1. Lecture 1 (2/5/2018)

1.1. Motivation. The broad aim of this subject is to understand the special values of $L$-functions. Interesting examples of $L$-functions include:

- $\zeta(s)$, the Riemann zeta function,
- $\zeta_K(s)$, the Dedekind zeta function of an number field $K/\mathbb{Q}$,
- $L(E, s)$, the $L$-function of an elliptic curve.

The special values of these functions tend to reflect interesting arithmetic. For example, 

$$\text{ord}_{s=0} \zeta_K(s) = \text{rank } \mathcal{O}_K^\times.$$ 

By a Theorem of Dirichlet, $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r + s - 1$. Dirichlet’s class number formula tells us the leading term at 0:

$$\zeta^K_*(0) = -\frac{h_K R_K}{w_K}.$$ 

The $L$-functions of elliptic curves are expected to enjoy a similar phenomenon. The BSD conjecture predicts that 

$$\text{ord}_{s=1} L(E, s) \overset{?}{=} \text{rank } E(\mathbb{Q})$$
and the leading term is

$$L^*(E, 1) = \Omega_E \frac{\# \Pi(E/\mathbb{Q}) R(E(\mathbb{Q}))}{(#E(\mathbb{Q})_{\text{tors}})^2} \times \prod_{\ell | N_E} c_\ell.$$ 

Here

- $\Omega_E$ is a period,
- $\Pi(E/\mathbb{Q})$ is a mysterious group that is analogous to the class number,
- $R(E(\mathbb{Q}))$ is a regulator,
- $c_\ell$ is the “Tamagawa number” (at $\ell$), having to do with components of integral models.
Thus we have found that the kernel of \( \kappa \) for all \( \sigma \) sending \( \sigma \) sending \( P \) computation shows that \( \phi \) \( \# \) rational points \( L \) from the class number. For imaginary quadratic fields there is no regulator, so bounds on \( L \)-functions are the same as bounds on class numbers. This is why we know a lot more about class numbers of imaginary quadratic fields than those of real quadratic fields.

1.2. The Mordell-Weil Theorem. Let \( E/\Q \) be an elliptic curve. We are really interested in the rational points \( E(\Q) \).

**Theorem 1.2.1** (Mordell-Weil). \( E(\Q) \) is a finitely generated abelian group.

A key ingredient in the proof is the so-called weak Mordell-Weil theorem, which says that \( E(\Q)/mE(\Q) < \infty \). This fact doesn't prove finite generation because a priori \( E(\Q) \) could have a divisible part that would disappear in the quotient \( E(\Q)/mE(\Q) \). Combining this with the theory of heights lets you deduce finite generation. Then, after the fact, bounding \( E(\Q)/mE(\Q) \) gives bounds on rank \( E(\Q) \).

We will sketch the proof of the weak Mordell-Weil Theorem, as it is a good lead-in to the ideas that we want to discuss.

**Proof of weak Mordell-Weil.** Let \( P \in E(\Q) \). We are going to do descent in the guise of Kummer theory. Let \( Q \in E(\Q) \) be such that \( mQ = P \). Then we have a map

\[
\phi_Q : G_Q := \text{Gal}(\overline{\Q}/\Q) \to E[m]
\]

sending \( \sigma \to \sigma(Q) - Q \). (This lies in \( E[m] \) because \( \sigma(Q) \) is another \( m \)th root of \( P \).) An easy computation shows that \( \phi_Q \) is a cocycle, hence induces a cohomology class \( c_P \in H^1(\Q, E[m]) \). To see that the cohomology class is well-defined, suppose we chose another \( m \)th root of \( P \), necessarily of the form \( Q' = Q + R \) where \( R \in E[m] \). Then \( \phi_Q' - \phi_Q \) is the coboundary \( \sigma \to \sigma(R) - R \).

So we have produced a map

\[
E(\Q) \to H^1(\Q, E[m]) \tag{1.2.1}
\]

sending \( P \to c_P \). If \( c_P = 0 \) then \( \sigma(Q) - Q = \sigma(R) - R \) for some \( R \in E[m] \), hence \( \sigma(Q - R) = Q - R \) for all \( \sigma \in G_Q \). This implies that \( Q - R \) is defined over \( \Q \), and \( m(Q - R) = P \), i.e. \( P \in mE(\Q) \). Thus we have found that the kernel of \( \kappa \) is \( mE(\Q) \), i.e. the map \((1.2.1)\) factors through

\[
\begin{array}{ccc}
E(\Q) & \xrightarrow{\kappa} & H^1(\Q, E[m]) \\
\downarrow & & \downarrow \\
E(\Q)/mE(\Q) & \to & H^1(\Q, E[m]) \tag{1.2.2}
\end{array}
\]

Is this useful? We've injected \( E(\Q)/mE(\Q) \) into the group \( H^1(\Q, E[m]) \), but unfortunately this is still infinite. However, we will be able to cut out a finite subspace thereof which contains the image of \( \kappa \).

To do this we actually have to use some algebraic geometry, namely the following. If \( \ell \nmid m \) is prime and \( E \) has good reduction at \( \ell \), then \( E[m] \) is unramified at \( \ell \). So we can choose \( Q \) so that \( \phi_Q = 0 \). This means that

\[
c_P \in \ker \left( H^1(\Q, E[m]) \to \prod_{\ell \mid m} H^1(I_{\ell}, E[m]) \right) \text{.}
\]
Let $\Sigma$ be the set of “bad places” $q$, consisting of those $q$ dividing $m\infty$ and the places of bad reduction. Let $Q_\Sigma/Q$ be the maximal extension unramified away from $\Sigma$. The above is just $H^1(Q_\Sigma, E[m])$. Since $\text{Gal}(Q_\Sigma/Q)$ is topologically finitely generated, it is reasonable to expect that this is more reasonable.

If $E[m]$ were a trivial $G_\Sigma$-module then $H^1(Q_\Sigma, E[m])$ would parametrize homomorphisms $\text{Gal}(Q_\Sigma/Q) \rightarrow E[m]$, which is equivalent to (certain types of) abelian extensions unramified away from a finite set. The point is that this is finite by class field theory.

The general case reduces to this one by inflation-restriction. Namely, for $L = Q(E[m]) \subset Q_\Sigma$, we have a short exact sequence

$$0 \rightarrow H^1(\text{Gal}(L/Q), E[m]) \rightarrow H^1(G_\Sigma, E[m]) \xrightarrow{\text{res}} H^1(\text{Gal}(Q_\Sigma/L), E[m]).$$

We want the middle term to be finite. The rightmost term is finite by the argument of the preceding paragraph, and the left term is finite since it is the cohomology of a finite group with finite coefficients.

1.3. Selmer groups: first encounter. Our proof of weak Mordell-Weil worked by “trapping” $E(Q)/mE(Q)$ inside a finite subgroup of Galois cohomology. We might ask what is the most restrictive condition we can put on Galois cohomology that will still “trap” $E(Q)/mE(Q)$. This is a “Selmer group”. It is defined by imposing the most obvious restrictive conditions on the classes in $H^1(Q, E[m])$.

Let $E$ be an elliptic curve, we have a Kummer map $\kappa: E(F)/mE(F) \hookrightarrow H^1(F, E[m])$.

For a place $v$ of $F$, let $F_v$ be the completion at $v$. We can consider the local Kummer map $E(F_v)/mE(F_v) \hookrightarrow H^1(F_v, E[m])$.

A choice of embedding $\overline{F} \hookrightarrow \overline{F}_v$ induces an inclusion $G_{F_v} \hookrightarrow G_F$. We have a well-defined (arithmetic) Frobenius $\text{Frob}_v \in G_{F_v}/I_v$. Fixing such a choice, the local and global Kummer maps are compatible via the diagram

$$\begin{array}{ccc}
E(F)/mE(F) & \xrightarrow{\kappa} & H^1(F, E[m]) \\
\downarrow & & \downarrow \\
E(F_v)/mE(F_v) & \xrightarrow{\kappa_v} & H^1(F_v, E[m]).
\end{array}$$

This motivates the following definition:

**Definition 1.3.1.** We define the Selmer group

$$\text{Sel}_m(E/F) = \{ c \in H^1(F, E[m]) : \text{res}_v(c) \in \text{Im}(\kappa_v) \text{ for all } v \}.$$

**Remark 1.3.2.** If $v \nmid m$, then $E$ has good reduction at $v$ so $\text{Im} \kappa_v$ is unramified, i.e.

$$\text{Im} \kappa_v \subset \ker\{ H^1(K_v, E[m]) \rightarrow H^1(I_v, E[m]) \}.$$

Another way of expressing this is in terms of the short exact sequence

$$0 \rightarrow E[m] \rightarrow E \xrightarrow{m} E \rightarrow 0$$

which gives a long exact sequence

$$0 \rightarrow E[m](F) \rightarrow E(F) \xrightarrow{m} E(F) \rightarrow H^1(F, E[m]) \rightarrow H^1(F, E)[m] \rightarrow 0.$$
Repeating this story over $F_v$, and using our embedding $G_{F_v} \hookrightarrow G_F$, we have a diagram

$$
\begin{array}{ccccccccc}
E[m](F) & \longrightarrow & E(F) & \overset{m}{\longrightarrow} & E(F) & \overset{\kappa}{\longrightarrow} & H^1(F, E[m]) & \longrightarrow & H^1(F, E)[m] & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
E[m](F_v) & \longrightarrow & E(F_v) & \overset{m}{\longrightarrow} & E(F_v) & \overset{\kappa_v}{\longrightarrow} & H^1(F_v, E[m]) & \longrightarrow & H^1(F_v, E)[m] & \longrightarrow & 0
\end{array}
$$

From this we see

$$\text{Im } \kappa_v = \ker \left( H^1(F_v, E[m]) \to H^1(F_v, E)[m] \right).$$

Therefore, another way to phrase the same definition is

$$\text{Sel}_m(E/F) = \{ c \in H^1(F, E[m]) : \text{res}_v(c) \in \ker \left( H^1(F_v, E[m]) \to H^1(F_v, E)[m] \right) \text{ for all } v \}.$$  

So we now have an exact sequence

$$0 \to E(F)/mE(F) \to \text{Sel}_m(E/F) \to \ker \left( H^1(F, E)[m] \to \prod_v H^1(F_v, E)[m] \right) \to 0. \quad (1.3.1)$$

We define

$$\text{III}(E/F) := \ker \left( H^1(F, E) \to \prod_v H^1(F_v, E) \right)$$

so that the earlier $\ker \left( H^1(F, E)[m] \to \prod_v H^1(F_v, E)[m] \right) = \text{III}(E/F)[m]$. In these terms, we can rewrite (1.3.1) as

$$0 \to E(F)/mE(F) \to \text{Sel}_m(E/F) \to \text{III}(E/F)[m] \to 0. \quad (1.3.2)$$

Thus the Selmer group sort of combines the regulator (related to $E(F)/mE(F)$) and the “class number” $\text{III}(E/F)[m]$. This is a philosophical reason why it is easier to study.

The group $\text{III}(E/F)[m]$ is mysterious. It classifies $E$-torsors over $F$. Similarly, $\text{Sel}_m(E/F)$ classifies $E[m]$-torsors. For small $m$, one can turn these descriptions into something concrete - this lies at the center of Bhargava’s counting methods.

### 1.4. Some questions

The group $\text{III}(E/F)$ is conjectured to be finite. If it is finite, then by the existence of a nondegenerate alternating pairing (the Cassels-Tate pairing) we must have

$$\text{III}(E/F) \cong N \oplus N$$

for a finite abelian group $N$.

Continuing to assume that $\text{III}(E/F)$ is finite, for $p$ a prime, $\text{Sel}_p(E/F)$ is a vector space over $F_p$. Suppose we have $\dim_{F_p} \text{Sel}_p(E/F) = 1$. Since $\text{III}_p(E/F)$ is even-dimensional, all the contribution would have to come from $E(F)/pE(F)$. This is either a contribution from the rank or the $p$-torsion. If one assumes further that $E(F)$ has no $p$-torsion, then we would have $\text{rank } E(F) = 1$. We can then pose the following question, which would be a consequence of finiteness of $\text{III}(E/F)$:

**Question 1.4.1.** Assuming $\dim_{F_p} \text{Sel}_p(E/F) = 1$ and $E(F)[p] = 0$, can we show that $\text{rank } E(F) > 0$?

If $m | m'$ then $E[m] \subset E[m']$, so we get a map $\text{Sel}_m(E/F) \to \text{Sel}_{m'}(E/F)$. Ranging over $m$ of the form $p^n$, we define

$$\text{Sel}_{p^n}(E/F) := \lim_{n} \text{Sel}_{p^n}(E/F).$$
The direct limit lives inside $H^1(F, E[p^\infty])$. We can describe it succinctly as

$$\text{Sel}_{p^\infty}(E/F) = \ker \left( H^1(F, E[p^\infty]) \to \prod_v H^1(F_v, E) \right).$$

Taking the direct limit of the sequences (1.3.2) gives

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p K \to \text{Sel}_{p^\infty}(E/F) \to \text{III}(E/F)[p^\infty] \to 0.$$ 

Now $E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\text{rank } E(F)}$, since the torsion is killed by tensoring with a divisible group. Also $\text{III}(E/F)[p^\infty]$ should be finite. So $\text{Sel}_{p^\infty}(E/F)$ should be detecting the rank of the Mordell-Weil group.

Consider homomorphisms into $\mathbb{Q}_p/\mathbb{Z}_p$; we expect to have

$$\text{Hom}(\text{Sel}_{p^\infty}(E/F), \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_p^{\text{rank } E(F)} \times \text{finite group.}$$

By definition, the $\mathbb{Z}_p$ rank of $\text{Hom}(\text{Sel}_{p^\infty}(E/F), \mathbb{Q}_p/\mathbb{Z}_p)$ is the $\mathbb{Z}_p$ -corank of $\text{Sel}_{p^\infty}(E/\mathbb{Q})$. So the rank of $E(F)$ should be the $\mathbb{Z}_p$ -corank of $\text{Sel}_{p^\infty}(E/\mathbb{Q})$.

**Question 1.4.2.** Can we prove that

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(E/F) = \text{rank}_{\mathbb{Z}_p} E(F)?$$

For $F = \mathbb{Q}$, we have significant progress thanks to the work of Gross-Zagier and Kolyvagin. Over more general number fields, we don’t know much.

Since Selmer groups are easier to handle (they don’t separate the “class group” from the “regulator”) we might be able to address the more modest question:

**Question 1.4.3.** Can we prove that

$$\text{ord}_{s=1} L(E, s) > 0 \implies \text{corank} \text{Sel}_{p^\infty}(E/F) > 0.$$  

1.5. **Bloch-Kato Selmer groups.** Next we want to explain that we can define $\text{Sel}_{p^\infty}(E/F)$ purely in terms of $E[p^\infty]$, without making reference to $E$.

For $v \nmid p$, say of residue characteristic $\ell$, $E(F_v)$ contains a pro-$\ell$-group with finite index. This implies that $E(F_v)/p^n E(F_v)$ is bounded, hence becomes 0 in the direct limit. Hence for $v \nmid p$ the local condition is simply $c \in H^1(F_v, E[p^\infty])$ such that $\text{res}_v(c) = 0$. What about $v \mid p$?

If $E$ has good reduction at $v$, then $E$ can have either supersingular or ordinary reduction. Writing $#E(F_v) = 1 + q_v - a_v(E)$, the reduction is supersingular if $v \mid a_v(E)$ (this is rare if $E$ does not have CM) and ordinary if $v \nmid a_v(E)$.

Now, $T_p E \cong \mathbb{Z}_p \times \mathbb{Z}_p$. In the case of ordinary reduction, there is a rank-1 $\mathbb{Z}_p$ -summand $T^+_p \subset T_p$ stable under $G_{F_v}$. The quotient $T_p(E)/T_v(E)$ is also a rank-1 $\mathbb{Z}_p$ -module, with an action of $G_{F_v}$. In other words, we have an exact sequence of $\mathbb{Z}_p[G_{F_v}]$-modules

$$0 \to T^+_v \to T_p E \to T^-_v \to 0.$$ 

Moreover, we can actually identify the Galois actions on the $T^+_v$, $T^-_v$. The determinant is given by the Weil pairing

$$E[m] \times E[m] \to \mu_m.$$ 

The action of $G_{F_v}$ on $T^+_v$ is by $\epsilon_{\text{cyc}} \alpha^{-1}$ where $\alpha$ is a finite order unramified character, determined by the condition that it sends Frobenius to the unit root of $x^2 - a_v x + q_v$. This equation has two distinct roots in the residue field, one of which is a unit, and there is a unique lift to $\mathbb{Z}_p$.

Therefore, the Galois action on $T_p(E)$ gives a Galois representation

$$\rho_{E,p} : G_{F_v} \to \text{GL}_2(\mathbb{Z}_p).$$
of the form
\[ \rho_{E,p} \cong \begin{pmatrix} \alpha^{-1} & \epsilon_{\text{cyc}} & * \\ 0 & \alpha \end{pmatrix}. \]

Where does this structure come from? We have an exact sequence
\[ 0 \to \tilde{E}(F_v) \to E(F_v) \to E(\overline{F}_v) \to 0. \]

Here \( \tilde{E} \) is the formal group. The hypothesis of ordinary reduction says that \( E(\overline{F}_v) \cong \mathbb{Z}_p \), and the Galois action is visibly unramified.

Now consider tensoring with \( \mathbb{Q}_p/\mathbb{Z}_p \). We claim that
\[ T_p(E) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong E[p^\infty], \]
via the map
\[ (P_n) \otimes \frac{1}{p^m} \to p^n P_{n+m}. \]

Hence we have a short exact sequence
\[ 0 \to T_v^+ \otimes \mathbb{Q}_p/\mathbb{Z}_p \to T_p(E) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to T_v^- \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0. \]

We claim that
\[ \text{Im } \kappa_v = \ker \left( H^1(F_v, E[p^\infty]) \to H^1(F_v, T^- \otimes \mathbb{Q}_p/\mathbb{Z}_p) \right)_{\text{div}}. \]

We won't prove this.

