

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, $L(E,s) = \prod_{p \mid N} (1 - a_p p^{-s})^{-1} \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1}$ with $\text{Re}(s) > 3/2$.

and $a_p = \begin{cases} p + 1 - \# E(\mathbb{F}_p) & p \mid N \\ 0 & E \text{ additive at } p \\ 1 & \text{ split multi at } p \\ -1 & \text{ non split multi at } p \\ \end{cases}$, $N = \text{cond}(E)$.

Note. $L(E,1)'' = \prod_{p \mid N} (1 - \frac{p}{\# E(\mathbb{F}_p)}) = \prod_{p} \mathbb{F}_p$ where $N_p = \# E(\mathbb{F}_p)$.

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

1. $\text{ord}_{s=1} L(E,s) = \text{rk}_E E(\mathbb{Q}) = r$

2. $\lim_{s \to 1} \frac{L(E,s)}{(s-1)^r} = \# \text{III}(E, \mathbb{Q}) \frac{\det((P_i,P_j))}{\# E(\mathbb{Q})_{\text{tor}}} \prod_{v | N} c_v$, where $\{P_1\}$ 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 $\&(E,s) = (2\pi)^{-s} \Gamma(s) N^{s/2} L(E,s)$. We have $\&(E,s) = -\epsilon \& (E,2-s)$ 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 sign$(E,Q)$.

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

1.2 Class field theory

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

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

Lemma. Let $G_n = \text{Gal}(K_n/K_1)$. Then $G_n \cong \text{Pic}(O_n)/\text{Pic}(O_K) \cong (O_K/nO_K)^* / (\mathbb{Z}/n\mathbb{Z})^*$. In particular, if $\ell$ is an odd prime unramified in $K$, then $G_\ell$ 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 $G_n \cong \prod_{\ell | n} G_\ell$. 

Euler Systems
1.3 Complex Multiplication

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

**Theorem** (Main Theorem of Complex Multiplication). Let $\sigma \in \text{Aut}(\mathbb{C}/K) \sim \sigma|_{\mathcal{N}_n} \in \text{Gal}(K_n/K) \cong \text{Pic}(O_n)$ so $\sigma|_{\mathcal{N}_n} \sim [a_{\sigma}]$.

\[
\chi_n = [\mathbb{C}/a_{\sigma}^{-1} \rightarrow \mathbb{C}/\mathcal{N}_n^{-1}a_{\sigma}^{-1}]
\]

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

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

Also have the Trace map: $\text{Tr}_\ell : \text{Div}X_0(N)(K_n) \rightarrow \text{Div}X_0(N)(K_n)$.

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

1. As elements in $\text{Div}X_0(N)(K_n)$, $\text{Tr}_\ell(\chi_n) = \begin{cases} T_\ell \chi_n & \text{if } \ell \nmid n \text{ is inert in } K \\ (T_\ell - \text{Frob}_0 - \text{Frob}_0^{-1}) \chi_n & \text{if } \ell = n \text{ split in } K \\ T_\ell \chi_n - \chi_n/\ell & \ell | n \end{cases}$

2. If $\ell \nmid n$ is inert in $K$, $\lambda = \ell \mathcal{O}_K$, $\lambda_n$ is a prime in $K_n$ above $\lambda$. Then $\text{red}_{\lambda_n}(\chi_n) = \text{red}_{\lambda_n}(\chi_n^{\text{Frob}_\lambda}) \in X_0(N)(\mathbb{F}_{\lambda_n})$.

1.4 Heegner points on $E$

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

$y_K = \text{Tr}_{K/K}(y_n)$ (in $E(K)$) is “the basis Heegner point”

**Proposition.** $\ell \nmid ND$:

\[
\text{Tr}_\ell(y_n) = \begin{cases} a_\ell y_n & \text{if } \ell \nmid n \text{ is inert in } K \\ (a_\ell - \text{Frob}_\lambda - \text{Frob}_\lambda^{-1}) y_n & \text{if } \ell = n \text{ split in } K \\ a_\ell y_n - y_n/\ell & \ell | n \end{cases}
\]

\[
\text{red}_{\lambda_n}(y_n) = \text{red}_{\lambda_n}(y_n^{\text{Frob}_\lambda}) 
\]

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

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 $\{ f : G \rightarrow M | f \text{ continuous and } \forall g, h \in G, f(gh) = f(g) + f(h) \}$

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

**Definition 2.1.** $H^1(G, M) = \{ \text{1-cocycles} \}/\{ \text{1-coboundary} \}, H^0(G, M) = M^G$

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

\[
0 \rightarrow M^G \rightarrow M^G \rightarrow M''^G \rightarrow H^1(G, M') \rightarrow H^1(G, M) \rightarrow H^1(G, M'') \rightarrow H^2 \ldots
\]

We have some useful maps between cohomology groups:
• Let $H \leq G$, we get a map $\text{Res} : H^1(G, M) \to H^1(H, M)$.

• Let $H < G$ be a normal closed subgroup of $G$, then we have $\text{inf} : H^1(G/H, M^H) \to H^1(G, M)$

We have the following relationship between $\text{inf}$ and $\text{Res}$ called the Hochschild-Serre spectral sequence

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)^{G/H} \to H^2(G/H, M^H) \to \ldots$$

### 2.2 Galois Cohomology

Fix prime $\ell, p$ and $|K : \mathbb{Q}| < \infty$ and let $K^\text{un}$ be the maximal unramified extension of $K$ and let $I_K = \text{Gal}(K/K^\text{un})$ be the Inertia group.

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

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 $T^* = \text{Hom}(T, M_p)$. **Fact.** If $\ell \neq p$ and $T$ is unramified then $H^1(G_K^\text{un}, T)$ and $H^1(G_K^\text{un}, T^*)$ 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 $H^1_{j,F}(G_K, T)$.

