Computational Aspects of the Birch and Swinnerton-Dyer Conjecture

Lectures by: Céline Maistret
Notes by: Ross Paterson

These notes were taken live during lectures at the CMI-HIMR Computational Number Theory summer school held at the University of Bristol in June 2019. In particular, any mistakes are the fault of the transcriber and not of the lecturer. Remarks in red were not written on the board, and were often added later by the transcriber.

Lecture List

Contents

Lecture 1: The Birch and Swinnerton-Dyer Conjecture

The layout will be as follows:

1. The Birch and Swinnerton Dyer Conjecture,
2. Shaferevich-Tate group and the Cassels-Tate pairing,
3. Tamagawa Numbers,
4. Explicit Computations of Parities of Rank for some Abelian Varieties.

Notes are available on the webpage. We begin with the conjecture

1 BSD

1.1 Elliptic Curves over Q

Let $E/\mathbb{Q}$ be an elliptic curve, recall the Mordell(-Weil) theorem which tells us that $E(\mathbb{Q})$ is a finitely generated abelian group:

$$E(\mathbb{Q}) = \mathbb{Z}^{\mathrm{rk}(E/\mathbb{Q})} \oplus E(\mathbb{Q})_{\mathrm{tors}}$$

Where $E(\mathbb{Q})_{\mathrm{tors}}$ is a finite abelian group and $\mathrm{rk}(E/\mathbb{Q}) \geq 0$ is an integer.

Problem: There is no provable method to compute $\mathrm{rk}(E/\mathbb{Q})$.

In the mid 1960's, Birch and Swinnerton-Dyer (based on numberical experiments) conjectured that $\mathrm{rk}(E/\mathbb{Q})$ can be computed by studying the L-function of $E/\mathbb{Q}$.

Rationale: fix some prime $p \nmid \Delta_E$ not dividing the discriminant of E. Then the reduced curve $\tilde{E}/\mathbb{F}_p$ is an elliptic curve, and we denote

$$N_p := \#\tilde{E}(\mathbb{F}_p)$$

Main idea: a large rank over $\mathbb{Q}$ gives rise to a lot of $\mathbb{Q}$-rational points on $E/\mathbb{Q}$, which should make N_p large. Look at

$$\prod_{p<X} \frac{N_p}{p}$$

Conjecture 1. *There exists a constant C_E depending only on E such that for some $X > 0$*

$$\prod_{p<X} \frac{N_p}{p} \sim C_E (\log X)^{\mathrm{rk}(E/\mathbb{Q})}$$

as $X \to \infty$.

Note: It is not convenient to study the value of $\prod_{p<X} \frac{N_p}{p}$, but for each p, the value of N_p is packaged up into the L-function of $E/\mathbb{Q}$ via $N_p = p + 1 - a_p$ since

$$L(E/\mathbb{Q}, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{-2s+1}}.$$

If we discard all convergence problems, "evaluating" (ignoring all convergence problems for now) at $s = 1$ gives

$$L(E/\mathbb{Q}, 1)\text{“} =\text{”} \prod_p \frac{p}{N_p}.$$

Thus $L(E/\mathbb{Q}, s)$ at $s = 1$ should contain information about $\mathrm{rk}(E/\mathbb{Q})$.

Conjecture 2 (BSD 1)**.** *The L-function $L(E/\mathbb{Q}, s)$ extends to an entire function on $\mathbb{C}$ and*

$$L(E/\mathbb{Q}, 1) \neq 0 \iff \#E(\mathbb{Q}) < \infty$$

and moreover $\mathrm{rk}(E/\mathbb{Q})$ *is the order of vanishing of $L(E/\mathbb{Q}, s)$ at $s = 1$.*

In fact they went further!

Conjecture 3 (BSD 2)**.**

$$\lim_{s\to 1} \frac{L(E/\mathbb{Q}, s)}{(s-1)^{\mathrm{rk}(E/\mathbb{Q})}} = \frac{|Ш(E/\mathbb{Q})|\, R(E/\mathbb{Q})\omega_{\mathbb{R}} \prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}$$

where

- $Ш(E/\mathbb{Q})$ *is the Shaferevich-Tate group (see lecture 2!)*
- $R(E/\mathbb{Q})$ *is the regulator of $E/\mathbb{Q}$ (see Steffens lecture in week 2)*
- c_p *are the Tamagawa numbers at a prime p (see lecture 3)*
- $\omega_{\mathbb{R}}$ *is the real period of $E/\mathbb{Q}$.*

There are some great notes of Cremona, these are linked to on Maistrets webpage or available on Cremonas.

Known Results: For $E/\mathbb{Q}$, Gross-Zagier, Kolyvragin proved that

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$$

then $\mathrm{rk}(E/\mathbb{Q}) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$.

Skinner-Urban, Zhang probved that if $\mathrm{rk}(E/\mathbb{Q}) \leq 1$ then $\mathrm{rk}(E/\mathbb{Q}) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$

1.2 Abelian Varieties over Number Fields

Let A/K be an abelian variety of dimension d.

