm{rk}_{\mathbb{Z}}E(\mathbb{Q}) = r$
2. $\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r} = \#Ш(E,\mathbb{Q})\frac{\det(\langle P_i,P_j\rangle)}{\#E(\mathbb{Q})^2_{\text{tor}}}\prod_{v|N}c_v$, *where $\{P_i\}$ are generators of $E(\mathbb{Q})$.*

Suppose that E is modular (now we know this is always true): there exists $f \in S_2(\Gamma_0(N))$ a newform $f(q) = \sum_{n=1}^{\infty} a_n q^n$ such that $L(E,s) = L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Or equivalently $a_p(E) = a_p(f)$. This implies that $L(E,s)$ has analytic continuation to $\mathbb{C}$. It has a functorial equation $\wedge(E,s) = (2\pi)^{-s}\Gamma(s)N^{s/2}L(E,s)$. We have $\wedge(E,s) = -\epsilon\wedge(E,2-s)$ where $\epsilon \in \{\pm 1\}$ and is determined by $w_N(f) = \epsilon\cdot f$ where w is the Atkin-Lehner function. We shall call $-\epsilon$ the $\mathrm{sign}(E,\mathbb{Q})$.

$f \rightsquigarrow$modular representation. $\phi : X_0(N)_{/\mathbb{Q}} \longrightarrow E_{/\mathbb{Q}}$ non-constant morphism defined over $\mathbb{Q}$.

$$\begin{tikzcd} X_0(N)_{/\mathbb{Q}} \arrow[rr, "\phi"] \arrow[dr, "AJ"'] & & E_{/\mathbb{Q}} \\ & J_0(N) = \mathrm{Jac}X_0(N) \arrow[ur, "\text{Hecke}-\text{op}"'] & \end{tikzcd}$$

1.2 Class field theory

Let $K \subseteq \mathbb{C}$ be an imaginary quadratic field. Let $O_n \subseteq K$ be an order, $O_n = \mathbb{Z} + n\mathcal{O}_K$, $n \geq 1$ an integer.

By class field theory: There is a map rec : $\mathrm{Pic}(O_n) \cong \mathrm{Gal}(K_n/K)$ where K_n/K is an abelian extension unramified away from n. Recall that $\mathrm{Pic}(O_n) = I(n)/P(n)$ where $I(n) = \{$fractional ideals coprime to $n\}$, $P(n) = \langle(\alpha) : \alpha \in \mathcal{O}_K, \alpha \equiv a \mod n\mathcal{O}_K, a \in \mathbb{Z}\rangle$. The map is defined by $[\mathfrak{p}] \mapsto \mathrm{Frob}_{\mathfrak{p}}^{-1}$

Lemma. *Let $G_n = \mathrm{Gal}(K_n/K_1)$. Then $G_n \cong \mathrm{Pic}(O_n)/\mathrm{Pic}(\mathcal{O}_K) \cong (\mathcal{O}_K/n\mathcal{O}_K)^*/(\mathbb{Z}/n\mathbb{Z})^*$. In particular, if ℓ is an odd prime unramified in K, then G_ℓ is cyclic and* $[K_\ell : K_1] = \begin{cases} \ell+1 & \ell\,\text{inert in}\,K \\ \ell-1 & \ell\,\text{split in}\,K \end{cases}$

If n is square free then $G_n \cong \prod_{\ell|n} G_\ell$.

1.3 Complex Multiplication

$X_0(N)$ classifies (up to isomorphism) cyclic N-isogonies, $A \to A'$ where $\ker(A \to A')$ is cyclic of order N. Let $K/\mathbb{Q}$ imaginary field satisfying *Heegner Hypothesis:* $\ell | N \Rightarrow \ell$ splits in K. Can pick an ideal $\mathcal{N} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ (cyclic). Consider $O_n = \mathbb{Z} + n\mathcal{O}_K$, $\chi_n = [\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1}] \in X_0(N)(\mathbb{C})$ where $\mathcal{N}_n = \mathcal{N} \cap O_n$ ($\Rightarrow O_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$) .

Theorem (Main Theorem of Complex Multiplication). *Let* $\sigma \in \mathrm{Aut}(\mathbb{C}/K) \rightsquigarrow \sigma|_{K_n} \in \mathrm{Gal}(K_n/K) \cong \mathrm{Pic}(O_n)$ *so* $\sigma|_{K_n} \rightsquigarrow [\mathfrak{a}_\sigma]$.

$$\chi_n^\sigma = \left[\mathbb{C}/\mathfrak{a}_\sigma^{-1} \to \mathbb{C}/\mathcal{N}_n^{-1}\mathfrak{a}_\sigma^{-1}\right]$$

Remark. Suppose $\sigma|_{K_n} = 1$. Then $\chi_n^\sigma = \chi_n$. Hence $\chi_n \in X_0(N)(K_n)$.

Hecke action (On $\chi_0(N)$): For each $\ell \nmid N$, T_ℓ is a correspondence on $X_0(N) \rightsquigarrow T_\ell : (\mathrm{Div}X_0(N))(F) \to \mathrm{Div}X_0(N)(F)$ defined by $[\phi : A \mapsto A'] \mapsto \sum_{C \subset A[\ell], \text{cyclic subgp of order } \ell} [A/C \to A'/\phi(C)]$.

Also have the Trace map: $\mathrm{Tr}_\ell : \mathrm{Div}X_0(N)(K_{n\ell}) \to \mathrm{Div}X_0(N)(K_n)$.

Proposition. *Consider* $\{\chi_n\}_n$, $(n, ND) = 1$ *where* $D = \mathrm{disc}(K)$. *Let* $\ell \nmid ND$*, then*

1. *As elements in* $\mathrm{Div}X_0(N)(K_n)$, $\mathrm{Tr}_\ell(\chi_{n\ell}) = \begin{cases} T_\ell \chi_n & \text{if } \ell \nmid n \text{ is inert in } K \\ (T_\ell - \mathrm{Frob}_\lambda - \mathrm{Frob}_\lambda^{-1})\chi_n & \text{if } \ell = \lambda\bar{\lambda} \nmid n \text{ split in } K \\ T_\ell \chi_n - \chi_{n/\ell} & \ell | n \end{cases}$
2. *If* $\ell \nmid N$ *is inert in* K, $\lambda = \ell\mathcal{O}_K$, λ_n *is a prime in* K_n *above* λ. *Then* $\mathrm{red}_{\lambda_{n\ell}}(\chi_{n\ell}) = \mathrm{red}_{\lambda_n}(\chi_n^{\mathrm{Frob}\lambda_n}) \in X_0(N)(\mathbb{F}_{\lambda_n})$.

1.4 Heegner points on E

Let $\phi : X_0(N) \to E$. $y_n := \phi(\chi_n)$ is the Heegner point of conductor n (in $E(K_n)$).

$y_K = \mathrm{Tr}_{K_1/K}(y_1)$ (in $E(K)$) is "the basis Heegner point"

Proposition. $\ell \nmid ND$:

$$\mathrm{Tr}_\ell(y_{n\ell}) = \begin{cases} a_\ell y_n & \text{if } \ell \text{ is inert in } K, \ell \nmid n \\ (a_\ell - \mathrm{Frob}_\lambda - \mathrm{Frob}_\lambda^{-1})y_n & \mathrm{red}_{\lambda_n \ell}(y_{n\ell}) = \mathrm{red}_{\lambda n}(y_n^{\mathrm{Frob}\lambda_n}) \\ a_\ell y_n - y_{n/\ell} & E(\mathbb{F}_{\lambda_n}) \end{cases}$$

Proposition. *If* τ *is a complex conjugation, then there exists* $\sigma \in \mathrm{Gal}(K_n/K)$ *such that* $y_n^\tau = \epsilon y_n^\sigma$ *on* $E(K)/E(K)_{\mathrm{tors}}$.

2 Local Cohomology

2.1 Introduction to cohomology

Let G be a group and M a G-module. Both G and M have topology.

1-cocycles: Are $\{f : G \to M | f \text{ continuous and } \forall g, h \in G, f(gh) = f(g) + gf(h)\}$

1-coboundary: Are $\{f : G \to M | f \text{ continuous and } f(g) = g \cdot m - m \text{ for some } m \in M\}$

Definition 2.1. $H^1(G, M)$ ={1-cocylce}/{1-coboundary}, $H^0(G, M) = M^G$

Consider the short exact sequence of G-modules, $0 \to M' \to M \to M'' \to 0$ and $M'' \to M$ is a continuous section of sets. Then we get a long exact sequence

$$0 \to M'^G \to M^G \to M''^G \to H^1(G, M') \to H^1(G, M) \to H^1(G, M'') \to H^2 \ldots$$

We have some useful maps between cohomology groups:

- Let $H \leq G$, we get a map $\mathrm{Res} : H^1(G, M) \to H^1(H, M)$.
- Let $H \lhd G$ be a normal closed subgroup of G, then we have $\inf : H^1(G/H, M^H) \to H^1(G, M)$

We have the following relationship between inf and Res called the Hochschild-Serre spectral sequence

$$0 \to H^1(G/H, M^H) \stackrel{\inf}{\to} H^1(G, M) \stackrel{\mathrm{Res}}{\to} H^1(H, M)^{G/H} \to H^2(G/H, M^H) \to \dots$$

2.2 Galois Cohomology

Fox prime ℓ,p and $|K : \mathbb{Q}_\ell| < \infty$ and let K^{un} be the maximal unramified extension of K and let $I_K = \mathrm{Gal}(\overline{K}/K^{\mathrm{un}})$ be the *Inertia* group

Denote by $G_K = \mathrm{Gal}(\overline{K}/K)$ and $G_K^{\mathrm{un}} = \mathrm{Gal}(K^{\mathrm{un}}/K) \cong G_K/I_K$ $(\cong \widehat{\mathbb{Z}})$

Let T be a finite dimensional $\mathbb{F}_p$-vector space with discrete G_K action. We say that T is unramified if I_K acts trivially on T.

There is a perfect pairing of $\mathbb{F}_p$-vector spaces $H^1(G_K, T) \otimes_{\mathbb{F}_p} H^1(G_K, T^*) \to \mathbb{F}_p$ where $T^* = \mathrm{Hom}(T, M_{p^\infty})$.

Fact. *If $\ell \neq p$ and T is unramified then $H^1(G_K^{\mathrm{un}}, T)$ and $H^1(G_K^{\mathrm{un}}, T^*)$ are exact orthogonal complements with respect to $\langle \, , \rangle$.*

Definition 2.2. A *local Selmer structure* F for T is a choice of $\mathbb{F}_p$-subspace of $H^1(G_K, T)$ denoted $H^1_{f,F}(G_K, T)$. We call the quotient $H^1_{S,F}(G_K, T) := H^1(G_K, T)/H^1_{f,F}(G_K, T)$ the singular quotient.

$$0 \to H^1_{f,F}(G_K, T) \to H^1(G_K, T) \to H^1_{S,F}(G_K, T) \to 0 \; (\dagger)$$

We say F is an unramified structure if $H^1_{f,F}(G_K, T) = H^1(G_K^{\mathrm{un}}, T^{I_K})$ (via inf). In this case $(\dagger)$ identifies with inf-res. Using the Tate pairing we define the Dual Selmer structure F^* on T^* to be the exact orthogonal complement of $H^1_{f,F}(G_K, T)$.

In particular $H^1_{S,F}(G_K, T) \otimes_{\mathbb{F}_p} H_{f,F^*}(G_K, T^*) \to \mathbb{F}_p$ we get an induced perfect pairing.