\textbf{Remark 1.5.1.} If \( E \) has bad, multiplicative reduction then we still have
\[ \rho_{E,p} \cong \begin{pmatrix} \epsilon_{\text{cyc}} & \alpha^{-1} & * \\ 0 & \alpha \end{pmatrix} \]
where \( \alpha \) is unramified,
\[ \alpha(Frob_v) = \begin{cases} 1 & \text{split mult}, \\ -1 & \text{non-split mult}. \end{cases} \]

This comes from Tate's parametrization of elliptic curves with split multiplicative reduction:
\[ \mathbb{F}_p^\times \otimes \mathbb{Z}_p \cong E(\overline{F}_v). \]

\textbf{Example 1.5.2.} If \( E/F \) has multiplicative ordinary reduction at all \( v \mid p \), then
\[ \text{Sel}_{p^\infty}(E/F) = \left\{ c \in H^1(F, E[p^\infty]) : \begin{array}{c} \text{res}_v(c) = 0 \text{ for all } v \neq p \\ \text{res}_v(c) \in \ker \left( H^1(F_v, E[p^\infty]) \to H^1(F_v, T^- \otimes \mathbb{Q}_p/\mathbb{Z}_p) \right) \text{ for } v \mid p \end{array} \right\}. \]

This is consistent with the philosophy that the \( p \)-divisible of an elliptic curve should capture almost everything about it.

What about supersingular or additive reduction? In these cases we need the notion of the \textit{Bloch-Kato Selmer group}. We have
\[ 0 \to T_p(E) \to V_p(E) \to T_p(E) \otimes \mathbb{Q}_p/\mathbb{Z}_p = E[p^\infty] \to 0. \]

Bloch-Kato defined a Selmer group \( H^1_{\text{BK}}(F_v, V_p(E)) \subset H^1(F_v, V_p(E)) \) as
\[ H^1_{\text{BK}}(F_v, V_p(E)) := \ker \left( H^1(F_v, V_p(E)) \to H^1(F_v, V_p(E) \otimes \mathbb{Q}_p \text{ B}_{\text{cris}}) \right). \]

Bloch and Kato showed that \( H^1_{\text{BK}}(F_v, V_p(E)) = \text{Im } \kappa_v \) for \( v \mid p \).

What does this mean? We can interpret \( H^1(F_v, V_p(E)) \) as classifying extensions of \( \mathbb{Q}_p[G_{F_v}] \)-modules
\[ 0 \to V_p(E) \to X \to \mathbb{Q}_p \to 0. \]
The associated extension class is obtained as the boundary of $1 \in H^0(G_{\overline{F}_p}, \mathbb{Q}_p)$. Another perspective is that such an extension is controlled by a Galois representation

$$\begin{pmatrix} \rho_{E, p} & \psi \\ 0 & 1 \end{pmatrix}$$

and $\psi$ is the cocycle. The extensions parametrized by $H^1_{\text{cris}}$ are those which are “as crystalline as they could be”. Given such an extension, we get

$$0 \to V_\rho(E) \otimes_{\mathbb{Q}_p} B_{\text{cris}} \to X \otimes_{\mathbb{Q}_p} B_{\text{cris}} \to \mathbb{Q}_p \otimes_{\mathbb{Q}_p} B_{\text{cris}} \to 0$$

The boundary map gives

$$(\mathbb{Q}_p \otimes_{\mathbb{Q}_p} B_{\text{cris}})^{G_{\overline{F}_p}} = \mathbb{Q}_p \otimes (B_{\text{cris}})^{G_{\overline{F}_p}} = F^1_{\text{unr}} \to H^1(F_\nu, V_\rho(E) \otimes B_{\text{cris}}).$$

If this boundary map is 0, then we have exactness of

$$0 \to D_{\text{cris}}(V_\rho(E)) \to D_{\text{cris}}(X) \to F^1_{\text{unr}} \to 0.$$
2. Lecture 2 (2/12/2018)

2.1. Recap of Selmer groups. Last time we discussed how to define a Selmer group $\text{Sel}_{p^\infty}(E/F) \subset H^1(F, E[p^\infty])$. The key points were:

1. It can be defined solely in terms of $E[p^\infty]$.
2. There is a fundamental exact sequence

$$0 \to E(F) \otimes Q_p/Z_p \to \text{Sel}_{p^\infty}(E/F) \to \Pi(E/F)[p^\infty] \to 0.$$  

We then explained that more generally there are Bloch-Kato Selmer groups for any $G_F$-representation $V$ finite-dimensional over any finite extension $L/Q_p$. For $O_L \subset L$ the ring of integers, we can choose a $G_F$-stable $\vartheta$-lattice $T \subset V$. Then we set

$$W := V/T = T \otimes Q_p/Z_p = T \otimes_{O_L} L/\vartheta.$$  

The Bloch-Kato Selmer group for $V$ is defined by local conditions

$$H^1_f(F_v, V) = \left\{ \begin{array}{ll} \ker\{ H^1(F_v, V) \to H^1(I_v, V) \} & v \nmid p \\ \ker\{ H^1(F_v, V) \to H^1(F_v, V \otimes B_{\text{cris}}) \} & v \mid p. \end{array} \right.$$  

We propagate these local conditions to $H^1_f(F_v, T)$ and $H^1_f(F_v, W)$ via the obvious maps.

Remark 2.1.1. The pre-image of $H^1_f(F_v, V)$ in $H^1(F_v, T)$ will automatically contain all the torsion.

For $? = T, W, V$ we define the global Selmer group

$$H^1_f(F, ?) = \{ c \in H^1(F, ?) : \text{res}_v(c) \in H^1_f(F_v, ?) \text{ for all } v \}.$$  

Example 2.1.2. For $V = T_p(E) \otimes_{Z_p} Q_p$ and $W = E[p^\infty]$, we have

$$H^1_f(F, W) = \text{Sel}_{p^\infty}(E/F).$$  

Why consider these Bloch-Kato Selmer groups if we’re just interested in elliptic curves? The point is that it is useful to put objects into families, e.g. a family of twists of the Galois representation.

2.2. Algebraic Hecke characters. We are going to discuss a special class of characters. Let $\chi : G_F \to \overline{Q}_p^\times$ be a continuous character, which is unramified away from finitely many places $v$ and Hodge-Tate at $v \mid p$. There’s a dictionary between such characters and algebraic Hecke characters $\psi : F^\times \backslash A_F^\times \to \overline{C}^\times$. The latter means that there is an algebraic character $\rho : F^\times \to \overline{Q}$, i.e. induced by a morphism of algebraic groups, such that $\psi|_{|F \otimes R|} = \rho|_{|F \otimes R|}$. Concretely this is asking for $\psi|_{|F \otimes R|}$ to be a product of integral powers of the real embeddings of $F$ into $R$.

To give the dictionary between $\chi$ and $\psi$ we fix embeddings $\overline{Q} \leftarrow C$ and $\overline{Q} \leftarrow \overline{Q}_p$. Then we can consider

$$\alpha \mapsto \psi(\alpha)\rho(\alpha_{\infty})^{-1}$$  

which is valued in $\overline{Q}^\times$ by the algebraicity hypothesis. Using our fixed embedding, we can view it as valued in $\overline{Q}_p^\times$. Then we can define a character

$$\rho \psi : G_F \to \overline{Q}_p^\times$$  

1It’s less clear how to define $\text{Sel}_{p^m}(E/F)$ solely in terms of $E[p^m]$. In some cases it can be done using flat cohomology.
χ2.3. Iwasawa theory. We define Example 2.3.1. Show that if ψ = |NmF/Q(χ)|−1 then σψ is the ρ-p-adic cyclotomic character, with the arithmetic normalization (where the local p goes to Frobp under the reciprocity map).

The Hodge-Tate weights can be read off from ρ. In the simplest case where p splits completely in F, a place v | p corresponds to the valuation v obtained by embedding F ← τQ ⊂ Qp with the last inclusion coming from our fixed embedding. Normalize so that the Hodge-Tate weight of the cyclotomic character is 1. Then if

$$\psi|_{F \otimes R^1_v} = \rho|_{F \otimes R^1_v} = \prod \tau^{n_v}$$

the Hodge-Tate weight of χψ at v is −nχ.

Example 2.2.2. For a character χ, the local Bloch-Kato group $H^1_f(G_{Q_p}, Q_p(\chi))$ is the full $H^1_f(G_{Q_p}, Q_p(\chi))$ if HT(χ) > 1 and $H^1_f(G_{Q_p}, Q_p(\chi)) = 0$ if HT(χ) < 0.

Example 2.2.3. Let E be an elliptic curve with ordinary/multiplicative reduction at v | p, so $V_p(1)$ has HT weights 1 and 0.

Suppose χ = χψ and V = $V_p(E) \otimes L(\chi)$, so the Galois representation is $\rho_E \otimes \chi$. Take the lattice $T = T_p(E) \otimes O(\chi)$.

Then we have a filtration

$$0 \rightarrow V^+_v \rightarrow V \rightarrow V^-_v \rightarrow 0$$

where the Galois action on the sub and quotient is through the characters $\epsilon_a^{-1} \chi$ and $a_v \chi$, respectively, and

$$H^1_f(F_v, V) = \ker(H^1(F_v, V) \rightarrow H^1(F_v, V^-)).$$

If all the HT weights of χ at v are > 1, then $H^1_f(F_v, V(\chi)) = H^1(F_v, V(\chi))$. If all the HT weights of χ are < −1, then $H^1_f(F_v, V(\chi)) = 0$.

2.3. Iwasawa theory. The idea of Iwasawa theory is to package all the $V_p(E) \otimes L(\chi)$ together for certain families of χ.

Classically, consider a Γ = Z_p$^d$-extension $F_\infty / F$. Where could it be ramified? If $v \nmid p$, then the inertia group is an image of $O_{F_v}^\times$. Since the latter is pro-ℓ, the image is finite. But $Z_p^d$ has no torsion, so the image has to be 0, i.e. the extension is unramified away from p.

Example 2.3.1. We define

$$\operatorname{Sel}_{p,\infty}(E/F_\infty) = \lim_{F \subset F' \subset F_\infty} \operatorname{Sel}_{p,\infty}(E/F').$$

This is a $Z_p$-module with an action of Γ, so we can consider it as a $\Lambda := Z_p[[\Gamma]]$-module. We have a non-canonical isomorphism

$$Z_p[[\Gamma]] \approx Z_p[[T_1, \ldots, T_d]]$$

by picking topological generators γ1, . . . , γd and sending γi → 1 + Ti.
Greenberg introduced another, essentially equivalent, way of defining the Selmer group, where the finite-order characters of $\Gamma$. We have a canonical character $\Phi: G_F \twoheadrightarrow \Gamma \subset \Lambda^\times$. Then composing with a character of $\Gamma$ gives a corresponding Galois character, so $\Phi$ is a “universal” character.

Let $\Lambda^\ast = \text{Hom}_{ct}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$, a discrete module. This has a $\Lambda$-module structure via $\lambda \cdot f(x) = f(\lambda x)$. We define the $G_F$-action to be through $\Phi^{-1}$.

Let $V$ be a $G_F$-representation, $T \subset V$ a Galois-stable lattice and $W = V/T$. Define $M = T \otimes_{\mathbb{Z}_p} \Lambda^\ast = \text{Hom}(\Lambda, W)$.

Then $G_F$ acts on $M$ through $\rho_T \otimes \Phi^{-1}$. For $\gamma_1, \ldots, \gamma_d$ topological generators of $\Gamma$, and $\chi$ a character of $\Gamma$, we have

$$M[\{\gamma_i - \chi(\gamma_i)\}] \cong W(\chi^{-1}).$$

So you can think of $M$ as a Galois representation that interpolates all the twists. We might then try to define a Selmer group $\text{Sel}(M) \subset H^1(F, M)$. Note that since $F_\infty$ is only ramified above $p$, and $T$ is unramified at almost every place, this $M$ is still a “reasonable” Galois representation.

**Example 2.3.2.** If $E$ has multiplicative/ordinary reduction at all $v | p$, then

$$\text{Sel}(M) = \ker\left(H^1(F, M) \to \prod_{v | p} H^1(I_v, M) \times \prod_{v \not| p} H^1(I_v, M_v^-)\right).$$

Here $M_v^- = T_v^- \otimes \Lambda^\ast$. This is the same as $\text{Sel}(E/F_\infty)$, since Shapiro’s Lemma says that the composite

$$H^1(F, M) \xrightarrow{\text{res}} H^1(F_\infty, M) \xrightarrow{\text{eval at triv}} H^1(F_\infty, T)$$

is an isomorphism.

**Example 2.3.3.** What if $E$ has supersingular reduction? Assume that every $v | p$ is ramified in $\Gamma$. Then by a result of Greenberg-Coates,

$$\text{Sel}(E/F_\infty) = \ker\left(H^1(F, M) \to \prod_{v | p} H^1(I_v, M)\right).$$

This is huge – it has positive $\Lambda$-corank.

**Example 2.3.4.** If instead of twisting by finite order characters, we twist by characters with big/small HT weights, then the local conditions will become degenerate by Example 2.2.3.

2.4. **Imaginary quadratic fields.** Suppose $F = K$ is an imaginary quadratic field. By class field theory, $K$ has a $\mathbb{Z}_p^2$ extension $K_\infty/K$.
Here we have marked the $\mathbb{Z}_p$-subextension $K^{\text{cyc}} \subset K_\infty$ and also the anti-cyclotomic extension $\mathbb{Z}_p$-subextension $K^{\text{ac}}$, which is characterized by the property that the involution $\text{Gal}(K/Q)$ acts by negation on $\text{Gal}(K^{\text{ac}}/K)$.

In the cyclotomic subextension, any prime of $K$ has finite splitting behavior. In the anticyclotomic extension, a prime which is split in $K/Q$ has a finite amount of splitting, but an inert prime will split completely.

Suppose $p$ splits as $p = v \overline{v}$ in $K$. Define

$$ \text{Sel}_v(\mathcal{M}) = \ker \left( H^1(F, \mathcal{M}) \to \prod_{w \nmid p} H^1(I_w, \mathcal{M}) \times H^1_I(\overline{v}, \mathcal{M}) \right). $$

In particular there is no condition at $v$. What happens if we look at $\text{Sel}(\mathcal{M})[\gamma - \chi(\gamma)]$ for $\chi$ of finite order (so as to preserve the filtration)? This is the “specialization of the Selmer group to $\chi$”, and we’d like to compare it to Selmer group of the specialization of the Galois representation, which under our normalization is $W(\chi^{-1})$. We have a short exact sequence

$$ 0 \to W(\chi^{-1}) \to M \xrightarrow{\gamma - \chi(\gamma)} M \to 0. $$

From this we get a commutative diagram

$$ \begin{array}{ccc}
\text{Sel}(W(\chi^{-1})) & \to & \text{Sel}(\mathcal{M})[\gamma - \chi(\gamma)] \\
\downarrow & & \downarrow \\
H^1(F, W(\chi^{-1})) & \to & H^1(F, \mathcal{M})[\gamma - \chi(\gamma)] \\
\end{array} $$

If $M^{G_F} = 0$, then the horizontal maps are injective. If furthermore $\chi$ has extreme HT weights, so that the HT weights of $W(\chi^{-1})$ lie outside $[-1, 1]$ then the map is an isomorphism.

**Example 2.4.1.** Suppose $E(K)$ has rank 1. Then we have a diagram

$$ \begin{array}{ccc}
E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \to & \text{Sel}(E/K) \\
\downarrow & & \downarrow \\
E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \to & H^1(K_v, E[p^\infty])
\end{array} $$

These points don’t contribute to $\text{Sel}_v$, since they won’t be unramified at $\overline{v}$. If $\text{Sel}(E/K) \cong \mathbb{Q}_p/\mathbb{Z}_p \oplus \Pi(E/K)[p^\infty]$ then $\text{Sel}_v(E[p^\infty]) \cong \Pi(E/K)[p^\infty]$. Thus, $\text{Sel}_v$ defines a family specializing from the usual Selmer group to $\Pi$. This demonstrates why you might want to consider non finite-order twists.

### 2.5. Comparison of Selmer groups

Suppose

- $E$ has ordinary or multiplicative reduction at $v | p$.
- $E[p]$ is irreducible as a $G_F$-module; what we will actually use is that $E[p](F) = 0$.
- $\Gamma = \text{Gal}(F^{\text{cyc}}/F) \cong \mathbb{Z}_p$,
- $\Sigma$ is a set of places of $F$ containing all $v | p$ and primes of bad reduction.

We now seek to give a precise description of $\text{Sel}(M)[\gamma - \chi(\gamma)]$, especially comparing it to $\text{Sel}(W(\chi^{-1}))$. 
Lemma 2.5.1. We have a short exact sequence.

$$0 \to E[p^\infty] \to M \xrightarrow{\gamma-1} M \to 0.$$  

Proof. By definition,

$$M[\gamma-1] = \text{Hom}_\text{cts}(\Lambda, T \otimes \mathbb{Q}_p/\mathbb{Z}_p)[\gamma-1] = \text{Hom}_\text{cts}(\Lambda/(\gamma-1), T \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

and we have $\Lambda/(\gamma-1) \cong \mathbb{Z}_p$, and $T \otimes \mathbb{Q}_p/\mathbb{Z}_p = E[p^\infty]$. □

Corollary 2.5.2. If $E[p]^{G_F} = 0$, then $M^{G_F} = 0$.