Conjecture 4 (Generalised BSD)**.** *Let L-function of A/K extends to an entire functioon on $\mathbb{C}$ and*

1. $\mathrm{rk}(A/K) = \mathrm{ord}_{s=1} L(A/K, s)$
2. $\lim_{s\to 1} \frac{L(A/K,s)}{(s-1)^{\mathrm{rk}(A/K)}} = \frac{2^{dr_2} |Ш(A/K)| R(A/K) \prod_{v|\infty} \int_{A(K_v)} |\omega|_v \prod_{v\nmid\infty} c_v \left|\frac{\omega}{\omega_0}\right|_v}{\sqrt{|d_K|^d} |A(K)|_{\mathrm{tors}} \left|\check{A}(K)_{\mathrm{tors}}\right|}$.

Where:

- r_2 *is the number of complex places of K.*
- d_K *is the discriminant of K*
- ω *is a choice of non-zero exterior d-form.*
- *For a place $v \in M_K$, ω_v^0 is the Néron differential for A/K_v*
- $\check{A}/K$ *is the dual variety of A/K.*

1.3 Consequences of BSD: The Parity Conjecture

Remark 1.1. *Recall that if we write* $\mathrm{rk}_{an}(A/K) := \mathrm{ord}_{s=1} L(A/K, s)$ *for the analytic rank, then BSD claims that*

$$\mathrm{rk}_{an}(A/K) = \mathrm{rk}(A/K).$$

On the other hand, the completed L-function $L^*(A/K, s)$ *(adding some Gamma factors for the infinite places) is conjectured to satisfy a functional equation:*

$$L^*(A/K, s) = wL^*(A/K, 2 - s)$$

where $w \in \{\pm 1\}$*. is called the* ***sign*** *of the functional equation.*

- *If* $w = 1$*, then* $\mathrm{ord}_{s=1} L(A/K, s)$ *is even*
- *If* $w = -1$*, then* $\mathrm{ord}_{s=1} L(A/K, s)$ *is odd*

$\Rightarrow (-1)^{\mathrm{rk}_{an}\, A/K} = w$ *+ BSD means that we should expect* $(-1)^{\mathrm{rk}\, A/K} = w$*. Lastly, the sign* ω *is conjectured to be equal to the* ***global root number*** $W := \prod_v w_v$ *where the* w_v *are* ***local root numbers****.*

Conjecture 5 (Parity Conjecture)**.**

$$(-1)^{\mathrm{rk}(A/K)} = W$$

Example 1. *Consider* $E/\mathbb{Q} : y^2 + y = x^3 + x^2 - 7x + 5$*.*

$$\begin{aligned} \Delta_E &= -7 \cdot 13, \\ \omega_\infty &= -1, \\ \omega_7 = \omega_1 3 &= -1, \\ W = (-1)^3 &= -1 \\ &\Rightarrow \mathrm{rk}(E/\mathbb{Q}) \text{ is odd.} \end{aligned}$$

1.4 A Formula for the Parity of the Rank

Theorem 1.2 (BSD invariance under isogeny, Cassels '65)**.** *Assume that* $Ш(E/\mathbb{Q})$ *is finite, and that* $\varphi : E \to E'$ *is a* $\mathbb{Q}$*-isogeny. Then*

$$\frac{|Ш(E/\mathbb{Q})|\, R(E/\mathbb{Q})\omega_{\mathbb{R}} \prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2} = \frac{|Ш(E'/\mathbb{Q})|\, R(E'/\mathbb{Q})\omega_{\mathbb{R}} \prod_p c_p}{|E'(\mathbb{Q})_{\mathrm{tors}}|^2}$$

Note that this does not assert that hte individual constants are unchanged under isogeny, in fact these will change. It is astounding that they correct one another so that this expression is unchanged.

Lemma 1.3 (Dokchitser-Dokchitser)**.** *Let* $\varphi : E/\mathbb{Q} \to E'/\mathbb{Q}$ *be a* $\mathbb{Q}$*-isogeny of degree* d*. Then*

$$\frac{R(E/\mathbb{Q})}{R(E'/\mathbb{Q})} = d^{\mathrm{rk}(E/\mathbb{Q})} \mod (\mathbb{Q}^\times)^2$$

Corollary 1.4. *Let* ℓ *be a prime and* $E/\mathbb{Q}$ *admitting an isogeny of degree* ℓ*. Assume that* $Ш(E/\mathbb{Q})$ *is finite. Then*

$$(-1)^{\mathrm{rk}(E/\mathbb{Q})} = (-1)^{\mathrm{ord}_\ell(\frac{\omega_{\mathbb{R}}}{\omega'_{\mathbb{R}}} \prod_p \frac{c_p}{c'_p})}$$