2.3 Local cohomology for elliptic curves

Let E be an elliptic curve over K. We let $T = E[p] = E(\overline{K})[P]$. We have the Weil pairing $E[P] \otimes \mathbb{F}_p E[P] \to \mu_p$ $(\Rightarrow E[P]^* \cong E[P])$. We have a short exact sequence of G_K-module

$$0 \to E[P] \to E(\overline{K}) \stackrel{p}{\to} E(\overline{K}) \to 0$$

If we take the associated long exact sequence

$$0 \to E[P]^{G_K} \to E(\overline{K})^{G_K} \to E(\overline{K})^{G_K} \to H^1(G_K, E[P]) \to H^1(G_K, E(\overline{K})) \to \dots (\dagger\dagger)$$

From $(\dagger\dagger)$ we get:

$$0 \to E(K)/pE(K) \stackrel{\delta}{\to} H^1(G_K, E[p]) \to H^1(G_K, E(\overline{K}))[p] \to 0$$

where δ is defined as follows: for $Q \in E(K)$ fix $L \in E(\overline{K})$ such that $pL = Q$. Then $\delta(Q)$ is the 1-cocycle which sends $\sigma \in G_K$ to $\sigma(L) - L \in E[P]$.

Definition 2.3. The *geometric local Selmer structure* F on $E[P]$ is the image of δ in $H^1(G_K, E[p])$.

Fact. *The* dual geometric local Selmer structure *is the geometric local Selmer structure (it make sense since $E[P]^* \cong E[P]$)*

If E has good reduction over K and $\ell \neq p$. Then $E[p]$ is an unramified G_K-module and the geometric structures agrees with the unramified structure.

3 Global Section

In this talk K will be a number field, v a place of K, K_v the completion of K at v, $G_v = \mathrm{Gal}(\overline{K}_v/K_v)$ and I_v the inertia subgroup of G_v. As in the last talk we let T to be a finite dimensional $\mathbb{F}_p$-vector space with a discrete G_K-action. $G_K \times T \to T$ is continuous when T is given the discrete topology. We choose an embedding $\overline{K} \hookrightarrow \overline{K}_v$ which gives us an embedding $G_v \hookrightarrow G_K$.

Since T is finite dimensional and G_K acts discretely, this implies that T is unramified almost everywhere.

For each place v we have a restriction map $\mathrm{Res}_v : H^1(K,T) \to H^1(K_v,T)$.

3.1 Selmer Groups

Definition 3.1. A *global Selmer structure* F on T is a choice of a local Selmer structure $H^1_{f,F}(K_v,T)$ for each place v such that $H^1_{f,F}(K_v,T) = H^1(K_v^{\mathrm{unr}}, T^{I_v})$ almost everywhere.

The *Selmer group* $\mathrm{Sel}_F(K,T)$ of F is defined to be $\ker\left(H^1(K,T) \to \oplus_v H^1_{s,F}(K_v,T)\right)$.

If we take E to be an elliptic curve over K and $T = E[p]$.

Definition 3.2. The *geometric global Selmer structure* F on $E[p]$ is defined to be the global Selmer structure obtained by setting $H^1_{f,F}(K_v,T)$ to be the local geometric structure at each v.

In this setting $\mathrm{Sel}_F(K,E[p]) = \mathrm{Sel}^{(p)}(E)$.

3.2 Global Duality

Definition 3.3. Let F be a global Selmer structure on T. The *Cartier dual Selmer structure* F^* on $T^* = \mathrm{Hom}_{\mathbb{F}_p}(T,\mu_p)$ is defined to be the global Selmer structure obtained by setting $H^1_{f,F^*}(K_v,T^*)$ to be the local Cartier dual Selmer structure.

We now fix an F and F^* and start omitting it from notation.

Given an ideal $\mathfrak{a} \lhd \mathcal{O}_K$, we define $\mathrm{Sel}_{\mathfrak{a}}(K,T) = \{c \in H^1(K,T) : c_v \in H^1_{f,F}(K_v,T) \text{ for all } v \nmid \mathfrak{a}\}$.

$\mathrm{Sel}^{\mathfrak{a}}(K,T) = \{c \in \mathrm{Sel}_F(K,T) : c_v = 0, \forall v|\mathfrak{a}\}$. This gives us the following exact sequences

$$0 \to \mathrm{Sel}(K,T) \to \mathrm{Sel}_{\mathfrak{a}}(K,T) \to \oplus_{v|\mathfrak{a}} H^1_{S,F}(K_v,T) \to 0$$

$$0 \to \mathrm{Sel}^{\mathfrak{a}}(K,T^*) \to \mathrm{Sel}(K,T^*) \to \oplus_{v|\mathfrak{a}} H^1_{f,F}(K_v,T^*) \to 0$$

We have $\oplus_{v|\mathfrak{a}} H^1_{s,F}(K_v,T) \cong \oplus_{v|\mathfrak{a}} H^1_{f,F^*}(K_v,T^*)^\vee$. We can put the two sequences above together as follows

$$0 \to \mathrm{Sel}(K,T) \to \mathrm{Sel}_{\mathfrak{a}}(K,T) \to \bigoplus_{v|\mathfrak{a}} H^1_{s,F}(K,T) \to \mathrm{Sel}(K,T^*)^\vee \to \mathrm{Sel}^{\mathfrak{a}}(K,T^*)^\vee \to 0$$

Proposition 3.4. *The above sequence is exact.*

The exactness of this sequence yields

$$0 \to \left(\oplus_{v|\mathfrak{a}} H^1_{s,F}(K_v,T)\right) / \mathrm{im}(\mathrm{Sel}_{\mathfrak{a}}(K,T)) \to \mathrm{Sel}_{F^*}(K,T^*)^\vee \to \mathrm{Sel}^{\mathfrak{a}}(K,T^*)^\vee \to 0$$

3.3 Bounding $\mathrm{Sel}^{\mathfrak{a}}$

From now on $p \neq 2$. If $\tau \in G_K$ is an involution, we have a decomposition $T = T^+ \oplus T^-$, where $T^\epsilon = \{t \in T : \tau(t) = \epsilon t\}$. We say that τ is non-scalor if $T^+ \neq 0$, $T^- \neq 0$.

From now on, T will be assumed to be irreducible. L/K = finite Galois extension such that the action of G_K on T factors through $\mathrm{Gal}(L/K)$.

If $S \subseteq H^1(K,T)$ finite dimensional $\mathbb{F}_p$-subspace $S^{\mathfrak{a}} = \{s \in S : s_v \in H^1_{f,F}(K_v,T) \text{ and } (s_V = 0 \forall v|\mathfrak{a})\}$. We can find a finite Galois extension M/L such that $S \subseteq \inf(H^1(M/K,T))$. Assume that $\tau \in \mathrm{Gal}(L/K)$ is a non-scalar involution and that it extends to an involution in $\mathrm{Gal}(M/K)$. Let $\{\gamma_1, \dots, \gamma_r\}$ be a set of group generators for $\mathrm{Gal}(M/L)$.

Proposition 3.5. *Let $\omega_1, \dots, \omega_r$ be places of M such that $\mathrm{Frob}_{M/K}(w_i) = \tau\gamma_i$. Let v_i be the restricted places to K and set $\mathfrak{a} = v_1 \cdots v_r$. Then we have $S^{\mathfrak{a}} \subseteq \inf(H^1(L/K, T))$.*

Let E be an elliptic curve over $\mathbb{Q}$ without CM, $T = E[p]$. $\rho : G_K \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_p)$, $H^1(\mathbb{Q}(E[p])/\mathbb{Q}, E[p]) = 0$.

Let L_0/K be an extension such that G_K factors through $\mathrm{Gal}(L_0/K)$, and we assume that K is a quadratic extension of K_0. We also assume that the action $\mathrm{Gal}(L_0/K)$ is a restriction of a $\mathrm{Gal}(L_0/K_0)$-action on T. We have

$$\begin{tikzcd} M \arrow[d, dash] \\ L \arrow[d, dash] \\ L_0 \arrow[d, dash] \\ K \arrow[d, dash, "2"] \\ K_0 \end{tikzcd}$$

S will be a finite dimensional subspace of $H^1(M/K, T)$ and τ will be a non-scalor involution in $\mathrm{Gal}(M/K_0)$ which projects to the non-trivial element of $\mathrm{Gal}(K/K_0)$. By the action of τ on $H^1(M/K, T)$, we have the decomposition

$$H^1(M/K, T) = H^1(M/K, T)^+ \oplus H^1(M/K, T)^-$$

We further assume that $S \subseteq H^1(M/K, T)^\epsilon$ for some $\epsilon \in \{\pm\}$. Let $\sigma \in \mathrm{Gal}(M/L_0)$ be such that $\tau\sigma\tau^{-1} = \sigma^{-1}$. We again let $\{\gamma_1, \dots, \gamma_r\}$ be a set of generators of $\mathrm{Gal}(M/L)$.

Proposition 3.6. *Let $w_1, \dots, w_r$ be places of M such that $\mathrm{Frob}_{M/K}(w_i) = \tau\sigma\gamma_i$ and let v_i be the restrictions of w_i to K. Set $\mathfrak{a} = v_1 \cdots v_r$, then $S^{\mathfrak{a}} \subseteq \inf(H^1(L/K, T)^\epsilon)$.*

4 Calculations in Galois Cohomology

Let E be an elliptic curve over $\mathbb{Q}$.

$K/\mathbb{Q}$ an imaginary quadratic extension where all primes dividing $\mathrm{Cond}(E)$ split.

Fix $y_k \in E(K)$ a Heegner point

Theorem 4.1. *Let $p \geq 3$ be such that*

1. *E has good reduction at p*
2. $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$
3. $y_k \notin pE(K)$

The $\mathrm{Sel}(K, E[p])$ is of $\mathbb{F}_p$ dimension 1 and generated by $\kappa(y_k)$.

Condition 2.) implies $\mathrm{Gal}(K(E[p])/K) \cong \mathrm{GL}_2(\mathbb{F}_p)$

Fact. *Under complex conjugation $y_k \mapsto \epsilon y_k$ (up to torsion) where ϵ is the global root number. ($\Rightarrow y_k \in (E(K)/pE(K))^\epsilon$)*

Recall: $\mathrm{Sel}^{\mathfrak{a}}(K, E[p])$ restricted.

$\mathrm{Sel}_{\mathfrak{a}}(K, E[p])$ relaxed.

this gives the exact sequence

$$\mathrm{Sel}_{\mathfrak{a}}(K, E[p]) \to \bigoplus_{v|\mathfrak{a}} H^1_s(K_v, E[p]) \to \mathrm{Sel}(K, E[p])^\vee \to \mathrm{Sel}^{\mathfrak{a}}(K, E[p])^\vee \to 0$$

Complex conjugation commutes with the maps so splits into a $+$ part and the $-$ part.

Let $L_0 = K(E[p])$. For z such that $pz = y_k$ let $L = L_0(z)$.

Lemma 4.2. *There exists an ideal $\mathfrak{a}$ of K such that $\mathrm{Sel}^{\mathfrak{a}}(K, E[p])^\pm \subseteq H^1(L/K, E[p])^\pm$. Moreover if we fix $\sigma \in \mathrm{Gal}(L/L_0)$ such that $\tau\sigma\tau^{-1} = \sigma^{-1}$.*

We can choose $\mathfrak{a}$ such that $\mathfrak{a}$ is divisible by primes lying above primes of $\mathbb{Q}$ with $\mathrm{Frob}_{L/\mathbb{Q}} \sim \tau\sigma$.

