On the structure of Selmer group of elliptic curves

Alberto Angurel Andrés

University of Nottingham

September 6

- Let E be an elliptic curve defined over $\mathbb{Q}$.
- The object we want to study is $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$, where p is an odd prime number such that E has good, ordinary reduction at p. We will also need to assume p satisfies some technical hypothesis.
- There is a short exact sequence

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

- The structure of the Selmer group gives an upper bound for the rank of the elliptic curve.
- If $Ш(E/\mathbb{Q})$ is finite, then the Selmer group determine the exact rank of the curve.
- There is a modular form such that $L(E, s) = L(f, s)$.
- I will use f to define modular symbols, which can be related to the structure of the Selmer group.

Modular symbols

Modular symbols

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

Remark

Modular symbols are related to the special values of the L-function.

$$\left[\frac{0}{1}\right] = L(f, 1)$$

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

A minor modification of θ_{p^∞} is the p-adic L-funcion of the elliptic curve

$$\vartheta_{p^\infty} \in \varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})]$$

Quantities δ_m

Let $\mathcal{P}$ be the set of good reduction primes satisfying the following

- $l \equiv 1 \mod p$
- $\widetilde{E}(\mathbb{F}_l) \cong \mathbb{Z}/p$

Let $\mathcal{N}$ be the square-free products of primes in $\mathcal{P}$. Assume $m \in \mathcal{N}$.

$$\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) = \mathcal{G}_1 \times \cdots \times \mathcal{G}_r, \text{ where } \mathcal{G}_i := \mathrm{Gal}(\mathbb{Q}(\mu_{l_i})/\mathbb{Q})$$

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

$$\theta_m \equiv \pm\delta_m(\tau_1 - 1)\cdots(\tau_r - 1) \mod \left(p, (\tau_1 - 1)^2, \ldots, (\tau_r - 1)^2\right)$$

Remark

The value of δ_m might depend on the chosen generators τ_i. However, whether δ_m vanishes or not is independent of the generators.

Remark

The quantities δ_m are effectively computable.

Bounding the Selmer group

Under our assumptions, $\mathrm{Sel}(\mathbb{Q}, E[p]) = \mathrm{Sel}(\mathbb{Q}, E[p^\infty])[p]$.

There is a canonical map

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

Theorem (Kurihara)

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

$$\dim_{\mathbb{F}_p} (\mathrm{Sel}(\mathbb{Q}, E[p])) \leq \nu(m)$$

where $\nu(m)$ is the number of prime divisors of m.

When is this bound the best possible?

Definition

We say that $m \in \mathcal{N}$ is δ-minimal if

- $\delta_m \neq 0$
- $\delta_d = 0$ for every proper divisor

Theorem (Kim, Sakamoto)

If $m \in \mathcal{N}$ is δ-minimal. Then

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

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

Structure of $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])$

- Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of the rationals.
- We will consider the group $X := \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p)$
- The Galois group $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ acts on X.
- X is a module over $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] \cong \mathbb{Z}_p[[T]]$
- X is a finitely generated, torsion Λ module.
- $X \sim \prod_i \Lambda/(f_i)^{\beta_i} \times \prod_j \Lambda/(p)^{\alpha_j}$
- Define $\mathrm{char}(X) = \prod_i (f_i)^{\beta_i} \prod_j (p)^{\alpha_j}$

Iwasawa main conjecture

It is the following equality of ideals in Λ

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

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

Theorem (Sakamoto)

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

Structure of the Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$

- From now on, I will assume Iwasawa main conjecture and other technical conditions.
- $$\boxed{\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee \cong \mathbb{Z}_p^s \times (\mathbb{Z}_p/p^{\alpha_1})^2 \times \cdots \times (\mathbb{Z}_p/p^{\alpha_t})^2}$$
- Our goal is computing $s, \alpha_1, \ldots, \alpha_t$.

Structure of the Selmer group

Define the ideals

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

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!