Proof. From Theorem 1.2:

$$\frac{R(E/\mathbb{Q})}{R(E'/\mathbb{Q})} = \frac{|E'(\mathbb{Q})_{\text{tors}}|^2 \, |Ш(E/\mathbb{Q})| \, \omega_{\mathbb{R}} \prod_p c_p}{|E(\mathbb{Q})_{\text{tors}}|^2 \, |Ш(E'/\mathbb{Q})| \, \omega'_{\mathbb{R}} \prod_p c'_p} = \frac{\omega'_{\mathbb{R}} \prod_p c'_p}{\omega_{\mathbb{R}} \prod_p c_p}$$

□

Lecture 2: Shaferevich-Tate Groups

2 Shaferevich-Tate Groups

Recall that Mordell-Weil tells us that $E(\mathbb{Q})$ is a finitely generated abelian group, and BSD2 tells us what the rank is.

2.1 Why Does Ш Appear in a Formula Directly Related to Rank?

For $n \geq 2$ recall the short exact sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{n} E \longrightarrow 0. \tag{1}$$

Taking Galois cohomology we obtain the long exact sequence

$$0 \longrightarrow E(\mathbb{Q})[n] \longrightarrow E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}) \longrightarrow H^1(G_{\mathbb{Q}}, E[n]) \longrightarrow H^1(G_{\mathbb{Q}}, E) \tag{2}$$

and so it follows that we have an inclusion $E(\mathbb{Q})/nE(\mathbb{Q}) \subset H^1(G_{\mathbb{Q}}, E[n])$, relating the rank to $Ш(E/\mathbb{Q})$.

2.2 Definition of Principle Homogeneous Spaces (PHS)

Definition 2.1. *A **twist** of $E/\mathbb{Q}$ is a smooth curve $C'/\mathbb{Q}$ that is isomorphic to E over $\overline{\mathbb{Q}}$. If $C_1/\mathbb{Q}$, $C_2/\mathbb{Q}$ are twists of $E/\mathbb{Q}$ such that $C_1 \cong_{\mathbb{Q}} C_2$ then we say that C_1 is equivalent to C_2 modulo $\mathbb{Q}$-isomorphism.*

Theorem 2.2. *The twists of $E/\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, are in 1-1 correspondence with the elements of $H^1(G_{\mathbb{Q}}, \text{Isom}(E))$, where $\text{Isom}(E)$ denotes the group of $\overline{\mathbb{Q}}$-isomorphisms of E to itself.*

Remark 2.3. $\text{Isom}(E)$ *contains* $\text{Aut}(E)$*, the group of automorphisms which send the identity point $\mathcal{O}_E$ to itself, and the translations $\tau_p : E \to E$ sending $\tau_P(Q) = P + Q$.*

Sketch proof of Theorem 2.2.

$$\begin{array}{ccc} \{C'/\mathbb{Q}, \phi : C' \to E\} & & \{\xi : G_{\mathbb{Q}} \to \text{Isom}(E)\} \\ [C', \phi] \Rightarrow & & \sigma \mapsto \phi^{\sigma}\phi^{-1} \end{array}$$

Check that this is indeed a cocycle. Note that this is really just measuring how far away the isomorphism is from being a $\mathbb{Q}$-isomorphism. □

View $E(\overline{\mathbb{Q}})$ as the set of translations in $\mathrm{Isom}(E)$ via $E(\overline{\mathbb{Q}}) \ni P \leftrightarrow \tau_P : Q \mapsto P + Q$.

Definition 2.4 (2.5)**.** *A **Principle Homogeneous Space (PHS)** for $E/\mathbb{Q}$ is a smooth curve C/K with a simply transitive algebraic group action of E on C defined over $\mathbb{Q}$. i.e. there is a morphism $\mu : C \times E \to C$ defined over $\mathbb{Q}$ such that*

- *$\mu(\mathfrak{p}, \mathcal{O}_E) = P$ for all $\mathfrak{p} \in C$.*
- *$\mu(\mu(\mathfrak{p}, P), Q) = \mu(\mathfrak{p}, P + Q)$ for all $\mathfrak{p} \in C$ and $P, Q \in E$.*
- *For all $\mathfrak{p}, \mathfrak{q} \in C$ there exists a unique $P \in E$ such that $\mu(\mathfrak{p}, P) = \mathfrak{q}$.*

This las axiom tells us that there is a subtraction map on C

$$\begin{aligned} C \times C &\to E \\ \mathfrak{p}, \mathfrak{q} &\mapsto P \end{aligned}$$

where P is the unique above.

From now on we write $\mathfrak{p} + P := \mu(\mathfrak{p}, P)$.

Proposition 2.5 (2.7)**.** *Let $C/\mathbb{Q}$ be a PHS for $E/\mathbb{Q}$. Fix a point $\mathfrak{p}_0 \in C$. Then the map*

$$\begin{aligned} \theta : E &\to C \\ P &\mapsto \mathfrak{p}_0 + P \end{aligned}$$

is a $\mathbb{Q}(\mathfrak{p}_0)$-isomorphism.