Proof. By Lemma 2.5.1 we know that. Now, $M^{G_F}[\gamma-1, p]$ is Pontrjagin dual to

$$\text{Hom}(M^{G_F}, \mathbb{Q}_p/\mathbb{Z}_p)/(\gamma-1, p).$$

Since $(\gamma-1, p)$ is the maximal ideal of $\Lambda$, and $M^{G_F}$ is a finitely generated $\Lambda$-module, Nakayama’s Lemma implies that $\text{Hom}(M^{G_F}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, so $M^{G_F} = 0$. □

Taking the cohomology long exact sequence for Lemma 2.5.1 and using Corollary 2.5.2 we find an isomorphism

$$H^1(F, E[p^\infty]) \xrightarrow{\sim} H^1(F, M)[\gamma-1].$$

Next we want to analyze the Selmer groups. Let’s restrict attention to $v \nmid p$ first. We saw that for $v \nmid p$ the local condition is simply that

$$\text{Sel}(E[p^\infty]) \subset \ker\left(H^1(F, E[p^\infty]) \to H^1(F, E[p^\infty])\right)$$

On the other hand, for $M$ the local condition at $v \nmid p$ is that

$$\text{Sel}(M) \subset \ker\left(H^1(F, M) \to H^1(I_v, M)\right).$$

What is the difference between these conditions? Consider the diagram

$$\begin{array}{cccc}
0 & \to & H^1(F, E[p^\infty]) & \xrightarrow{\sim} & H^1(F, M)[\gamma-1] \\
\downarrow & & \downarrow & & \downarrow \\
\prod_{v \mid p} M^{I_v}/(\gamma-1)M^{I_v} & \to & \prod_{v \mid p} H^1(I_v, E[p^\infty]) & \to & \prod_{v \mid p} H^1(I_v, M)[\gamma-1]
\end{array}$$

A class in $\text{Sel}(E[p^\infty])$ is required to vanish in $H^1(F_v, E[p^\infty])$. However the Selmer condition for $H^1(F, M)$ only requires it to vanish in $H^1(I_v, M)$. How far is this from vanishing in $H^1(I_v, E[p^\infty])$? The difference is measured by $M^{I_v}/(\gamma-1)M^{I_v}$. For $v \notin \Sigma$, we know that $I_v$ acts trivially on everything, so $M^{I_v} = M$. Then $M/(\gamma-1)M = 0$ because $\gamma-1$ is a unit in $\Lambda$. The conclusion is that for $v \nmid p$ we actually have $M^{I_v}/(\gamma-1)M^{I_v} = 0$; in fact this is true for all $v \nmid p$.

Then we have to analyze the failure of the map

$$H^1(F_v, E[p^\infty]) \to H^1(I_v, E[p^\infty])$$

to be injective. The kernel is, by definition, the unramified cohomology $H^1_{\text{ur}}(F_v, E[p^\infty])$.

Similarly, for the places $v \mid p$, we have to consider

$$\prod_{v \mid p} (M^{\gamma-1}/(\gamma-1)M^{\gamma-1}) \xleftarrow{\sim} \prod_{v \mid p} H^1(I_v, W_v^-) \xrightarrow{\sim} \prod_{v \mid p} H^1(I_v, M_v^-)[\gamma-1]$$

We have $((\gamma-1)M^{\gamma-1}) = 0$ since $I_v$ acts nontrivially on the $\mathbb{Z}_p$-extension, so $(M^{\gamma-1}) = (\gamma-1)(M^{\gamma-1})$. Taking $G_{F_v}$-invariants, we get

$$\prod_{v \mid p} (T_v^- \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{G_{F_v}} \xrightarrow{\sim} \prod_{v \mid p} H^1(I_v, W_v^-)^{G_{F_v}} \xrightarrow{\sim} \prod_{v \mid p} H^1(I_v, M_v^-)[\gamma-1]^{G_{F_v}}$$
and \((T_v^- \otimes \mathbb{Q}_p/\mathbb{Z}_p)_{G_{\nu}} = (T_v^- \otimes \mathbb{Q}_p/\mathbb{Z}_p)[a_v - 1]\). This has size \(#\mathbb{Z}_p/(a_v - 1)\mathbb{Z}_p\).

The upshot is that we get an exact sequence

\[ 0 \rightarrow \text{Sel}(E[p^\infty]) \rightarrow \text{Sel}(M) \rightarrow ? \tag{2.5.1} \]

where ? can be taken to be, if there are no places with split multiplicative reduction,

\[ ? = \prod_{\nu | p} H^1_{ur}(F_{\nu}, E[p^\infty])_{\nu} \times \prod_{\nu \nmid p} H^1_{ur}(F_{\nu}, T_v^- \otimes \mathbb{Q}_p/\mathbb{Z}_p)_{\nu} \prod_{\nu | p} (T_v^- \otimes \mathbb{Q}_p/\mathbb{Z}_p)_{G_{\nu}} \frac{(a_v - 1)\mathbb{Z}_p}{\mathbb{Z}_p} \]

Note that we are not claiming any surjectivity on the right end of (2.5.1).

**Remark 2.5.3.** If \(\nu\) is a place of split multiplicative reduction then \(a_v = 1\), and (2.5.1) is sort of useless.

**Remark 2.5.4.** Assume that \(E\) has no places with split multiplicative reduction. If we also assume that \(#\text{Sel}(E[p^\infty]) < \infty\), then the sequence (2.5.1) is actually right-exact. Thus one finds that

\[ #\text{Sel}(M)[\gamma - 1] = \#\text{III}(E/F)[p^\infty] \cdot \prod_\nu (p\text{-part of Tamagawa number}) \cdot \prod_{\nu | p} \frac{(a_p - 1)\mathbb{Z}_p}{\mathbb{Z}_p}^2 \]

The interesting thing about this is that it incorporates all the special factors in the BSD Conjecture, in one package.

**2.6. \(\Lambda\)-modules.** We have non-canonically \(\Lambda \cong \mathbb{Z}_p[[T]]\). Let \(N\) be a finitely generated \(\Lambda\)-module. Since \(\Lambda\) is integrally closed noetherian, its localizations at height 1 primes are DVRs. Hence there is a structure theorem for finitely generated modules. The point is that this almost holds true for \(\Lambda\) itself. There is a map

\[ N \rightarrow \Lambda^r \times \prod_{i=1}^s \Lambda/(f_i) \]

with finite kernel and cokernel. Equivalently, the localizations of the (co)kernel at height 1 primes are 0.

The ideal \(\xi(N) := \prod f_i \subset \Lambda\) is uniquely determined. If \(N\) is a torsion \(\Lambda\)-module (so \(r = 0\)), then it is called the characteristic ideal of \(N\).

Now suppose that \(N\) has no non-zero finite order \(\Lambda\)-submodules. Then we have a short exact sequence

\[ 0 \rightarrow N \rightarrow \prod \Lambda/(f_i) \rightarrow \text{coker} \rightarrow 0. \]

Multiply by \(\gamma - 1\) and apply the snake lemma to obtain the exact sequence

\[ 0 \rightarrow N[\gamma - 1] \rightarrow \prod (\Lambda/(f_i))[\gamma - 1] \rightarrow \text{coker}[\gamma - 1] \rightarrow 0. \]

Recalling that \(\gamma - 1 \rightarrow T\), so modding out by \(\gamma - 1\) is like modding out by \(T\). So multiplication by \(T\) has a kernel on \(\Lambda/(f_i)\) if and only if \(T \mid f_i\), which happens if and only if \(f_i(0) \neq 0\). Hence if \(\xi(N) = (f)\) with \(f(0) \neq 0\), then we have

\[ 0 \rightarrow \text{coker}[\gamma - 1] \rightarrow N/(\gamma - 1) \rightarrow \prod \mathbb{Z}_p/(f_i(0)) \rightarrow \text{coker}/(\gamma - 1)\text{coker} \rightarrow 0. \]

Since \(#\text{coker}[\gamma - 1] = \#\text{coker}/(\gamma - 1)\text{coker}\), we conclude that

\[ \#N/(\gamma - 1) = \prod \#\mathbb{Z}_p/(f_i(0)). \]
We summarize the preceding discussion in the following Lemma.

**Lemma 2.6.1.** Let $N$ be a finitely generated $\Lambda$-module, torsion, with no pseudo-null submodules. If $\xi(N) = (f)$, then
\[
\# N / (\gamma - 1) N = \#(\mathbb{Z}_p / f(0) \mathbb{Z}_p)
\]
with the understanding that if $f(0) = 0$, then both sides are $\infty$.

Let $S = \text{Sel}(M) \subset H^1(G_{F,\Sigma}, M)$.

**Lemma 2.6.2.** Define $X := S^* = \text{Hom}_{\text{cts}}(S, Q_p / \mathbb{Z}_p)$. Then $X$ is a finite generated $\Lambda$-module.

**Proof.** We have a surjection
\[
H := H^1(G_{F,\Sigma}, M)^* \twoheadrightarrow X.
\]
We want to show that $H$ is finitely generated. Since $H$ is compact (being the dual of a discrete $\Lambda$-module), we just need to show that $H / (p, \gamma - 1) H$ is finite. We have $H / (p, \gamma - 1) H \cong H^1(G_{F,\Sigma}, M)[\gamma - 1, p]^*$, which by Lemma 2.5.1 is the same as $H^1(G_{F,\Sigma}, E[p])^*$, which is finite. \hfill $\Box$

Now that we know that $X$ is a cofinitely generated $\Lambda$-module, we'd then like to apply the preceding discussion to $X$. Is it torsion? This is a difficult question. It turns out that if $\text{Sel}(E[p^\infty])$ is finite then $X$ is torsion. If there are no places of split multiplicative reduction, you can see this because then $S[\gamma - 1]$ is finite, hence $X / (\gamma - 1)$ has finite order, so $X$ must be $\Lambda$-torsion.

What about the condition having no pseudo-null submodules? It is also true under the assumption that $\text{Sel}(E[p^\infty])$ is finite. This amounts to the fact that
\[
0 \to S \to H^1(G_{\Sigma}) \to \prod_v H^1(F_v, M) \to 0
\]
is right exact by a global duality argument. If $X$ has a pseudo-null submodule then we would have $S \to P^*$, hence $S / x S \to P^* / x P^*$ would be a finite order quotient, and then argue using the snake lemma.

Anyway, we can conclude that
\[
\# X / (\gamma - 1) X = \#(\mathbb{Z}_p / f(0) \mathbb{Z}_p)
\]
where $(f) = \xi(X)$, and the left side is $\# S[\gamma - 1]$, which is what we want to understand. Therefore, if $\text{Sel}(E[p^\infty])$ is finite then
\[
\# \text{Sel}(E/F)[p^\infty] \cdot \prod_v c_v, \mathbb{Z}_p \prod_v \#(\mathbb{Z}_p / (\alpha_v - 1) \mathbb{Z}_p)^2 = \#(\mathbb{Z}_p / f(0) \mathbb{Z}_p).
\]
This reformulates BSD as
\[
f(0) = \text{(unit)} \cdot \prod_v (\alpha_v - 1)^2 \cdot \frac{L(E/F, 1)}{\Omega_{E/F}}.
\]

### 3. Lecture 3 (2/19/2018)

#### 3.1. Review.

Let $E / \mathbb{Q}$ be an elliptic curve and $p > 2$ be a prime. Assume that $E$ has (good) ordinary or multiplicative reduction at $p$. Let
\[
T = T_p(E),
\]
\[
V = V_p(E) := T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,
\]
\[
W = V / T \sim E[p^\infty].
\]
Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension. We remind you that $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ is canonically identified with $\mathbb{Z}_p^\times$ via the cyclotomic character. Then we have a decomposition $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1+p\mathbb{Z}_p) =: \Delta \times \Gamma$. So $\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})^\Lambda$, with

$$\Gamma \xrightarrow{\sim} \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p.$$

Define $\Lambda = \Lambda_\mathbb{Q} := \mathbb{Z}_p[[\Gamma_\mathbb{Q}]]$. We have a canonical homomorphism

$$\Psi = \Psi_\mathbb{Q} : G_\mathbb{Q} \to \Gamma_\mathbb{Q} \subset \Lambda_\mathbb{Q}^\times$$

which we will use to identify $\Gamma_\mathbb{Q}$-characters with $G_\mathbb{Q}$-characters.

Define $M := T \otimes \Lambda^\times$, where $\Lambda^\times = \text{Hom}_{\text{cts}}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$. We have a $G_\mathbb{Q}$-action on $M$ through $\rho_{E,p} \otimes \Psi^{-1}$. For any (continuous) character $\chi : \Gamma_\mathbb{Q} \to Q_\mathbb{Q}^\times$ we considered $M[\gamma - \chi(\gamma)] = W(\chi^{-1})$. This is isomorphic to $W \otimes_{\mathbb{Z}_p} \mathcal{O}_L$ with the Galois action via $\rho_{E,p} \otimes \chi^{-1}$.

The Iwasawa-theoretic Selmer group (for $\mathbb{Q}_\infty$ and $E$) is

$$S(E/\mathbb{Q}_\infty) = \ker \left( H^1(Q, M) \to \prod_{\ell \neq p} H^1(I_p, M) \times H^1(I_p, M^-) \right).$$

What is $M^-$? Recall that we have a $G_{Q_p}$-filtration

$$0 \to T^+ \to T \to T^- \to 0$$

where $G_{Q_p}$ acts via the characters $\epsilon \alpha^{-1}$ and $\alpha$ on the sub and quotient, and $\alpha$ is the unramified character sending

$$\text{Frob}_p \to a_p = \begin{cases} \text{unit root of } x^2 - a_p(E)x + p & p \nmid N_E, \\ a_p(E) & p \mid N_E. \end{cases}$$

Finally, we defined $M^+ = T^+ \otimes_{\mathbb{Z}_p} \Lambda^\times$ and $M^- = M/M^+ \cong T^- \otimes_{\mathbb{Z}_p} \Lambda^\times$.

Recall the following facts discussed last time.

1. For $\Sigma \supset \{p, \ell \mid N_E, \infty\}$,

$$S(E/\mathbb{Q}_\infty) \subset H^1(G_\Sigma, M)$$

is $\Lambda$-cofinitely generated. This says that $X := S(E/\mathbb{Q}_\infty)^{\ast}$ is a finitely generated $\Lambda$-module. Hence it has a characteristic ideal $(f_E)$. Under an identification $\mathbb{Z}_p[[\Gamma_\mathbb{Q}]] \cong \mathbb{Z}_p[[T]]$, obtained by setting $\gamma - 1 \leftrightarrow T$ for a topological generator $\gamma$ of $\Gamma_\mathbb{Q}$, the values of $f_E$ at special points are related to the sizes of Selmer groups.

2. If $E[p]^\text{tor} = 0$, then we proved a control result, in the form of an exact sequence

$$0 \to \text{Sel}_{p^\infty}(E/\mathbb{Q}) \to S(E/\mathbb{Q}_\infty)[\gamma - 1] \to \prod_{\ell \mid N_E, \ell \neq p} H^1_{ur}(Q_{\ell}, W) \times (\mathbb{Z}_p/(\alpha_p - 1)\mathbb{Z}_p)^2.$$

If $\text{Sel}_{p^\infty}(E/\mathbb{Q})$ has finite order, then we can say something about the right exactness. If $E$ has good reduction at $p$, it is actually surjective.

**Remark 3.1.1.** There is a similar statement for $W(\chi^{-1})$, where $\chi$ is any finite-order character.

Keeping the notation of the preceding discussion, we have the following upshot. If $X(E/\mathbb{Q}_\infty) = S(E/\mathbb{Q}_\infty)^{\ast}$ is a $\Lambda$-finitely generated $\Lambda$-torsion module, then we can recover

$$\#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \#(\Lambda/(\xi(E/\mathbb{Q}_\infty), \gamma - 1)) = \#(\mathbb{Z}_p/f_E(0)).$$
3.2. **The $p$-adic $L$-function.** The Main Conjecture (for $E/\Q_{\infty}$) identifies a generator of $\xi(E/\Q_{\infty})$ as a $p$-adic $L$-function. What is the $p$-adic $L$-function for $E/\Q_{\infty}$? It is an analytic analogue of the big Selmer group. The big Selmer group packages the Selmer groups for all twists; the $p$-adic $L$-function packages special values of the complex $L$-function twisted by characters.

More precisely, the $p$-adic $L$-function will be an object $L_p(E/\Q_{\infty}) \in \Lambda_{Q} \otimes \Q$, which will lie in $\Lambda_{Q}$ if $E[p]$ is an irreducible $G_{Q}$-module. Here is the defining property. Let $\chi: \Gamma_{Q} \rightarrow \Q^\times$ be a finite-order character. Then $\chi(\gamma) = \zeta$, a primitive $p$th root of unity. We can extend $\chi$ to a $\Z_{p}$-algebra homomorphism $\phi_{\chi}: \Lambda_{Q} \rightarrow \Q_{p}$ sending $[\gamma] \mapsto \chi(\gamma)$. The $p$-adic $L$-function satisfies

$$\phi_{\chi}(L_p(E/\Q_{\infty})) = e_p(\chi) \frac{L(E, \chi^{-1}, 1)}{\Lambda_{E}}$$

(3.2.1)

where $\Lambda_{E}$ is a Néron period (the integral of a generator of the differentials on a Néron model along a cycle of $E$), and

$$e_p(\chi) = \begin{cases} \alpha_p^{t-1} & \zeta \neq 1 \\ \alpha_p^{-1}(1-1/\alpha_p)^m_p & \zeta = 1 \end{cases}$$

and

$$m_p = \begin{cases} 2 & E \text{ has good reduction at } p \\ 1 & E \text{ has multiplicative reduction at } p \end{cases}$$

The interpolation property (3.2.1) characterizes the element in $\Lambda$. More generally, given non-zero $f(T) \in \Z_{p}[[T]]$ the Weierstrass Preparation Theorem says that it can be written as

$$f(T) = p^{\mu} h(T) u(T)$$

where

- $\mu \geq 0$ is an integer,
- $u(T) \in \Lambda_{Q}^\times$, and
- $h(T) = T^{\lambda} + a_{\lambda-1}T^{\lambda-1} + \ldots + a_i$ with $p \mid a_i$ for all $i$.

