Cassels-Tate pairing on 2-Selmer groups of elliptic curves

Himanshu Shukla

Mathematisches Institut, Universität Bayreuth

Oberseminar Arithmetic Geometry

10th December, 2020

Outline

Some notations

- Fix a number field k.
- $f := X^3 + aX + b = (X - e_1)(X - e_2)(X - e_3) \in k[X]$, with $e_1 \neq e_2 \neq e_3 \neq e_1 \in \bar{k}$.
- Define
$$E := Y^2 = f(X). \tag{1}$$
- For a place v of k, k_v denotes its completion with respect to v and $\mathfrak{k}_v$ the residue field.
- Let E_v denote the curve E defined over k_v.
- G_F we will denote the absolute galois group of the field F.

Some theoretical aspects

Theorem (Mordell-Weil)

$$E(k) \cong E(k)_{tors} \oplus Z^{r_E},$$

where $\#E(k)_{tors} < \infty$

Theorem (Lutz-Nagell)

$P := (x, y) \in E(\mathbb{Q})_{tors}$, *then* $x, y \in \mathbb{Z}$, *and* $y^2 | 4a^3 - 27b^2$ *or* $y = 0$.

- A faster way to compute $E(k)_{tors}$ is to use the injection $E(k)_{tors} \hookrightarrow \bar{E}_v(\mathfrak{k}_v)$, $\bar{E}_v$ denotes E over $\mathfrak{k}_v$ for a place of good reduction.
- No unconditional algorithm to compute r_E is known.
- Assuming BSD, r_E may be computed using $\mathrm{ord}(L(E, s = 1))$.

Upper and lower bounds

- **Lower bound:** Find points and check for independence.
- **Upper bound:** Use descent.
- See if they match!

The Kummer sequence:

$$0 \longrightarrow E[n] \hookrightarrow E \longrightarrow E \longrightarrow 0 \tag{2}$$

Applying galois cohomology:

$$\begin{tikzcd}
0 \arrow[r] & \frac{E(k)}{nE(k)} \arrow[r, hook] \arrow[d] & H^1(G_k, E[n]) \arrow[r] \arrow[d] \arrow[dr, "\alpha"] & H^1(G_k, E)[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v \frac{E(k_v)}{nE(k_v)} \arrow[r, hook] & \prod_v H^1(G_{k_v}, E[n]) \arrow[r] & \prod_v H^1(G_{k_v}, E_v)[n] \arrow[r] & 0,
\end{tikzcd}$$

Descent sequence

We have the $n-$descent sequence.

$$0 \longrightarrow \frac{E(k)}{nE(k)} \hookrightarrow \mathrm{Sel}^{(n)}(E) \longrightarrow Ш[n] \longrightarrow 0, \qquad (3)$$

where n^{th} Selmer group

$$\mathrm{Sel}^{(n)}(E) = \ker(\alpha),$$

and the Tate-Shafarevich group

$$Ш := \ker\left(H^1(G_k, E) \longrightarrow \prod_v H^1(G_{k_v}, E_v) \right).$$

- $\mathrm{Sel}^{(n)}(E)$ is finite and effectively computable in principle.
- $\mathrm{rank}_{\mathbb{F}_p}(\mathrm{Sel}^{(p)}(E))$ bounds the $\mathrm{rank}_{\mathbb{F}_p}(\frac{E(k)}{pE(k)})$.
- If $Ш[n]$ is trivial then $\mathrm{Sel}^{(n)}(E) \cong \frac{E(k)}{nE(k)}$.

Higher descent

- If $(m, n) = 1$, $\mathrm{Sel}^{(mn)}(E) \cong \mathrm{Sel}^{(n)}(E) \times \mathrm{Sel}^{(m)}(E)$.
- If $l \geq 2$, then $\mathrm{Sel}^{p^l}(E)$ is known as **higher** $p-$**descent.**
- We have the following commutative diagram:

$$\begin{tikzcd} \frac{E(k)}{p^l E(k)} \arrow[r, hook] \arrow[d] & \mathrm{Sel}^{(p^l)}(E) \arrow[d, "p"] \\ \frac{E(k)}{p^{l-1} E(k)} \arrow[r, hook] & \mathrm{Sel}^{(p^{l-1})}(E) \end{tikzcd} \tag{4}$$

We have

$$\frac{E(k)}{pE(k)} \subseteq p\mathrm{Sel}^{(p^2)}(E) \subseteq \mathrm{Sel}^{(p)}(E). \tag{5}$$

Cassels-Tate pairing (CTP)

- CTP (denoted by $\langle .,. \rangle_{CT}$) was defined by **J.W.S. Cassels** for elliptic curves.
- **John Tate** generalized it to abelian varieties.
- CTP has following properties:
  - $\langle .,. \rangle_{CT} : Ш \times Ш \longrightarrow \mathbb{Q}/\mathbb{Z}$.
  - CTP is an anti-symmetric pairing.
  - For $\alpha \in Ш[n]$, $\langle \beta, \alpha \rangle_{CT} = 0 \iff \beta \in nШ$.