Definition 2.6. *Two PHS's $C/\mathbb{Q}$, $C'/\mathbb{Q}$ for $E/\mathbb{Q}$ are **equivalent** if there is a $\mathbb{Q}$-isomorphism $\theta : C \to C'$ that is compatible with the action of E on C and C'. i.e.*

$$\begin{array}{ccc} C & \xrightarrow{\phi} & E \\ \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \tau_P} \\ C' & \xrightarrow{\phi'} & E \end{array}$$

commutes for all $P \in E(\overline{\mathbb{Q}})$.

Proposition 2.7. *Let $C/\mathbb{Q}$ be a PHS for $E/\mathbb{Q}$. Then $C/\mathbb{Q}$ is the trivial class iff $C(\mathbb{Q})$ is not empty.*

Proof. This is Proposition 2.5 with $\mathfrak{p}_0 \in C(\mathbb{Q})$, as we have a $\mathbb{Q}$-isomorphism with this point. It is worth checking the definition of the map from the proof of Theorem 2.2 to ensure that the trivial class corresponds to E itself. □

Definition 2.8 (Weil-Ch$\widehat{a}$telet Group)**.** *the Weil-Chatelet group of $E/\mathbb{Q}$ is $\mathrm{WC}(E/\mathbb{Q})$, which is the equivalence classes of PHS. (note that it should not be clear that has any group structure just yet)*

Theorem 2.9 (2.11)**.** *There is a natural bijection between $\mathrm{WC}(E/\mathbb{Q})$ and $H^1(G_{\mathbb{Q}}, E)$, defined by*

$$\{C/\mathbb{Q}\} \mapsto \{\sigma \mapsto \mathfrak{p}_0^\sigma - \mathfrak{p}_0\}$$

for a fixed $\mathfrak{p}_0 \in C$.

Now recall the sequence (2) from the beginning of the lecture. Truncating this gives the exact sequence

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow H^1(G_{\mathbb{Q}}, E[n]) \longrightarrow H^1(G_{\mathbb{Q}}, E)[n] \longrightarrow 0$$

We know we can replace $H^1(G_{\mathbb{Q}}, E)$ by the Weil-Chatelet group $\mathrm{WC}(E/\mathbb{Q})$ by Theorem 2.9, and then consider the local sequences to obtain the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \longrightarrow & H^1(G_{\mathbb{Q}}, E[n]) & \longrightarrow & \mathrm{WC}(E/\mathbb{Q})[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & \overset{\alpha}{\searrow} & \downarrow{\scriptstyle \mathrm{res}} & & \\ 0 & \longrightarrow & \prod_v E(\mathbb{Q}_v)/nE(\mathbb{Q}_v) & \longrightarrow & \prod_v H^1(G_{\mathbb{Q}_v}, E[n]) & \longrightarrow & \prod_v \mathrm{WC}(E/\mathbb{Q}_v)[n] & \longrightarrow & 0 \end{array} \tag{3}$$

Definition 2.10. *The n-Selmer group of $E/\mathbb{Q}$ is defined by*

$$\mathrm{Sel}^{(n)}(E/\mathbb{Q}) = \ker(\alpha) = \ker\left(H^1(G_{\mathbb{Q}}, E[n]) \to \prod_v WC(E/\mathbb{Q}_v) \right)$$

The Shaferevich-Tate group is the subgroup of $\mathrm{WC}(E/\mathbb{Q})$ defined by

$$Ш(E/\mathbb{Q}) = \ker\left(\mathrm{WC}(E/\mathbb{Q}) \to \prod_v WC(E/\mathbb{Q}_v) \right)$$

We should really think of elements of $Ш(E/\mathbb{Q})$ in this way, as genus 1 curves which have points everywhere locally but not globally.

Remark 2.11. *We have a short exact sequence arising from* (3) *which relates rank, selmer groups and the torsion in $Ш(E/\mathbb{Q})$.*

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(n)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[n] \longrightarrow 0$$

2.3 $Ш(E/\mathbb{Q})$ and p^∞ Selmer Rank

Proposition 2.12. *If the Weil-Châtelet group and $Ш(E/\mathbb{Q})$ are torsion then*

$$Ш(E/\mathbb{Q}) = \bigoplus_p Ш_{p^\infty}(E/\mathbb{Q})$$

where $Ш_{p^\infty}(E/\mathbb{Q})$ denotes the p-primary part of $Ш(E/\mathbb{Q})$, the subgroup of elements whose order is a power of p.

Moreover for $n \geq 2$, if $Ш(E/\mathbb{Q})[n]$ is finite then

$$Ш_{p^\infty}(E/\mathbb{Q}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p} \oplus T_p$$

where $\delta_p \in \mathbb{Z}_{\geq 0}$ and T_p is a finite abelian group. The subgroup $\bigoplus_p (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p}$ is called the infinitely divisible subgroup, and we denote it $Ш_{\mathrm{div}}(E/\mathbb{Q})$.