In particular, $f(T)$ has finitely many zeroes in the disk $|z-1|_{p} < 1$. So if you had two power series satisfying (3.2.1), their difference would have infinitely many zeros and hence be 0. This is analogous to the statement that any complex analytic function can have only finitely many zeros in a compact region.

That gives uniqueness. But why does $L_p(E/\Q)$ exist? First of all to even talk about the value of $L(E, s)$ at $s = 1$ we need to know analytic continuation of the $L$-function, which holds because $E$ is modular. This means that there is a uniformization

$$X_0(N_E) \xrightarrow{\phi_{E}} E$$

with

$$\phi_{E}^* \omega_{E} = c_{E} 2\pi i \int_{E} \omega_{E}(\tau) d\tau$$

for a normalized newform $f_{E}$. Note that $c_{E}$ is not unique, as we can compose $\phi_{E}$ with an isogeny. The point is that

$$L(E, s) = L(f_{E}, s).$$

We will pretend that $c_{E} = \pm 1$.

---

It is actually expected that this should usually be the case; recent progress has been made by Cesnavicius.
We can view 
\[ \omega_f := 2\pi i f_E(\tau)d\tau \in \Omega^1(X_0(N)) \subset H^1_{\text{dR}}(X_0(N), \mathbb{C}). \]
Then the complex conjugate is 
\[ \overline{\omega_f} = -2\pi i f_E(\overline{\tau})d\overline{\tau} \in \overline{\Omega^1}. \]
Finally, define 
\[ \omega_f^\pm = \omega_f \pm \overline{\omega_f}. \]
Now \( H^1_{\text{dR}}(X_0(N), \mathbb{C}) = H^1(X_0(N), \mathbb{C}). \) This has a lattice coming from integral cohomology, because \( H^1(X_0(N), \mathbb{C}) = H^1(X_0(N), \mathbb{Z}) \otimes \mathbb{Q} \mathbb{C}. \) We can choose \( \Omega_f^\pm \in \mathbb{C}^* \) so that \( \eta_f^\pm := \Omega_f^\pm \omega_f^\pm \) is a \( \mathbb{Z}- \) generator.

We consider pairing the \( \eta_f^\pm \) against elements of \( H_1(X_0(N), \text{cusps}; \mathcal{O}), \) which is generated by modular symbols of the form \( \{ \frac{a}{b} \to \infty \}. \) The pairing looks like 
\[ \langle \eta_f^\pm, \{ \frac{a}{b} \to \infty \} \rangle = 2\pi i \int_0^\infty f(\frac{a}{b} + iy)idy, \]
so for \( f = \sum a_n e^{2\pi in\tau} \) we get 
\[ \langle \eta_f^\pm, \{ \frac{a}{b} \to \infty \} \rangle \sim \sum a_n e^{2\pi in\tau} n^{-1}, \]
which up to scalars we may have botched is 
\[ g(\chi^{-1}) \frac{L(f, \chi^{-1}, 1)}{\Omega_f^\pm} \in \mathbb{Z}[\chi]. \]
The choice of sign depends on \( \chi(-1). \) [MTT] showed that if \( a_p \) is a unit, then we these values interpolate to a \( p \)-adic \( L \)-function \( \mathcal{L}_p(E, \mathbb{Q}_\infty) \) in \( \Lambda_\mathbb{Q} = \mathbb{Z}_p[[\Gamma_0]] \), which is thought of as the space of \( \mathbb{Z}_p \)-valued measures on \( \Gamma_0. \)

**Remark 3.2.1.** There's another way to construct the \( p \)-adic \( L \)-function which is even more automorphic, using the Rankin-Selberg method. Let \( f \in S_2^{\text{new}}(\Gamma_0(N)) \). Take an Eisenstein series \( E_1, X_1, X_2 \subset M_1(\Gamma_0(M)). \) Consider also \( E_{1, (\chi_1, \chi_2)}^{-1, 1} \subset M_1(\Gamma_0(M)). \) Then we can view \( E_1 E_2 \subset M'' \) such that \( N | M''. \) Then 
\[ \langle f, E_1 E_2 \rangle_{\Gamma_0(N)} = (\epsilon)L(f, \chi_1, 1)L(f, \chi_2, 1). \]
The idea is that you can write down Fourier expansions of Eisenstein series very easily, so you can write down a \( p \)-adic family of Eisenstein series. Varying \( E_1 E_2 \) in a \( p \)-adic family, you can realize the pairing with \( f \) as a projection of some Hecke operator. This gives a \( p \)-adic interpolation of the right hand side. (See [MTT] and [Hid93].)

**Remark 3.2.2.** A big part of Iwasawa theory concerns the construction of \( p \)-adic \( L \)-functions for more general motives. There are conjectures of Coates, Greenberg, and Perrin-Riou predicting when \( p \)-adic \( L \)-functions should exist and what they should look like.

### 3.3. The Main Conjecture for elliptic curves

We now state the Main Conjecture for \( E/\mathbb{Q}_\infty \):

**Conjecture 3.3.1 (Iwasawa Main Conjecture).** Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Then

1. \( X(E/\mathbb{Q}_\infty) \) is a torsion \( \Lambda \)-module, and
2. \( \xi(E/\mathbb{Q}_\infty) = (\mathcal{L}_p(E/\mathbb{Q}_\infty)) \in \Lambda \otimes \mathbb{Q}_p. \) The equality can even be taken in \( \Lambda \) if \( E[p] \) is an irreducible \( \mathbb{Q}_p \)-module.
Remark 3.3.2. From what we’ve already said, we have the following interesting consequence. Suppose \( E \) has good reduction at \( p \) and \( E[p] \) is an irreducible \( G_{\mathbb{Q}} \)-representation, and the Iwasawa Main Conjecture is true. Then
\[
\left. \frac{L(E, 1)}{\Omega_E} \right|_p = \left. \# \text{Sel}_{p^{\infty}}(E/\mathbb{Q}) \prod_{\ell \mid N_E} c_\ell(E/\mathbb{Q}) \right|_p^{-1}
\]
This is the \( p \)-part of BSD when \( L(E, 1) \neq 0 \).

What is known about the Main Conjecture? If \( E \) has CM, then Rubin proved Conjecture 3.3.1, using the Euler system of elliptic units.

For general \( E \) (under some technical assumptions), Kato proved (1) in Conjecture 3.3.1 and one inclusion in (2): that \( \xi(E/\mathbb{Q}_\infty) \supset (\mathcal{L}_p(E/\mathbb{Q}_\infty)) \) in \( \Lambda \otimes \mathbb{Q}_p \), and even in \( \Lambda \) under certain hypotheses.

**Theorem 3.3.3** (Kato, Skinner-Urban). If

1. \( E \) has ordinary or multiplicative reduction at \( p \geq 3 \),
2. \( E[p] \) is an irreducible \( G_{\mathbb{Q}} \)-representation,
3. There exists \( \ell \mid N_E \) (i.e. multiplicative reduction at \( \ell \)), \( \ell \neq p \), such that \( E[p] \) is ramified at \( \ell \) (i.e. \( p \nmid c_\ell(E/\mathbb{Q}) \), i.e. \( p \nmid \text{ord}_\ell(\Delta_{\text{min}}^\text{E}) \))

then Conjecture 3.3.1 holds.

**Remark 3.3.4.** Concerning the hypotheses of Theorem 3.3.3. If \( E \) has semistable reduction, i.e. \( N_E \) is square-free, and \( p \nmid N_E \), then (2) implies (3) by one of Ribet’s level-lowering results.

Also, (2) holds if \( p \geq 11 \) by work of Mazur, etc.

**Remark 3.3.5.** Work of Greenberg-Vatsal and Kato implies some cases of Conjecture 3.3.1 when \( E[p] \) is reducible.

There are also “numerical conditions” that imply the Iwasawa Main Conjecture, which are usually of the form “if something is a unit, then the Iwasawa Main Conjecture holds”.

**Corollary 3.3.6.** For \( E \) satisfying the hypotheses of Theorem 3.3.1 then we have

1. If \( L(E, 1) \neq 0 \), then
\[
\left. \frac{L(E, 1)}{\Omega_E} \right|_p = \left. \# \text{III}(E/\mathbb{Q}) \cdot p^{\infty} \prod_{\ell \mid N_E} c_\ell(E/\mathbb{Q}) \right|_p.
\]
2. If \( L(E, 1) = 0 \), then \( \text{Sel}_{p^{\infty}}(E/\mathbb{Q}) \) has corank \( \geq 1 \).

3.4. **Idea of the proofs.** The pieces are proved very differently. Kato’s proof is an Euler system argument.

The argument of Skinner-Urban uses congruences between cusp forms and Eisenstein series on \( GU(2, 2) \), plus Galois representations attached to the cusp forms. This generalizes ideas of Ribet, which were extended by Wiles, for \( GL_2 \).

The Skinner-Urban approach constructs subgroups of \( S(E/\mathbb{Q}_\infty) \), which are related to the \( p \)-adic \( L \)-function.

We need both components. For the classical Iwasawa main conjecture you only need one, since you have the analytic class number formula. (In other words, either containment implies both.)

---

3 By work of Nekovar and others, we know a parity form of BSD, so if moreover \( w_E = +1 \), then \( \text{Sel}_{p^{\infty}}(E/\mathbb{Q}) \) has corank \( \geq 2 \).
3.4.1. \textit{Kato's proof.} I want to sketch the flavor of Kato’s argument. We have $S(E/Q_\infty) \subset H^1(Q,M)$. This is a direct limit. Euler systems are an inverse limit, so Kato studies the dual. For $M = T \otimes \Lambda^*$, $M^* = T \otimes \Lambda$ with the Galois action $\rho_E \otimes \wp_Q$.

The Euler systems have to do with constructing elements of $H^1(Q,T \otimes \Lambda)$. Kato constructs a class $z_{Kato} \in H^1(Z[1/p], T \otimes \Lambda)$. The idea is to look at the tower of modular curves $X_i(p^n N_E)$, defined over $Q(\zeta_{p^n})$. Take two units $u_1, u_2 \in \mathcal{O}(Y_1(p^n N_E))^\times$. By Kummer theory we can view these in $H^1(Y_1(p^n N_E), \mathbb{Z}_p(1))$. Then their cup product lies in $H^2(Y_1(p^n N_E)/Q(\zeta_{p^n}), \mathbb{Z}_p(2))$.

Using a spectral sequence you get a class in $H^1(QH^1(Y_1(p^n N_E), \mathbb{Z}_p(1)))$. Then you take corestriction down to $Q$. By some general fact about good reduction, the class comes from $Z[1/p]$.

Using the good reduction at $p$, we have a sequence

$$ H^1(Z[1/p], T \otimes \Lambda) \xrightarrow{\text{res}} H^1(Q_p, T \otimes \Lambda) \xrightarrow{\sim} (H^1(Q_p, M^*))^\vee \rightarrow S(E/Q_\infty)^\vee \rightarrow S_{str}(E/Q_\infty)^\vee. \quad (3.4.1) $$

This is exact for the first three terms.

We have $\Lambda \cdot z_{Kato} \in H^1(Z[1/p], T \otimes \Lambda)$. There is a Coleman map

$$ H^1(Q_p, T \otimes \Lambda) \xrightarrow{\sim} \Lambda. $$

The Euler system argument implies that the first map in (4.4.2) is injective. Under the Coleman map the image of $z_{Kato}$ turns out to be $\mathcal{L}_p(E/Q_\infty)$, up to a unit. This can be computed thanks to an explicit reciprocity law. We know that $\mathcal{L}_p(E/Q_\infty) \neq 0$ since a theorem of Rohrlich implies that the $p$-adic $L$-function is non-zero. By an Euler characteristic argument for (4.4.2), the Iwasawa Main Conjecture

$$ \text{char}_\Lambda(\Lambda/\mathcal{L}_p) = \text{char}_\Lambda(S(E/Q_\infty)^\vee) $$

can be reformulated as

$$ \text{char}_\Lambda\left(\frac{H^1(Z[1/p], T \otimes \Lambda)}{\Lambda z_{Kato}}\right) = \text{char}_\Lambda(S_{str}(E/Q_\infty)^\vee). $$

Kato shows the divisibility $\subseteq$.

3.4.2. \textit{Ribet’s converse to Herbrand.} What about the other direction? The idea goes back to Ribet’s proof of the converse to Herbrand’s theorem, which we now review. Suppose $p \mid \zeta(1-2k)$. We have an Eisenstein series

$$ E_{2k}(\tau) = \frac{\zeta(1-2k)}{2} + \sum_{n=1}^{\infty} \left( \sum_{d|n} q^{2k-1} \right) q^n. $$

The divisibility assumption implies that

$$ E_{2k} \equiv \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n \pmod{p} $$

which in particular “looks like a cusp form” mod $p$. Then some appropriate linear combination $E_{2k} - \zeta(1-2k) G_4^a G_6^b$ actually is a cuspform in $S_{2k}(1)$. Moreover, there is a cuspidal eigenform congruent to $E_{2k}$ mod $p$,

$$ f = \sum_{n=1}^{\infty} c_n q^n \in S_{2k}(1, O) $$
for \( \mathcal{O} = \mathcal{O}_L \) in some finite extension \( L/\mathbb{Q}_p \).

The congruence implies that \( c_t \equiv 1 + \ell^{2k-1} \) for all primes \( \ell \), and in particular \( c_p \in \mathcal{O}^\times \), i.e. \( f \) is ordinary. Then the Galois representation \( \rho_{f,p} : \mathbb{G}_Q \rightarrow \text{GL}_2(\mathcal{O}) \) looks like

\[
\rho_{f,p}|_{\mathcal{O}_p} \sim \begin{pmatrix} \ell^{2k-1} \alpha^{-1} & \ast \\ 0 & \alpha \end{pmatrix}
\]

where \( \alpha_p := \alpha(Frob_p) \) is the unit root of \( X^2 - a_p X + p^{2k-1} \). Because \( f \) is a cusp form, \( \rho_{f,p} \otimes \mathbb{Q}_p \) is irreducible. Let \( V \) be the 2-dimensional \( L \)-space underlying \( \rho_{f,p} \). Choose \( \omega \in V \) spanning the \( L(\ell^{2k-1} \alpha^{-1}) \) line. Then consider \( T = \mathcal{O}[\mathbb{G}_Q] \omega \subset V \). By the irreducibility of \( \rho_{f,p} \), \( T \) is a lattice, hence \( T \cong \mathcal{O}^2 \), so \( T/pT \cong \mathbb{F}^2 \). For \( \ell \neq p \), \( V \) is unramified and

\[
\text{Tr}(\text{Frob}_\ell) = c_t \equiv 1 + \ell^{2k-1} \quad (\text{mod } p).
\]

This shows that

\[
\overline{\rho}_{f,p} \sim \begin{pmatrix} 1 & \ast \\ \omega^{2k-1} & \ast \end{pmatrix}.
\]

Then some work shows that

\[
\overline{\rho}_{f,p} \sim \begin{pmatrix} 1 & \ast \\ 0 & \omega^{2k-1} \end{pmatrix}
\]

with \( \ast \neq 0 \), i.e. a non-split extension. (The extension has to be in this direction because of the way we choose the lattice, since we arranged that the reduction of \( \nu \) should generate the whole representation.) It is unramified at \( \ell \neq p \), and turns out to be split at \( p \). Therefore the entry \( \ast \) defines an every unramified extension of \( \mathbb{Q}(\mu_p) \).


4.1. Last week's episode. Last time we discussed the cyclotomic Main Conjecture for \( E \). Let

\[
\Gamma = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong 1 + p\mathbb{Z}_p \cong \mathbb{Z}_p.
\]

Choose \( \gamma := 1 + p \) as a topological generator for \( 1 + p\mathbb{Z}_p \) as a multiplicative group \( 1 + p\mathbb{Z}_p \). Let \( \Lambda = \mathbb{Z}_p[[\Gamma]] \), which is non-canonically isomorphic to \( \mathbb{Z}_p[[T]] \) via the map \( \gamma \rightarrow 1 + T \).

The Main Conjecture predicts that

\[
\text{char}_\Lambda(S(E/\mathbb{Q}_\infty \gamma)) \cong (\mathcal{L}_p(E/\mathbb{Q}_\infty)).
\]

What is this good for? If \( L(E,1) \neq 0 \) then it implies that \( L(E,1) \) is equal to the expected value under BSD, namely

\[
\left| \frac{L(E,1)}{\Omega_E} \right|_p^{-1} = \left| \frac{\#\text{III}(E/\mathbb{Q})[p^\infty]}{(\text{#E}_{\text{tors}}(\mathbb{Q}))^2} \times \prod_{\ell | \Omega_E} c_\ell(E/\mathbb{Q}) \right|_p^{-1}.
\]

Also, it shows that if \( L(E,1) = 0 \) then \( \text{Sel}_{p^\infty}(E/\mathbb{Q}) \) has rank \( \geq 1 \).

Suppose \( \text{ord}_{s=1} L(E,s) = 1 \). Then theorems of Gross-Zagier and Kolyvagin imply that \( \text{rank } E(\mathbb{Q}) = 1 \), and \( \#\text{III}(E/\mathbb{Q}) < \infty \). In particular, \( \#\text{Sel}_{p^\infty}(E/\mathbb{Q}) \) has corank equal to 1. We can ask the following questions.

**Question 4.1.1.** If \( \text{Sel}_{p^\infty}(E/\mathbb{Q}) \) has corank 1, can we prove that \( \text{ord}_{s=1} L(E,s) = 1 \)?
Question 4.1.2. If Sel\(_{p^\infty}(E/\mathbb{Q})\) has corank 1, can we say anything about

\[
\left| \frac{L'(E,1)}{\Omega_{E/R}(E/\mathbb{Q})} \right|_p^{-1}
\]

(The fraction is rational by Gross-Zagier.)

We will discuss some progress towards these questions.

4.2. Gross-Zagier. Let’s review the Gross-Zagier formula. We continue to assume that \(E/\mathbb{Q}\) is an elliptic curve such that \(\text{ord}_s L(E,s) = 1\).