Pulling back $\langle .,. \rangle_{CT}$ on $\mathrm{Sel}^{(n)}(E)$, we have:

Theorem (Cassels)

$\langle \alpha, \beta \rangle_{CT} = 0$ *for all* $\beta \in \mathrm{Sel}^{(n)}(E)$, $\iff \alpha \in n\mathrm{Sel}^{(n^2)}(E)$.

Weil-pairing based definition

- Consider the "evaluation" based pairings:
  - $\langle .,. \rangle_1 : (\mathrm{Princ}(E) \times \mathrm{Div}^0(E))^\perp \longrightarrow \overline{k}^\times$,
  - $\langle .,. \rangle_2 : (\mathrm{Div}^0(E) \times \mathrm{Princ}(E))^\perp \longrightarrow \overline{k}^\times$,

  with $\langle \mathrm{div}(f), D \rangle_1 = \langle D, \mathrm{div}(f) \rangle_2 = \prod_P f(P)^{v_P(D)}$.
- $\langle .,. \rangle_1 = \langle .,. \rangle_2$ on $(\mathrm{Princ}(E) \times \mathrm{Princ}(E))^\perp$ (Weil-reciprocity!).
- Let $e_n(.,.) : E[n] \times E[n] \longrightarrow \mu_n$, denote the **Weil-pairing** with

$$e_n(P, Q) = \langle n\mathfrak{p}, \mathfrak{q} \rangle_1 - \langle \mathfrak{p}, n\mathfrak{q} \rangle_2,$$

  where $\mathfrak{p}, \mathfrak{q}$ denote the representatives of P, Q (resp.) in $\mathrm{Div}^0(E)$.
- Let $\cup$ denote the cup product on $H^*(G_k, E[n])$ induced by Weil-pairing.

Weil-pairing based definition (cont.)

Let $\alpha, \alpha' \in \mathrm{Sel}^{(n)}(E)$.

- **Global part:**
  - Lift α, α' to $\mathfrak{a}, \mathfrak{a}' \in Z^1(G_k, E[n])$.
  - Let $a \in C^1(G_k, E[n^2])$, with $na = \mathfrak{a}$.
  - $\partial a \cup \mathfrak{a}' \in Z^3(G_k, \bar{k}^\times) \Longrightarrow \partial a \cup \mathfrak{a}' = \partial \epsilon$, for $\epsilon \in C^2(G_k, \bar{k}^\times)$.
  - The above statements follow from galois cohomology on

    $$0 \longrightarrow E[n] \hookrightarrow E[n^2] \longrightarrow E[n] \longrightarrow 0$$

    and that $H^3(G_k, \bar{k}^\times)$ is trivial.
- **Local part:**
  - $\alpha_v = 0 \Longrightarrow \exists P_v \in E_v$, with $\partial P_v = \alpha_v$.
  - Choose $Q_v \in E_v$, with $nQ_v = P_v$ and let $\mathfrak{q}_v := \partial Q_v$.
  - $a_v - \mathfrak{q}_v$ take values in $E[n]$.
  - Define $\gamma_v := (a_v - \mathfrak{q}_v) \cup \mathfrak{a}'_v - \epsilon_v \in Z^2(G_{k_v}, \bar{k_v}^\times)$.

Weil-pairing based definition (contd.)

γ_v represents some class $c_v \in H^2(G_{k_v}, \bar{k}_v^\times) \cong \mathrm{Br}(k_v)$.

Definition

For $(\alpha, \alpha') \in \mathrm{Sel}^{(n)}(E) \times \mathrm{Sel}^{(n)}(E)$ we have:

$$\langle \alpha, \alpha' \rangle_{CT} = \sum_v \mathrm{inv}_v(c_v)$$

Effectiveness of CTP: Cassels effectively defined a pairing $\langle ., . \rangle_{Cas}$ on $\mathrm{Sel}^{(2)}(E) \times \mathrm{Sel}^{(2)}(E)$, with properties same as CTP.

Known results

- **Fischer, Schaefer and Stoll**, showed that $\langle \cdot, \cdot \rangle_{Cas} = \langle \cdot, \cdot \rangle_{CT}$ on $\mathrm{Sel}^{(2)}(E) \times \mathrm{Sel}^{(2)}(E)$.
- **Swinnerton-Dyer** extended this approach to compute CTP between $\mathrm{Sel}^{(2)}(E)$ and $\mathrm{Sel}^{(2^n)}(E)$.
- **Fischer and Newton** computed CTP on $\mathrm{Sel}^{(3)}(E)$.
- **van Beek and Fischer** compute CTP on Selmer groups of odd prime degree isogeny.
- The above computations were based on Weil-pairing based definition.

Known results (contd.)

- **Fischer and Donelly** used homogenous space based definition to compute CTP on $\mathrm{Sel}^{(2)}(E)$.
- **Tom Fischer** has a similar approach to compute CTP on $\mathrm{Sel}^{(3)}(E)$ using homogenous space definition.
- CTP can be defined in general for $Ш(A) \times Ш(A^\vee)$, for an abelian variety A and its dual $A^\vee$.
- We compute CTP using **Albanese-Albanese** definition given by **Poonen and Stoll**.
- We aim to compute CTP on jacobians of genus 2 curves.