We call the quotient $H^1_{j,F}(G_K, T) := H^1(G_K, T)/H^1_{j,F}(G_K, T)$ the singular quotient.

$$0 \to H^1_{j,F}(G_K, T) \to H^1(G_K, T) \to H^1_{\text{Sing},F}(G_K, T) \to 0 \ (\dagger)$$

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

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

### 2.3 Local cohomology for elliptic curves

Let $E$ be an elliptic curve over $K$. We let $T = [E] = E(\overline{K})[p]$. 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

$$0 \to E[p] \to E(\overline{K}) \xrightarrow{\delta} E(\overline{K}) \to 0$$

If we take the associated long exact sequence

$$0 \to E[p]^{G_K} \to E(\overline{K})^{G_K} \to E(\overline{K})^{G_K} \to H^1(G_K, E[p]) \to H^1(G_K, E(\overline{K})) \to \ldots \ (\ddagger)$$

From $(\ddagger)$ we get:

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

where $\delta$ 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 $\delta$ 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 $v$, $G_v = \text{Gal}(\overline{K}_v/K_v)$ 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 $\text{Res}_v : H^1(K,T) \to H^1(K_v,T)$.

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 $H^1_{f,F}(K_v,T) = H^1(K_v^{\text{nr}}, T_{I_v})$ almost everywhere.

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

If we take $E$ to be an elliptic curve over $K$ then $\text{Sel}_E(K,T)$ is called the geometric global Selmer structure.

3.2 Global Duality

**Definition 3.3.** Let $F$ be a global Selmer structure on $T$. The Cartier dual Selmer structure $F^* = \text{Hom}_{\mathbb{F}_p}(T,\mu_p)$ 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 $a \triangleleft \mathcal{O}_K$, we define $\text{Sel}_a(K,T) = \{ c \in H^1(K,T) : c_v \in H^1_{f,F}(K_v,T) \text{ for all } v \nmid a \}$.

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

$$0 \to \text{Sel}(K,T) \to \text{Sel}_a(K,T) \to \bigoplus_v \text{Sel}_{a_v}(K_v,T) \to 0$$

$$0 \to \text{Sel}(K,T^*) \to \text{Sel}(K,T)^\vee \to \bigoplus_v \text{Sel}_{a_v}(K_v,T^*) \to 0$$

We have $\bigoplus_v \text{Sel}_{a_v}(K_v,T) \cong \bigoplus_v \text{Sel}_{a_v}(K_v,T^*)^\vee$. We can put the two sequences above together as follows

$$0 \to \text{Sel}(K,T) \to \text{Sel}_a(K,T) \to \bigoplus_v H^1_{f,a_v}(K_v,T) \to \text{Sel}(K,T)^\vee \to \text{Sel}_a(K,T)^\vee \to 0$$

**Proposition 3.4.** The above sequence is exact.

The exactness of this sequence yields

$$0 \to \left( \bigoplus_v H^1_{f,a_v}(K_v,T) \right) / \text{im}(\text{Sel}_a(K,T)) \to \text{Sel}_a(K,T)^\vee \to \text{Sel}_a(K,T^*)^\vee \to 0$$

3.3 Bounding $\text{Sel}_a$

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

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

If $S \subseteq H^1(K,T)$ finite dimensional $\mathbb{F}_p$-subspace $S^* = \{ s \in S : s_v \in H^1_{f,F}(K_v,T) \text{ and } (s_v = 0, \forall v|a) \}$. We can find a finite Galois extension $M/L$ such that $S \subseteq \text{inf}(H^1(M/K,T))$. Assume that $\tau \in \text{Gal}(L/K)$ is a non-scalar involution and that it extends to an involution in $\text{Gal}(M/K)$. Let $\{ \gamma_1, \ldots, \gamma_r \}$ be a set of group generators for $\text{Gal}(M/L)$. 
Proposition 3.5. Let $\omega_1, \ldots, \omega_r$ be places of $M$ such that $\text{Frob}_{M/K}(w_i) = \tau \gamma_i$. Let $v_i$ be the restricted places to $K$ and set $a = v_1 \cdots v_r$. Then we have $S^a \subseteq \inf(H^1(L/K, T))$.

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

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

\[
\begin{array}{c|c|c|c|c}
M & L & L_0 & K & K_0 \\
\hline
\end{array}
\]

$S$ will be a finite dimensional subspace of $H^1(M/K, T)$ and $\tau$ will be a non-scalor involution in $\text{Gal}(M/K_0)$ which projects to the non-trivial element of $\text{Gal}(K/K_0)$. By the action of $\tau$ 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 $\sigma \in \text{Gal}(M/L_0)$ be such that $\tau \sigma \tau^{-1} = \sigma^{-1}$. We again let $\{\gamma_1, \ldots, \gamma_r\}$ be a set of generators of $\text{Gal}(M/L)$.

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

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 $\text{Cond}(E)$ 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. $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_p)$
3. $y_k \notin pE(K)$

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

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

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

Recall: $\text{Sel}^a(K, E[p])$ restricted. $\text{Sel}_a(K, E[p])$ relaxed.

$\text{Sel}_a(K, E[p])$ relaxed.

this gives the exact sequence

$$\text{Sel}_a(K, E[p]) \to \bigoplus_{v \mid a} H^1(K_v, E[p]) \to \text{Sel}(K, E[p])^\vee \to \text{Sel}^a(K, E[p])^\vee \to 0$$

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 $a$ of $K$ such that $\text{Sel}^a(K, E[p])^\pm \subseteq H^1(L/K, E[p])^\pm$. Moreover if we fix $\sigma \in \text{Gal}(L/L_0)$ such that $\tau \sigma \tau^{-1} = \sigma^{-1}$.

