On the 2-Selmer group of hyperelliptic curves.

Ariel Pacetti

Center for Research and Development in Mathematics and Applications (CIDMA),
University of Aveiro

February 6th 2023

Symposium on Arithmetic Geometry and its Applications
joint work with Daniel Barrera Salazar and Gonzalo Tornaría

Descent on elliptic curves

Let E/K be an elliptic curve and let n be a positive integer. The short exact sequence of Gal_K-modules

$$1 \longrightarrow E(\overline{K})[n] \longrightarrow E(\overline{K}) \xrightarrow{\times n} E(\overline{K}) \longrightarrow 1$$

induces a long exact sequence

$$1 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} \mathrm{H}^1(\mathrm{Gal}_K, E[n]) \longrightarrow \mathrm{H}^1(\mathrm{Gal}_K, E) \rightarrow$$

Then to compute/bound $E(K)$ it is enough to compute:

- The finite group $E(K)[n]$,
- The cohomology group $\mathrm{H}^1(\mathrm{Gal}_K, E[n])$.

⚠ The group $\mathrm{H}^1(\mathrm{Gal}_K, E[n])$ is not finite (we need to impose some ramification condition)

An easy case

Suppose that $E(K)[n] = E[n]$. In particular, $\zeta_n \in K$. Then

- $\mathrm{H}^1(\mathrm{Gal}_K, E[n]) \simeq \mathrm{Hom}(\mathrm{Gal}_K, \mathbb{Z}/n) \times \mathrm{Hom}(\mathrm{Gal}_K, \mathbb{Z}/n)$.
- $\mathrm{Hom}(\mathrm{Gal}_K, \mathbb{Z}/n) \leftrightsquigarrow$ cyclic degree n field extensions of K,
- By Kummer's theory, cyclic degree n field extensions of K correspond to elements in $K^\times/(K^\times)^n$.

Let S be the set of primes of bad reduction of E together with the primes dividing n and let

$$K(S,n) = \{b \in K^\times \,:\, n \mid v_{\mathfrak{p}}(b) \text{ for all } \mathfrak{p} \notin S\}/(K^\times)^n.$$

Then one can actually prove that $E(K)/nE(K) \hookrightarrow K(S,n) \times K(S,n)$.
⚠ It is a hard problem to determine which elements of $K(S,n)$ actually lie in the image

Improvements

- When $E(K)[n] \subsetneq E[n]$, one can look at $K(E[n])$ and do a similar computation. Can we do better?
- (Cassels) If
$$E : y^2 = p(x)$$
and $n = 2$ it is enough to look at $A_K = K[x]/(p(x))$.
- Under some hypothesis, we can remove the bad primes and 2 from the ramification set.
- Instead of looking at $\mathrm{H}^1(\mathrm{Gal}_{K,S}, E[n])$, work with $\mathrm{Sel}_n(E)$ (the n-th Selmer group).

Hyperelliptic curves

Let K be a number field with odd class number and let

$$\mathscr{C} : y^2 = p(x),$$

where $p(x) \in \mathcal{O}[x]$ monic, of odd degree and a_{d-1} even. Let J denote its Jacobian. Let

$$A_K := K[x]/(p(x)).$$

Theorem

Under the following hypothesis

$$\begin{aligned} \dim_{\mathbb{F}_2} \mathrm{Cl}_*(A_K, \mathscr{C})[2] - \sum_{v|2} \left(r_v - 1 - \dim_{\mathbb{F}_2}(W_v)\right) \quad &\leq \\ \leq \quad \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J) \quad &\leq \quad \dim_{\mathbb{F}_2} \mathrm{Cl}_*(A_K, \mathscr{C})[2] + g\,[K:\mathbb{Q}]\,. \end{aligned}$$

Formula:

$$\dim_{\mathbb{F}_2} \mathrm{Cl}_*(A_K,\mathscr{C})[2] - \sum_{v|2}\left(r_v - 1 - \dim_{\mathbb{F}_2}(W_v)\right) \quad \leq$$

$$\leq \quad \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J) \quad \leq \quad \dim_{\mathbb{F}_2} \mathrm{Cl}_*(A_K,\mathscr{C})[2] + g\,[K:\mathbb{Q}]. \quad (1)$$