Let \(K/\mathbb{Q}\) be an imaginary quadratic field. We have another elliptic curve \(E^K/\mathbb{Q}\), which is the twist of \(E\) corresponding to the cocycle \(H^1(\mathbb{Q}, \text{Aut}(E))\) obtained by taking the quadratic character associated to \(K/\mathbb{Q}\) by class field theory, and mapping it via \(H^1(\mathbb{Q}, \{\pm 1\}) \rightarrow H^1(\mathbb{Q}, \text{Aut}(E))\).

Assume that \(\text{ord}_s L(E^K/s) = 1\), which is equivalent to \(L(E^K, 1) \neq 0\) because \(L(E/K, 1) = L(E, s)L(E^K, s)\).

Remark 4.2.1. Note that \(w_E = 1\), and the assumption \(\text{ord}_s L(E/K, s) = 1\) implies \(w(E) = +1\), or equivalently \(w(E/K) = -1\). This is assured by the “Heegner condition” \(^4\) \((D_K, N_E) = 1\) and every prime \(\ell \mid N_E\) splits in \(K\).

The Heegner condition can be relaxed\(^5\). Continue to assume that \((D_K, N_E) = 1\) and \(N_E = N_+ \cdot N_-\). If \(N_-\) is squarefree, you have split or nonsplit multiplicative reduction, which contributes \(-1\) or \(+1\) respectively to the local sign, but nonsplit reduction becomes split in an inert extension, so we are okay as long as there are an even number of primes dividing \(N_-.\)

An arithmetic progression of discriminants will satisfy these Heegner conditions. Then analytical results imply that there exist infinitely many \(K\) such that the order of vanishing is as desired, i.e. \(L(E^K, 1) \neq 0\).

Let \(B\) be a quaternion algebra of discriminant \(N^-\). Let \(R_{N^+} \subset B\) be an Eichler order (an analogue of \(\Gamma_0(N^+)\)), and \(\iota: K \rightarrow B\) an optimal embedding, i.e. \(\iota(K) \cap R_{N^+} = \mathcal{O}_K\).

This data gives rise to a Shimura curve \(X_B\), of level \(\Gamma_0(N^+)\), and a CM point \(z \in X_B\) (coming from \(\iota\)) defined over the Hilbert class field \(H\) of \(K\).

The modularity of \(E\) implies that there is a modular parametrization

\[
\phi: X_B \rightarrow E.
\]

(The issue of normalization is tricky because there are no cusps on a Shimura curve.) Then \(\phi(z) \in E(H)\), and we define

\[
y_K := \sum_{\sigma \in \text{Gal}(H/K)} \sigma \phi(z) \in E(K).
\]

This is the “Heegner point”.

The Gross-Zagier formula says that

\[
\frac{L'(E/K, 1)}{\Omega_{E/K}} = (*)\langle y_K, y_K \rangle_{NT}\]

(4.2.1)

where \((*)\) is some fudge factor.

\(^4\)This is the classical Heegner condition used by Gross-Zagier.

\(^5\)As appears in refinements by Shouwu Zhang
According to BSD, we should have (under our hypotheses)
\[
\frac{L'(E/K, 1)}{\Omega_{E/K}} = \frac{\#\text{III}(E/K) R(E/K)}{(\#E_{\text{tors}}(K))^2} \prod_v c_v(E/K).
\] (4.2.2)

Kolyvagin proved that if \( y_K \) is not torsion, then \( \text{rank} E(K) = 1 \), and even more precisely that \( \text{rank} E(\mathbb{Q}) = 1 \), \( \text{rank} E^K(\mathbb{Q}) = 0 \), \( \#\text{III}(E/\mathbb{Q}) < \infty \) and \( \#S(K^e/\mathbb{Q}) < \infty \).

Since \( E(K) \) has rank 1, we have \( y_K = mP \) for some \( m \), hence
\[
m^2 \langle P, P \rangle_{\text{NT}} = \langle y_K, y_K \rangle_{\text{NT}}.
\]

Combining this with (4.2.1) and (4.2.2), we see that we should relate the index of \( y_K \) to the order of \( \#X(E/K) \).

The value of the derivative of \( L(E/K) \) is
\[
L'(E, 1) \frac{R(E/K)}{(\#E_{\text{tors}}(K))^2} \prod_v c_v(E/K).
\]

We can use the Main Conjecture to understand the second factor.

To get a \( p \)-adic statement, the naive idea might be to try to differentiate the \( p \)-adic \( L \)-function.

We have
\[
L_p(E/\mathbb{Q}_\infty) \in \Lambda \cong \mathbb{Z}_p[[T]],
\]
and then take
\[
\frac{d}{dT} L_p|_{T=0}.
\]

A \( p \)-adic BSD might predict that
\[
\frac{d}{dT} L_p|_{T=0} = \frac{\#\text{III}(E/\mathbb{Q}) R_p(E/\mathbb{Q})}{\#E_{\text{tors}}(\mathbb{Q})} \prod_v c_v(E/\mathbb{Q}).
\]

Here \( R_p \) is a \( p \)-adic regulator. The issue is that \( R_p(E/\mathbb{Q}) \) is not known to be non-zero, i.e. the \( p \)-adic height pairing is not known to be non-degenerate.

4.3. The Bertolini-Darmon-Prasad formula. Work of Bertolini-Darmon-Prasanna proved a formula relating the \textit{value} (as opposed to the derivative) of a \( p \)-adic \( L \)-function to the \( p \)-adic logarithm of the Heegner point. We will explain their formula now.

Let \( E/\mathbb{Q} \) be an elliptic curve, of conductor \( N_E \). Let \( K \) be an imaginary quadratic field, satisfying the Heegner condition. (Recall that this implies \( w(E/K) = -1 \).) Assume that \( p = v \bar{v} \) splits in \( K \). Choose an embedding \( \mathbb{Q} \hookrightarrow \mathbb{Q}_p \) inducing \( v \) on \( K \).

They construct a \( p \)-adic \( L \)-function\(^6\) \( L_{\text{BDP}} \) (which depends on the anticyclotomic extension \( K_{\infty}^{ac} \)). Then \( L_{\text{BDP}} \in \mathbb{Z}_p[[\Gamma_{\infty}^{\text{ac}}]] \), and it is characterized by the interpolation property
\[
\phi_\chi(L_{\text{BDP}}) = \frac{L(E, \chi^{-1}_\text{alg}, 1) \Omega_\infty^{4m}}{\Omega_\infty^{4m} \Omega_p} \quad (4.3.1)
\]

for characters \( \chi \) of the following form. We consider characters
\[
\chi : G_K \to \Gamma_{\text{ac}} \to \mathbb{Q}_p^\times
\]
which are crystalline at \( v, \bar{v} \) with HT weight at \( v \) being \(-m < -1\) and the HT weight at \( \bar{v} \) being \( m > 1 \). (The negation comes from the fact that the extension is anticyclotomic.) In terms of the corresponding algebraic Hecke character \( \chi_{\text{alg}} \), this means that
\[
\chi_{\text{alg}}|_{\mathbb{Q}(\mathbb{R})^*} = \left( \frac{Z}{\mathbb{R}} \right)^m.
\]

\(^6\)Actually BDP construct a square root of this \( L \)-function.
Remark 4.3.1. Notice that the periods are independent of $E$. This is partly because of the nature of the characters $\chi$. Note that $\chi^{-1}_{alg} \cdot |-|^m$ has infinity type $z^{-2m}$. This implies (e.g. by the Converse Theorem) that the character is naturally attached to a newform of weight $2m + 1$, say $g_{\chi^{-1}_{alg}}$. Hence

$$L(E, \chi^{-1}_{alg}, 1) = L(E, \chi^{-1}_{alg}, m + 1) = L(f_E \times g_{\chi^{-1}_{alg}}, m + 1).$$

The point is that $f_E$ has weight 2 and $g_{\chi^{-1}_{alg}}$ has weight $2m + 1 > 2$. In Rankin-Selberg $L$-functions, the period is the one for the form of higher weight, which is $g$. Classically, $g$ would have weight 1, and then the period would be that for $f$.

It makes sense to consider $\chi = 1$, although this falls out of the range of HT weights for interpolation. Bertolini-Darmon-Prasanna show that

$$\phi_1(\mathcal{L}_{BDP}) = \frac{1 - a_p + p}{p} \log_{E(K_p) \otimes \mathbb{Q}_p}(y_K)^2. \tag{4.3.2}$$

If $y_K$ is non-torsion, then the logarithm isn’t 0, and BSD would predict that the value of $\mathcal{L}_{BDP}$ is related to the size of III. This type of question, relating the values of $L$-functions to the sizes of Tate-Shafarevich groups, is the domain of Iwasawa theory.

Our discussion suggests that there is a Main Conjecture for the Selmer group associated to $T_p(E) \otimes \chi$. What Selmer group is it? Let $\Lambda_{ac} = \mathbb{Z}_p[[\Gamma_{ac}]]$. Strictly speaking the $p$-adic $L$-function only lives in the extended ring $\Lambda_{ur} := \mathbb{Z}_p[[\Gamma_{ac}]][\varpi]$.\footnote{This is because of the choice of periods. We could have made a choice so that the $p$-adic $L$-function would actually live in $\Lambda_{ac}$.}

We define a Selmer group

$$S_{BDP} = S_{BDP}(E/K_{ac}^\infty) \subset H^1(K, T_p(E) \otimes \mathbb{Z}_p \Lambda_{ac}^\vee)$$

with $G_K$ acting on $T_p(E) \otimes \mathbb{Z}_p \Lambda_{ac}^\vee$ through $\rho_{E,p} \otimes \psi_{ac}^{-1}$. The Selmer group is defined by local conditions

$$\text{res}_w(c) = \begin{cases} \text{unramified} & w \nmid p, \text{ res. deg}(w) = 1 \\ 0 & w \nmid p, \text{ res. deg}(w) = 2 \\ 0 & w = \overline{v} \\ \text{anything} & w = v. \end{cases} \tag{4.3.3}$$

Remark 4.3.2. The second condition has to do with anticyclotomic theory. It is almost the same as unramified, except by powers of $p$ that we don’t want to include. The last conditions are a translation of crystallinity, when the HT weights lie in the range of interpolation.

Conjecture 4.3.3. $X_{BDP} := S_{BDP}^{\ast}$ is a torsion $\Lambda$-module, and moreover

$$\text{char}_{\Lambda_{ac}}(X_{BDP}) \Lambda_{ur}^{ac} = (\mathcal{L}_{BDP}).$$

In the cyclotomic case, the torsion property was a consequence of Kato’s work (producing Euler systems). In this case, it can be deduced from work of Cornul-Vatsal and Kolyvagin (using Heegner points). Namely, Cornul-Vatsal prove that for all but finitely many finite-order $\chi$, $L(E, \chi, 1) \neq 0$, hence $y_K(\chi)$ is non-torsion by Gross-Zagier. By Kolyvagin, this is equivalent to $H^1_f(K, W(\chi))$ having corank 1, where $W(\chi) = E[p^\infty] \otimes \mathbb{Z}_p \phi(\chi)$. In other words, $H^1_f(K, V_p(E(\chi)))$ is 1-dimensional and spanned by $y_K$, so the same arguments as for trivial $\chi$ imply that $S_{BDP}(E, \chi)$ is finite.
Recall from the control theorem that we have a short exact sequence
\[ 0 \rightarrow S_{\text{BDP}}(E, \chi) \rightarrow S_{\text{BDP}}[\gamma - \chi(\gamma)^{-1}] \rightarrow \text{finite order} \]
so \( X_{\text{BDP}}/(\gamma - \chi^{-1}(\gamma)) \) has finite order, hence \( X_{\text{BDP}} \) is a torsion \( \Lambda_{\text{ac}} \)-module. So the first statement of the conjecture is a theorem.

I figured that the BDP formula should be useful for BSD. Suppose that \( \text{rank } E(K) = 1 \) and \( \#\text{III}(E/K)[p\infty] < \infty \). This implies that \( \text{Sel}_{p\infty}(E/K) \) has corank 1. We have a map \( \text{Sel}_{p\infty}(E/K) \rightarrow E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \) from the definition of the Selmer group, which is then necessarily an isomorphism (since the rank of \( \text{Sel}_{p\infty}(E/K) \) comes from a global rational point).

Suppose we start with the assumption that \( \text{rank } \text{Sel}_{p\infty}(E/K) = 1 \) and that the maps
\[
\text{Sel}_{p\infty}(E/K) \rightarrow E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \\
\text{Sel}_{p\infty}(E/K) \rightarrow E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p
\]
are surjections. Can we prove that \( \text{rank } E(K) = 1 \)? More specifically, can we prove that the Heegner point is non-torsion?

We have a surjection \( H^1_f(K, V_p(E)) \rightarrow \text{Sel}_{p\infty}(E/K) \) and the hypothesis is equivalent to assuming that the restriction map
\[
H^1_f(K, V_p(E)) \approx \mathbb{Q}_p \rightarrow H^1_f(K_w, V_p(E)) \approx \mathbb{Q}_p
\]
is surjective. This implies that \( H^1_{\text{BDP}}(K, V_p(E)) = 0 \), where the BDP condition is as in (4.3.3), in particular 0 at \( \mathfrak{v} \) and no condition at \( v \). The reason is that \( H^1_{\text{unr outside } p}(K, V_p(E)) \) has 2-dimensional image in the 4-dimensional space \( \prod_{w | p} H^1(K_w, V_p(E)) \). We have assumed that \( H^1_f(K, V_p(E)) \) has 1-dimensional image in this 4-dimensional space, so if \( H^1_{\text{BDP}}(K, V_p(E)) = 0 \) is non-zero then it and the conjugate Selmer group would together contribute a 2-dimensional image.

Then we can prove a control theorem
\[ 0 \rightarrow \text{Sel}_{\text{BDP}}(E/K) \rightarrow \text{Sel}_{\text{BDP}}[\gamma_{\text{ac}} - 1] \rightarrow \text{finite cokernel} \]
hence the finiteness of \( \text{Sel}_{\text{BDP}}(E/K) \) implies the finiteness of \( \text{Sel}_{\text{BDP}}[\gamma_{\text{ac}} - 1] \), hence
\[
\Lambda_{\text{ac}}/\gamma_{\text{ac}} - 1, \text{char } A(S_{\text{BDP}}) = \# \mathbb{Z}_p/\gamma_{\text{BDP}}(0) < \infty,
\]
where \( g_{\text{BDP}} \) is a generator of the characteristic ideal. Then (half of) a Main Conjecture would imply \( \phi_1(\mathscr{L}_{\text{BDP}}) \neq 0 \), and then BDP formula (4.3.2) would imply \( \log_{E(K_v)}/Y_K \neq 0 \).

X. Wan has proved the relevant Main Conjecture for squarefree \( N_E \), using automorphic congruences on \( U(3, 1) \). The signature is actually important; for the cyclotomic case we looked at \( U(2, 2) \).

What about the hypotheses that we imposed? The conditions \( \text{Sel}_p(E/K) \cong \mathbb{Z}/p\mathbb{Z} \) and \( E[p](K) = 0 \) imply \( \text{Sel}_{p\infty}(E/K) \cong \mathbb{Q}_p/\mathbb{Z}_p \). If we didn't have the further condition on the local restriction, then we would be done. In fact we can get rid of that assumption.

### 4.4. The Beilinson-Flach Euler system.

In the cyclotomic case, we saw a way to reformulate the Main Conjecture without \( L \)-functions. The reformulation was in terms of an Euler system \( z_{\text{Kato}} \), and said
\[
\text{char}_{A}\left( \frac{H^1[\mathbb{Z}/p], T_p(E) \otimes \mathbb{Z}_p \Lambda}{Z_{\text{Kato}}} \right) = \text{char}_{A}(S_{\text{str}}(E/\mathbb{Q}_\infty)) \tag{4.4.1}
\]
where “strict” means “trivial at \( p \)”. The equivalence came from an exact sequence
\begin{align*}
H^1(\mathbb{Z}[1/p], T \otimes \Lambda) & \xrightarrow{\text{res}} H^1(\mathbb{Q}_p, T \otimes \Lambda) \\
& \cong (H^1(\mathbb{Q}_p, M^+))^\vee \to S(E/\mathbb{Q}_\infty)^\vee \to S_{\text{str}}(E/\mathbb{Q}_\infty)^\vee. \quad (4.4.2)
\end{align*}

Since \(E[p]\) is irreducible over \(G_{\mathbb{Q}}\), \(H^1(\mathbb{Z}[1/p], T \otimes \Lambda)\) is torsion-free, and by the assumption it has rank 1. Hence
\[
0 \to \frac{H^1(\mathbb{Z}[1/p], T \otimes \Lambda)}{z_{\text{Kato}}} \xrightarrow{\text{res}} \frac{H^1(\mathbb{Q}_p, T \otimes \Lambda)}{H^1(\mathbb{Q}_p, T^+ \otimes \Lambda), z_{\text{Kato}}} \cong (H^1(\mathbb{Q}_p, M^+))^\vee \to S(E/\mathbb{Q}_\infty)^\vee \to S_{\text{str}}(E/\mathbb{Q}_\infty)^\vee
\]
is exact. On the other hand, there is a Coleman regulator map identifying
\[
H^1(\mathbb{Q}_p, T \otimes \Lambda) \xrightarrow{\text{res}} \Lambda \to (\mathbb{Z}_p)^\vee.
\]

Putting these two facts together, and taking Euler characteristics led to (4.4.1).