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

**Lemma 4.3.** Let \( \ell \) be a prime of \( \mathbb{Q} \) such that

1. \( E \) has good reduction at \( \ell \)
2. \( \ell \neq p \)
3. \( \text{Frob}_{K(E[p])/\mathbb{Q}} \sim \tau \)

Then \( H^1_S(K, E[p]) \) 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 \( \ell \) and so all primes above \( \ell \) in \( K \) are unramified in \( K(E[p]) \). \( \text{Frob}_{K/E} \sim \tau \neq \text{id} \), the residue class of \( \ell \) in \( K/E \) is 2, and the residue class degree of \( \ell \) in \( K(E[p])/K \) is 1. Hence \( \ell \) splits completely in \( K(E[p])/K \). So \( K(E[p])_\ell = K_\ell \), i.e., \( E[p] \subseteq E(K_\ell) \).

\[
H^1_S(K_\ell, E[p]) \cong H^1(I_\ell, E[p])^\text{G}_{K_\ell} \\
= \text{Hom}_{\text{G}_{K_\ell}}(I_\ell, E[p]) \\
= \text{Hom}_{\text{G}_{K_\ell}}(I_\ell/pI_\ell, E[p])
\]

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

4.2 \(-\epsilon\) eigenspace

**Lemma 4.5.** \( H^1(L_0/K, E[p]) = 0 \) for all \( i \)

**Lemma 4.6.** \( H^1(L/K, E[p]) \) is 1-dimensional \( \mathbb{F}_p \)-vector-space generated by \( \kappa(y_K) \).

Consider \( \text{Gal}(L/L_0) \to E[p] \) 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 \( H^1(L_0/E[p])^{\text{Gal}(L_0/K)} \).

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

**Theorem 4.8.** \( \text{Sel}(K, E[p])^{\tau_\ell} = 0 \).

**Proof.** \( 1 \neq \sigma \in \text{Gal}(L/L_0) \) such that \( \tau \sigma \tau = \sigma^{-1} \). There exists a such that \( \text{Sel}^a(K, E[p])^{\tau_\ell} \subset H^1(L/K, E[p])^{\tau_\ell} \). But the second thing is 1-dimensional and is generated by \( \kappa(y_K) \). If we pick a such that it is divisible only by primes lying over \( \ell_1, \ldots, \ell_r \in \mathbb{Z} \) with \( \text{Frob}_{L_i/Q} \sim \tau_i \sigma \). \( \oplus_{\ell_i} \text{H}^1(K, E[p])^{\tau_\ell} \) has dimension \( r \), but we use the fact there exists \( c(\ell_1) \) such that \( c(\ell_1) \neq 0 \) 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 $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_p)$.
• $\tau$ 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 $\ell$ is inert in $K/\mathbb{Q}$ and splits in $K(E[p])/K$. Setting $\lambda = \ell O_K$, $\lambda$ splits completely in $K_n$ and is totally ramified in $K_{n\ell}$. In the case $n$ and $\ell$ are coprime we get:

Note that $K_{n,\lambda} = K_{\lambda}$.
• $\text{red}_{\lambda_n}$ the reduction map $E(K_{n,\lambda_n}) \to E(\mathbb{F}_p)$.

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 $H^1_f(K, E[p]) = \text{im} k$.

We also recall that if $E$ has good reduction at $\ell$, then $H^1_s(K_{\lambda}, E[p]) \cong \text{Hom}(I_{\lambda}, E[p])^{G_{K_{\lambda}}^n}$, with $G_{K_{\lambda}}^n = \text{Gal}(K_{n,\lambda}^n/K_{\lambda})$.

**Theorem 5.1.** For any integer $n$ not dividing $ND$ there exists a point $y_n \in E(K_n)$ such that

\[ \ell \nmid ND \text{ then } Tr_{\ell y_n} = a_{\ell y_n} \in E(K_n) \]
\[ \ell \nmid ND \text{ and is inert in } K, \text{red}_{\lambda_n}(y_{n\ell}) = \text{red}_{\lambda_n}(\text{Frob}_{K_{n,\lambda_n}} \cdot y_n) \]

There exists $\sigma \in \text{Gal}(K_n/K)$ such that $\tau y_n = \sigma y_n$ in $E(K)/E(K)_{\text{tors}}$.

• $L_0 = K(E[p])$, 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 $p$
• $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_p)$
• $y_K \notin pE(K)$

Then $\text{Sel}(K, E[p])$ 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 $\text{Sel}(K, E[p])^{\pm \epsilon}$ using the restricted and relaxed $\text{Sel}^\pm(K, E[p])$ and $\text{Sel}_\alpha(K, E[p])$. 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 $\text{Frob}_{L_0/L} \sim \tau$ and $\ell$ not splitting completely in $L/L_0$. There exists $c(\ell) \in \text{Sel}_\lambda(K, E[p])^{\pm \epsilon}$ with $c(\ell)^* \neq 0$ in $H^1(K_{\lambda}, E[p])$.

**Proposition.** Assume that $y_k \notin pE(K)$. Let $\ell \in \mathbb{Q}$ be a prime with $\text{Frob}_{L/L} \sim \tau$ and $\ell$ not splitting completely in $L'/L$. There exists $c(q\ell) \in \text{Sel}_\lambda(K, E[p])^{\pm \epsilon}$ with $c(q\ell)^* \neq 0$ 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 \( \text{Frob}_{K(E[p])/K} \sim \tau \). This implies that \( \ell \) is inert in \( K/Q \) and splits in \( K(E[p])/K \), and that \( E \) has good reduction at \( \ell \).

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

**Proof.** As on \( E[p] \), complex conjugation and \( \text{Frob} \) are conjugate, their characteristic polynomial must be the same mod \( p \)

Recall that, for \( \ell \in \mathcal{R}, G_{\ell} = \text{Gal}(K_{\ell}/K) \) is cyclic (Marc’s talk) of order \( \ell + 1 \) (as \( \ell \) is inert in \( K \)).