4.1 Preliminaries

Lemma 4.3. *Let ℓ be a prime of $\mathbb{Q}$ such that*

1. *E has good reduction at ℓ*

2. *$\ell \neq p$*

3. *$\mathrm{Frob}_{K(E[p])/\mathbb{Q}}\ell \sim \tau$*

Then $H^1_S(K_\lambda, E[p])^\pm$ is a 1-dimensional $\mathbb{F}_p$-vector-space.

Proof. $K(E[p])$ is the fixed field of the kernel of the mod p representation. Then Neron-Ogg-Shar implies that $E[p]$ is unramified at ℓ and so all primes above ℓ in K are unramified in $K(E[p])$. $\mathrm{Frob}_{K/\mathbb{Q}}\ell \sim \tau \neq \mathrm{id}$, the residue class of ℓ in $K/\mathbb{Q}$ is 2, and the residue class degree of ℓ in $K(E[p])/K$ is 1. Hence ℓ splits completely in $K(E[p])/K$. So $K(E[p])_\lambda = K_\ell$, i.e., $E[p] \subseteq E(K_\ell)$.

$$
\begin{aligned}
H^1_S(K_\ell, E[p]) &\cong H^1(I_\ell, E[p])^{G^{\mathrm{unr}}_{K_\ell}} \\
&= \mathrm{Hom}_{G^{\mathrm{unr}}_{K_\ell}}(I_\ell, E[p]) \\
&= \mathrm{Hom}_{G^{\mathrm{unr}}_{K_\ell}}(I_\ell/pI_\ell, E[p])
\end{aligned}
$$

$I_\ell/pI_\ell \cong \mathrm{Gal}(K^{\mathrm{unr}}_\ell(\ell^{1/p})/K^{\mathrm{unr}}_\ell) \cong \mu_p$. $H^1_S(K_\ell, E[p]) \cong \mathrm{Hom}(\mu_p, E[p])$. Everything done so far commutes with complex conjugations. We also get $\mathrm{Hom}(\mu_p, E[p])^\pm \to E[p]^\mp$. ☐

4.2 $-\epsilon$ eigenspace

Lemma 4.4. *$H^i(L_0/K, E[p]) = 0$ for all i*

Lemma 4.5. *$H^1(L/K, E[p])$ is 1-dimensional $\mathbb{F}_p$ -vector-space generated by $\kappa(y_K)$.*

Lemma 4.6. *$\mathrm{Gal}(L/L_0)$ is isomorphic to $E[p]$ as $\mathrm{Gal}(L_0/K)$-modules. And $\mathrm{Gal}(L/L_0)^\pm$ is 1-dimensional.*

Consider $\mathrm{Gal}(L/L_0) \hookrightarrow E[p]$ defined by $\sigma : \{z \mapsto z + q\} \mapsto q$. This map is actually the image of $\kappa(y_K) \in H^1(K, E[p])$ under the restriction to $H^1(L_0, E[p])^{\mathrm{Gal}(L_0/K)}$.

Proposition 4.7. *Let ℓ be a prime of $\mathbb{Q}$ with $\mathrm{Frob}_{L_0/\mathbb{Q}} \sim \tau$ which does not split completely in L/L_0. Then there exists $c(\ell) \in \mathrm{Sel}_\lambda(K_\lambda, E[p])^\pm$ such that $c(\ell)^s_\lambda \neq 0$ in $H^1_\lambda(K_\lambda, E[p])$.*

Theorem 4.8. $\mathrm{Sel}(K, E[p])^{-\epsilon} = 0$.

Proof. $1 \neq \sigma \in \mathrm{Gal}(L/L_0)$ such that $\tau\sigma\tau = \sigma^{-1}$. There exists $\mathfrak{a}$ such that $\mathrm{Sel}^{\mathfrak{a}}(K, E[p])^{-\epsilon} \subseteq H^1(L/K, E[p])^{-\epsilon}$. But the second thing is 1-dimensional and is generated by $\kappa(y_K)$. If we pick $\mathfrak{a}$ such that it is divisible only by primes lying over $\ell_1, \ldots, \ell_r \in \mathbb{Z}$ with $\mathrm{Frob}_{L/\mathbb{Q}} L_i \sim \tau\sigma$. $\oplus_{l_i|\mathfrak{a}} H^1_i(K_{\ell_i}, E[p])^{-\epsilon}$ has dimension r, but we use the fact there exists $c(\ell_1)$ such that $c(\ell_i)^s_\lambda \neq 0$ with linear independent images. Hence the cokernel is 0. ☐

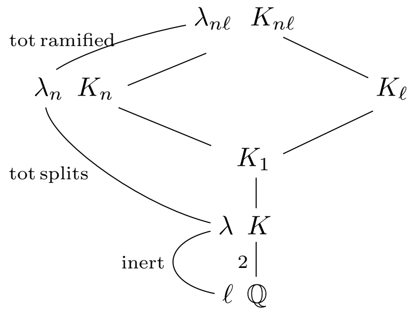
5 Finishing the proof

5.1 Notation and Recap

Notation.

- E an elliptic curve of conductor N
- $\phi : X_0(N) \to E$ a modular parametrization
- K an imaginary quadratic field with discriminant D, in which every prime dividing N splits.

- p a prime at which E has good reduction.
- Assume $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$.
- τ complex conjugation
- K_n the ring class field of K of conductor n, which (among other properties) is an abelian extension K_n/K unramified away from n.
- Let $\ell \in \mathbb{Z}$ be a prime such that ℓ is inert in $K/\mathbb{Q}$ and splits in $K(E[p])/K$. Setting $\lambda = \ell O_K$, λ splits completely in K_n and is totally ramified in $K_{n\ell}$. In the case n and ℓ are coprime we get:



- Note that $K_{n,\lambda_n} = K_\lambda$.
- red_{λ_n} the reduction map $E(K_{n,\lambda_n}) \to E(\mathbb{F}_\lambda)$.

We have the short exact sequence $0 \to H^1_f(K, E[p]) \to H^1(K, E[p]) \to H^1_s(K, E[p]) \to 0$, with $H^1_f(K, E[p]) = \mathrm{im}\kappa$.

We also recall that if E has good reduction at ℓ, then $H^1_s(K_\lambda, E[p]) \cong \mathrm{Hom}(I_\lambda, E[p])^{G^{\mathrm{un}}_{K_\lambda}}$, with $G^{\mathrm{un}}_{K_\lambda} = \mathrm{Gal}(K^{\mathrm{un}}_\lambda/K_\lambda)$.

Theorem 5.1. *For any integer n not dividing ND there exists a point $y_n \in E(K_n)$ such that*
$\ell \nmid ND$ then $\mathrm{Tr}_\ell y_{n\ell} = a_\ell y_n \in E(K_n)$
$\ell \nmid ND$ and is inert in K, $\mathrm{red}_{\lambda_{n\ell}}(y_{n\ell}) = \mathrm{red}_{\lambda_n}(\mathrm{Frob}_{K_n/K}\lambda_n \cdot y_n)$
There exists $\sigma \in \mathrm{Gal}(K_n/K)$ such that $\tau y_n = \epsilon\sigma y_n$ in $E(K)/E(K)_{\mathrm{tors}}$.

- $L_0 = K(E[p])$, For z such that $pz = y_k$ let $L = L_0(z)$.

This 5 weeks have been building towards proving

Theorem. *Let p be an odd prime such that:*

- *E has good reduction at p*
- $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$
- $y_K \notin pE(K)$

Then $\mathrm{Sel}(K, E[p])$ has order p; it is generated by the image of y_K under the Kummer map.

This was done by using the cohomology tools that Chris and Pedro set up, to bound $\mathrm{Sel}(K, E[p])^{\pm\epsilon}$ using the restricted and relaxed $\mathrm{Sel}^{\mathfrak{a}}(K, E[p])$ and $\mathrm{Sel}_{\mathfrak{a}}(K, E[p])$. Alex proved this last week under the assumption of the following two proposition, which we will prove this week.

Proposition. *Assume that $y_k \notin pE(K)$. Let $\ell \in \mathbb{Q}$ be a prime with $\mathrm{Frob}_{L_0/\mathbb{Q}}\ell \sim \tau$ and ℓ not splitting completely in L/L_0. There there exists $c(\ell) \in \mathrm{Sel}_\lambda(K, E[p])^{-\epsilon}$ with $c(\ell)^s_\lambda \neq 0$ in $H^1(K_\lambda, E[p])$*

Proposition. *Assume that $y_k \notin pE(K)$. Let $\ell \in \mathbb{Q}$ be a prime with $\mathrm{Frob}_{L/\mathbb{Q}}\ell \sim \tau$ and ℓ not splitting completely in L'/L. There there exists $c(q\ell) \in \mathrm{Sel}_\lambda(K, E[p])^{\epsilon}$ with $c(q\ell)^s_\lambda \neq 0$ in $H^1(K_\lambda, E[p])$.*

We will prove this using the Heegner points that Marc introduced in the first week to construct a class in $H^1(K, E[p])$ that satisfy those conditions.

5.2 The derivative operator

Let $\mathcal{R}$ be the set of square free integers, $\gcd(n, pND) = 1$ and if $\ell | n$ then $\mathrm{Frob}_{K(E[p])/\mathbb{Q}}\ell \sim \tau$. This implies that ℓ is inert in $K/\mathbb{Q}$ and splits in $K(E[p])/K$, and that E has good reduction at ℓ.

Lemma 5.2. *For all primes $\ell \in R$, $p | \ell + 1$ and $p | a_\ell = \ell + 1 - \#(\mathbb{F}_\ell)$*

Proof. As on $E[p]$, complex conjugation and Frob are conjugate, their characteristic polynomial must be the same mod p □

Recall that, for $\ell \in R$, $G_\ell = \mathrm{Gal}(K_\ell/K_1)$ is cyclic (Marc's talk) of order $\ell + 1$ (as ℓ is inert in K).
Fix a generator σ_ℓ and for a prime ℓ define

- $D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i$,
- $T_\ell = \sum_{i=0}^{l} \sigma_\ell^i$.
- For $n \in \mathcal{R}$ we define $D_n = \prod_{\ell | n} D_\ell$ (using the fact that $G_n \cong \prod_{\ell | n} G_\ell$)
- Let γ_i be a set of coset representative for G_n in $\mathrm{Gal}(K_n/K)$. $\mathrm{T} = \sum_i \gamma_i$, $\mathrm{T}^{-1} = \sum_i \gamma_i^{-1}$.

Lemma 5.3. *For any $n \in \mathcal{R}$ we have $D_n\gamma_n \in (E(K_n)/pE(K_n))^{G_n}$.*

Proof. As $G_n = \prod_{\ell | n} G_\ell$, we just need to show that $(\sigma_\ell - 1)D_n y_n \in pE(K_n)$. This is calculations using the identity $(\sigma_\ell - 1)D_\ell = \ell + 1 - T_\ell$, Theorem 5.1 and Lemma 5.2. □

We define $P_n = \mathrm{T}D_n y_n \in E(K_n)$. If we consider P_n in $E(K_n)/pE(K_n)$, then by the above it is $\mathrm{Gal}(K_n/K)$-invariant and independent of the choice made for T.