Recently Lei-Loeffler-Zerbes introduced a new Euler system for Rankin-Selberg convolutions. Their construction is motivated by Beilinson's conjectures, which predicts special values of \(L\)-functions up to a rational factor. The construction of Lei-Loeffler-Zerbes involves an integral refinement of Beilinson's conjectures. They construct "Beilinson-Flach elements" in \(H^3(\mathbb{Q}_2, \mathbb{Z}_p(2))\). The idea is to push forward via
\[
H^1_{\text{et}}(Y, \mathbb{Z}_p(1)) \to H^3_{\text{et}}(Y^2, \mathbb{Z}_p(2)).
\]

By Kummer theory, the class in \(H^1_{\text{et}}(Y, \mathbb{Z}_p(1))\) is obtained from \(\mathcal{O}(Y)^{\vee} \otimes \mathbb{Z}_p\). Pushing forward via perturbations of the diagonal map, we can make some appropriate class in \(H^3_{\text{et}}(\mathbb{Q}_2, \mathbb{Z}_p(2))\). Then by a spectral sequence we have a map
\[
H^3_{\text{et}}(\mathbb{Q}_2, \mathbb{Z}_p(2)) \to H^1(\mathbb{Q}_p, H^2(\mathbb{Q}_2^\vee, \mathbb{Z}_p(2))_{\text{str}}).
\]

Now \(H^2(\mathbb{Q}_2^\vee, \mathbb{Z}_p(2))_{\text{str}}\) contains a contribution from \(H^1(\mathbb{Q}_p, \mathbb{Z}_p(1))\) \(\otimes \mathbb{Z}_p\), which contains \(\rho_f \otimes \rho_g\). Actually the Tate twists give us a problem, so we should consider \(H^1(\mathbb{Q}_\infty, H^2(\mathbb{Q}_2^\vee, \mathbb{Z}_p(2))_{\text{str}})\) instead. Then we want to vary this story \(p\)-adically. In practice, we might be interested in \(\rho_f\) coming from an elliptic curve and \(\rho_g\) coming from a Hecke character of \(K\).

Assume that \(p\) splits in \(K\) and \(E\) is ordinary at \(p\). Let \(\Lambda_K = \mathbb{Z}_p[[I_K = \text{Gal}(\mathbb{K}_\infty/K) \cong \mathbb{Z}_p^2]]\). The \(p\)-adic variation leads to the Beilinson-Flach class
\[
z_{\text{BF}} \subset H^1(K, T_p E \otimes \Lambda_K).
\]

In fact the class lives in the Selmer group consisting of elements "unramified away from \(p\)", "ordinary at \(v\)", i.e. \(\text{res}_v \in \text{Im } H^1(K_v, T^+_v \otimes \Lambda_K)\), and relaxed (i.e. no condition) at \(\overline{v}\). Let's write this Selmer group as \(H^1_{\text{ord,rel}}(\mathcal{O}_K[1/p], T_p E \otimes \mathbb{Z}_p \Lambda_K)\). Then the reformulation of the Main Conjecture is
\[
\text{char}_{\Lambda_K} \left( \frac{H^1_{\text{ord,rel}}(\mathcal{O}_K[1/p], T_p E \otimes \mathbb{Z}_p \Lambda_K)}{z_{\text{BF}}} \right) = \text{char}_{\Lambda_K} (S_{\text{str}}(E/\mathbb{K}_\infty)^\vee). \quad (4.4.3)
\]

We can tease out consequences of this using \textit{two} exact sequences, coming from \(\text{res}_v\) and \(\text{res}_\overline{v}\).
\[
H^1_{\text{ord,rel}}(K, T \otimes \Lambda) \xrightarrow{\text{res}_v} \text{Im } H^1_{\text{ord}}(K_v, T \otimes \Lambda) \cong \left( \frac{H^1(K_v, M)}{H^1_{\text{ord}}(K_v, M)} \right)^\vee \to X_{\text{rel},0} \to X_{\text{ord},0} \to 0.
\]
Then the Main Conjecture (4.4.3) implies that

\[
\text{char}_v \left( \frac{\text{Im} \ H^1_{\text{ord}}(K_v, T \otimes \Lambda)}{\text{res}_v(z_{\text{BF}})} \right) \cong \text{char}_v(X_{\text{rel,str}}).
\]

By Perrin-Riou’s big logarithm,

\[
\frac{\text{Im} \ H^1_{\text{ord}}(K_v, T \otimes \Lambda)}{\text{res}_v(z_{\text{BF}})} \cong \Lambda_{K_v}^{\text{ur}} \frac{L_{\text{Gr}}(E/K_{\infty})}{\mathbb{L}}
\]

where the image of \( \text{Log}_v(z_{\text{BF}}) \) is \( L_{\text{Gr}}(E/K_{\infty}) \), a \textit{two}-variable \( L \)-function (for the cyclotomic and anticyclotomic directions).

There is a parallel story for \( T \). The exact sequence is

\[
H^1_{\text{ord,rel}}(K, T \otimes \Lambda) \xrightarrow{\text{res}_v} \text{Im} \ H^1_{\text{ord}}(K_v, T \otimes \Lambda) \cong \left( H^1_{\text{ord}}(K_{\text{Frob}}, M) \right)^V \rightarrow X_{\text{ord,ord}} \rightarrow X_{\text{ord,0}} \rightarrow 0.
\]

There is a Coleman map again to \( \Lambda_K \), and the image of \( z_{\text{BF}} \) is \( L_{\text{Gr}}(E/K_{\infty}) \).

5. Lecture 5 (3/12/2018)

5.1. Selmer structures. Let \( F \) be a number field and \( M \) a compact or discrete \( G_F \)-module.

**Definition 5.1.1.** A Selmer structure on \( M \) is a collection of submodules

\[ \mathcal{L} = (\mathcal{L}_v \subset H^1(F_v, M))_v, \]

indexed by the places \( v \) of \( F \), such that \( \mathcal{L}_v = H^1_{\text{ur}}(F_v, M) \) for all but finitely many \( v \).

The Selmer group associated to \( \mathcal{L} \) is

\[ H^1_{\mathcal{L}}(F, M) = \{ c \in H^1(F, M) : \text{res}_v(c) \in \mathcal{L}_v \text{ for all } v \}. \]

**Example 5.1.2.** Let \( M = E[m] \) for \( E/F \) an elliptic curve. We can define

\[ \mathcal{L}_v = \text{Im} \left( E(F_v) / m E(F_v) \hookrightarrow H^1(K_v, E[m]) \right). \]

This coincides with \( H^1_{\text{ur}}(F_v, M) \) if \( v \nmid m N_E \). Then \( H^1_{\mathcal{L}}(F, E[m]) \) is what we called \( \text{Sel}_m(E/F) \).

**Example 5.1.3.** Let \( T = T_p(E) \) for \( E/F \) an elliptic curve, \( V = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \), and \( M = W = E[p^\infty] = V/T \). We define \( \mathcal{L}_v = H^1_{\mathcal{L}}(F_v, W) \). Then \( H^1_{\mathcal{L}}(F, W) \) is what we called \( \text{Sel}_{p^\infty}(E/F) \).

**Example 5.1.4.** Let \( V \) be a finite-dimensional vector space over a finite extension \( L \) of \( \mathbb{Q}_p \).

Suppose that we have a continuous geometric representation of \( G_F \) on \( V \). Let \( T \subset V \) be a \( G_F \)-stable \( \mathcal{O}_L \)-lattice and \( M = W = V/T \). Define a Selmer structure via \( \mathcal{L}_v = H^1_{\mathcal{L}}(F_v, M) \).

For \( v \nmid p \) such that \( V \) is unramified at \( v \),

\[ H^1_{\mathcal{L}}(F_v, W) = \text{Im} \left( H^1_{\mathcal{L}}(F_v, V) \rightarrow H^1(F_v, W) \right). \]

We have

\[
\begin{array}{ccc}
H^1(F_v, V) & \longrightarrow & H^1(F_v, W) \\
\| & & \| \\
V/(\text{Frob}_v - 1)V & \longrightarrow & W/(\text{Frob}_v - 1)W
\end{array}
\]

The surjectivity of \( H^1(F_v, V) \rightarrow H^1(F_v, W) \) shows that the image is \( H^1_{\text{ur}}(F_v, W) \).
Example 5.1.5. Let $M = T_p(E) \otimes_{\mathbb{Z}_p} \Lambda^*$ for $\Lambda$ the Iwasawa algebra for some $\mathbb{Z}_p^d$-extension $F_\infty/F$.

Write $\Gamma = \text{Gal}(F_\infty/F) \approx \mathbb{Z}_p^d$. We defined a Selmer group $S(E/F_\infty)$ by demanding that $\text{res}_v(c) = 0$ for $v \nmid p$, and a more complicated condition at $p$. In the ordinary case the local subgroup was

$$\text{Im} \left( H^1(F_v, T_v^+ \otimes_{\mathbb{Z}_p} \Lambda^*) \to H^1(F_v, M) \right).$$

To see that this is a Selmer structure, we check that $H^1_{\text{ur}}(F_v, M) = 0$ for $v \nmid pN_F$. Indeed, for such $v$ we have

$$H^1_{\text{ur}}(F_v, M) \cong M/(\text{Frob}_v - 1)M = 0.$$

Remark 5.1.6. By definition, Selmer structures can only differ at finitely many places. When dealing with $p$-adic representations, it’s really only the conditions at $p$ that matter. For finite modules, the other places can matter.

Definition 5.1.7. Let $\mathcal{L}_1 = (\mathcal{L}_{1,v})$ and $\mathcal{L}_2 = (\mathcal{L}_{2,v})$ be Selmer structures for $M$. We say that $\mathcal{L}_1 \leq \mathcal{L}_2$ if $\mathcal{L}_{1,v} \leq \mathcal{L}_{2,v}$ for all $v$.

Let $M$ be a $\mathbb{Z}_p$-module. We have $M^\vee(1) = \text{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p(1))$. Local Tate duality gives a perfect pairing

$$H^1(F_v, M) \times H^2-i(F_v, M^\vee(1)) \sim H^2(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong \mathbb{Q}_p/\mathbb{Z}_p.$$

This allows to express $H^2$ in terms of $H^0$. By Tate’s Euler characteristic formula, one can also express $H^1$ in terms of $H^0$ and $H^2$, hence entirely in terms of $H^0$.

Remark 5.1.8. For $v \nmid p$, $H^1_{\text{ur}}(F_v, M)$ and $H^1_{\text{ur}}(F_v, M^*)$ are mutual annihilators.

Now given a Selmer structure $\mathcal{L} = (\mathcal{L}_v)$ for $M$, we define the dual Selmer structure $\mathcal{L}^\vee = (\mathcal{L}_v^\vee(1) := \mathcal{L}_{1,v}^\vee)$ for $M^\vee(1)$. Note that $\mathcal{L}_1 \leq \mathcal{L}_2 \iff \mathcal{L}_1^\vee \leq \mathcal{L}_2^\vee$.

There is an extremely useful exact sequence coming from global duality. Suppose $\mathcal{L}_1 \leq \mathcal{L}_2$. Then we have an exact sequence

$$0 \to H^1_{\mathcal{L}_1}(F, M) \to H^1_{\mathcal{L}_2}(F, M) \xrightarrow{\text{res}} \prod_v \left( \frac{\mathcal{L}_{2,v}^\vee}{\mathcal{L}_{1,v}^\vee} \right) \xrightarrow{\prod_v (\mathcal{L}_{2,v}^\vee/\mathcal{L}_{1,v}^\vee)^\vee} \prod_v (\mathcal{L}_{2,v}^\vee/\mathcal{L}_{1,v}^\vee)^\vee \to H^1_{\mathcal{L}_1}(F, M^\vee(1))^\vee \to H^1_{\mathcal{L}_2}(F, M^\vee(1))^\vee \to 0$$

(5.1.1)

The exactness is clear except at the middle, where it follows from Poitou-Tate duality. The idea of Euler systems is to control $H^1_{\mathcal{L}_1}(F, M^*)^\vee$ by choosing a $\mathcal{L}_1 \leq \mathcal{L}_2$ such that you can control the flanking terms, $H^1_{\mathcal{L}_2}(F, M^*)^\vee$ and the image of res. The difficulty in Euler systems is concerned with producing ramified classes, since most of our methods for producing cohomology classes via geometry don’t have ramification. Most constructions go through a tower of field extensions.
because the Kolyvagin derivative allows one to produce a ramified cohomology class over a
ground field.

5.2. Kato’s Main Conjecture. Let \( \Lambda = \mathbb{Z}_p[[\Gamma]] \), where \( \Gamma = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \). We have a character
\( \Psi : G_\mathbb{Q} \to \Gamma \hookrightarrow \Lambda^* \) giving a Galois action on \( \Lambda \). Then \( M^\vee(1) = T_p(E) \otimes_{\mathbb{Z}_p} \Lambda^* \), which has a Galois
action via \( \rho_{E,p} \otimes \Psi^{-1} \).

Assume that \( E \) is ordinary at \( p \). Then we can define
\[
L_{1,p} = \text{Im} \left( H^1(\mathbb{Q}_p, T_p E^+ \otimes_{\mathbb{Z}_p} \Lambda) \to H^1(\mathbb{Q}_p, M) \right)
\]
\[
L_{2,p} = H^1(\mathbb{Q}_p, M).
\]

We extend these to Selmer structures by defining \( L_{i,v} = 0 \) for \( v \neq p \). Then (5.1.1) specializes to
\[
0 \to H^1_{L_1}(F, M) \to H^1_{L_2}(F, M) \to \text{res} \left( \frac{H^1(\mathbb{Q}_p, T \otimes \Lambda)}{\text{Im} \left( H^1(\mathbb{Q}_p, T_p E^+ \otimes_{\mathbb{Z}_p} \Lambda) \to H^1(\mathbb{Q}_p, M) \right)} \right) \to H^1(\mathbb{Q}_p, M)^\vee \to \text{res}^* \to \to H^1_{L_2}(F, M^*)^\vee = \text{X}_{\text{str}}(E/\mathbb{Q}_\infty) \to 0
\]

Kato constructed a free \( \Lambda \)-module of rank 1, \( z_{\text{Kato}} \subset H^1_{L_2}(\mathbb{Q}, T \otimes_{\mathbb{Z}_p} \Lambda) \). He showed that it is non-
zero using a reciprocity isomorphism

\[
\frac{H^1(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda)}{\text{Im} \left( H^1(\mathbb{Q}_p, T_p E^+ \otimes_{\mathbb{Z}_p} \Lambda) \to H^1(\mathbb{Q}_p, M) \right)} \cong \Lambda.
\]

The real meat of Kato’s argument is the computation that this isomorphism takes
\( z_{\text{Kato}} \mapsto (\mathcal{L}(E/\mathbb{Q}_\infty)) \).

Then by analytic arguments (establishing existence of non-zero \( L \)-values in families of twists)
one knows that \( \mathcal{L}(E/\mathbb{Q}_\infty) \neq 0 \). The algebraic theory then ensures that as soon as \( \mathcal{L}(E/\mathbb{Q}_\infty) \neq 0 \neq 0 \), all but finitely many twists are non-zero.

Remark 5.2.1. The \( z_{\text{Kato}} \) is the base layer of an Euler system.

The non-vanishing of \( z_{\text{Kato}} \) implies (using that \( H^1_{L_2}(\mathbb{Q}, T \otimes_{\mathbb{Z}_p} \Lambda) \) is a free \( \Lambda \)-module of rank 1),
by the general machinery of Euler systems, that
\[
\xi \left( \frac{H^1_{L_2}(\mathbb{Q}, T \otimes_{\mathbb{Z}_p} \Lambda)}{z_{\text{Kato}}} \right) \subset \xi(\text{X}_{\text{str}}(E/\mathbb{Q}_\infty)).
\]
under some technical assumptions.
This gives an exact sequence

$$0 \longrightarrow H^1_{\mathcal{L}_2}(Q, M)/z_{\text{Kato}} \longrightarrow \Lambda(\mathcal{L}) \longrightarrow X \longrightarrow X_{\text{str}} \longrightarrow 0$$

hence

$$\xi(X_{\text{str}})\xi(\Lambda/\mathcal{L}) = \xi(X)\xi(H^1_{\mathcal{L}_2}(Q, M)/z_{\text{Kato}}).$$

Since the Euler system argument establishes \(\xi(X_{\text{str}})\xi(H^1_{\mathcal{L}_2}(Q, M)/z_{\text{Kato}})\), we deduce \(\xi(X)|\mathcal{L}\).

5.3. **Elliptic curves over \(Q\).** Let \(K\) be an imaginary quadratic field, such that \(p\) splits as \(p = v \overline{v}\) in \(K\). Let \(K_{\infty}/K\) be a maximal \(\mathbb{Z}_p^d\)-extension and \(M = T \otimes \mathbb{Z}_p \Lambda_K\), so \(M'\)(1) = \(T \otimes \mathbb{Z}_p \Lambda_K^\ast\). In this case \(\Gamma_K = \text{Gal}(K_{\infty}/K) \cong \mathbb{Z}_p^2\). Let \(\Lambda_K = \mathbb{Z}_p[[\Gamma_K]]\).

We will define a collection of Selmer conditions. For \(w \notdiv p\), we define \(\mathcal{L}_w = 0\). For \(w \div p\) we will define \(\mathcal{L}_{w, \ast}\) where \(\ast \in \{\text{rel}, \text{str}, \text{ord}\}\). We set \(\mathcal{L}_{w, \text{rel}} = H^1(K_w, ?)\), i.e. no condition, \(\mathcal{L}_{w, \text{str}} = 0\), and \(\mathcal{L}_{w, \text{ord}} = \text{Im } H^1(K_w, T^+ \otimes \Lambda_K)\) or \(\text{Im } H^1(K_w, T^+ \otimes \Lambda_K^\ast)\) as appropriate. Then we define \(\mathcal{L}_{\ast, \ast}\) to be “\(\ast\) at \(v\) and \(\ast\) at \(\overline{v}\)”. Consequently we have

\[
\mathcal{L}_{\ast, \text{rel}}^\dag(M) = \mathcal{L}_{\text{str, rel}}^\dag(M^{\ast}(1)),
\]

\[
\mathcal{L}_{\ast, \text{ord}}^\dag(M) = \mathcal{L}_{\text{str, ord}}^\dag(M^{\ast}(1)).
\]

We will write \(H^1_{\ast, \ast} = H^1_{\mathcal{L}_{\ast, \ast}}\).