Fix a generator \( \sigma_{\ell} \) and for a prime \( \ell \) define

- \( D_{\ell} = \sum_{i=1}^{\ell} i \sigma_{\ell}^{i} \),
- \( T_{\ell} = \sum_{i=0}^{\ell-1} \sigma_{\ell}^{i} \).
- 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 \( \gamma_{i} \) be a set of coset representative for \( G_{n} \) in \( \text{Gal}(K_{n}/K) \). \( T = \sum_{i} \gamma_{i}, T^{-1} = \sum_{i} \gamma_{i}^{-1} \).

**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 \( (\sigma_{\ell} - 1)D_{n}y_{n} \in \text{pE}(K_{n}) \). This is calculations using the identity \( (\sigma_{\ell} - 1)D_{\ell} = \ell + 1 - T_{\ell} \), Theorem 5.1 and Lemma 5.2.

We define \( P_{n} = TD_{n}y_{n} \in E(K_{n}) \). If we consider \( P_{n} \) in \( E(K_{n})/\text{pE}(K_{n}) \), then by the above it is \( \text{Gal}(K_{n}/K) \)-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 \( P_{n} \in E(K_{n})/\text{pE}(K_{n}) \)

\[
\begin{align*}
E(K_{n})/\text{pE}(K_{n}) & \xrightarrow{\kappa} H^{1}(K_{n}, E[p]) \\
H^{1}(K_{n}, E[p]) & \xrightarrow{\text{res}} H^{1}(K_{n}, E[p])^{\text{Gal}(K_{n}/K)}
\end{align*}
\]

As the Kummer map is equivariant, \( \kappa(P_{n}) \in H^{1}(K_{n}, E[p])^{\text{Gal}(K_{n}/K)} \).

**Lemma 5.4.** The restriction map is an isomorphism

**Proof.** Using long exact sequence have that the kernel and cokernel of res is \( H^{i}(K_{n}/K, E[p])^{\text{Gal}(K_{n}/K)} \) 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 \( c(n) \in H^{1}(K, E[p])^{(-1)^{k+1}}. \)
Proof. As \( \tau \) commutes with \( \kappa \) and \( \text{res} \), we show \( \tau P_n = (-1)^k \ell P_n \) in \( E(K_n)/pE(K_n) \).

\[
\tau P_n = \tau T \prod_{\ell | n} \mathcal{D}_\ell \eta_n \quad \text{Definition} \\
= T^{-1} \prod_{\ell | n} \tau \mathcal{D}_\ell \eta_n \quad \text{by } \tau T = T^{-1} \tau \\
= T^{-1} \prod_{\ell | n} (\ell T_\ell - \sigma_\ell D_\ell) \tau \eta_n \\
= T^{-1} \prod_{\ell | n} (\ell T_\ell - \sigma_\ell D_\ell) \xi \eta_n \quad \text{Lemma 5.1} \\
= T^{-1} \prod_{\ell | n} (-\sigma_\ell D_\ell) \xi \eta_n \quad \text{since } \tau \ell \eta_n = a \ell \eta_n / \ell = 0 \text{ in } E(K_n)/pE(K_n) \\
= (-1)^k \ell \sigma_\ell T^{-1} D_n \eta_n
\]

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

Lemma 5.6. Fix \( n = \ell_1 \ldots \ell_s \mathcal{R} \), then \( c(n) \in \text{Sel}_{\lambda_1 \ldots \lambda_s} (K, E[p]) \)

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

\[
\begin{array}{cccc}
E(K_\nu)/pE(K_\nu) & \xrightarrow{\kappa} & H^1(K_\nu, E[p]) & \xrightarrow{\text{res}} & \text{Hom}(I_\nu, E[p]) \\
\downarrow & & \downarrow & & \downarrow \\
E(K_{n,w})/pE(K_{n,w}) & \xrightarrow{\kappa} & H^1(K_{n,w}, E[p]) & \xrightarrow{\text{res}} & \text{Hom}(I_\nu, E[p])
\end{array}
\]

where we use \( \text{Hom}(I_\nu, E[p])^{G_K}_{\nu} \subseteq \text{Hom}(I_\nu, E[p])^{G_K}_{\nu} \). Then it is just a matter of diagram chasing.

By definition \( \text{res}(n)_\nu = \kappa(P_n) \), so \( \text{res}(n)_\nu^* = 0 \). Hence \( c(n)_\nu^* = 0 \).

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

\[
Q_{n,\ell} = \frac{\ell + 1}{p} TD_n \gamma_n - \frac{\alpha_\ell}{p} P_n \quad (\dag)
\]

(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, \( Q_{n,\ell} \) is the unique point in \( K_{n,\ell} \) with that property.

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

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

\[
\text{red}_{\lambda_n}(y_{n,\ell}) = \text{red}_{\sigma^{-1} \lambda_n}(\text{Frob}_{K_n/K}(\sigma^{-1} \lambda_n) \cdot y_{n,\ell}) \\
\text{red}_{\lambda_n}(\sigma y_{n,\ell}) = \text{red}_{\lambda_n}(\sigma \text{Frob}_{K_n/K}(\sigma^{-1} \lambda_n) \cdot y_{n,\ell})
\]

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

\[
\text{red}_{\lambda_n}(T D_n \lambda_n \ell) = \text{red}_{\lambda_n}(\text{Frob}_{K_n/K} \lambda_n \cdot T D_n \eta_n)
\]
Hence combining this with (†) we get
\[
\text{red}_{\lambda,n}(Q_{n,\ell}) = \text{red}_\lambda \left( \left( \frac{\ell + 1}{p} \cdot \text{Frob}_{K_n/K} \lambda - \frac{a_\ell}{p} \right) P_n \right)
\]

Claim: \((\ell + 1)\text{Frob}_{K_n/K} \lambda_n - a_\ell\) annihilates \(E(\mathbb{F}_\lambda)\). Note that \(E(\mathbb{F}_\lambda) = E(\mathbb{F}_\lambda)^+ \oplus E(\mathbb{F}_\lambda)^-\) as \(\text{Frob}_{K_n/K} \lambda_n\) 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 \(\text{Frob}_{K_n/K} \lambda_n\) is the reduction of a complex conjugation, so \(\text{Frob}_{K_n/K} \lambda_n P_n = \tau P_n\), which by the proof of Lemma 2.4 \(\tau P_n = (-1)^n \ell P_n\) in \(E(K_n)/pE(K_n)\), so \(\text{Frob}_{K_n/K} \lambda_n P_n = \nu P_n + pQ\) for some \(\nu \in \{\pm 1\}\) and \(Q \in E(K_n)\).