Consider the following, we want to get an element in $H^1(K, E[p])$ from ~~$P_n \in E(K_n)/pE(K_n)$~~

$$\begin{tikzcd} & E(K_n)/pE(K_n) \arrow[d, "\kappa"'] \\ & H^1(K_n, E[p]) \\ H^1(K, E[p]) \arrow[r, "\mathrm{res}"'] & H^1(K_n, E[p])^{\mathrm{Gal}(K_n/K)} \end{tikzcd}$$

As the Kummer map is equivariant, $\kappa(P_n) \in H^1(K_n, E[p])^{\mathrm{Gal}(K_n/K)}$.

Lemma 5.4. *The restriction map is an isomorphism*

Proof. Using long exact sequence have that the kernel and cokernel of res is $H^i(K_n/K, E[p]^{\mathrm{Gal}(K_n/K)})$ for $i = 1, 2$ respectively. Using the non-trivial fact that E has no K_n-rational p-torsion for $n \in \mathcal{R}$, these two groups are trivial. Hence the restriction map is an isomorphism □

So we let $c(n) \in H^1(K, E[p])$ be such that $c(n) = \kappa(P_n)$.

Recap: At this point we have constructed a class $c(n) \in H^1(K, E[p])$ which comes from an Heegner point $y_n \in E(K_n)$. We now show it lies in one of the $+$ or $-$ space

Lemma 5.5. *Let $n \in \mathcal{R}$ have k prime factors. Then $c(n) \in H^1(K, E[p])^{(-1)^k\epsilon}$.*

Proof. As τ commutes with κ and res, we show $\tau P_n = (-1)^k \epsilon P_n$ in $E(K_n)/pE(K_n)$.

$$\begin{aligned}
\tau P_n &= \tau \mathrm{T} \prod_{\ell | n} D_\ell y_n \text{ Definition} \\
&= \mathrm{T}^{-1} \prod_{\ell | n} \tau D_\ell y_n \text{ by } \tau \mathrm{T} = \mathrm{T}^{-1} \tau \\
&= \mathrm{T}^{-1} \prod_{\ell | n} (\ell \mathrm{T}_\ell - \sigma_\ell D_\ell) \tau y_n \\
&= \mathrm{T}^{-1} \prod_{\ell | n} (\ell \mathrm{T}_\ell - \sigma_\ell D_\ell) \epsilon \sigma y_n \text{ Lemma 5.1} \\
&= \mathrm{T}^{-1} \prod_{\ell | n} (-\sigma_\ell D_\ell) \epsilon \sigma y_n \text{ since } \mathrm{T}_\ell y_n = a_\ell y_{n/\ell} = 0 \text{ in } E(K_n)/pE(K_n) \\
&= (-1)^k \epsilon \sigma \prod_{\ell | n} \sigma_\ell \mathrm{T}^{-1} D_n y_n
\end{aligned}$$

Then using the fact that $D_n y_n$ is G_n-invariant, and P_n is $\mathrm{Gal}(K_n/K)$-invariant, this collapse down to what we want. ☐

Lemma 5.6. *Fix $n = \ell_1 \dots \ell_r \mathcal{R}$, then $c(n) \in \mathrm{Sel}_{\lambda_1 \dots \lambda_r}(K, E[p])$*

Proof. Let ν be a place of K distinct from λ_i such that E has good reduction at ν (The proof of ν has bad reduction is more involved and uses tools we have not developed). Instead of showing $c(n)_\nu \in H^1_f(K_\nu, E[p])$, we show $c(n)^s_\nu = 0$ in $H^1_s(K_\nu, E[p])$. We have $H^1_s(K_\nu, E[p]) = \mathrm{Hom}(I_\nu, E[p])^{G^{\mathrm{unr}}_{K_\nu}}$. Let w be a place of K_n above ν and note that $K_{n,w}/K_\nu$ is unramified. Hence its inertia group is also I_ν, and using the exact sequence we get the following commuting diagram:

$$\begin{array}{ccccc}
E(K_\nu)/pE(K_\nu) & \xrightarrow{\kappa} & H^1(K_\nu, E[p]) & \longrightarrow & \mathrm{Hom}(I_\nu, E[p]) \\
 & & \downarrow{\scriptstyle \mathrm{res}} & & \| \\
E(K_{n,w})/pE(K_{n,w}) & \xrightarrow[\kappa]{} & H^1(K_{n,w}, E[p]) & \longrightarrow & \mathrm{Hom}(I_\nu, E[p])
\end{array}$$

where we use $\mathrm{Hom}(I_\nu, E[p])^{G^{\mathrm{unr}}_{K_\nu}} \subseteq \mathrm{Hom}(I_\nu, E[p])^{G^{\mathrm{unr}}_{K_{n,w}}} \subseteq \mathrm{Hom}(I_\nu, E[p])$. Then it is jut a matter of diagram chasing.

By definition $\mathrm{res} c(n)_\nu = \kappa(P_n)$, so $(\mathrm{res} c(n)_\nu)^s = 0$. Hence $c(n)^s_\nu = 0$. ☐

As $P_{n\ell} \in E(K_{n\ell})$ is $\mathrm{Gal}(K_{n\ell}/K)$-invariant in $E(K_{n\ell})/pE(K_{n\ell})$, and $G_\ell = \mathrm{Gal}(K_\ell/K_1) \leq \mathrm{Gal}(K_{n\ell}/K)$, we have $(\sigma_\ell - 1)P_{n\ell} \in pE(K_{n\ell})$. Setting

$$Q_{n,\ell} = \frac{\ell+1}{p} \mathrm{T} D_n \gamma_{n\ell} - \frac{a_\ell}{p} P_n \quad (\dagger)$$

(which makes sense by Lemma 5.2) we see $pQ_{n,\ell} = (\sigma_\ell - 1)P_{n\ell}$ (using Lemma 5.3). Note that by the fact that E has no $K_{n\ell}$-rational p-torsion point, $Q_{n,l}$ is the unique point in $K_{n\ell}$ with that property.

Lemma 5.7. $\mathrm{red}_{\lambda_{n\ell}}(Q_{n,\ell})$ *is trivial in $E(\mathbb{F}_\lambda)$ if and only if $P_n \in pE(K_\lambda)$*

Proof. First we show $\mathrm{red}_{\lambda_{n\ell}}(\sigma y_{n\ell}) = \mathrm{red}_{\lambda_n}(\mathrm{Frob}_{K_n/K} \lambda_n \cdot \sigma y_n)$ for all $\sigma \in \mathrm{Gal}(K_n/K)$. This is true by Theorem 5.1 for $\sigma = 1$, and we use Theorem 5.1 with the ideal $\sigma^{-1}\lambda_n$.

$$\begin{aligned}
\mathrm{red}_{\sigma^{-1}\lambda_{n\ell}}(y_{n\ell}) &= \mathrm{red}_{\sigma^{-1}\lambda_n}(\mathrm{Frob}_{K_n/K}(\sigma^{-1}\lambda_n) \cdot y_n) \\
\mathrm{red}_{\lambda_{n\ell}}(\sigma y_{n\ell}) &= \mathrm{red}_{\lambda_n}(\sigma \mathrm{Frob}_{K_n/K}(\sigma^{-1}\lambda_n) \cdot y_n)
\end{aligned}$$

but as $\mathrm{Frob}_{K_n/K}(\sigma^{-1}\lambda_n) = \sigma^{-1}\mathrm{Frob}_{K_n/K}\lambda_n \sigma$ we are done. By the definition of $D_n$and T, we have

$$\mathrm{red}_{\lambda_{n\ell}}(\mathrm{T} D_n \lambda_{n\ell}) = \mathrm{red}_{\lambda_n}(\mathrm{Frob}_{K_n/K}\lambda_n \cdot \mathrm{T} D_n y_n)$$

Hence combining this with (†) we get

$$\mathrm{red}_{\lambda_{n\ell}}(Q_{n,\ell}) = \mathrm{red}_{\lambda_n}\left(\left(\frac{\ell+1}{p}\mathrm{Frob}_{K_n/K}\lambda_n - \frac{a_\ell}{p}\right)P_n\right)$$

Claim: $(\ell+1)\mathrm{Frob}_{K_n/K}\lambda_n - a_\ell$ annihilates $E(\mathbb{F}_\lambda)$. Note that $E(\mathbb{F}_\lambda) = E(\mathbb{F}_\lambda)^+ \oplus E(\mathbb{F}_\lambda)^-$ as $\mathrm{Frob}_{K_n/K}\lambda_n$ is an involution. But $E(\mathbb{F}_\lambda)^+ = E(\mathbb{F}_\ell)$ which by definition has order $\ell+1-a_\ell$. Then by the Weil conjectures $E(\mathbb{F}_\lambda)^-$ has order $l+1+a_\ell$.

Now $\mathrm{Frob}_{K_n/K}\lambda_n$ is the reduction of a complex conjugation, so $\mathrm{Frob}_{K_n/K}\lambda_n P_n = \tau P_n$, which by the proof of Lemma 2.4 $\tau P_n = (-1)^k\epsilon P_n$ in $E(K_n)/pE(K_n)$, so $\mathrm{Frob}_{K_n/K}\lambda_n P_n = \nu P_n + pQ$ for some $\nu \in \{\pm 1\}$ and $Q \in E(K_n)$.

$$\mathrm{red}_{\lambda_{n\ell}}(Q_{n,\ell}) = \frac{(\ell+1)\nu - a_\ell}{p}\mathrm{red}_{\lambda_n}(P_n) \in E(\mathbb{F}_\lambda)^\nu / pE(\mathbb{F}_\lambda)^\nu$$

We now claim that the p-primary part of $E(\mathbb{F}_\lambda)^\nu$ is cyclic. First we note that $p|(l+1) \pm a_\ell$, so we have at least p p-torsion point in $E(\mathbb{F}_\lambda)^\pm$. Suppose we had more than p p-torsion point in one of $E(\mathbb{F}_\lambda)^\pm$, then we would have p^2 of them, but $p^2 > |E(\mathbb{F}_\lambda)^+[p]| + |E(\mathbb{F}_\lambda)^-[p]| = |E(\mathbb{F}_\lambda)[p]|$which is a contradiction (as ℓ is a good prime, $\left|E(\overline{\mathbb{F}}_\lambda)[p]\right| = p^2$). We can conclude that $E(\mathbb{F}_\lambda)^\nu/pE(\mathbb{F}_\lambda)^\nu$ is cyclic of order p.

Hence $\mathrm{red}_{\lambda_{n\ell}}(Q_{n,\ell}) = 0$ if and only if $\mathrm{red}_{\lambda_n}(P_n) \in pE(K_{n,\lambda_n}) = pE(K_\lambda)$. But the kernel of red_{λ_n} is pro-ℓ, which is coprime to p, so $P_n \in pE(K_\lambda)$ □

Lemma 5.8. *Let $n\ell \in \mathcal{R}$ with ℓ prime. Then $c(n\ell)^s_\lambda = 0$ if and only if $P_n \in pE(K_\lambda)$.*

Proof. Since $\ell \in \mathcal{R}$ we have $H^1_s(K_\lambda, E[p]) = \mathrm{Hom}(I_\lambda, E[p])^{G^{\mathrm{un}}_{K_\lambda}}$ so we can view $c(n\ell)^s_\lambda$ as a homomorphism $I_\lambda \to E[p]$. We shall show this factors as follows:

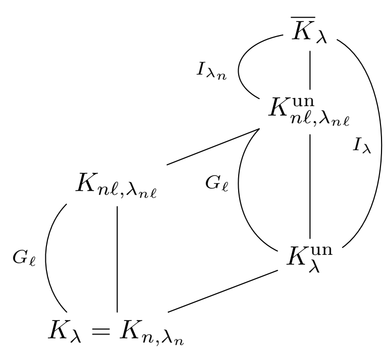
$$\begin{tikzcd} I_\lambda \arrow[r] \arrow[dr] & E[p] \\ & I_\lambda/I_{\lambda_{n\ell}} \cong G_\ell \arrow[u] \end{tikzcd}$$

To see this we consider the diagram

$$\begin{tikzcd} & H^1(K_\lambda, E[p]) \arrow[d, "\mathrm{res}"'] & \\ E(K_{n\ell})/pE(K_{n\ell}) \arrow[r, "\kappa"'] & H^1(K_{n\ell,\lambda_{n\ell}}, E[p]) \arrow[r] & \mathrm{Hom}(I_{\lambda_{nl}}, E[p]) \end{tikzcd}$$

Then $c(n\ell)$ lies in the image of the Kummer map, hence $c(n\ell)(I_{\lambda_{n\ell}}) = 0$.