Remark 2.13. *Note that $Ш(E/\mathbb{Q})$ finite will mean that $\delta_p = 0$ for all p.*

Definition 2.14. *Fix a prime p, define the p^∞-Selmer group as the direct limit*

$$\varinjlim \mathrm{Sel}^{(p^n)}(E/\mathbb{Q})$$

and the p^∞-Selmer rank, denoted $\mathrm{rk}_p(E/\mathbb{Q})$ is

$$\mathrm{rk}_p(E/\mathbb{Q}) = \mathrm{rk}(E/\mathbb{Q}) + \delta_p.$$

Lecture 3: The Cassels-Tate Pairing

2.4 Cassels-Tate Pairing

Let A/K be an abelian variety over a number field, and denote $A^\vee/K$ its dual.

Proposition 2.15. *There exists a bilinear pairing*

$$\Gamma : Ш(A/K) \times Ш(A^\vee/K) \to \mathbb{Q}/\mathbb{Z}$$

*called the **Cassels-Tate** pairing, whose kernel on both sides is $Ш_{\mathrm{Div}}$. In particular, if $Ш$ is finite then this pairing is nondegenerate.*

Remark 2.16. *Consider a principally polarized abelian variety A/K and $\lambda : A \to A^\vee$ be a principal polarisation. We define*

$$\langle , \rangle_\lambda : Ш(A/K) \times Ш(A/K)$$

to be $\langle a, a' \rangle_\lambda = \Gamma(a, \lambda(a'))$.

2.4.1 Definition of the Cassels-Tate Pairing

Take $a \in Ш(A/K)$ and denote by X/K the associated locally trivial PHS for A/K. Denote by K^{sep} the seperable closure of the field K, and $K^{\mathrm{sep}}(X)$ the function field of $X \times_K K^{\mathrm{sep}}$.

The following exact sequence

$$0 \longrightarrow K^{\mathrm{sep},\times} \longrightarrow K^{\mathrm{sep}}(X)^\times \longrightarrow \frac{K^{\mathrm{sep}}(X)^\times}{K^{\mathrm{sep},\times}} \longrightarrow 0 \tag{4}$$

yields

$$\begin{array}{ccccccc} \mathrm{Br}(K) & \longrightarrow & H^2(G_K, K^{\mathrm{sep}}(X)^\times) & \longrightarrow & H^2(G_K, \frac{K^{\mathrm{sep}}(X)^\times}{K^{\mathrm{sep},\times}}) & \longrightarrow & 0 \\ \downarrow \mathrm{res} & & \downarrow \mathrm{res} & & \downarrow \mathrm{res} & & \\ 0 \longrightarrow \prod_v \mathrm{Br}(K_v) & \longrightarrow & \prod_v H^2(G_{K_v}, K_v^{\mathrm{sep}}(X)^\times) & \longrightarrow & \prod_v H^2(G_{K_v}, \frac{K_v^{\mathrm{sep}}(X)^\times}{K_v^{\mathrm{sep},\times}}) & & \end{array} \tag{5}$$

On the other hand, we have

$$0 \longrightarrow \frac{K_v^{\mathrm{sep}}(X)^\times}{K_v^{\mathrm{sep},\times}} \longrightarrow \mathrm{Div}^0(X \times_K K^{\mathrm{sep}}) \longrightarrow \mathrm{Pic}^0(X \times_K K^{\mathrm{sep}}) \longrightarrow 0 \tag{6}$$

Which yields

$$H^1(K, \mathrm{Div}^0(X \times_K K^{\mathrm{sep}})) \longrightarrow H^1(K, \mathrm{Pic}^0(X \times_K K^{\mathrm{sep}})) \longrightarrow H^2(K, \tfrac{K_v^{\mathrm{sep}}(X)^\times}{K_v^{\mathrm{sep},\times}}) \longrightarrow \dots \tag{7}$$

Now, over K^{sep}, $A \times_K K^{\mathrm{sep}} \cong X \times_K K^{\mathrm{sep}}$ and hence $\mathrm{Pic}^0(A \times_K K^{\mathrm{sep}}) \cong \mathrm{Pic}^0(X \times_k K^{\mathrm{sep}})$. Hence one gets a map

$$H^1(K, A^\vee) = H^1(K, \mathrm{Pic}^0(A \times_K K^{\mathrm{sep}})) \longrightarrow H^2(K, \tfrac{K_v^{\mathrm{sep}}(X)^\times}{K_v^{\mathrm{sep},\times}})$$

Let $a' \in Ш(A^\vee/K) = H^1(K, A^\vee)$ and denote by b' its image in $H^2(K, \frac{K_v^{\mathrm{sep}}(X)^\times}{K_v^{\mathrm{sep},\times}})$. So in diagram (5) we send b' in the top right to f' some lift, restrict it to get $\mathrm{res}(f')$.

