Structure of Selmer groups in terms of modular symbols

Alberto Angurel Andrés

University of Nottingham

July 25

Setting

- $E/\mathbb{Q}$ is an elliptic curve defined over the rationals.
- f is its associated modular form: $L(E,s) = L(f,s)$.
- We fix a prime p satisfying the following conditions
  - $p > 2$
  - E has good ordinary reduction at p.
  - The natural action $G_{\mathbb{Q}}$ on $T_p(E)$ is surjective.
  - Other conditions: $\mu = 0$, $p \not| \prod c_v$, $p \not| \# E(\mathbb{F}_p)$
- $\mathbb{Q}_\infty/\mathbb{Q}$ is the cyclotomic $\mathbb{Z}_p$-extension.

Selmer group of an elliptic curve

Kummer sequence

$$0 \longrightarrow E[p^N] \longrightarrow E \xrightarrow{\cdot p^N} E \longrightarrow 0$$

Taking Galois cohomology,

$$\begin{array}{ccccccc} 0 \to E(K)/p^N E(K) & \longrightarrow & H^1(K, E[p^N]) & \longrightarrow & H^1(K, E)[p^N] & \to 0 \\ \downarrow & & \downarrow \scriptstyle{Res} & \searrow & \downarrow \scriptstyle{Res} & \\ 0 \to \prod_v E(K_v)/p^N E(K_v) & \to & \prod_v H^1(K_v, E[p^N]) & \to & H^1(K_v, E)[p^N] & \to 0 \end{array}$$

Definition

$$\mathrm{Sel}(K, E[p^N]) := \ker\left(H^1(K, E[p^N]) \to \prod_v \frac{H^1(K_v, E[p^N])}{E(K_v) \otimes \mathbb{Z}/p^N} \right)$$

Fact

$\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Sel}(K, E[p^N])$ by conjugation.
The Selmer group is a $\mathbb{Z}_p[Gal(K/\mathbb{Q})]$ module.

Relation with the Mordell-Weil group

Definition

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) = \varinjlim \mathrm{Sel}(\mathbb{Q}, E[p^N])$$

The Kummer sequence can be written in this case as

$$0 \longrightarrow E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \longrightarrow Ш(E/\mathbb{Q})[p^\infty] \longrightarrow 0$$

- $E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$
- $\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^s \times (\mathit{finite}) \Rightarrow s \geq r$
- Conjecturally $Ш(E/\mathbb{Q})$ finite, so $r = s$.
- Assuming this conjecture, $\#Ш(\mathbb{E}/\mathbb{Q})[p^\infty] = \#(\mathit{finite})$.
- $\#Ш(E/\mathbb{Q})$ appears in the BSD formula.

Modular symbols

Modular symbols

$$\left[\frac{a}{m}\right] = 2\pi i \int_{\infty}^{\frac{a}{m}} f(z)\, dz, \quad \left[\frac{a}{m}\right]^{+} = \frac{1}{\Omega_E^{+}}\left(\left[\frac{a}{m}\right] + \left[\frac{-a}{m}\right]\right) \in \mathbb{Z}_{(p)}$$

Mazur-Tate element

$$\theta_m = \sum_{(a,m)=1} \left[\frac{a}{m}\right]^{+} \sigma_a \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})]$$

Remark

θ is related to the p-adic L-function

$$\vartheta_{p^n} = \alpha^{-n}\left(\theta_{p^n} - \nu_{p^n,p^{n-1}}\theta_{p^{n-1}}\right); \quad \vartheta_{p^\infty} = \varprojlim \vartheta_{p^n} \in \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$$

where α is a root of $x^2 - a_p x + p$.

Quantities δ_m

Proposition/definition

Let $m = l_1 \cdots l_r$ be a square-free integer. Then we have that

$$\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) = \mathcal{G}_{l_1} \times \cdots \times \mathcal{G}_{l_r}, \text{ where } \mathcal{G}_{l_i} := \mathrm{Gal}(\mathbb{Q}(\mu_{l_i})/\mathbb{Q})$$

Fix τ_i a generator of $\mathcal{G}_{l_i}$.
Then there exists some element $\delta_m \in \mathbb{Z}/p^N$ such that

$$\theta_m \equiv (-1)^r \delta_m (\tau_{l_1} - 1) \cdots (\tau_{l_r} - 1) \mod \left(p^N, (\tau_{l_1} - 1)^2, \ldots, (\tau_{l_r} - 1)^2\right)$$

Remark

The value of δ_m might depend on the chosen generators σ_{l_i} but $\mathrm{ord}_p(\delta_m)$ does not.