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

We now claim that the \(p\)-primary part of \(E(\mathbb{F}_\lambda)^+\) is cyclic. First we note that \(p|\ell + 1 \pm a_\ell\), 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 \(p^2 > |E(\mathbb{F}_\lambda)^+[p]| + |E(\mathbb{F}_\lambda)^-| = |E(\mathbb{F}_\lambda)|p\) which is a contradiction (as \(\ell\) is a good prime, \(|E(\mathbb{F}_\lambda)|p\)). We can conclude that \(E(\mathbb{F}_\lambda)^+/pE(\mathbb{F}_\lambda)^+\) is cyclic of order \(p\).

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

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

**Proof.** Since \(\ell \in \mathcal{R}\) we have \(H_1^\lambda(K_\lambda, E[p]) = \text{Hom}(I_\lambda, E[p])^{G_n^\lambda}\) so we can view \(c(n\ell)_A^\lambda\) as a homomorphism \(I_\lambda \to E[p]\). We shall show this factors as follows:

\[
\begin{array}{ccc}
I_\lambda & \xrightarrow{} & E[p] \\
\downarrow & & \uparrow \\
I_\lambda / I_{\lambda,n} & \cong & G_\ell
\end{array}
\]

To see this we consider the diagram

\[
\begin{array}{ccc}
H^1(K_\lambda, E[p]) & \xrightarrow{\text{res}} & E(K_\lambda)/pE(K_\lambda) \\
\downarrow & & \downarrow \kappa \\
H^1(K_{n\ell,n\ell}, E[p]) & \xrightarrow{\text{Hom}(I_{n\ell,n\ell}, E[p])} & \text{Hom}(I_{n\ell}, E[p])
\end{array}
\]

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

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

\[
\begin{array}{ccc}
I_\lambda \ar@{-}[d] & \xrightarrow{\kappa} & E[p] \\
K_{n\ell,n\ell} & \xrightarrow{G_\ell} & I_\lambda
\end{array}
\]

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

Fix \(Q \in E(K_\lambda)\) 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 \(p\)th 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 $\text{resc}(n\ell) = \kappa(P_{n\ell})$, 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 $c(n\ell)(\sigma) = (\sigma - 1)Q - Q_{n,\ell}$ (as we had $pQ_{n,\ell} = (\sigma - 1)P$).

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

Hence $c(n\ell)(\sigma) = 0$ if and only if $\text{red}(Q_{n,\ell}) = 0$ 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 $\text{Frob}_{L_0/\mathbb{Q}} \sim \tau$ and $\ell$ not splitting completely in $L/L_0$. There there exists $c(\ell) \in \text{Sel}_1(K, E[p])^{-\tau}$ with $c(\ell)^* \neq 0$ 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 $c(\ell) \in \text{Sel}_1(K, E[p])^{-\tau}$. Lemma 5.8 tells us that $c(\ell)^* \neq 0$ if and only if $P_1 \neq pE(K_\lambda)$.

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 $\lambda$ splits completely in $L/L_0$. By assumption it does not, hence $y_k \notin pE(K_\lambda)$.

For the $\text{Sel}(K, E[p])^{-\tau}$ space we need to reintroduce some work done by Alex. Let $q$ be a prime satisfying the previous proposition, so $c(q) \in \text{Sel}_q(K, E[p])^{-\tau}$ and $c(q)^*_q \neq 0$. 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 $\ell$ be a prime with $\text{Frob}_{L_0/\mathbb{Q}} \sim \tau$. Then $P_q \in pE(K_\lambda)$ if and only if $\ell$ splits completely in $L'/L$.

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

**Proof.** By the same argument as above we have $c(q\ell) \in \text{Sel}_q(K, E[p])^{-\tau}$. Then using the previous lemma and Lemma 5.8 we have that $c(q\ell)^*_q \neq 0$ in $H^1(K_\lambda, E[p])$.

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

6 (Angelos)

6.1 Notation

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

Comment: Since, $A$ may not be a discrete $\mathbb{G}_K$-module, then it doesn’t hold that $H^i(K, A) = \lim_{\leftarrow} H^i(G_m, A_m)$ 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

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

is perfect

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

If $F$ 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 $F^*$ for $A^*$ by

$$H^1_f(K_v, A^*) = \lim_{\longleftarrow} H^1_f(K_v, A_m).$$

**Proposition 6.2.** It holds that $H^1_f(K, A) = \lim H^1_f(K, A_m)$ and $H^1_f(K, A^*) = \lim H^1_f(K, A_m^*)$.

**Definition 6.3.** If $F, G$ are Selmer structure of $A$, we say that $G \subseteq F$ if $H^1_f(K_v, A) \subseteq H^1_f(K_v, A)$ for all $v$.

Note that if $G \subseteq F$ then

- $H^1_f(K, A) \subseteq H^1_f(K, A)$
- $F^* \subseteq G^*$

**Theorem 6.4.** Suppose $F_1, F_2$ are Selmer structure for a finite $G_K$-module $A$ and $F_1 \subset F_2$. Then

- $0 \to H^1_f(K, A) \to H^1_f(K, A) \xrightarrow{\oplus_{\text{res}}} \bigoplus H^1_f(K_v, A)/H^1_f(K_v, A)$
- $0 \to H^1_f(K, A) \to H^1_f(K, A) \xrightarrow{\oplus_{\text{res}}} \bigoplus H^1_f(K_v, A)/H^1_f(K_v, A)$

Summing over $v$ such that $H^1_f(K_v, A) \neq H^1_f(K_v, A)$. The images of $\oplus_{\text{res}}$ are orthogonal complement of each other with respect to the Tate pairing.