Looking at the diagram in the introduction (since $\ell \nmid n$), we see that G_ℓ is the inertia group of $\mathrm{Gal}(K_{n\ell}/K)$ at λ. Hence considering the diagram



we have $I_\lambda/I_{\lambda_{n\ell}} \cong G_\ell$. Hence $c(n\ell)^s_\lambda = 0$ if and only if $c(n\ell)(\sigma_\ell) = 0$.

Fix $Q \in E(\overline{K})$ such that $pQ = P_{n\ell}$, then we claim that the cocycle $G_K \to E[p]$ given by $\sigma \mapsto (\sigma-1)Q - \frac{1}{p}(\sigma-1)P_{n\ell}$ represents $c(n\ell)$ (where $\frac{1}{p}(\sigma-1)P_{n\ell}$ is the unique point in $E(K_{n\ell})$ which is a pth root of $(\sigma-1)P_{n\ell}$). This expression is easy to see is in $E[p]$. To see it represents $c(n\ell)$ one checks that $\mathrm{res}c(n\ell) = \kappa(P_{n\ell})$, but $\kappa(P_{n\ell})$ is just the cocycle $\sigma \mapsto (\sigma-1)Q$ and for all $\sigma \in G_{K_{n\ell}}$ $(\sigma-1)P = 0$.

Now $c(n\ell)(\sigma_\ell) = (\sigma_\ell - 1)Q - Q_{n,\ell}$ (as we had $pQ_{n,\ell} = (\sigma_\ell - 1)P$).

Fix a prime $\overline{\lambda}$ of $\overline{K}$ over λ and consider $\mathrm{red} : E(\overline{K}) \to E(\overline{k}_\lambda)$. As E has good reduction at p, this map is injective on p-torsions, so $c(n\ell)(\sigma_\ell) = 0$ if and only if $\mathrm{red}((\sigma_\ell - 1)Q - Q_{n,\ell}) = 1$. Note that $\mathrm{red}((\sigma_\ell - 1)Q)$ and $\mathrm{red}(Q_{n,\ell})$ are p-torsion (we had $\mathrm{red}(Q_{n,\ell}) = \frac{1}{p}((l+1)\nu - a_\ell)\mathrm{red}(P_n))$, and σ_ℓ lies in inertia and hence acts trivially, we have that $\mathrm{red}((\sigma_\ell - 1)Q) = 0$. So $\mathrm{red}((\sigma_\ell - 1)Q - Q_{n,\ell}) = -\mathrm{red}(Q_{n,\ell})$.

Hence $c(n\ell)(\sigma_\ell) = 0$ if and only if $\mathrm{red}(Q_{n,\ell}) = 0$ if and only if $P_n \in pE(K_\lambda)$ □

Proposition. *Assume that $y_k \notin pE(K)$. Let $\ell \in \mathbb{Q}$ be a prime with $\mathrm{Frob}_{L_0/\mathbb{Q}}\ell \sim \tau$ and ℓ not splitting completely in L/L_0. There there exists $c(\ell) \in \mathrm{Sel}_\lambda(K, E[p])^{-\epsilon}$ with $c(\ell)^s_\lambda \neq 0$ in $H^1(K_\lambda, E[p])$*

Proof. We let $c(\ell)$ be the class defined by the Heegner point y_k. Then Lemma 5.5 and 5.6 shows that $c(\ell) \in \mathrm{Sel}_\lambda(K, E[p])^{-\epsilon}$. Lemma 5.8 tells us that $c(\ell)^s_\lambda \neq 0$ if and only if $P_1 \notin pE(K_\lambda)$.

But $P_1 \in E(K)$ is the point y_k by definition. Since by definition L is the minimal extension of L_0 which y_k is divisible by p, we have that y_k is divisible by p in $E(K_\lambda)$ if and only if λ splits completely in L/L_0. By assumption it does not, hence $y_k \notin pE(K_\lambda)$. □

For the $\mathrm{Sel}(K, E[p])^\epsilon$ space we need to reintroduce some work done by Alex. Let q be a prime satisfying the previous proposition, so $c(q) \in \mathrm{Sel}_{\mathfrak{q}}(K, E[p])^{-\epsilon}$ and $c(q)^s_{\mathfrak{q}} \neq 0$. We let L' be the smallest extension of L such that $c(q) \in H^1(K, E[p])$ is defined, i.e., $c(q) \in H^1(L', E[p])$.

Lemma 5.9. *Let ℓ be a prime with $\mathrm{Frob}_{L/\mathbb{Q}}\ell \sim \tau$. Then $P_q \in pE(K_\lambda)$ if and only if ℓ splits completely in L'/L.*

Proposition. *Assume that $y_k \notin pE(K)$. Let $\ell \in \mathbb{Q}$ be a prime with $\mathrm{Frob}_{L/\mathbb{Q}}\ell \sim \tau$ and ℓ not splitting completely in L'/L. There there exists $c(q\ell) \in \mathrm{Sel}_\lambda(K, E[p])^\epsilon$ with $c(q\ell)^s_\lambda \neq 0$ in $H^1(K_\lambda, E[p])$.*

Proof. By the same argument as above we have $c(q\ell) \in \mathrm{Sel}_{\mathfrak{q}\lambda}(K, E[p])^\epsilon$. Then using the previous lemma and Lemma 5.8 we have that $c(q\ell)^s_\lambda \neq 0$ in $H^1_s(K_\lambda, E[p])$.

It remains to show that $c(q\ell) \in \mathrm{Sel}_\lambda(K, E[p])^\epsilon$ or equivalently that $c(q\ell)^s_{\mathfrak{q}} = 0$. As $\mathrm{Frob}_{L/\mathbb{Q}}\ell \sim \tau$ we have that ℓ splits in L/L_0, hence $\gamma_K \in pE(K_\lambda)$ using the proof of the above proposition. So considering $c(\ell) \in \mathrm{Sel}_\lambda(K, E[p])^{-\epsilon}$, by Lemma 2.7, we have $c(\ell)^s_\lambda = 0$ and hence $c(\ell) \in \mathrm{Sel}(K, E[p])^{-\epsilon} = 0$ as Alex proved last week. Hence $c(\ell) = 0$ itself, and since by construction $\mathrm{res}c(\ell) = \kappa(P_\ell) = 0$, we must have P_ℓ to be 0 in $E[K_\ell]/pE[K_\ell]$, i.e., $P_\ell \in pE(K_\ell)$. So $P_\ell \in pE(K_{\ell,\mathfrak{q}})$, hence by Lemma 2.7 $c(q\ell)^s_{\mathfrak{q}} = 0$. □

6 __ (Angelos)

6.1 Notation

- p, ℓ are primes such that p is fixed $p \neq \ell$
- K is a field and K_v denotes the completion of K at v
- $G_K = \mathrm{Gal}(\overline{K}^{\mathrm{sep}}/K)$
- A is a G_K-module and $A^* = \mathrm{Hom}(A, \mu_\infty)$. In general, A is a free $\mathbb{Z}_p$-module of finite rank then $A_m = A/p^m A$ $(\overline{A} = A_1)$, $A^*_m = A^*[p^m]$
- $H^i(K, A) = H^i(G_m, A)$

Comment: Since, A may not be a discrete G_K-module, then it doesn't hold that $H^i(G_K, A) = \varprojlim H^i(G_K, A_m)$ for $i > 1$.For A^* everything is fine since it has discrete topology

6.2 Dualing

Theorem 6.1. *Suppose A is finite G_K-module, then the pair*

$$H^1(G_{K_v}, A) \times H^1(G_{K_v}, A^*) \xrightarrow{\cup} H^2(G_{K_v}, \mu_\infty) \xrightarrow{\mathrm{inv}_{K_v}} \mathbb{Q}/\mathbb{Z}$$

is perfect

Remark. $H^1_f(\mathbb{Q}_\ell, E[p^m])^\perp = H^1_f(\mathbb{Q}_\ell, E[p^m])$

If $\mathcal{F}$ is Selmer structure of A then we get a Selmer structure for A_m just using the canonical map $H^1(K_v, A) \to H^1(K_v, A_m)$. This defines a Selmer structure for A^*_m and from that we define Selmer structure $\mathcal{F}^*$ for A^* by $H^1_{\mathcal{F}^*}(K_v, A^*) = \varprojlim H^1_{\mathcal{F}^*}(K_v, A^*_m)$.

Proposition 6.2. *It holds that $H^1_{\mathcal{F}}(K, A) = \varprojlim H^1_{\mathcal{F}}(K, A_m)$ and $H^1_{\mathcal{F}^*}(K, A^*) = \varinjlim H^1_{\mathcal{F}}(K, A^*_m)$.*

Definition 6.3. If $\mathcal{F}, \mathcal{G}$ are Selmer structure of A, we say that $\mathcal{G} \subset \mathcal{F}$ if $H^1_{\mathcal{G}}(K_v, A) \subset H^1_{\mathcal{F}}(K_v, A)$ for all v.

Note that if $\mathcal{G} \subset \mathcal{F}$ then

- $H^1_{\mathcal{G}}(K, A) \subset H^1_{\mathcal{F}}(K, A)$
- $\mathcal{F}^* \subset \mathcal{G}^*$

Theorem 6.4. *Suppose $\mathcal{F}_1, \mathcal{F}_2$ are Selmer structure for a finite G_K-module A and $\mathcal{F}_1 \subset \mathcal{F}_2$. Then*

- $0 \to H^1_{\mathcal{F}_1}(K, A) \to H^1_{\mathcal{F}_2}(K, A) \xrightarrow{\oplus \mathrm{res}} \bigoplus H^1_{\mathcal{F}_2}(K_v, A)/H^1_{\mathcal{F}_1}(K_v, A)$
- $0 \to H^1_{\mathcal{F}_2^*}(K, A) \to H^1_{\mathcal{F}_1^*}(K, A) \xrightarrow{\oplus \mathrm{res}} \bigoplus H^1_{\mathcal{F}_1^*}(K_v, A)/H^1_{\mathcal{F}_2^*}(K_v, A)$

Summing over v such that $H^1_{\mathcal{F}_1}(K_v, A) \neq H^1_{\mathcal{F}_2}(K_v, A)$. The images of $\oplus\mathrm{res}$ are orthogonal complement of each other with respect to the Tate pairing.

From now on K will be $\mathbb{Q}$.