Where for $v \mid 2$,

- r_v is the number of factors of $p(x)$ modulo v.
- If $A_{K_v} \simeq K_1 \times \cdots \times K_r$, with $K_i = K_v[x_i]/(p_i(x_i))$. Then

$$W_v := \langle \mathrm{Tr}_{k_i/k}(\overline{x}_i) \ : \ i = 1, ..., r \rangle \subset k.$$

- g is the genus of $\mathscr{C} = \frac{d-1}{2}$.
- $\mathrm{Cl}_*(A_K,\mathscr{C})[2]$ is the two torsion of the class group with the following hypothesis at infinity

Hypotheses and ideas

- The group $\mathrm{H}^1(\mathrm{Gal}_K, J[2])$ is isomorphic to $(A_K^\times/(A_K^\times)^2)_\square$.
- For bounding $\mathrm{Sel}_2(J)$, compute for each place v the image of

$$\delta_v : J(K_v)/2J(K_v) \hookrightarrow (A_{K_v}^\times/(A_{K_v}^\times)^2)_\square$$

- $p(x)$ satisfies condition $(\dagger)$ if one of the following holds:
  - $(\dagger.\mathrm{i})$ The K-algebra A_K is a field extension of K.
  - $(\dagger.\mathrm{ii})$ The ring of integers $A_\mathcal{O}$ equals $\mathcal{O}[x]/(p(x))$.
  - $(\dagger.\mathrm{iii})$ The residual characteristic of K is odd and the order of the component group $[J(K) : J^0(K)]$ is odd.

Theorem

If the polynomial $p(x)$ satisfies $(\dagger)$ then $\mathrm{Im}(\delta_v) \subset (A_{\mathcal{O}_v}^\times/(A_{\mathcal{O}_v}^\times)^2)_\square$.

If $v \nmid 2$ we get equality. This implies no ramification at v

Places dividing 2 and ∞

- When $v \mid 2$, construct a set W_v such that

$$W_v \subset \mathrm{Im}(\delta_v) \subset (A^{\times}_{\mathcal{O}_v}/(A^{\times}_{\mathcal{O}_v})^2)_{\square}$$

  and compute $\#W_v/(A^{\times}_{\mathcal{O}_v})^2$ (need to construct local points).
- A similar construction at infinity.
- Define "class groups" $C_W(\mathscr{C}), \tilde{C}(\mathscr{C})$ and prove that

$$C_W(\mathscr{C}) \subset \mathrm{Sel}_2(J) \subset \tilde{C}(\mathscr{C})$$

- Relate $\tilde{C}(\mathscr{C})$ to $\mathrm{Cl}_*(A_K, \mathscr{C})[2]$ and compute $[\tilde{C}(\mathscr{C}) : C_W(\mathscr{C})]$.
- **Remark:** have many examples that prove that the lower and the upper bound are optimal.

Applications I: quadratic twists

If $a \in \mathcal{O}$ the twist of $\mathscr{C}$ by a equals

$$\mathscr{C}_a : y^2 = a^d p(x/d).$$

- If $p(x)$ is irreducible and all prime ideals dividing a are inert or totally ramified in A_K/K, then if $\mathscr{C}$ satisfies † so does $\mathscr{C}_a$. ▸ H

Theorem

Suppose that the Galois group of the Galois closure of A_K over K contains an element of order d. Then among all quadratic twists by principal prime ideals, there exists a subset of positive density $\mathcal{S}$ such that the abelian varieties $J(\mathscr{C}_a)$ have the same 2-Selmer group for all $a \in \mathcal{S}$.