From now on $K$ is $\mathbb{Q}$.

**Definition 6.5.** The canonical Selmer structure $F_{\text{con}}$ for $A$ is defined to be

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

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

**Proposition 6.7.** If $F = F_{\text{con}}$. The following are the same

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

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

6.3 The Hypotheses

**H.1** $A$ is an absolutely irreducible $\mathbb{F}_p[G_Q]$-module, not isomorphic to $\mathbb{F}_p$ or $\mu_p$

**H.2** There is $\tau \in G_Q$ such that $\tau = 1$ on $\mu_{p\infty}$ and $A/(\tau - 1)A$ is free of rank one over $\mathbb{Z}_p$

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

**H.4** Either $A \not\cong \overline{A}$ or $p \geq 5$
Let $\Sigma$ be a finite set of primes which contains $\infty$, $p$ and $\ell$ such that $A$ is ramified at $\ell$ and all $\ell$ such that $H^1_{\ell}(\mathbb{Q}_\ell, A) \neq H^1_{un}(\mathbb{Q}_\ell, A)$. For every $\ell \in \Sigma$, $H^1(\mathbb{Q}_\ell, A)/H^1_{\ell}(\mathbb{Q}_\ell, A)$ is torsion-free.

Remark. $\mathcal{F}_{con}$ satisfies H.5
Let $A = T_p(E)$ with $\mathcal{F}_{con}$ 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 $\Sigma$ be a finite set of primes containing $\infty$, $p$ and all primes where $A$ ramifies. If $\ell \not\in \Sigma$, $P_\ell(x) = \det(1 - \text{Frob}_\ell x|_A) \in \mathbb{Z}_p[x]$. Let $\mathcal{N} = \{np^k : n$ is square free product of primes $\ell \not\in \Sigma, k \geq 0\}$.

**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 $\operatorname{ES}(A)$ denote the $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module of Euler system of $A$.

### 7 Kolyvagin Systems (Céline)

**Notation.** $K$ a non-archimedean local field of characteristic 0. $I_K \subset G_K, \phi \in \text{Gal}(K^{un}/K)$, $k$ 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 $H^1_L(K, A) \subset H^1(K, A)$ to be $H^1_L(K, A) = \ker[H^1(K, A) \to H^1(L, A)] = H^1(L/K, A)^{G_L}$.

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

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

**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

\[H^1_{\phi x}(K, A) \xrightarrow{\sim} A/(\phi - 1)A \xrightarrow{Q(\phi^{-1})} A^{\phi = 1} \to H^1_L(K, A)\]

**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 $\phi^{\phi x}$ is an isomorphism.
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 $A_n := A/p^nA$. For a given Selmer structure $\mathcal{F}$ for $A$, let $\Sigma$ be a finite set of places of $\mathbb{Q}$ containing $p$, $\infty$, $\ell$ where $A$ ramifies, all $\ell$ where $H^1_{\mathcal{F}}(\mathbb{Q}/\ell, A) \neq H^1(\mathbb{Q}/\ell, A)$.

**Definition 7.4.** Let $c$ be a positive integer such that $c$ is not divisible by any prime in $\Sigma$. We define $\mathcal{F}(c)$ for $A$ as follows, $H^1_{\mathcal{F}(c)}(\mathbb{Q}, A) = \left\{ \begin{array}{ll} H^1_{\mathcal{F}}(\mathbb{Q}, A) & \nu \nmid c \\ H^1(\mathbb{Q}, A) & \nu | c \end{array} \right.$.

Fix a $G_{\mathbb{Q}}$-module $A$ and a Selmer structure $\mathcal{F}$ for $A$ satisfying H.1 to H.5. If $\ell \notin \Sigma$, let $v(\ell) = \max\{m|l = 1 \text{ mod } p^m\}$ and $A_n/(\phi_\ell - 1)A_n$ 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 $\{\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbb{Q}, A_\nu(n))| n \in \mathcal{N}_A\}$ such that if $n\ell \in \mathcal{N}_A$ the following commutes

$$\begin{array}{c}
\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbb{Q}, A_\nu(n)) \\
\downarrow \\
H^1_n(\mathbb{Q}/\ell, A_\nu(n)) \\
\downarrow \phi^{\mu_1} \\
\kappa_{n\ell} \in H^1_{\mathcal{F}(n\ell)}(\mathbb{Q}, A_\nu(n\ell)) \xrightarrow{\text{res}} H^1(\mathbb{Q}/\ell, A_\nu(n))
\end{array}$$

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

### 7.3 Kolyvagin system construction

There exists a canonical map $ES(A) \rightarrow K_{\mathcal{S}}(A, \mathcal{F}_{\text{can}})$ such that if $\xi \rightarrow \kappa$ 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 $n = n_1n_2$, $\Gamma_n = \Gamma_{n_1} \times \Gamma_{n_2}$. With this identification $\Gamma_n = \prod_{\ell|n} \Gamma_\ell$.

For $\ell \notin \Sigma$, fix a generator $\sigma_\ell$ for $\Gamma_\ell$, 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 $H^1(\mathbb{Q}(\mu_n), A) \rightarrow H^1(\mathbb{Q}(\mu_n), A_\nu(n))$ 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 $H^1(\mathbb{Q}, A_\nu(n)) \rightarrow H^1(\mathbb{Q}(\mu_n), A_\nu(n))^{\Gamma_n}$.

Denote $\xi'_n$ to be the canonical inverse image of $D_n\xi_n$ as above. Let $\xi' = \{\xi'_n| n \in \mathcal{N}_A\}$.