Definition 6.5. The canonical Selmer structure $\mathcal{F}_{\mathrm{con}}$ for A is defined to be

- If $v \in \{\infty, p\}$ then $H^1_{\mathcal{F}_{\mathrm{con}}}(\mathbb{Q}_v, A) = H^1(\mathbb{Q}_v, A)$
- If $v \notin \{\infty, p\}$ then $H^1_{\mathcal{F}_{\mathrm{con}}}(\mathbb{Q}_v, A) = \ker[H^1(\mathbb{Q}_v, A) \to H^1(\mathbb{Q}_v^{\mathrm{un}}, A) \otimes \mathbb{Q}_p]$.

Proposition 6.6. *If $\mathcal{F} = \mathcal{F}_{\mathrm{con}}$ for $A = E[p^m]$ and $\ell \neq p$, then $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, E[p^m]) = H^1_{\mathcal{F}^*}(\mathbb{Q}_\ell, E[p^m]^*) = H^1_f(\mathbb{Q}_\ell, E[p^m])$*

Proposition 6.7. *If $\mathcal{F} = \mathcal{F}_{\mathrm{con}}$. The following are the same*

$$0 \to \mathrm{Sel}_{p^m}(E/\mathbb{Q}) \to H^1_{\mathcal{F}}(\mathbb{Q}, E[p^m]) \to H^1_{\mathcal{F}}(\mathbb{Q}_p, E[p^m])/H^1_f(\mathbb{Q}_p, E[p^m])$$

$$0 \to H^1_{\mathcal{F}^*}(\mathbb{Q}, E[p^m]) \to \mathrm{Sel}_{p^m}(E/\mathbb{Q}) \to H^1_f(\mathbb{Q}_p, E[p^m])/H^1_{\mathcal{F}^*}(\mathbb{Q}_p, E[p^m])$$

6.3 The Hypotheses

H.1 $\overline{A}$ is an absolutely irreducible $\mathbb{F}_p[G_{\mathbb{Q}}]$-module, not isomorphic to $\mathbb{F}_p$ or μ_p

H.2 There is $\tau \in G_{\mathbb{Q}}$ such that $\tau = 1$ on μ_{p^∞} and $A/(\tau - 1)A$ is free of rank one over $\mathbb{Z}_p$

H.3 $H^1(\mathbb{Q}(A)/\mathbb{Q}, \overline{A}) = H^1(\mathbb{Q}(A^*)/\mathbb{Q}, \overline{A}^*) = 0$ where $\mathbb{Q}(A)$ is the fixed field of the kernel of $G_{\mathbb{Q}} \to \mathrm{Aut}(A)$.

H.4 Either $\overline{A} \ncong \overline{A^*}$ or $p \geq 5$

H.5 Let Σ be a finite set of primes which contains ∞, p and ℓ such that A is ramified at ℓ and all ℓ such that $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, A) \neq H^1_{\text{un}}(\mathbb{Q}_\ell, A)$. For every $\ell \in \Sigma$, $H^1(\mathbb{Q}_v, A)/H^1_{\mathcal{F}}(\mathbb{Q}_v, A)$ is torsion-free.

Remark. $\mathcal{F}_{\text{con}}$ satisfies H.5

Let $A = T_p(E)$ with $\mathcal{F}_{\text{con}}$ Selmer structure. Assuming

- $p \geq 5$
- the p-adic representations $G_{\mathbb{Q}} \to \text{Aut}(E[p^\infty]) = \text{GL}_2(\mathbb{Z}_p)$ is surjective (for $p \geq 5$ this is the same as $G_{\mathbb{Q}} \to \text{Aut}(E[p])$ is surjective). Then $T_p(E)$ satisfies H.1 to H.5.

6.4 Euler - Kolyvagin Systems

Let Σ be a finite set of primes containing ∞, p and all primes where A ramifies. If $\ell \notin \Sigma$, $P_\ell(x) = \det(1-\text{Frob}_\ell x|_A) \in \mathbb{Z}_p[x]$. Let $\mathcal{N} = \{np^k : n \,\text{is square free product of primes}\, \ell \notin \Sigma, k \geq 0\}$.

Definition 6.8. An Euler system for A is a collection $\mathcal{F} = \{\mathcal{F}_n \in H^1(\mathbb{Q}(\mu_n), A), n \in \mathcal{N}\}$ such that for $n\ell \in \mathcal{N}$ $\mathcal{F}_{n\ell} = \begin{cases} P_\ell(\text{Frob}_\ell^{-1})\mathcal{F}_n & \ell \neq p \\ \mathcal{F}_n & \text{otherwise} \end{cases}$. Let $\text{ES}(A)$ denote the $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module of Euler system of A.

7 Kolyvagin Systems (Céline)

Notation. K a non-archimedian local field of characteristic 0. $I_K \subset G_K$, $\phi \in \text{Gal}(K^{\text{un}}/K)$, k residue field, $|k| = q$. A G_K-Module

7.1 Transverse and Unramified cohomology groups

Definition 7.1. Suppose L/K is totally tamely ramified extension of degree $q-1$. Then there is a canonical isomorphism $\text{Gal}(L/K) = k^*$.

In this talk, $K = \mathbb{Q}_\ell$ and $L = \mathbb{Q}_\ell(\mu_\ell)$.

We define the *L-transverse cohomology* subgroup $H^1_t(K, A) \subset H^1(K, A)$ to be $H^1_t(K, A) = \ker[H^1(K, A) \to H^1(L, A)] = H^1(L/K, A^{G_L})$.

Proposition 7.2. *Suppose that A is a finite unramified G_K-module such that $(q-1)A = 0$. Then*

1. $H^1_t(K, A) \cong \text{Hom}(\text{Gal}(L/K), A^{\phi=1})$
2. $H^1_t(K, A) \cong A^{\phi=1}$
3. *Direct sum decomposition:* $H^1(K, A) = H^1_u(K, A) \oplus H^1_t(K, A)$

Definition 7.3. Suppose that $n|q-1$, let $R = \mathbb{Z}/mn\mathbb{Z}$. Suppose that A is an unramified G_K-module, free of finite rank over R, $\det(1-\phi|_A) = 0$. Consider $P(x) = \det(1-\phi|_A x) \in R[x]$. By assumption $P(1) = 0$ so $P(x) = (x-1)Q(x)$ with $Q(x) \in R(x)$. By Cayley-Hamilton, $P(\phi^{-1}) = 0$, then $Q(\phi^{-1})A \subset A^{\phi=1}$. Define the *unramified-transverse comparison map* by

$$\underbrace{H^1_u(K, A) \xrightarrow{\sim} A/(\phi-1)A \xrightarrow{Q(\phi^{-1})} A^{\phi=1} \to H^1_t(K, A)}_{\phi^{ut}}$$

Example. Under the same hypotheses: $A^{\phi=1}$ is free of rank one if and only if $A/(\phi-1)A$ is also as well. In this case ϕ^{ut} is an isomorphism.

7.2 Kolyvagin Systems: Definition

Let A be a $\mathbb{Z}_p$-module of finite rank with a continuous action of $G_{\mathbb{Q}}$. Assume that A is ramified at only finitely many primes. For every positive integer m, we have finite $G_{\mathbb{Q}}$-module $A_n := A/p^n A$. For a given Selmer structure $\mathcal{F}$ for A, let Σ be a finite set of places of $\mathbb{Q}$ containing p, ∞, ℓ where A ramifies, all ℓ where $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, A) \neq H^1_u(\mathbb{Q}_\ell, A)$.

Definition 7.4. Let c be a positive integer such that c is not divisible by any prime in Σ. We define $\mathcal{F}(c)$ for A as follows, $H^1_{\mathcal{F}(c)}(\mathbb{Q}_v, A) = \begin{cases} H^1_{\mathcal{F}}(\mathbb{Q}_v, A) & v \nmid c \\ H^1_t(\mathbb{Q}_v, A) & v | c \end{cases}$.

Fix a $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module A and a Selmer structure $\mathcal{F}$ for A satisfying H.1 to H.5. If $\ell \notin \Sigma$, let $\nu(\ell) = \max\{m | l \equiv 1 \mod p^m \text{and } A_m/(\phi_\ell - 1)A_m \text{ is free of rank 1 over } \mathbb{Z}/p^m\mathbb{Z}\}$. Define $\mathcal{N}_A$ =be the set of square free product of primes $\ell \notin \Sigma$. If $n \in \mathcal{N}_A$ then we define $\nu(n) = \min\{\nu(\ell) | \ell | n\}$ and set $\nu(1) = \infty$.

Definition 7.5. A Kolyvagin System is a collection $\left\{\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbb{Q}, A_{\nu(n)}) | n \in \mathcal{N}_A\right\}$ such that if $n\ell \in \mathcal{N}_A$ the following commutes

$$\begin{array}{ccc} & & \kappa_n \in H^1_{\mathcal{F}(n)}(\mathbb{Q}, A_{\nu(n)}) \\ & & \downarrow \\ & & H^1_u(\mathbb{Q}_\ell, A_{\nu(n)}) \\ & & \phi^{ut}\downarrow \\ \kappa_{n\ell} \in H^1_{\mathcal{F}(n\ell)}(\mathbb{Q}, A_{\nu(n\ell)}) & \xrightarrow{\text{res}_\ell} & H^1_t(\mathbb{Q}_\ell, A_{\nu(nl)}) \end{array}$$

Let $KS(A)$ be the $\mathbb{Z}_p$-module of the Kolyvagin system for A.

7.3 Kolyvagin system construction

There exists a canonical map $ES(A) \to KS(A, \mathcal{F}_{\text{can}})$ such that if $\xi \to \kappa$ then $\kappa_1 = \xi_1$ in $H^1_{\mathcal{F}_{\text{can}}}(\mathbb{Q}, A)$

Construction:

For every $n \in \mathcal{N}_A$, let $\Gamma_n = \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. If $n = n_1 n_2$, $\Gamma_n = \Gamma_{n_1} \times \Gamma_{n_2}$. With this identification $\Gamma_n = \prod_{\ell | n} \Gamma_\ell$.

For $\ell \notin \Sigma$, fix a generator σ_ℓ for Γ_ℓ, define the Kolyvagin's Derivative operator $D_\ell := \sum_{i=1}^{\ell-2} i\sigma_\ell^i \in \mathbb{Z}[\Gamma_\ell]$. If $n \in \mathcal{N}_A$, $D_n = \prod_{\ell|n} D_\ell \in \mathbb{Z}[\Gamma_n]$.

Proposition 7.6. *If $\xi \in ES(A)$, $n \in \mathcal{N}_A$, then the image of $D_n \xi_n$ under $H^1(\mathbb{Q}(\mu_n), A) \to H^1(\mathbb{Q}(\mu_n), A_{\nu(n)})$ lies in $H^1(\mathbb{Q}(\mu_n), A_{\nu(n)})^{\Gamma_n}$.*

Proposition 7.7. *If $\xi \in ES(A)$, $n \in \mathcal{N}_A$, then the image of $D_n \xi_n$ has a canonical inverse image in $H^1(\mathbb{Q}, A_{\nu(n)})$ under the restriction map $H^1(\mathbb{Q}, A_{\nu(n)}) \to H^1(\mathbb{Q}(\mu_n), A_{\nu(n)})^{\Gamma_n}$.*

Denote ξ'_n to be the canonical inverse image of $D_n \xi_n$ as above. Let $\xi' = \{\xi'_n | n \in \mathcal{N}_A\}$.
Recall: $H^1(\mathbb{Q}_\ell, A_{\nu(n)}) = H^1_u(\mathbb{Q}_\ell, A_{\nu(n)}) \oplus H^1_t(\mathbb{Q}_\ell, A_{\nu(n)})$, $\text{Res}_\ell(\xi'_n), (\xi'_n)_{\ell,u}, (\xi'_n)_{\ell,t}$.
For ξ' to be a Kolyvagin system we need:

1. $\text{Res}_\ell(\xi'_n) \in H^1_{\mathcal{F}_{\text{can}}}(\mathbb{Q}_\ell, A_{\nu(n)})$ if $\ell \nmid n$
2. $\text{Res}(\xi'_n) \in H^1_t(\mathbb{Q}_\ell, A_{\nu(n)})$ if $\ell | n$
3. $\phi^{ut} \circ \text{Res}_\ell(\xi'_{n/\ell}) = (\xi'_n)_{\ell,t} \in H^1_t(\mathbb{Q}_\ell, A_{\nu(n)})$ for $\ell | n$

ξ' satisfies 1 and 3, but $(\xi'_n)_{\ell,u} \neq 0$ in general. But we can define a Weak Kolyvagin System by ignoring 2. and then refining it to create a Strong Kolyvagin System.