Albanese-Albanese defintion

Let $\alpha, \alpha' \in \mathrm{Sel}^{(n)}(E)$.

- **Global part:**
  - Lift α, α' to $\mathfrak{a}, \mathfrak{a}' \in C^1(G_k, \mathrm{Div}^0(E))$.
  - $\partial\mathfrak{a}, \partial\mathfrak{a}'$ take values in $\mathrm{Princ}(E)$.
  - Let $\eta := \langle \partial\mathfrak{a}, \mathfrak{a}' \rangle_1 - \langle \mathfrak{a}, \partial\mathfrak{a}' \rangle_2 \in Z^3(G_k, \bar{k}^\times) \implies \eta = \partial\epsilon$, for $\epsilon \in C^2(G_k, \bar{k}^\times)$.
  - The above statements follow using the galois cohomology on Kummer sequence and on

$$0 \longrightarrow \mathrm{Princ}(E) \hookrightarrow \mathrm{Div}^0(E) \longrightarrow \mathrm{Pic}^0(E) \longrightarrow 0,$$

    and using $H^3(G_k, \bar{k}^\times)$ is trivial.
- **Local part:**
  - There exists $P_v \in E_v$, with $\partial P_v = \alpha_v$.
  - Lift P_v to a degree zero divisor $\mathfrak{p}_v$, and $\mathfrak{a}_v - \partial\mathfrak{p}_v$ takes values in $\mathrm{Princ}(E)$.
  - Consider $\gamma_v := \langle (\mathfrak{a}_v - \mathfrak{p}_v), \mathfrak{a}'_v \rangle_1 - \langle \mathfrak{p}_v, \partial\mathfrak{a}'_v \rangle_2 - \epsilon_v$.

Albanese-Albanese definition (contd.)

γ_v represents some class $c_v \in H^2(G_{k_v}, \bar{k_v}^{\times}) \cong \mathrm{Br}(k_v)$.

Definition

For $(\alpha, \alpha') \in \mathrm{Sel}^{(n)}(E) \times \mathrm{Sel}^{(n)}(E)$ we have:

$$\langle \alpha, \alpha' \rangle_{CT} = \sum_v \mathrm{inv}_v(c_v)$$

Theorem (Poonen and Stoll)

Weil-pairing based definition and Albanese-Albanese definition of the Cassels-Tate pairing are equal.

We prove the following theorem:

Theorem

Let $\alpha, \alpha' \in \mathrm{Sel}^{(2)}(E)$, *represented by* $(\beta_1, \beta_2, \beta_3)$, $(\beta'_1, \beta'_2, \beta'_3)$, *with* $\beta_1\beta_2\beta_3 \in k^2$, *and* $\beta'_1\beta'_2\beta'_3 \in k^2$ *and* $\beta_i, \beta'_i \in k(e_i)$.
$(-1)^{2\langle \alpha, \alpha' \rangle_{CT}} = \prod_v [\alpha, \alpha]_v$, *where*

$$[\alpha, \alpha]_v = \begin{cases} \prod_{i=1}^{3} (\delta_{v,i}, \beta'_i)_{k_v}, & f \text{ splits over } k, \\ (\delta_{v,1}, \beta'_1)_{k_v} (\delta_{v,2}, \beta'_2)_{k_v(e_2)} & e_1 \in k \text{ and } [k(e_2) : k] = 2, \\ (\delta_{v,1}, \beta'_1)_{k_v(e_1)} & [k(e_1) : k] \geq 3, \end{cases}$$

where $\delta_{vi} \in k_v(e_i)$.

Corollary

The above pairing exactly matches the $\langle ., . \rangle_{Cas}$.

A bottleneck and exploiting freedom of choices!

- An important step is to find $\epsilon \in C^2(G_k, \bar{k}^\times)$ such that $\partial\epsilon = \eta$.
- Solving "skewed" linear equations:

$$\frac{\sigma\epsilon(\tau,\rho)\epsilon(\sigma,\tau\rho)}{\epsilon(\sigma\tau,\rho)\epsilon(\sigma,\tau)} = \eta(\sigma,\tau,\rho).$$

- We exploit the everywhere local solubility of 2-coverings to get global solution to certain norm equations.

A simplification: Consider a different lift of α' to $\mathfrak{a}$ with values in $\mathrm{Div}^0(E)$.

Exploiting freedom of choices

Assume f splits over k.

$$\alpha' := \sum_{i=1}^{3} \alpha'_i,$$

with α'_i being $1-$cocycles.
This splits

$$\eta = \sum_{i=1}^{3} \eta_i,$$

with $\eta_i \in H^3(G_k, \bar{k}^\times)$ using bilinearity of cup-product.
Find ϵ_i, with

$$\partial \epsilon_i = \eta_i.$$

Thank You!