Recall: $H^1(\mathbb{Q}/\ell, A_\nu(n)) = H^1_n(\mathbb{Q}/\ell, A_\nu(n)) \oplus H^1(\mathbb{Q}/\ell, A_\nu(n))$, $\text{Res}_\ell(\xi'_n), (\xi'_n)_{\ell, n}, (\xi'_n)_{\ell, \ell}$.

For $\ell'$ 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. $\text{Res}_\ell(\xi'_n) \in H^1(\mathbb{Q}/\ell, A_\nu(n))$ if $\ell | n$
3. $\phi^{\mu_1} \circ \text{Res}_\ell(\xi'_n/\ell) = (\xi'_n)_{\ell, n} \in H^1(\mathbb{Q}/\ell, A_\nu(n))$ for $\ell | n$

$\xi'_n$ satisfies 1 and 3, but $(\xi'_n)_{\ell, n} \neq 0$ 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 $\delta(K) = \max\{j|\kappa_1 \in p^jH^1_{\mathcal{F}}(\mathbb{Q}, A)\}$. 

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 $N$.

$T = T_p E$

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

$N = \{\text{squarefree product of } \ell \in \Sigma \times \mathbb{P}^1\}$

$\text{Co}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)} \zeta_n t = \begin{cases} P_t(\text{Frob}_\ell^{-1}) \zeta_n & \ell \neq p \\ \zeta_n & \ell = p \end{cases}$

8.1 Overview of construction

$(\mathcal{O}(Y(n, L))^*)^2 \xrightarrow{\mathcal{O}(Y(n, L))^*} H^1_{\text{et}}(Y(n, L), \mathbb{Z}_p(1))^2 \xrightarrow{\mathcal{O}(Y(n, L))^*} H^1_{\text{et}}(Y(n, L), \mathbb{Z}_p(1))^2$

$H^2_{\text{et}}(Y(n, L), \mathbb{Z}_p(2))$

$H^1(\mathbb{Q}(\zeta_n), H^1_{\text{et}}(Y(n, L), \mathbb{Z}_p(2))$

$H^1(\mathbb{Q}(\zeta_n), T(1))$

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

1. divisors $c^2(0) - E[c]$

2. For all a coprime to $c$, $[a]_* : \mathcal{O}(E \setminus E[ac])^* \to \mathcal{O}(E \setminus E[c])^*$, $[a]_* E \theta_E = e \theta_E$.

**Proof.**

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

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

**Definition 8.2.** $N \geq 3$, $Y(N)$ modular curve over $\mathbb{Q}$ represent $S \to \{(E, e_1, e_2) \to E/S, e_1, e_2 \in \text{basis of } N \text{ torsion}\}$. $Y(N)(\mathbb{C}) \cong (\mathbb{Z}/N\mathbb{Z})^* \times \Gamma(N)\backslash \mathbb{H}$. 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 $g_{\alpha, \beta} := L_{\alpha, \beta}(e \theta_E)$, $L_{\alpha, \beta} = ae_1 + be_2 : Y(N) \to E[N]$.

$GL_2(\mathbb{Z}/N\mathbb{Z}) \circ Y(N)$

**Proposition 8.4.**

1. $\sigma \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$, $\sigma^* g_{\alpha, \beta} = g_{\sigma(\alpha, \beta)\sigma}$

2. if a prime to $c$: then $g_{\alpha, \beta} = \prod_{\alpha' = \alpha, \beta' = \beta} g_{\alpha', \beta'}$.

**Definition 8.5.** Let $M, N \geq 3, M|L, N|L$ and define $Y(M, N) := G \setminus Y(L)$ where $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ mod } \begin{pmatrix} M & M \\ N & N \end{pmatrix} \right\}$. $GL_2(\mathbb{Z}/L\mathbb{Z})$, $S \to \{(E, e_1, e_2) : E/S, e_1 \in M \text{ torsion}, e_2 \in N \text{ torsion, } (a, b) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to ae_1 + be_2 \text{ is injective}\}$.

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

15
\( H^1_\text{et}(X, \mathbb{Z}_p(k)) \times H^2_\text{et}(X, \mathbb{Z}_p(k')) \overset{\iota}{\rightarrow} H^{i+j}_\text{et}(X, \mathbb{Z}_p(k+k')) \), \( f, g \in \mathcal{O}(X)^* \), \( \{ f, g \} := \kappa(f) \cup \kappa(g) \in H^2_\text{et}(X, \mathbb{Z}_p(2)) \).

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

**Definition 8.8.** \( M, N \geq 3 \), \((c, 6M) = 1\) and \((d, 6N) = 1\). Define \( c, dZ_{M,N} := \{ c, d \} \).

**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 \( Y(M', N') \rightarrow Y(M, N) \). The push-forwards of \( c, dZ_{M', N'} \) is \( c, dZ_{M,N} \).

If \( \ell \nmid N \)

\[
\begin{align*}
Y(M, N) & \xrightarrow{\sim} Y(M, N(\ell)) \oplus T'(\ell) \\
Y(M, N(\ell)) & \rightarrow Y(M, N)
\end{align*}
\]

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

\[
c, dZ_{M,N(\ell)} \mapsto \left( 1 - T'(\ell) \begin{pmatrix} 1/\ell & 0 \\ 0 & 1/\ell \end{pmatrix} \right)^* \cdot c, dZ_{M,N}
\]

Let \( Y_1(N) = Y(N, 1) \), \( n, N \geq 3 \), \( nL, N|L \) and \( \text{primes}(L) = \text{primes}(nN) \). Then \( Y_1(N)_{\mathbb{Q}(\zeta_n)} \cong G \backslash Y(L) \).

\[
G = \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\} \mod N, \det \equiv 1 \mod n \}
\]

\[
Y(n, L) \rightarrow Y_1(N)_{\mathbb{Q}(\zeta_n)}
\]

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

**Proposition.** \( \ell \nmid nN \)

\[
c, dZ_{1,n,\ell N} \mapsto \left( 1 - T'(\ell) \sigma_\ell^{-1} + \left( \begin{pmatrix} \ell & 0 \\ 0 & 1/\ell \end{pmatrix} \right)^* \sigma_\ell^{-2} \right) \cdot c, dZ_{1,n,N}
\]

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

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

**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. \( \Sigma = \text{finite set of prime containing } p, \infty, \) 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, \( \zeta \in ES(T) \). If \( \text{loc}_p^\circ(c_1) \neq 0 \in H^1(\mathbb{Q}_p, T)/H^1_\ell(\mathbb{Q}_p, T) \), then \( \text{Sel}(\mathbb{Q}, E[p^\infty]) \) is finite.