7.4 Application

Give a Kolyvagin system for A, if $\kappa_1 \neq 0$, then $H^1_{\mathcal{F}^*}(\mathbb{Q}, A^*)$ is finite and has length or equal to $\delta(K)$ where $\delta(K) = \max\{j | \kappa_1 \in p^j H^1_{\mathcal{F}}(\mathbb{Q}, A)\}$.

8 Kato's Euler system

Let $p \geq 5$ be prime. $E/\mathbb{Q}$ modular Elliptic Curve over $\mathbb{Q}$ conductor N. f newform weight 2, level N.

$T = T_pE$

Euler system: $(\zeta_n \in H^1(\mathbb{Q}(\zeta_n), T))_{n\in\mathcal{N}}$, $\Sigma \supset \{\infty, p\} \cup \text{primes}(N)$

$\mathcal{N} = \{\text{squarefree product of } \ell \in \Sigma \times p^k\}$

$$\mathrm{Co}_{\mathbb{Q}(\zeta_{n\ell})/\mathbb{Q}(\zeta_n)}\zeta_{n\ell} = \begin{cases} P_\ell(\mathrm{Frob}_\ell^{-1})\zeta_n & \ell \neq p \\ \zeta_n & \ell = p \end{cases}$$

8.1 Overview of construction

$$\begin{array}{ccccc}
(\mathcal{O}(Y(n,L))^*)^2 & \longrightarrow & H^1_{\text{ét}}(Y(n,L), \mathbb{Z}_p(1))^2 & \longrightarrow & H^2_{\text{ét}}(Y_1(N)_{\mathbb{Q}(\zeta_n)}, \mathbb{Z}_p(1))^2 \\
 & & & & \downarrow \\
 & & & & H^2_{\text{ét}}(Y_1(N)_{\mathbb{Q}(\zeta_n)}, \mathbb{Z}_p(2)) \\
 & & & & \downarrow \\
 & & & & H^1(\mathbb{Q}(\zeta_n), H^1_{\text{ét}}(Y_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(2)) \\
 & & & & \downarrow \\
 & & & & H^1(\mathbb{Q}(\zeta_n), T(1))
\end{array}$$

Proposition 8.1. *Let E/S be an elliptic curve, c prime to 6. Then there exists a unique ${}_c\theta_E \in \mathcal{O}(E\backslash E[c])^*$ such that*

1. *divisors $c^2(0) - E[c]$*
2. *For all a coprime to c, $[a]_* : \mathcal{O}(E\backslash E[ac])^* \to \mathcal{O}(E\backslash E[c])^*$, $[a]_*\, {}_c\theta_E = {}_c\theta_E$.*

Proof.

Uniqueness: Let $f = ug$, $u \in \mathcal{O}(S)^*$, $f = [a]_*f = [a]_*ug = u^{a^2}[a]_*g = u^{a^2}g$, Hence $u^{a^2-1} = 1$ so $a = 2, 3$ and $u = 1$.

Existence: $[a]_*f = u_af$ with $u \in \mathcal{O}(S)^*$. If we let $u_a^{b^2-1} = u_b^{a^2-1}$, $g = u_2^{-3}u_3f$.

□

Definition 8.2. $N \geq 3$, $Y(N)$ modular curve over $\mathbb{Q}$ represent $S \to \begin{cases} (E, e_1, e_2) & E/S \\ e_1, e_2 & \mathbb{Z}/N\mathbb{Z} - \text{basis of } N \text{ torsion} \end{cases}$.
$Y(N)(\mathbb{C}) \cong (\mathbb{Z}/N\mathbb{Z})^* \times \Gamma(N)\backslash\mathcal{H}$. If $N|N'$, there is a map $Y(N') \to Y(N)$ so $\mathcal{O}(Y(N)) \subset \mathcal{O}(Y(N'))$.

Definition 8.3. Let $N \geq 3$, c coprime to $6N$. $(\alpha, \beta) = (\frac{a}{N}, \frac{b}{N}) \subset (\mathbb{Q}/\mathbb{Z})^2 \setminus \{(0,0)\}$. Then ${}_cg_{\alpha,\beta} := L^*_{\alpha,\beta}({}_c\theta_E)$, $L_{\alpha,\beta} = ae_1 + be_2 : Y(N) \to E[N]$.

$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \circlearrowleft Y(N)$

Proposition 8.4.

1. *$\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, $\sigma^*\, {}_cg_{\alpha,\beta} = {}_cg_{(\alpha,\beta)\sigma}$*
2. *if a prime to c: then ${}_cg_{\alpha,\beta} = \prod_{a\alpha'=\alpha, a\beta'=\beta} {}_cg_{\alpha',\beta'}$.*

Definition 8.5. Let $M, N \geq 3$, $M|L$, $N|L$ and define $Y(M,N) := G\backslash Y(L)$ where $G = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod \begin{pmatrix} M & M \\ N & N \end{pmatrix}\right\} \subset$
$\mathrm{GL}_2(\mathbb{Z}/L\mathbb{Z})$, $S \to \{(E, e_1, e_2) : E/S, e_1 \text{ is } M \text{ torsion}, e_2 \text{ is } N \text{ torsion}, (a,b) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \mapsto ae_1 + be_2 \text{ is injective}\}$.

Definition 8.6. étale sheaves: $1 \to \mu_{p^n} \to \mathcal{O}^*_X \xrightarrow{p^n} \mathcal{O}^*_X \to 1$. $\mathcal{O}(X)^* \to H^1_{ét}(X, \mu_{p^n})$, $(\mathbb{Z}/p^n\mathbb{Z})(k) := (\mu_{p^n})^{\otimes k}$. Then $H^i_{\text{ét}}(X, \mathbb{Z}_p(k)) = \varprojlim H^i_{\text{ét}}(X, \mu_{p^n}(k))$. $\mathcal{O}(X)^* \to H^1_{\text{ét}}(X, \mathbb{Z}_p(1))$.

$H^i_{\text{ét}}(X,\mathbb{Z}_p(k)) \times H^j_{\text{ét}}(X,\mathbb{Z}_p(k')) \xrightarrow{\cup} H^{i+j}_{\text{ét}}(X,\mathbb{Z}_p(k+k'))$, $f,g \in \mathcal{O}(X)^*$, $\{f,g\} := \kappa(f)\cup\kappa(g) \in H^2_{\text{ét}}(X,\mathbb{Z}_p(2))$.

Lemma 8.7. *$f: U \to V$ finite étale, $u \in \mathcal{O}(U)^*$, $v \in \mathcal{O}(V)^*$, $f_*\{u, f^*v\} = \{f_*u, v\}$, $f_*\{f^*v, u\} = \{v, f_*u\}$.*

Definition 8.8. $M, N \geq 3$, $(c, 6M) = 1$ and $(d, 6N) = 1$. Define ${}_{c,d}Z_{M,N} := \{\, {}_cg_{\frac{1}{M},0},\ {}_dg_{0,\frac{1}{N}}\} \in H^2_{\text{ét}}(Y(M,N),\mathbb{Z}_p(2))$.

Proposition 8.9. *If we take $M|M'$, $N|N'$, $(c,6M') = 1$ and $(d,6N') = 1$ with $\text{primes}(M) = \text{primes}(M')$ and $\text{primes}(N) = \text{primes}(N')$. Then $Y(M',N') \to Y(M,N)$. The push-forwards of ${}_{c,d}Z_{M',N'}$ is ${}_{c,d}Z_{M,N}$.*

If $\ell \nmid N$

$$\begin{tikzcd}
Y(M,N(\ell)) \arrow[rr, "\sim"] \arrow[dr] & & Y(M(\ell),N) \ \circlearrowleft T'(\ell) \arrow[dl] \\
& Y(M,N) &
\end{tikzcd}$$

Proposition 8.10. *If we take $M|M'$, $N|N'$, $(c,6M') = 1$ and $(d,6N') = 1$, there is a map $Y(M\ell, N\ell) \to Y(M,N)$ defined by*

$${}_{c,d}Z_{M\ell,N\ell} \mapsto \left(1 - T'(\ell)\begin{pmatrix}1/\ell & 0\\ 0 & 1\end{pmatrix}^* + \begin{pmatrix}1/\ell & 0\\ 0 & 1/\ell\end{pmatrix}^* \ell\right)\cdot {}_{c,d}Z_{M,N}$$

Let $Y_1(N) = Y(N,1)$, $n, N \geq 3$, $n|L$, $N|L$ and $\text{primes}(L) = \text{primes}(nN)$. Then $Y_1(N)_{\mathbb{Q}(\zeta_n)} \cong G\backslash Y(L)$. $G = \left\{\begin{pmatrix}* & *\\ 0 & 1\end{pmatrix} \mod N, \det \equiv 1 \mod n\right\}$, $Y(n,L) \to Y_1(N)_{\mathbb{Q}(\zeta_n)}$

Definition 8.11. ${}_{c,d}Z_{1,n,N} \in H^2_{\text{ét}}(Y_1(N)\mathbb{Q}(\zeta_n),\mathbb{Z}_p(2))$ push-forward of ${}_{c,d}Z_{n,N}$

Proposition. $\ell \nmid nN$

$${}_{c,d}Z_{1,n\ell,N\ell} \mapsto \left(1 - T'(\ell)\sigma_\ell^{-1} + \begin{pmatrix}\ell & 0\\ 0 & 1/\ell\end{pmatrix}^* \sigma_\ell^{-2}\ell\right) {}_{c,d}Z_{1,n,N}$$

where $\sigma_\ell \in \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and $\begin{pmatrix}\ell & 0\\ 0 & 1\end{pmatrix}^* = \sigma_\ell$

Define ${}_{c,d}\zeta_n :=$map of ${}_{c,d}Z_{1,np,Np}$. $\Sigma = \text{primes}(6cdNp)$.

Theorem 8.12. *$({}_{c,d}\zeta_n)$ is an Euler system*

9 Euler Systems and BSD

Notation. Let E be an elliptic curve over $\mathbb{Q}$, $T = T_pE$ Tate module. Σ =finite set of prime containing p, ∞, and all primes at which T ramifies. Euler system $\{c_n\}$, $c_n \in H^1(\mathbb{Q}(\mu_n),T)\}$ with corestriction conditions

9.1 Recap: What can we do with Euler systems?

Mantra: Existence of Euler systems leads to bounds on Selmer groups.