Claim: $\mathrm{res}(f')$ is in the image of the local Brauer groups and so comes uniquely from some $(c_v) \in \prod_v \mathrm{Br}(K_v)$.

Proof. We have the diagram

$$\begin{array}{ccc} H^1(K, \mathrm{Pic}^0(A \times_K K^{\mathrm{sep}})) & \longrightarrow & H^2(K, \frac{K_v^{\mathrm{sep}}(X)^\times}{K_v^{\mathrm{sep},\times}}) \\ \downarrow & & \downarrow \\ \prod_v H^1(K_v, \mathrm{Pic}^0(A \times_K K^{\mathrm{sep}})) & \longrightarrow & \prod_v H^2(K_v, \frac{K^{\mathrm{sep}}(X)^\times}{K_v^{\mathrm{sep},\times}}) \end{array}$$

and a' is in the kernel of the left vertical. □

Note that it seems like there is no a dependence on this Cassels-Tate pairing but this is not true! In fact, note that X and the whole of diagram (5)is dependent solely on a.

Definition 2.17.

$$\langle a, a' \rangle = \sum_v \mathrm{inv}_v(c_v) \in \mathbb{Q}/\mathbb{Z}$$

where inv *is the local invariant map from class field theory.*

Exercise 1. *Prove that if λ comes from a rational divisor then the above pairing is alternating.*

What is a rational divisor? It is those divisors which are Galois invariant for G_K. Note that this does not just mean sums of K-rational points on curves, we can stick enough evenly coefficiented Galois conjugates.

Proposition 2.18. *Let A/K be a principally polarised abelian variety with principal polarisation λ. Assume that $Ш(A/K)$ is finite. If λ is given by a rational divisor then the order $\#Ш(A/K)$ is a square.*

Proof. By the above exercis, if λ is rational then the pairing is alternating. If moreover $Ш(A/K)$ is finite then the pairing is nondegenerate. The result then follows from the fact that a finite abelian group with a nondegenerate alternating pairing must square order. □

Definition 2.19. *Let C be a curve of genus g over a local field K_v, then we say that C is deficient at v if it has no K_v-rational divisor of degree $g-1$.*

Proposition 2.20. *Let J/K be the Jacobian of a smooth curve C/K and assume that $Ш(C/K)$ is finite. Then $\#Ш(J/K)$ is square if C/K has an even number of deficient places, and $\#Ш(J.K) \equiv 2$ mod squares if C/K has an odd number of deficient places.*

Proposition 2.21. *Let $K/\mathbb{Q}_p$ be a finite extension and C/K be a hyperelliptic curve of genus g. Denote by k the residue field of K, then TFAE:*

1. *C is definicient over K*
2. *C has even genus and has no rational point over any odd degree extension of K.*
3. *C has even genus and every component of the special fibre of its minimal regular model has either even multiplicity or a G_K-orbit of even length.*

If you wanted, at this point you could go away and use the cluster pictures from Adam Morgans course to construct curves with Jacobians with order twice a square.

3 Tamagawa Numbers

Let $K/\mathbb{Q}_p$ be a fintie extension for some prime p. Let A/K be an abelian variety, and recall that the group $A(K)/A_\circ(K)$ is finite, where $A_\circ(K)$ is the set of points reducing to the connected component of the identity of the Néron model of A/K.

Definition 3.1. *The **Tamagawa Number***

$$c(A/K) = \#\frac{A(K)}{A_\circ(K)}$$

Alternatively, this is also

$$c(A/K) = \#\frac{\tilde{\mathscr{A}}}{\tilde{\mathscr{A}}^\circ(\overline{k})^{\mathrm{Gal}(\overline{k}/k)}}$$

where k denotes the residue field of K and $\tilde{\mathscr{A}}, \tilde{\mathscr{A}}^\circ$ denote the reduction of the abelian variety and the reduction of the identity component of the Néron model respectively.

Lecture 4: Tamagawa Numbers and Explicit Computations

3.1 Elliptic Curves

Let $K/\mathbb{Q}_p$ be a fininte extension. In this case we need to compute $\#E(K)/E_0(k)$, where $E_0(K)$ can be defined by

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow{\pi} \tilde{E}_{ns}(k) \longrightarrow 0$$

where π is the canonical reduction map. Note that the surjectivity of the reduction map π depends crucially on the fact that we can use Hensels lemma to lift nonsingular points.

Example 2 (3.2)**.** *Let $p > 3$,*

1) Consider $E/\mathbb{Z}_p : y^2 = x(x-1)(x-2)$. Reducing mod p gives $\tilde{E}/\mathbb{F}_p : \tilde{y}^2 = \tilde{x}(\tilde{x}-1)(\tilde{x}-2)$. In this case, $\tilde{E}_{ns}(\mathbb{F}_p) = \tilde{E}(\mathbb{F}_p)$ so that $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$ and the Tamagawa number $c(E/\mathbb{Q}_p)$.