We will apply this with \(\mathcal{L}_2 = \mathcal{L}_{\text{ord, rel}}(T \otimes \Lambda_K)\). We will consider a few possibilities for \(\mathcal{L}_1\).

First consider \(\mathcal{L}_1 = \mathcal{L}_{\text{ord, ord}}\). Then [5.1.1] specializes to

\[
0 \longrightarrow H^1_{\text{ord, ord}}(K, M) \longrightarrow H^1_{\text{ord, rel}}(K, M) \longrightarrow \text{Im } H^1(K_{\infty, M'})/\text{Im } H^1(K_{\infty, M^+})
\]

\[
\downarrow
\]

\[
X_{\text{ord, ord}}
\]

\[
\downarrow
\]

\[
X_{\text{ord, str}}
\]

\[
\downarrow
\]

\[
0
\]

There is a Coleman isomorphism \(H^1(K_{\infty, M'})/\text{Im } H^1(K_{\infty, M^+}) \cong \Lambda_K\). Parallel to Kato’s argument, we might hope for a class in \(H^1_{\text{ord, rel}}(K, M)\) which is sent to a \(p\)-adic \(L\)-function under the Coleman isomorphism, and which divides \(\xi(X_{\text{ord, str}})\). A candidate class \(z_{\text{LLZ}}\) was constructed by Lei-Loeffler-Zerbes and computed its regulator to be \(\mathcal{L}_{E/K_{\infty}}\). But we don’t know the divisibility result.

Kato’s methods prove that \(X_{\text{ord, ord}}\) is torsion, hence so is \(X_{\text{ord, str}}\). Also by Kato’s method, we know that \(H^1_{\text{ord, ord}}(K, M)\) is also torsion. Hence if we additionally assume that \(E[p]\) is irreducible as a \(G_K\)-representation then we get that it is 0. In this case, we get an exact sequence

\[
0 \longrightarrow H^1_{\text{ord, ord}}(K, M)_{\text{LLZ}} \longrightarrow \Lambda(\mathcal{L}/E/K_{\infty}) \longrightarrow X_{\text{ord, ord}} \longrightarrow X_{\text{ord, str}} \longrightarrow 0
\]

and we believe that

\[
\xi(H^1_{\text{ord, ord}}(K, M)_{\text{LLZ}}) = \xi(X_{\text{ord, str}}).
\]

They called it a *Beilinson-Flach class* \(z_{BF}\).
This would imply a classical Greenberg-style Main Conjecture.

**Remark 5.3.1.** Under certain hypotheses, one can show that

\[ \xi(X_{\text{ord,ord}}) \subset (\mathcal{L}(E/K_{\infty})). \]

The conditions are

- \( E[p] \) is irreducible as a \( G_{\mathbb{Q}} \)-representation,
- there exists \( \ell \mid N_E \) such that \( E[p] \) is ramified at \( \ell \),
- \( (D_K, N_E p) = 1 \),
- \( N_E = N_+ N_- \) with \( N_+ \) split and \( N_- \) inert,
- \( N_- \) is a square-free product of an odd number of primes, and \( E[p] \) is ramified at all \( \ell \mid N_- \).

So from this plus Kato’s work, we get also \( \supset \) and hence equality, therefore also

\[ \xi \left( \frac{H^1_{\text{ord,rel}}}{z_{11Z}} \right) = \xi(X_{\text{ord,str}}). \]

Now suppose \( \mathcal{L}_1 = \mathcal{L}_{\text{str,ord}} \). Then (5.1.1) becomes

\[
\begin{array}{ccccccc}
0 & \longrightarrow & H^1_{\text{str,ord}}(K, M) & \longrightarrow & H^1_{\text{ord,rel}}(K, M) & \longrightarrow & \text{Im } H^1(K_v, M^+) & \longrightarrow & X_{\text{rel,str}} \\
& & & & & \downarrow & & & \downarrow \\
& & & & & X_{\text{ord,str}} & & & 0 \\
\end{array}
\]

The class \( z_{11Z} \) is send to \( \mathcal{L}_{\text{Gr}} \) under a Coleman map, where \( \mathcal{L}_{\text{Gr}} \) interpolates \( L(f, \chi, 1)/(\Omega_{\infty}/\Omega_p)^{4n} \) (after extending scalars to \( \overline{\mathbb{Z}}_{\pi}^{tr} \)) for characters \( \chi \) having Hodge-Tate weights \( n > 1 \) at \( v \) and \( <-1 \) at \( \overline{v} \). We can show that \( \xi(X_{\text{rel,str}}) \subset \mathcal{L}_{\text{Gr}} \) up to some exceptional primes.

5.4. **Converse to Gross-Zagier and Kolyvagin.** Let \( E/\mathbb{Q} \) be an elliptic curve of conductor \( N_E \). Let \( K \) be an imaginary quadratic field.

The classical Heegner hypothesis is that if \( \ell \mid N_E \) then \( \ell \) is split in \( K \). This implies that \( w(E/K) = -1 \), so \( L(E/K, s) \) has odd order of vanishing at \( s = 1 \). Under the Heegner hypothesis, Gross-Zagier proved that

\[ L'(E/K, 1) = (\ast)(y_K, y_K)_{NT} \]

where \( y_K \) is the Heegner point. This comes from a modular parametrization \( \phi : X_0(N) \to E \), normalized so that \( \infty \mapsto 0_E \). You have a orbit of CM points in \( X_0(N) \) upon choosing a factorization \( N_E = \pi \overline{\pi} \).

Kolyvagin proved that if \( y_K \) is non-torsion then \( \text{rank } E(\mathbb{Q}) = 1 \) and \( \text{III}(E/K) < \infty \), and is bounded in terms of the index of \( y_K \).

The Gross-Zagier theorem can be generalized in various ways. One is to allow twists by an anticyclotomic character \( \chi \) of \( K \). Then the formula becomes

\[ L'(E, \chi, 1) = (\ast)(y_K(\chi), y_K(\chi)) \]

with \( y_K(\chi) \in (E(H_{\text{cond}}(\chi)) \otimes \mathbb{C})^\chi \). It can also be generalized by relaxing the Heegner condition, by work of YZZ.
So if \( \text{ord}_{s=1} L(E/K, s) = 1 \) then we know that \( E(K) \) has rank 1 and \( \text{III}(E/K) \) is finite, hence \( \text{Sel}_{p^\infty}(E/K) \) has corank 1. One could ask about the converse: assuming that \( \text{Sel}_{p^\infty}(E/K) \) has corank 1, can one prove that \( \text{ord}_{s=1} L(E/K, s) = 1 \)?

We will explain how progress towards the Main Conjecture would give this, but the known progress is outside the Heegner condition.

Let \( K_{ac}^\infty/K \) be the anticyclotomic extension, with Galois group \( \Gamma_{ac} \). Cornut-Vatsal prove that under the Heegner hypothesis, \( \text{ord}_{s=1} L(E, \chi, s) = 1 \) for all but finitely many finite-order characters \( \chi : \Gamma_{ac} \to \mathbb{C}^\times \). In particular, \( E(K_{ac}^\infty) \otimes \mathbb{Z}_p \) is a \( \Lambda_{ac} \)-module of rank 1.

Let \( S_{ac} = S(E/K_{ac}^\infty) \) and \( X_{ac} = S_{ac}^* \). Assume that \( E \) is ordinary at \( p \) and \( E[p] \) is an irreducible \( G_K \)-representation. A theorem of Howard, proved via an Euler system argument, shows that

\[
X_{ac} \sim \Lambda \oplus M \oplus M
\]

where \( M \) is a torsion \( \Lambda_{ac} \)-module (corresponding to III). For simplicity we assume that \( p \) splits in \( K \). Then one has

\[
\xi(M) \mid \xi \left( \frac{H^1_{\text{ord,ord}}(K, T \otimes \mathbb{Z}_p \Lambda_{ac})}{z_{\text{Heeg}}} \right).
\]

(5.4.1)

Here \( z_{\text{Heeg}} \) is a free \( \Lambda_K \)-submodule of rank 1. Let \( \gamma \in \Gamma_{ac} \) be a topological generator. We have a map

\[
X_{ac}/(\gamma-1)X_{ac} \to \text{Sel}_{p^\infty}(E/K)^*
\]

with finite kernel (by dualizing the exact sequence \( \text{Sel}_{p^\infty}(E/K) \hookrightarrow S_{ac}[\gamma-1] \to \text{finite} \to 0 \)).

Suppose \( \text{corank Sel}_{p^\infty}(E/K)^* = 1 \). Then rank \( X_{ac}/(\gamma-1)X_{ac} = 1 \) so \( M/(\gamma-1)M \) is torsion (since if it were not torsion, it would contribute 2 to rank \( X_{ac}/(\gamma-1)X_{ac} \)). If we knew that \( \xi(M) = \xi \left( \frac{H^1_{\text{ord,ord}}(K, T \otimes \mathbb{Z}_p \Lambda_{ac})}{z_{\text{Heeg}}} \right) \), then we would have that \( \left( \frac{H^1_{\text{ord,ord}}(K, T \otimes \mathbb{Z}_p \Lambda_{ac})}{(\gamma-1)z_{\text{Heeg}}} \right) \) is torsion, hence the Heegner point is non-zero. But just the divisibility is not enough. We’ll see a way to get around this.

Let \( M = T \otimes \mathbb{Z}_p \Lambda_{ac} \). Restricting to \( \overline{\nu} \) gives an exact sequence

\[
0 \longrightarrow H^1_{\text{ord,ord}}(K, M) \longrightarrow H^1_{\text{ord,rel}}(K, M) \xrightarrow{\text{res}} H^1_{\text{res}}(K_{\overline{\nu}}, M) \xrightarrow{\text{Col}} \Lambda_{ac} \oplus M \oplus M \xrightarrow{\sim} X_{\text{ord,ord}} \xrightarrow{\text{res}} X_{\text{ord,str}} \longrightarrow 0
\]

(5.4.2)
The first vertical map is either 0 or injective, since the domain is free. On the other hand, restricting to \( v \) gives

\[
\begin{array}{c}
0 \rightarrow H^{1}_{\text{str,rel}}(K, M) \rightarrow H^{1}_{\text{ord,rel}}(K, M) \xrightarrow{\text{res}} \text{Im } H^{1}(K^{v}, M^{+}) \xrightarrow{\sim} \Lambda_{ac} \\
\downarrow \text{res}^{*} \downarrow \downarrow \downarrow \downarrow \downarrow \\
X_{\text{rel,str}} \rightarrow X_{\text{ord,str}} \rightarrow 0
\end{array}
\]

(5.4.3)

Cornut-Vatsal implies that \( X_{\text{rel,str}} \) is torsion, hence so is \( X_{\text{ord,str}} \). Since \( X_{\text{ord,str}} \) also appears in (5.4.2) we get information there as well, and we see that the map \( \text{res}^{*} \) is injective or else the cokernel would be too big. Then the previous map in the sequence would have to be 0, so we find that (5.4.2) looks like

\[
\begin{array}{c}
0 \rightarrow H^{1}_{\text{ord,ord}}(K, M) \rightarrow H^{1}_{\text{ord,rel}}(K, M) \rightarrow H^{1}(K^{v}, M^{+}) \xrightarrow{\sim} \Lambda_{ac} \\
\downarrow \text{res}^{*} \downarrow \downarrow \downarrow \downarrow \\
X_{\text{ord,ord}} \rightarrow X_{\text{ord,str}} \rightarrow N \oplus M \oplus M
\end{array}
\]

(5.4.4)

Another consequence is that \( X_{\text{ord,str}} \sim N \oplus M \oplus M \), which we can feed back into (5.4.3) to deduce that \( X_{\text{rel,str}} \sim N \oplus N \oplus M \oplus M \). Chasing through the exact sequence, we find that the image of \( H^{1}_{\text{ord,rel}}(K, M) \rightarrow \text{Im } H^{1}(K^{v}, M^{+}) \) is non-zero, hence \( H^{1}_{\text{str,rel}}(K, M) = 0 \). We have \( z_{\text{Heeg}} \in H^{1}_{\text{ord,ord}}(K, M) = H^{1}_{\text{ord,rel}}(K, M) \) (equality by (5.4.4)).

It is a fact that \( \mathcal{L}_{Gr} \in \Lambda_{K} \) specializes to \( \mathcal{L}_{BDP} \). The BDP formula said

\[
\phi_{1}(\mathcal{L}_{Gr}) = \frac{1-a_{p}(E)+p}{p} \log_{E(K^{v})} y_{K}
\]

and for finite order \( \chi \),

\[
\phi_{\chi}(\mathcal{L}_{Gr}) \sim \log_{E(H^{\text{cond},(2)})} y_{K}(\chi).
\]

We have \( (\log_{p}(z_{\text{Heeg}}))^{2} = (\mathcal{L}_{BDP}) \). On the other hand, the Main Conjecture predicts

\[
(\mathcal{L}_{BDP}) = \xi(X_{\text{rel,str}}).
\]
Putting these together, we should have

\[
\xi(\text{Im} H^1_{\text{res,Heeg}}) \gamma^2 = \xi(\text{H}^1_{\text{ind,Heeg}}(K,M)) \gamma^2 \cdot \xi(N)^2
\]

\[
\xi(\Lambda/\mathcal{L}_{\text{BDP}}) \quad \xi(X_{\text{rel,str}}) \quad \xi(N)^2 \xi(M)^2
\]

Canceling the \(\xi(N)^2\), we deduce a relationship between \(\xi(M)^2\) and \(z_{\text{Heeg}}\). This improves the divisibility \((5.4.1)\). The key is that the cancellation allows us to deduce a result without knowing \(\xi(N)^2\). After the fact, we can then use the non-vanishing of Heegner points implied by this equality to go back and deduce things about \(\xi(N)\).


Starting from now, we are going to shift focus towards Euler systems. In the first half of the course we considered a (compact or discrete) \(Z_p\)-module \(M\), with a continuous action of \(G_F\) (the absolute Galois group of a number field \(F\)) unramified away from finitely many places.

Let \(\mathcal{L} = (\mathcal{L}_v)\) be a Selmer structure for \(M\), meaning that \(L_v \subset H^1(F_v,M)\) such that \(L_v = H^1_{\text{ur}}(F_v,M)\) for almost all \(v\). Given such a Selmer structure, we form the Selmer group

\[
H^1_{\mathcal{L}}(F,M) = \{ c \in H^1(F,M) : \text{res}_v(c) \in \mathcal{L}_v \text{ for all } v \}.
\]

Let \(M^\vee(1) = \text{Hom}_{cts}(M, Q_p/\mathbb{Z}_p(1))\). Then given a Selmer structure \(\mathcal{L} := (\mathcal{L}_v)\) for \(M\), we get a dual Selmer structure \(\mathcal{L}^\vee := (\mathcal{L}^\vee_v)\), the annihilator with respect to the pairing of Tate local duality.

There is an obvious partial ordering on Selmer structures, and if \(\mathcal{L} \leq \mathcal{L}'\) then \(H^1_{\mathcal{L}'}(F,M) \subset H^1_{\mathcal{L}}(F,M)\). We have a 5-term sequence

\[
0 \rightarrow H^1_{\mathcal{L}'}(F,M) \rightarrow H^1_{\mathcal{L}}(F,M) \rightarrow \prod_v \mathcal{L}_v/\mathcal{L}_v \rightarrow \prod_v (\mathcal{L}_v/\mathcal{L}_v)^\vee
\]

\[
\downarrow
\]

\[
H^1_{\mathcal{L}'}(F,M^\vee(1))^\vee
\]

\[
\downarrow
\]

\[
H^1_{(\mathcal{L}')}\gamma_v(F,M^\vee(1))^\vee
\]

\[
\downarrow
\]

\[
0
\]

which is exact by Poitou-Tate global duality. Now I want to discuss what this has to do with Euler systems. In practice, one can show by some sort of Cebotarev density result that \(H^1_{\mathcal{L}}(F,M^\vee(1))^\vee\) is a quotient of local cohomology groups, i.e. \(H^1_{(\mathcal{L}')}\gamma_v(F,M^\vee(1))^\vee = 0\). One can further hope to control the image of \(H^1_{\mathcal{L}'}(F,M) \rightarrow \prod_v \mathcal{L}_v/\mathcal{L}_v\) using Euler systems, thus bounding \(H^1_{\mathcal{L}'}(F,M^\vee(1))^\vee\).
6.1. A simple setting. We're going to illustrate the Euler system argument in a simple case, which is essentially due to Kolyvagin. Let $F = K$ be a CM field and $K^+ \subset K$ the totally real subfield. Assume that $K/K^+$ is a totally imaginary quadratic extension. Let $c \in \text{Gal}(K/K^+)$ be the complex conjugation. For simplicity, we assume for now that $M = V$ is a finite-dimensional vector space over a finite extension $k/F_p$. As before, we suppose that $V$ is equipped with a finite-dimensional $G_K$-action unramified away from finitely many places.

We now impose some technical hypotheses on $V$.

(H1) $V$ is irreducible as a $G_K$-representation.
(H2) $\dim_k V \geq 2$.
(H3) There exists $\tau_0 \in G_{K(\mu_p)}$ such that $V/(\tau_0 - 1)V$ is 1-dimensional.
(H4) There exists a $k$-linear, $G_K$-equivariant, alternating perfect pairing

$$V \times V^c \to k(1),$$

where $V^c$ is $V$ but with the Galois action conjugated by $c$.

(H5) $H^1(\text{Gal}(K(V)/K), V) = 0$, where $K(V)$ is the splitting field of $V$.

Example 6.1.1. Let $V = E[p]$ for an elliptic curve $E/K^+$. Then $V^c \cong V$, and we can take the Weil pairing in (H4). More generally, we can twist $V$ by an anti-cyclotomic Hecke character $\chi$, i.e. such that $\chi^c = \chi^{-1}$.