Pedro, Alex and Florian: Used Heegner points to bound $\text{Sel}(\mathbb{Q},E[p])$

Céline: Kolyvagin systems, $\zeta \in KS(A)$, $\zeta_1 \neq 0 \Rightarrow \text{Sel}(\mathbb{Q},A^*)$ is finite.

Today we'll use a variant,

Theorem 9.1. *Let $E/\mathbb{Q}$ be an elliptic curve, T a Tate module, $\underline{c} \in ES(T)$. If $\text{loc}^s_p(c_1) \neq 0 \in H^1(\mathbb{Q}_p,T)/H^1_f(\mathbb{Q}_p,T)$, then $\text{Sel}(\mathbb{Q},E[p^\infty])$ is finite.*

Proposition 9.2. *There exists an exact sequence $0 \to E(\mathbb{Q})\otimes\mathbb{Q}_p/\mathbb{Z}_p \to \text{Sel}(\mathbb{Q},E[p^\infty]) \to Ш(E/\mathbb{Q})_{p^\infty} \to 0$*

Lemma 9.3. *If $\text{loc}^s_p(c_1) \neq 0$, then $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})_{p^\infty}$ are finite.*

9.2 Twisting

Recall: Aurel constructed an Euler System for the "wrong" module, $T(1)$, i.e., T twisted by the cyclotomic character χ_p.

Motivation: Bloeh-Kato conjecture: "existence of 'nice' cohomology classes" $\leftrightarrow$ "vanishing of L-values"

Euler Systems means lots of nice cohomology. So we might expect Euler systems to exists where there is a systematic vanishing of L-functions.

Fact. *For all elliptic curves over $\mathbb{Q}$, $L(E,S)$ has a simple zero at $s=0$. (More generally, $L(f,0)=0$ for all modular form f)*

Twisting by characters of finite order.

Let $\chi : G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ of finite order. Let $L := \overline{\mathbb{Q}}^{\ker\chi}$, $L/\mathbb{Q}$ finite. For all n, $G_{L\mathbb{Q}(\mu_n)} \subset \ker(\chi)$, hence the natural map on cocycles induces an isomorphism

$$\begin{tikzcd}
c_m \arrow[d, dash] & H^1(L\mathbb{Q}(\mu_n),T)\otimes\chi \arrow[r, "\cong"] & H^1(L\mathbb{Q}(\mu_n),T\otimes\chi) \arrow[d, "\mathrm{cor}"'] \\
c_n \arrow[d, dash] & c_m \in H^1(L\mathbb{Q}(\mu_n),T) \arrow[u, "\otimes z_\chi"'] & H^1(\mathbb{Q}(\mu_n),T) \ni c_n^\chi \\
c_1 & &
\end{tikzcd}$$

Theorem 9.4. *$\underline{c}^\chi = \{c_n^\chi\}$ is an Euler Systems for $\sum \cup \{\ell : \ell | \mathrm{cond}(\chi)\}$*

Twisting by χ_p

Problem: $L := \overline{\mathbb{Q}}^{\ker\chi} = \mathbb{Q}_\infty = \cup_k \mathbb{Q}(\mu_{p^k})$ so corestriction doesn't exist.

Idea: $\mathbb{Z}/p^n\mathbb{Z}(1)$ is a trivial $G_{\mathbb{Q}(\mu_{p^k})}$-module, hence $T/p^k \cong T/p^k \otimes \mathbb{Z}/p^k(1) \cong T/p^k(1)$ as $G_{\mathbb{Q}(\mu_{p^k})}$-modules. So $H^1(\mathbb{Q}(\mu_{p^k}), T/p^kT) \cong H^1(\mathbb{Q}(\mu_{p^k}), T/p^kT(1))$

Definition. The *Iwasawa cohomology group* for T over $\mathbb{Q}(\mu_n)$ is $H^1_\infty(\mathbb{Q}(\mu_n),T) = \varprojlim_k H^1(\mathbb{Q}(\mu_{np^k}),T)$ with respect to corestriction.

Proposition 9.5. $H^1_\infty(\mathbb{Q}(\mu_n),T) \cong \varprojlim_k H^1(\mathbb{Q}(\mu_{np^k}), T/p^kT)$

Corollary 9.6. $H^1_\infty(\mathbb{Q}(\mu_n),T) \cong H^1_\infty(\mathbb{Q}(\mu_n),T(1))$

Note: If $\underline{c} \in ES(T)$, then for any n, we can define $c_{n,\infty} = \{c_{np^k}\}_{k\geq 0} \in H^1_\infty(\mathbb{Q}(\mu_n),T)$.

Theorem 9.7. *$\underline{c}^{\chi_p} = \{c_n^{\chi_p}\}$ is an Euler System.*

9.3 BSD

General Euler systems machinery doesn't require conditions at p.

But: For the arithmetic applications, we'll need to be precise about conditions at p. Hence we will need p-adic Hodge Theory.

Fact. *There exists a specific $H^1_f(\mathbb{Q}_p,V) \subset H^1(\mathbb{Q}_p,V)$, which is a 1-dimensional $\mathbb{Q}_p$-vector space where $V = T\otimes\mathbb{Q}_p$, such that its Selmer group is equal to the usual Selmer group.*

There exists an isomorphism, $\exp^* : H^1_s(\mathbb{Q}_p,V) \to \mathbb{Q}_p\cdot\omega_E$, where ω_E is the regular differential for E.

Theorem 9.8 ((Kato))**.** *Let $E/\mathbb{Q}$ be an elliptic curve, T a Tate module, $\underline{c}$ the Euler system described by Aurel, $\underline{c}' = \underline{c}^{\chi_p^{-1}}$. Then there exists $r_E \in \mathbb{Z}\setminus\{0\}$ such that $\exp^*(\mathrm{loc}_p^s(c_1')) = \frac{r_E L_{Np}(E,1)\omega_E}{\Omega_E}$, where $\Omega_E =$ real period of E corresponding to ω_E.*

Corollary 9.9. *If $L_{Np}(E,1)\neq 0$, then $E(\mathbb{Q})$ and $\text{Ш}(E/\mathbb{Q})$ are finite.*

Proof. Euler factors are non-zero at $\ell | Np$. $\square$

Theorem 9.10. *Let $L/\mathbb{Q}$ be an abelian number field, $\chi : \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{C}^*$. If $L(E,\chi,1)\neq 0$ then $E(L)^\chi = \{P \in E(L)\otimes\mathbb{C} : \sigma(P) = \chi(\sigma)P \forall\sigma \in \mathrm{Gal}(L/\mathbb{Q})\}$ and $\text{Ш}(E/L)^\chi$ are finite.*

10 Euler Systems: Some Further Topics

10.1 Recap

Let $E/\mathbb{Q}$ be an elliptic curve.

Theorem 10.1. *If $L(E,1) \neq 0$, then $E(\mathbb{Q})$ is finite, and $Ш_{p^\infty}(E/\mathbb{Q})$ is finite for "many" primes p.*

Kolyvagin: Proof using Heegner points in $E(K_m)$ where K is imaginary quadratic field, K_m ring class field (abelian extension of K such that $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Gal}(K_m/K)$ as -1)

Kato: Proof using Siegel units - cohomology classes for T_pE over cyclotomic fields.

Kato can tell you about $L(E,\chi,1)$ where χ is a Dirichlet character

Kolyvagin: can tell you about $L(E/K,\psi,1)$ where ψ is a character of a ray class group of K such that $\psi^\sigma = \psi^{-1}$.

1. Can we say something about arbitrary abelian extension of K ($\leftrightarrow L$-functions $L(E/K),\psi,1)$ for any ray class character ψ)?
2. Are there Euler systems for other Galois representations (not just T_pE)?

10.2 An Euler System for two modular forms

Theorem 10.2. *Let f, g be two modular forms of weight 2. $\rightsquigarrow$ Galois representations $T_p(f), T_p(g)$. Then there exists an Euler system for $T = T_p(f) \otimes T_p(g)$.*

Starting point: Siegel units,

$$_cg_{\alpha,\beta} = c^2 g_{\alpha,\beta} - g_{c\alpha,c\beta}$$

$$g_{a/N,b/N} = q^w \prod_{n\geq 0}\left(1 - q^n q^{a/N} e^{2\pi i b/N}\right)\prod_{n\geq 1}\left(1 - q^n q^{-a/N} e^{-2\pi i b/N}\right)$$

where $w = \frac{1}{12} - \frac{a}{2N} + \frac{a^2}{2N^2}$.

Not a modular form, it has poles at cusps (like the j-function). This lives in $\mathcal{O}(Y(N))^*$. In particular can take $a = 0$, $b = 1$, $_cg_{0,1/N} \in \mathcal{O}(Y_1(N))^* \to H^1_{\text{ét}}(Y_1(N), \mathbb{Z}_p(1))$ using a Kummer map.

Consider $\Delta : Y_1(N) \hookrightarrow Y_1(N) \times Y_1(N)$ diagonally. We get the pushfoward $\Delta_* : H^1_{\text{ét}}(Y_1(N), \mathbb{Z}_p(1)) \to H^3_{\text{et}}(Y_1(N)^2, \mathbb{Z}_p(2)) \to H^1(\mathbb{Q}, T_p(f) \otimes T_p(g))$ for all f, g weight 2 level N.

This idea is due to Beilinson in 1984 ("Beilinson - Flach elements")

Theorem 10.3 (Lei-Loffler-Zerbes)**.** *Can extend this to an Euler System as follows: for $m \geq 1$, consider $\Delta_m : Y_1(m^2N) \to Y_1(N)^2$ defined by $z \mapsto (z, z + \frac{1}{m})$. Then take $c_m = (\Delta_m)_*(_cg_{0,1/m^2N})$. This is only defined over $\mathbb{Q}(\mu_n)$ not $\mathbb{Q}$.*

(40 pages later) Some version of norm-compatibility relation holds.

10.3 Twisting

Recall: In Kato's setting, had to twist from $T_p(E)(1)$ to $T_p(E)$. This was possible because, modulo any power p^r of p, $T_p(E)(1) \cong T_p(E)$ as representations of $\mathbb{Q}(\mu_{p^r})$.

Interesting cases for $T_p(f) \otimes T_p(g)$ are not the ones we've immediately get at. Their elements are related to $L(f, g, 1)$ always being 0 (like $L(E, 0) = 0$ in Kato's case).

Want to consider weight f is 2 and weight g is 1.

Idea: The Galois representation of $g \mod p^r$ shows up in cohomology of $Y_1(Np^r)$.

Special case: K imaginary quadratic field, ψ ray class character of K. ψ gives a weight 1 modular form θ_ψ. This answers Q1.

10.4 More Euler systems?

Suppose we have some variety $X$and we want Euler Systems in cohomology of X.We look for subvariety $Y \hookrightarrow X$ where Y is a modular curve (or product of modular curves). If you are lucky and pushforward of Siegel units lands in the right degree, then maybe that will give an Euler System.

This is reasonable if X and Y are <u>Shimura varieties</u> (comes from Matrix groups, like modular curves come from SL_2 over $\mathbb{Q}$)

Eg,

- $\mathrm{GL}_2 \hookrightarrow \mathrm{GL}_2 \times \mathrm{GL}_2$ (BF elts)
- $SO_2 \hookrightarrow \mathrm{GL}_2$ (Heegner points)
- $\mathrm{GL}_2 \times \mathrm{GL}_2 \hookrightarrow GSp_4$
- $\mathrm{SL}_2 \cong SU(1,1) \hookrightarrow SU(2,1)$

Problem: Very hard to show that these Euler Systems are not 0.