2) *Consider* $E/\mathbb{Z}_p : y^2 = (x+1)(x-p^2)(x+p^2)$. *Reducing mod* p *we get a nodal curve* $\tilde{y}^2 = \tilde{x}^2(\tilde{x}+1)$. *Here*

$$\tilde{E}_{ns}(\mathbb{F}_p) = \tilde{E}(\mathbb{F}_p) \setminus \{(0,0)\}$$

Hensels lemma is inconclusive at $(0,0)$. *From this model it is not possible to compute* $\#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. *We need a model which guarantees that singular points will NOT lift to* $\mathbb{Q}_p$ *points.*

Proposition 3.2. *Let* $\mathscr{C}/\mathbb{Z}_p$ *be a proper model for* E. *If* $\mathscr{C}$ *is regular then*

$$E(\mathbb{Q}_p) = \mathscr{C}(\mathbb{Z}_p) = \mathscr{C}^\circ(\mathbb{Z}_p)$$

where $\mathscr{C}^\circ = \mathscr{C} \setminus \{\text{singular points}\}$

This is telling us that if we know regular models of elliptic curves, then we can compute Tamagawa numbers! See the exercises for today.

Example 3. *Continuing with* $E/\mathbb{Z}_p : y^2 = (x+1)(x-p^2)(x+p^2)$, *construct the special fibre of a minimal regular model for* $E/\mathbb{Z}_p$. *(you can do this using clusters as in Adam Morgan's course)*

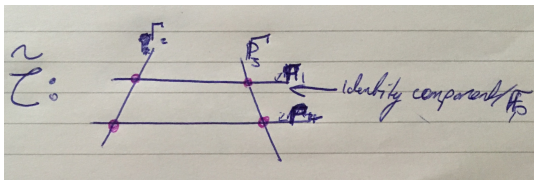

Figure 1: The special fibre of the minimal model of $E/\mathbb{Z}_p$

1. *Assume that* $\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$ *are defined over* $\mathbb{F}_p$ *(split multiplicative reduction). Then we just remove these 4 singular points and get*

$$\#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p) = 4$$

2. *Some components are not defined over* $\mathbb{F}_p$. *In this case the ony way for it to happen is* $\Gamma_2 = \mathrm{Frob}(\Gamma_3)$ *and* $\Gamma_3 = \mathrm{Frob}(\Gamma_2)$ *and* $\Gamma_4, \Gamma_1/\mathbb{F}_p$ *(non-split multiplicative reduction).*

$$\#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p) = 2$$

3.2 Jacobians of Curves

$K/\mathbb{Q}_p$, $\mathcal{O}_K$ its ring of integers, $k, \overline{k}$ the residue field and its algebraic closure. We need to compute $\#J(K)/J_0(K)$.

We want to compute Tamagawa numbers for Jacobians from a minimal regular model of their underlying curve.

Theorem 3.3 (3.5)**.** *let* C/K *be a semistable curve,* $\mathscr{C}/\mathcal{O}_K$ *a minimal regular model for this and denote by* $\mathscr{J}/\mathcal{O}_K$ *the Néron model of the Jacobian* J.

Consider $\overline{\mathscr{C}} = \mathscr{C} \times_{\mathcal{O}_K} \overline{k}$, *and let* $I = \{\Gamma_1, \ldots, \Gamma_n\}$ *denote the irreducible components of* $\overline{\mathscr{C}}$ *and let* d_i *denote their multiplicities.*

Define the map

$$\begin{aligned}\alpha : \mathbb{Z}^I &\to \mathbb{Z}^I \\ \Gamma_i &\mapsto \sum_j (\Gamma_i \cdot \Gamma_j)\Gamma_j\end{aligned}$$

where $\Gamma_i \cdot \Gamma_j$ *is the intersection number of the components* Γ_i *and* Γ_j*, and extend this* $\mathbb{Z}$*-linearly.*

Define the map

$$\begin{aligned}\beta : \mathbb{Z}^I &\to \mathbb{Z} \\ \Gamma_i &\mapsto d_i\end{aligned}$$

and again extend $\mathbb{Z}$*-linearly. Then* $\operatorname{im}(\alpha) \subset \ker(\beta)$ *and* $\mathscr{J}/\mathscr{J}^\circ(\overline{k}) \cong \ker(\beta)/\operatorname{im}(\alpha)$ *and this is equivariant for the action of* $\operatorname{Gal}(\overline{k}/k)$*.*

Here note that as we are assuming semistable, the components are all multiplicity 1.