Example 6.1.2. Let $\pi$ be a cuspidal automorphic representation of $U(n, 1)$ and $\tau$ a cuspidal automorphic representation of $U(n-1, 1)$. Let $V := V_{\pi} \otimes V_{\tau}(?)$. The pairing comes from the cup product on the Shimura varieties where these Galois representations appear.

Note that assumption (H4) implies that $V^c \cong V^\vee(1) = \text{Hom}_k(V, k(1))$, hence

$$H^1(K, V^\vee(1)) = H^1(K, V^c).$$

There is a twisting map $\text{Tw}_c : H^n(K, V) \to H^n(K, V^c)$, induced by the automorphism of $G_K$ given by conjugation by $c$. Note that this permutes the decomposition subgroups of $G_K$ above a split prime.

Kolyvagin showed how to bound the Selmer group in Example 6.1.1 with $K/Q$ imaginary quadratic.

Theorem 6.1.3. Assume

1. all primes $\ell \mid N_E$ split in $K$ (i.e. Heegner hypothesis), and
2. the Heegner point $y_E$ has non-trivial image in $\text{Sel}_p(E/K) = H^1_{\Sigma}(K, E[p])$, i.e. it's not divisible by $p$ in $E(K)$.

Then $\text{Sel}_p(E/K) = \mathbf{F}_p y_E$.

We will give a proof of a more general result, slightly different from Kolyvagin's original argument\footnote{This is a simple case of ongoing work in progress with D. Jetchev and J. Nekovar.} (We will use $\tau_0$ in place of $c$, so we don't need $V$ to be a representation of $G_{K^+}$.)

Theorem 6.1.4. Let $V$ be a $G_K$-representation satisfying (H1)-(H4). Let $\Sigma = (\Sigma_\pi)$ be a Selmer structure for $V$. Let $\Sigma^c = (\Sigma^c_\pi)$, where $\Sigma^c_\pi = \text{Tw}_c(\Sigma_\pi)$. Assume that $\Sigma^c$ is identified with $\Sigma^\vee$. Then

$$\dim_k H^1_{\Sigma}(G_K, V) = 1.$$ 

Proof. Suppose we have an initial $\kappa \in H^1_{\Sigma}(K, V)$. We want to show that it spans the whole Selmer group. Let $L = K(V, \mu_p)$, so that $L$ splits both $V$ and $V^\vee(1)$. By (H5), $\kappa|_{G_L} \in \text{Hom}_{G_L}(G_L, V)$ is non-zero. The irreducibility of $V$ implies that $\kappa(G_L) \subset V$ spans all of $V$ over $k$. 

This is a simple case of ongoing work in progress with D. Jetchev and J. Nekovar.
We want to find \( w \) such that \( \kappa|_{G_{Kw}} \) is non-zero. By the isomorphism

\[
H^1_{ur}(K_w, V) \xrightarrow{\sim} V / (\text{Frob}_w - 1)V
\]

it is equivalent to ask that \( \kappa(\text{Frob}_w) \) be non-zero in \( V / (\text{Frob}_w - 1)V \). The idea is that we can find \( \sigma \in G_L \) such that any \( w \) with \( \text{Frob}_w = \tau_0\sigma \in G_K \) has the desired property. Note that

\[
\kappa(\text{Frob}_w) = \kappa(\tau_0\sigma) = \tau_0\kappa(\sigma) + \kappa(\tau_0).
\]

So what we need is that

\[
\tau_0\kappa(\sigma) + \kappa(\tau_0) \notin (\tau_0 - 1)V \subseteq V.
\]

The bad set is a proper affine subspace of \( V \), so since we saw in the first paragraph that \( \kappa(G_L) \) spans \( V \), this can be done. By Cebotarev density there exists \( u_0 \) such that \( 0 \neq \text{res}_{w_0}(\kappa) \in H^1_{ur}(K_{u_0}, V) \), such that \( u_0 \nmid p \) and \( u_0 \) is unramified in \( L \). By Cebotarev, we can further choose \( u_0 \) to be a degree 1 prime of \( K \), so \( uw_0 \neq u_0 \).

The Euler system and Kolyvagin derivative gives us a class \( \kappa(u_0) \in H^1_{\varepsilon(u_0)}(K, V) \), where \( \varepsilon(u_0) \) is the Selmer structure with \( \varepsilon(u_0) \) relaxed (no condition), satisfying the following property. We have the identifications \( H^1_{ur}(K_{u_0}, V) \cong V / (\text{Frob}_{u_0} - 1)V \)

\[
\frac{H^1(K_{u_0}, V)}{H^1_{ur}(K_{u_0}, V)} \cong H^1(I_{u_0}, V)^{G_{u_0}} = \text{Hom}(I_{u_0}^{\text{tame}}, V)^{G_{u_0}} \cong \text{Hom}(\mathcal{F}, 1), V)^{G_{u_0}} = V^{G_{u_0}}
\]

where the last equality follows from the fact that \( \sigma \) and \( \tau \) act trivially on \( \mu_p \) by definition. To summarize, there is an identification

\[
\frac{H^1(K_{u_0}, V)}{H^1_{ur}(K_{u_0}, V)} \cong V^{G_{u_0}}
\]

taking \( \phi \) to its value on a generator of tame inertia.

There is an isomorphism \( \psi_{u_0} \) from \( H^1_{ur}(K_{u_0}, V) \cong V / (\text{Frob}_{u_0} - 1)V \cong V / (\tau_0 - 1)V \) to \( V^{	au_0 = 1} \). Roughly speaking, it is given by applying the characteristic polynomial of \( \text{Frob}_{u_0} \) divided out by \( \tau_0 - 1 \). Then the key property of \( \kappa(u_0) \in H^1_{\varepsilon(u_0)}(K, V) \) is that

\[
\psi_{u_0}(\kappa(\text{Frob}_{u_0})) = \kappa(u_0)(\text{generator of tame inertia}).
\]

(6.1.1)

We have not yet explained how to construct the class \( \kappa(u_0) \); we will do this next time. Now our exact sequence looks like

\[
H^1_{\varepsilon(u_0, \varpi)}(K, V) \xrightarrow{\sim} H^1(K_{u_0}, V) \cong H^1(K_{u_0}, V) = H^1(K_{u_0}, V) \cong H^1_{ur}(K_{u_0}, V) \xrightarrow{\sim} H^1_{ur}(K_{u_0}, V) \times H^1_{ur}(K_{u_0}, V) \cong H^1_{ur}(K_{u_0}, V) \times H^1_{ur}(K_{u_0}, V)
\]

The existence of \( \kappa(u_0)^c \) which has non-zero image in the 2-dimensional space

\[
\frac{H^1(K_{u_0}, V)}{H^1_{ur}(K_{u_0}, V)} \times \frac{H^1(K_{\varpi}, V)}{H^1_{ur}(K_{\varpi}, V)} \cong H^1_{ur}(K_{u_0}, V) \times H^1_{ur}(K_{\varpi}, V)
\]

constrains the image of \( H^1_{\varepsilon}(K, V) \) in the local cohomology group at \( u_0 \) to be 1-dimensional. In particular, if \( H^1_{\varepsilon}(K, V) \neq K \cdot \kappa \), then there exists \( \kappa' \in H^1_{\varepsilon}(K, V) \) such that \( \text{res}_{u_0}(\kappa') = 0 = \text{res}_{\varpi}(\kappa') \).

Now we want to show that \( \kappa' = 0 \).
Suppose otherwise. Then the three elements $\kappa, \kappa(w_0), \kappa'(w_0) \in H^1_{\mathfrak{p}'}(K, V)$ span a 3-dimensional space. So, using (H5) again, the restrictions $\kappa|_{G_L}, \kappa(w_0)|_{G_L}, \kappa'|_{G_L}$ span a 3-dimensional space in $\text{Hom}_{G_L}(G_L, V)$. In particular, the fixed fields of their kernels are disjoint over $L$; call them $M_\kappa, M_{\kappa(w_0)}$, and $M_{\kappa'}$, respectively. So we have a diagram of field extensions

$$
\begin{array}{ccc}
M & \rightarrow & M_{\kappa(w_0)} \\
\downarrow & & \downarrow \\
L & = K(V, \mu_p) & \rightarrow M_{\kappa'} \\
\downarrow & & \downarrow \\
K & & K
\end{array}
$$

We want now to find places $w_1 \neq \overline{w_1}$ of $K$ such that

1. the image of $\kappa, \kappa(w_0)$ span under the restriction map
$$
H^1_{\mathfrak{p}'}(K, V) \rightarrow H^1_{\text{ur}}(K_{w_1}, V) \times H^1_{\text{ur}}(K_{\overline{w_1}}, V)
$$

2. $\kappa'$ is sent to something non-zero. (The target is 2-dimensional.)

Suppose for the moment that we can find such a $w_1$. Then the Euler system and Kolyvagin derivatives would then give classes $\kappa(w_1) \in H^1_{\mathfrak{p}'}(K, V)$ and $\kappa(w_0 w_1) \in H^1_{\mathfrak{p}'}(K, V)$ such that

$$
\psi_{w_1}(\text{res}_{w_1} \kappa) = \text{image of } \kappa(w_1) \in H^1(K_{w_1}, V)/H^1_{\text{ur}}(K_{w_1}, V)
$$

and

$$
\psi_{w_1}(\text{res}_{w_1} \kappa(w_0)) = \text{image of } \kappa(w_0 w_1) \in H^1(K_{w_1}, V)/H^1_{\text{ur}}(K_{w_1}, V).
$$

In particular, the image of $\kappa(w_1), \kappa(w_0 w_1)$ spans the 2-dimensional space

$$
\frac{H^1(K_{w_1}, V)}{H^1_{\text{ur}}(K_{w_1}, V)} \times \frac{H^1(K_{\overline{w_1}}, V)}{H^1_{\text{ur}}(K_{\overline{w_1}}, V)}.
$$

Now we have the bigger exact sequence

$$
\begin{array}{cccc}
H^1_{\mathfrak{p}'}(K, V^c) & \rightarrow & H^1_{\text{ur}}(K_{w_1}, V^c) \times H^1_{\text{ur}}(K_{\overline{w_1}}, V^c) & \rightarrow \\
\downarrow & & \downarrow & \rightarrow \\
H^1_{\text{ur}}(K_{w_1}, V^c) & \times & H^1_{\text{ur}}(K_{\overline{w_1}}, V^c) & \times \\
\downarrow & & \downarrow & \rightarrow \\
H^1_{\text{ur}}(K_{w_1}, V^c) & \times & H^1_{\text{ur}}(K_{\overline{w_1}}, V^c) & \times \\
\downarrow & & \downarrow & \rightarrow \\
H^1_{\text{ur}}(K_{w_1}, V^c) & \times & H^1_{\text{ur}}(K_{\overline{w_1}}, V^c) & \times \\
\downarrow & & \downarrow & \rightarrow \\
H^1_{\text{ur}}(K_{w_1}, V^c) & \times & H^1_{\text{ur}}(K_{\overline{w_1}}, V^c) & \times \\
\downarrow & & \downarrow & \rightarrow \\
\cdots & & \cdots & \cdots
\end{array}
$$

We have $\kappa^c, \kappa(w_0)^c, \kappa(w_0 w_1)^c, \kappa(w_1)^c, \kappa'(w_1)^c \in H^1_{\mathfrak{p}'}(K, V^c)$. The classes $\kappa(w_0 w_1)^c, \kappa(w_1)^c$ generate $\frac{H^1(K_{w_1}, V^c)}{H^1_{\text{ur}}(K_{w_1}, V^c)} \times \frac{H^1(K_{\overline{w_1}}, V^c)}{H^1_{\text{ur}}(K_{\overline{w_1}}, V^c)}$ under the local restriction map, by design. Since $\kappa(w_0)^c$ maps trivially to this target (being unramified at $w_1$), and nontrivially to $\frac{H^1(K_{w_1}, V^c)}{H^1_{\text{ur}}(K_{w_1}, V^c)} \times \frac{H^1(K_{\overline{w_1}}, V^c)}{H^1_{\text{ur}}(K_{\overline{w_1}}, V^c)}$ by design, the three classes $\kappa(w_0 w_1)^c, \kappa(w_1)^c, \kappa(w_0)^c$ span a 3-dimensional space under the horizontal map. So the cokernel is at most 1-dimensional. This contradicts that the dual map
\(H^1_w(K, V) \rightarrow H^1_w(K_{w_1}, V) \times H^1_w(K\pi, V)\) was designed to have rank at least 2.

We now need to go back and explain some of the things we left out. How do you find \(w_1\) satisfying the right conditions? Pick \(\sigma_{\kappa'} \in \text{Gal}(M_{\kappa'}/L)\) just as we did for \(w_0\), i.e.

\[\kappa'(\text{Frob}_{w_1}) = \kappa'(\tau_0 \sigma_{\kappa'}) \neq 0 \in V/(\tau_0 - 1)V\]

and \(\sigma_{\kappa} \in \text{Gal}(M_{\kappa}/L)\) also as we did for \(w_0\), i.e.

\[\kappa(\text{Frob}_{w_0}) = \kappa(\tau_0 \sigma_{\kappa}) \neq 0 \in V/(\tau_0 - 1)V.\]

Finally, we pick \(\sigma_{\kappa(w_0)}\) such that

\[(\kappa(\text{Frob}_{w_1}), \kappa(\text{Frob}_{\pi}), \kappa(w_0)(\text{Frob}_{w_1}), \kappa(w_0)(\text{Frob}_{\pi}))\] (6.1.2)

are linearly independent in

\[\frac{V}{(\tau_0 - 1)V} \times \frac{V}{(c^{-1} \tau_0 c - 1)V}.\]

We can write (6.1.2) above as

\[(\kappa(\tau_0 \sigma_{\kappa}), \kappa(c^{-1} \tau_0 c), \kappa(w_0)(\tau_0 \sigma_{\kappa(w_0)}), \kappa(w_0)(c^{-1} \tau_0 c)).\]

Why is this possible? View \(\kappa, \kappa'\) as giving identifications of

\[\kappa: \text{Gal}(M_{\kappa}/L) \tilde{\rightarrow} V\]
\[\kappa': \text{Gal}(M_{\kappa'}/L) \tilde{\rightarrow} V\]
\[\kappa(w_0): \text{Gal}(M_{\kappa}/L) \tilde{\rightarrow} V\]

The position of \(\kappa(w_0)\) at \(w_1\) is given by

\[\frac{V}{(\tau_0 - 1)V} \times \frac{V}{(c^{-1} \tau_0 c - 1)V}.\]

We want to show that the image is 2-dimensional. By Shapiro's Lemma, we have

\[H^1(G_{K^+}, W) \cong H^1(K, V)\]

where \(W = \text{Ind}_{G_{K}}^{G_{K'}}(V)\). Assume first that \(W\) is irreducible as a \(G_{K^+}\)-representation. We have \(\kappa_1 = \kappa\) and \(\kappa_2 = \kappa(w_0)\) in \(H^1(G_{K^+}, W)\). Consider \(\kappa_1|_{G_{L}}, \kappa_2|_{G_{L}} \in \text{Hom}_{G_{K^+}}(G_{L}, W)\), which are distinct and whose images span \(W\) over \(k\), by irreducibility, and let \(M_1, M_2\) be their fixed fields.

\[
\begin{array}{ccc}
M_1 & \rightarrow & M_2 \\
\downarrow & & \downarrow \\
L & \rightarrow & K \\
\downarrow & & \downarrow \\
K^+ & \rightarrow & K^+
\end{array}
\]

By similar arguments to those before, we can choose \(\sigma_1, \sigma_2\) so that \(\kappa_1(\tau_0 \sigma_1)\) and \(\kappa_2(\tau_0 \sigma_2)\) span \(W/(\tau_0 - 1)W\), a 2-dimensional space. We can choose \(w_{1}^+\) of \(K^+\), split in \(K\), such that

\[\text{Frob}_{w_{1}^+} = \tau_0(\sigma_1, \sigma_2) \in \text{Gal}(M_1 M_2/K) \subset \text{Gal}(M_1 M_2/K^+).\]

Then the images of \(\kappa_1, \kappa_2\) span the 2-dimensional space \(H^1_w(K_{w_1}^+, W) = W/(\tau_0 - 1)W\).
In the reducible case, more work is required: we actually needed to choose \( w_0 \) so that \( \kappa(w_0) \in H^1(K, V)^{c=-1} \) and \( \kappa' \in H^1(K, V)^{c=1} \).

Finally, we need to explain the formalism of Euler systems that produces \( \kappa \to \kappa(w_i) \). For primes \( \ell_1, \ldots, \ell_r \) of \( K^+ \) such that

1. \( \ell_i \) splits in \( K \) as \( \ell_i = w_i \overline{w_i} \),
2. \( \text{Frob}_{w_i} \) fixes \( \mu_p \), and
3. \( \text{Frob}_{w_i} = \tau_0 \in \text{Gal}(L/K) \),

we construct \( z(\ell_1, \ldots, \ell_r) \in H^1(K[\ell_1, \ldots, \ell_r], V) \), where \( K[\ell_1, \ldots, \ell_r] \) is a ring class field for \( K \), whose image under the corestriction map to \( H^1(K[\ell_1, \ldots, \ell_r], V) = P_{w_r}(\text{Frob}_{w_r})z(\ell_1 \ldots \ell_{r-1}) \) for some polynomial \( P_{w_r} \). The “Kolyvagin derivative” of the \( z \)'s give classes \( \kappa(\ell_1 \ldots \ell_r) \in H^1_p(\ell_1 \ldots \ell_{r-1}, V) \) whose ramified local position is the same as the unramified local position of \( z(\ell_1, \ldots, \ell_r) \), under the identifications hinted at above. You ultimately end up with a theorem that the existence of a non-zero Euler system implies that \( \dim H^1_L(K, V) = 1 \).

\[ \square \]

REFERENCES