Application II: a particular family

Let a be a non-zero integer, and consider the genus 2 hyperelliptic curve

$$\mathscr{C}_a : y^2 = x^5 - ax.$$

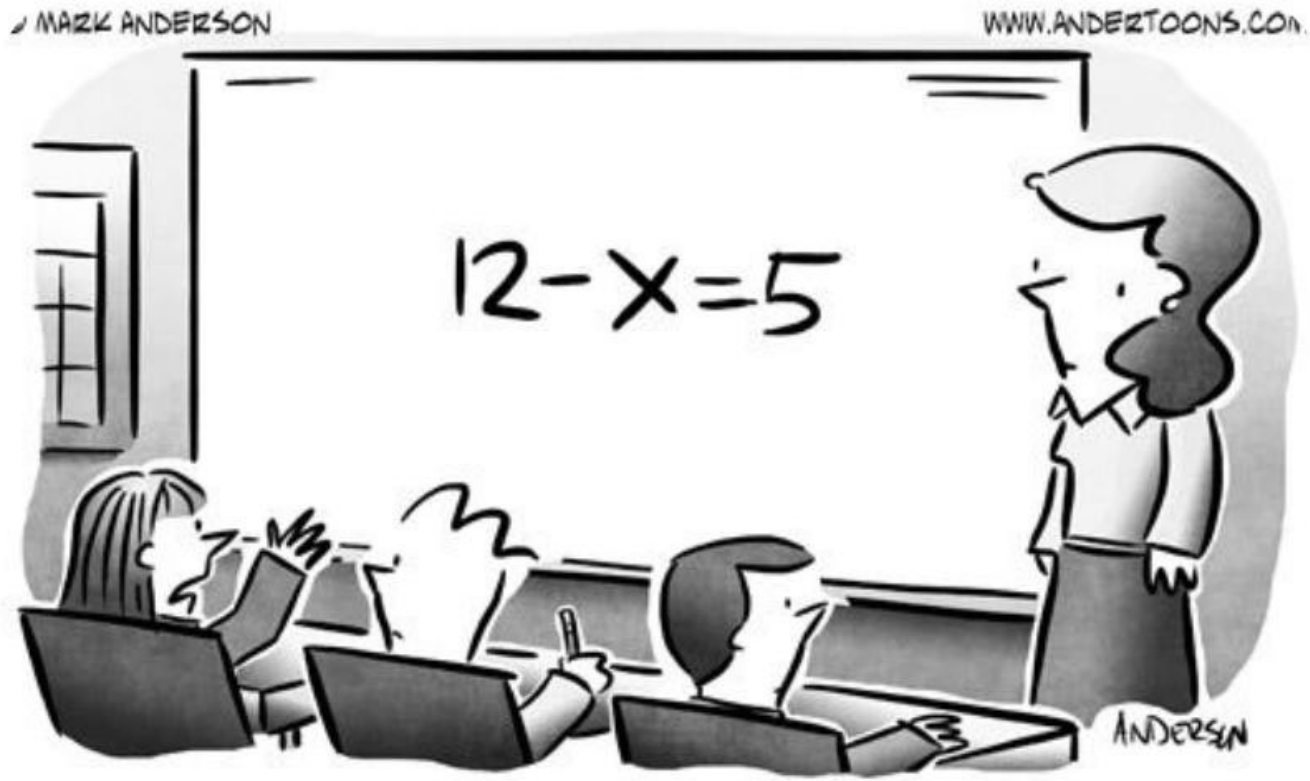
Theorem

Assuming the parity conjecture, $J(\mathscr{C}_p)$ has rank 1 for all primes $p \equiv 3 \pmod 8$.

Proof.

- If $p \equiv 3 \pmod 4$ then $\mathrm{Cl}(\mathbb{Q}[\sqrt[4]{p}])$ is odd.
- Applying our result to $\mathscr{C}_p$, $0 \leq \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J(\mathscr{C}_p)) \leq 2$.
- Since $J(\mathscr{C}(p))$ has a 2-torsion point, $1 \leq \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J(\mathscr{C}_p)) \leq 2$.
- Compute the root number (use the curve has CM).

Thank you for coming



"This time X is 7. Last time it was 4. And the time before that it was 12. Maybe X should take some time to reflect and decide for itself what it really wants to be."