Example 4. *Let* $p \geq 3$ *be an odd prime and consider* $C/\mathbb{Q}_p$ *the following hyperelliptic curve:*

$$y^2 = (x-2)((x-1)^2 - p^2)(x^2 - p^2)$$

Again we can use the cluster picture to prove that this is semistable. The root set is $\mathcal{R} = \{2, p, -p, p+1, -p+1\}$

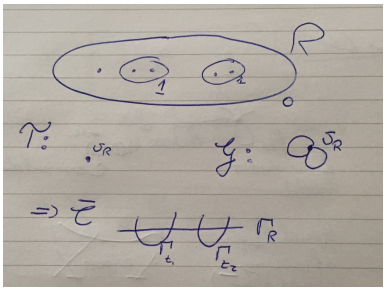

Figure 2: The cluster diagram for $E/\mathbb{Z}_p$

We have $I = \{\Gamma_R, \Gamma_{t_1}, \Gamma_{t_2}\}$ *and all components have multiplicity 1. Now,*

$$\ker \beta = \{n_R\Gamma_R + n_{t_1}\Gamma_{t_1} + n_{t_2}\Gamma_{t_2} \mid n_R + n_{t_1} + n_{t_2} = 0\}$$

(which you can verify for yourselves) and

$$\operatorname{im} \alpha = \{[\Gamma_R], [\Gamma_{t_1}], [\Gamma_{t_2}]\}$$

where

$$\begin{aligned}[\Gamma_R] &= -4\Gamma_R + 2\Gamma_{t_1} + 2\Gamma_{t_2} \\ [\Gamma_{t_1}] &= 2\Gamma_R - 2\Gamma_{t_1} \\ [\Gamma_{t_2}] &= 2\Gamma_R - 2\Gamma_{t_2}\end{aligned}$$

So we see that $\ker \beta/\operatorname{im} \alpha = \langle \Gamma_{t_1}, \Gamma_{t_2} \mid 2\Gamma_{t_1} = 2\Gamma_{t_2} = 0 \rangle$ *and so is* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*. Hence*

$$\#\mathscr{J}/\mathscr{J}^\circ(\overline{k})^{\operatorname{Gal}(\overline{k}/k)} = 4$$

4 Explicit Computations of Parity of Rank

4.1 Parity of $\mathrm{rk}_p(A/K)$

Recall that for a fixed prime p we defined $\mathrm{rk}_p(A/K) = \mathrm{rk}(A/K) + \delta_p$. Let K be a number field and let $\phi : A/K \to B/K$ be an isogeny of abelian varieties. Recall that $\phi\phi^\vee, \phi^\vee\phi = [p]$ and recall further that

$$Q(\phi) = |\mathrm{coker}(\phi : A(K)/A(K)_{\mathrm{tors}} \to B(K)/B(K)_{\mathrm{tors}})| \times |\ker(\phi : Ш_{\mathrm{div}}(A/K) \to Ш_{\mathrm{div}}(B/K))|$$

Proposition 4.1. *Fix nonzero global exterior forms ω_A, ω_B for A, B respectively.*

$$\frac{Q(\phi^\vee)}{Q(\phi)} = \frac{|B(K)_{\mathrm{tors}}|\,|B^\vee(K)_{\mathrm{tors}}|\,\Omega_A \prod_{v\nmid\infty} c(A/K_v) \left|\frac{\omega_A}{\omega^\circ_{A,v}}\right| |Ш_0(A)[p^\infty]|}{|A(K)_{\mathrm{tors}}|\,|A^\vee(K)_{\mathrm{tors}}|\,\Omega_B \prod_{v\nmid\infty} c(B/K_v) \left|\frac{\omega_B}{\omega^\circ_{B,v}}\right| |Ш_0(B)[p^\infty]|}$$

where $Ш_0 = Ш/Ш_{\mathrm{div}}$.

Recall that we showed $\frac{Q(\phi^\vee)}{\phi} = p^{\mathrm{rk}_p(A/K)} \mod (\mathbb{Q}^\times)^2$

Let C/K be a curve of genus 2 (The reason for genus 2 is we want an isogeny on its Jacobian, where we have the Richolet isogeny (the generalisation of 2-isogeny for elliptic curves)) such that its Jacobian admits a Richolet isogeny. Denote $\widehat{J}, \widehat{C}$ the isogenous Jacobian and underlying curve. Proposition 4.1 and Exercise 2.25 from the exercise sheet gives

$$(-1)^{\mathrm{rk}_2(J/K)} = -1^{\mathrm{ord}_2(\dagger)}$$

where

$$\dagger = \frac{\Omega_J \prod_{v\nmid 2\infty} c(J/K_v) \prod_{v|2} c(J/K_v) \left|\frac{\omega_J}{\omega^\circ_{J,v}}\right|_v |Ш_0(J)[2^\infty]|}{\Omega_{\widehat{J}} \prod_{v\nmid 2\infty} c(\widehat{J}/K_v) \prod_{v|2} c(\widehat{J}/K_v) \left|\frac{\omega_{\widehat{J}}}{\omega^\circ_{\widehat{J},v}}\right|_v \left|Ш_0(\widehat{J})[2^\infty]\right|}.$$