Remark

The quantities δ_m are effectively computable.

Bounding the Selmer group

Consider primes $l \equiv 1 \mod p^N$ such that E has good reduction at l and $\widetilde{E}(\mathbb{F}_l)[p^N] \cong \mathbb{Z}/p^N$.
Let $\mathcal{N}^{(N)}$ be the set of square-free products of those primes.
We have the following map

$$\mathrm{Sel}(\mathbb{Q}, E[p^N]) \to \bigoplus_{l|m} E(\mathbb{Q}_l) \otimes \mathbb{Z}/p^N \cong \bigoplus_{l|m} \widetilde{E}(\mathbb{F}_l) \otimes \mathbb{Z}/p^N \cong \left(\mathbb{Z}/p^N\right)^{\nu(m)}$$

Theorem (Kurihara)

If $m \in \mathcal{N}^{(N)}$ and δ_m is a unit in $\mathbb{Z}/p^N$, then the above map is injective.

Theorem (Kim, Sakamoto)

If $m \in \mathcal{N}^{(1)}$ is δ-minimal. Then we have that

$$\mathrm{Sel}(\mathbb{Q}, E[p]) \to \bigoplus_{l|m} E(\mathbb{Q}_l) \otimes \mathbb{Z}/p$$

is an isomorphism. In particular, $\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q}, E[p])) = \nu(m)$.

Its Pontryagin dual is a finitely generated torsion module over $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})] \cong \mathbb{Z}_p[[T]]$.

Theorem

Since $\mu = 0$, the dual of Selmer group is isomorphic (up to finite kernel and cokernel) to

$$X := \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p) \sim \prod_i \Lambda/(f_i)^{\beta_i}$$

Characteristic ideal

$$\mathrm{char}(X) := \prod_i (f_i)^{\beta_i} \subset \Lambda$$

Iwasawa main conjecture

It is the equality of ideals

$$(\vartheta_{p^\infty}) = \mathrm{char}(X)$$

- The inclusion $\subset$ was proven by Kato.
- The other inclusion has been proven under some conditions on the elliptic curve.

Theorem (Sakamoto)

The existence of some $m \in \mathcal{N}^{(1)}$ such that δ_m is a unit in $\mathbb{Z}/p$ is equivalent to the Iwasawa main conjecture.

Structure of the Selmer group

- Assumptions: Iwasawa main conjecture and non-degeneracy of the p-adic height pairing.
- Structure theorem and Cassels-Tate pairing: $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee \cong \mathbb{Z}_p^s \times (\mathbb{Z}_p/p^{\alpha_1})^2 \times \cdots (\mathbb{Z}_p/p^{\alpha_t})^2$
- Under our assumptions, $\mathrm{Sel}(\mathbb{Q}, E[p^N]) = \mathrm{Sel}(\mathbb{Q}, E[p^\infty])[p^N]$, so for N large enough

$$\mathrm{Sel}(\mathbb{Q}, E[p^N])^\vee \cong \left(\mathbb{Z}_p/p^N\right)^s \times (\mathbb{Z}_p/p^{\alpha_1})^2 \times \cdots (\mathbb{Z}_p/p^{\alpha_t})^2$$

- We want to find $s, \alpha_1 \geq \ldots \geq \alpha_t$.

Structure of the Selmer group

Define the ideals

$$\Theta_{i,N} = \left(\left\{ \delta_m : \nu(m) \leq i, m \in \mathcal{N}^{(N)} \right\} \right) \subset \mathbb{Z}/p^N$$

Theorem (Kurihara)

For N large enough, we have that

$$\Theta_{0,N} = \Theta_{1,N} = \cdots = \Theta_{s-1,N} = 0$$

$$\Theta_{s+2j,N} = \prod_{k=j+1}^{t} (p)^{2\alpha_j} \ \forall j = 0, \ldots, t$$

Corollary

If we write $\Theta_{i,N} = p^{n_{i,N}} \left(\mathbb{Z}/p^N \right)$, then $n_{i,N}$ does not depend on N when N is large enough. Then we can define $n_i = \lim n_{i,N}$ and we have that

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^s \times \left(\mathbb{Z}/p^{\frac{n_s - n_{s+2}}{2}} \right)^2 \times \cdots \times \left(\mathbb{Z}/p^{\frac{n_{s+2t-2} - n_{s+2t}}{2}} \right)^2$$

Thanks for your attention!