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

**Lemma 9.3.** If \( \text{loc}_p^\circ(c_1) \neq 0 \), then \( E(\mathbb{Q}) \) and \( \text{III}(E/\mathbb{Q})_{p^\infty} \) 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 $\chi_p$.

Motivation: Bloch-Kato conjecture: “existence of ‘nice’ cohomology classes” $\leftrightarrow$ “vanishing of $L$-values”

Euler Systems mean lots of nice cohomology. So we might expect Euler systems to exist 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 $L := \mathbb{Q}^{\ker \chi}$, $L/\mathbb{Q}$ finite. For all $n$, $G_{LQ(\mu_n)} \subset \ker(\chi)$, hence the natural map on cocycles induces an isomorphism

$$c_m \xrightarrow{H^1(LQ(\mu_n), T) \otimes \chi} c_n \in H^1(LQ(\mu_n), T) \quad H^1(\mathbb{Q}(\mu_n), T) \ni c_n$$

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

Twisting by $\chi_p$

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

Idea: $\mathbb{Z}/p\mathbb{Z}$ is a trivial $G_{\mathbb{Q}(\mu_{p^k})}$-module, hence $T/p^k \cong T/p^k \otimes \mathbb{Z}/p\mathbb{Z}$ 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 $H^1_{\infty}(\mathbb{Q}(\mu_n), T) = \lim_{\rightarrow k} H^1(\mathbb{Q}(\mu_{p^k}), T)$ with respect to corestriction.

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

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

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

**Theorem 9.7.** $\mathcal{E}^\chi_p = \{c_{n}^\chi_p\}$ 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, $\exp^* : H^1_f(\mathbb{Q}_p, V) \to \mathbb{Q}_p^* \cdot \omega_E$, where $\omega_E$ is the regular differential for $E$.

**Theorem 9.8 ((Kato)).** Let $E/Q$ be an elliptic curve, $T$ a Tate module, $\mathcal{C}$ the Euler system described by Aurel, $\mathcal{C} = \mathcal{C}^{\chi_p^{-1}}$. Then there exists $r_E \in \mathbb{Z} \setminus \{0\}$ such that $\exp^*(\log^p(c_1^\chi)) = \frac{r_E L_{\mu_p}(E, 1) \omega_E}{\Omega_E}$, where $\Omega_E$ is real period of $E$ corresponding to $\omega_E$.

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

**Proof.** Euler factors are non-zero at $\ell | N_p$.

**Theorem 9.10.** Let $L/Q$ be an abelian number field, $\chi : G(Q/L) \to \mathbb{C}^*$. If $L(E, \chi, 1) \neq 0$ then $E(L)^\chi = \{P \in E(L) \otimes \mathbb{C} : \sigma(P) = \chi(\sigma) P\sigma \in \text{Gal}(L/Q)\}$ and $\text{III}(E(L)^\chi)$ 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 $\Pi_{p \rightarrow \infty}(E/\mathbb{Q})$ 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 $\text{Gal}(K/\mathbb{Q})$ acts on $\text{Gal}(K_m/K)$ as $-1$)
- Kato: Proof using Siegel units - cohomology classes for $T_pE$ over cyclotomic fields.

Kolyvagin: can tell you about $L(E/K, \psi, 1)$ where $\psi$ 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 $K$ (→ $L$-functions $L(E/K), \psi, 1$) for any ray class character $\psi$?

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. $\leadsto$ 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,

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

$$g_{\alpha n, b_n/n} = q^{w} \prod_{n \geq 0} \left(1 - q^n q^{a^2/4} e^{2 \pi ib/3}\right) \prod_{n \geq 1} \left(1 - q^n q^{-a/n} e^{-2 \pi ib/3}\right)$$

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 $a = 0, b = 1$, $c_{0,1/N} \in \mathcal{O}(Y_1(N))^* \rightarrow H^1_{\text{et}}(Y_1(N), \mathbb{Z}_p(1))$ using a Kummer map.

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

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

Theorem 10.3 (Lei-Loeffler-Zerbès). Can extend this to an Euler System as follows: for $m \geq 1$, consider $\Delta_m : Y_1(m^2N) \rightarrow Y_1(N)^2$ defined by $z \mapsto (z, z + \frac{1}{m})$. Then take $c_m = (\Delta_m)_*(c_{0,1/m^2N})$. This is only defined over $\mathbb{Q}(\mu_m)$ 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, $\psi$ ray class character of $K$. $\psi$ gives a weight 1 modular form $\theta_{\psi}$. 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 Shimura varieties (comes from Matrix groups, like modular curves come from $\text{SL}_2$ over $\mathbb{Q}$)

Eg,

- $\text{GL}_2 \hookrightarrow \text{GL}_2 \times \text{GL}_2$ (BF elts)
- $\text{SO}_2 \hookrightarrow \text{GL}_2$ (Heegner points)
- $\text{GL}_2 \times \text{GL}_2 \hookrightarrow \text{GSp}_4$
- $\text{SL}_2 \cong \text{SU}(1, 1) \hookrightarrow \text{SU}(2, 1)$

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