1. The Birch and Swinnerton-Dyer Conjecture

Main references : [4], [5], [8]. In this section, K is a number field.

1.1. **Elliptic curves over $\mathbb{Q}$.** Let $E/\mathbb{Q}$ be an elliptic curve and recall that by Mordell's theorem we have

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

where $|E(\mathbb{Q})_{tors}| < \infty$ and $rk(E/\mathbb{Q}) \geq 0$ is an integer.

In this case, $E(\mathbb{Q})_{tors}$ is well understood so that knowing $rk(E/\mathbb{Q})$ completely characterises $E(\mathbb{Q})$.

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

In the mid 1960's Birch and Swinnerton-Dyer conjectured (based on numerical experiments) that $rk(E/\mathbb{Q})$ could be computed from the L-function of $E/\mathbb{Q}$. Their rationale went as follows:

Let $p \nmid \Delta_E$ be a prime. Then $\tilde{E}/\mathbb{F}_p$ is an elliptic curve and denote

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

the number of $\mathbb{F}_p$-rational points on the reduced curve.

Their main idea was that a large rank over $\mathbb{Q}$ gives rise to a lot of $\mathbb{Q}$-rational points, which in turns make N_p very large. Following this idea, for a given number X, Birch and Swinnerton-Dyer looked at

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

and conjectured the following:

Conjecture 1.1. *There exists a constant C_E depending only on E such that*

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

Now it is not convenient to study $\prod_{p<X} \frac{N_p}{p}$ analytically. However for each p, the value N_p is packed up in 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" at $s = 1$ gives

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

so that, by the above discussion and assuming analytic continuation to the whole of $\mathbb{C}$, the value of $L(E/\mathbb{Q}, s)$ at $s = 1$ should contain information about the rank of $E/\mathbb{Q}$.

Conjecture 1.2 (BSD1)**.** *The L-function $L(E/\mathbb{Q}, s)$ extends to an entire function on $\mathbb{C}$ and*

$$L(E/\mathbb{Q}, 1) \neq 0 \Leftrightarrow |E(\mathbb{Q})| < \infty.$$

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

Their conjecture goes further! Since we are assuming analytic continuation at $s = 1$, it makes sense to talk about the leading term of the Taylor expansion of $L(E/\mathbb{Q}, s)$ around $s = 1$.

Conjecture 1.3 (BSD2)**.**

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

where

- $Ш(E/\mathbb{Q})$ is the Shafarevich-Tate group of $E/\mathbb{Q}$, assuming it is finite (more on this in Lecture 2),
- $R(E/\mathbb{Q})$ is the regulator of $E/\mathbb{Q}$ (more on this in Steffen's lecture),
- c_p is the Tamagawa number of $E/\mathbb{Q}$ at the prime p (more on this in Lecture 3),
- $\omega_{\mathbb{R}}$ is the real period of $E/\mathbb{Q}$.

Remark 1.4. The real period $\omega_{\mathbb{R}}$ is defined by

$$\int_{E(\mathbb{R})} |\frac{dx}{y}| = [E(\mathbb{R}) : E^0(\mathbb{R})]\omega_{\mathbb{R}},$$

where $E^0(\mathbb{R})$ denotes the identity component.

! it depends on the choice of differential !

Known results (not comprehensive): For $E/\mathbb{Q}$, Gross-Zagier, Kolyvagin proved that if $ord_{s=1}L(E/\mathbb{Q}, s) \leq 1$ then $rk(E/\mathbb{Q}) = ord_{s=1}L(E/\mathbb{Q}, s)$. Under some technical assumptions Skinner-Urban, Wei Zhang proved the converse, i.e. if $rk(E/\mathbb{Q}) \leq 1$ then $ord_{s=1}L(E/\mathbb{Q}, s) = rk(E/\mathbb{Q})$.

1.2. **Abelian varieties over number fields.** Let A/K be an abelian variety of dimension d over a number field K. Shortly after Birch and Swinnerton-Dyer stated their conjecture, Tate generalized it to abelian varieties over number fields (see [3] for a conceptual formulation of BSD 2 via measure theory).

Conjecture 1.5 (Generalized BSD)**.** *The L-function $L(A/K, s)$ extends to an entire function on $\mathbb{C}$ and*

1) $ord_{s=1}L(A/K, s) = rk(A/K)$,

2)

$$\lim_{s\to 1} \frac{L(A/K, s)}{(s-1)^{rk(A/K)}} = \frac{2^{dr_2}|Ш(A/K)|R(A/K)\prod_{v|\infty}\int_{A(K_v)}|\omega|_v \prod_{v\nmid\infty} c_v|\frac{\omega}{\omega_v^o}|_v}{\sqrt{|d_K|}^d |A(K)_{tors}||A^\vee(K)_{tors}|},$$

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 global exterior d-form,*
- *for a place* v *of* K, ω_v^o *is the Néron differential for* A/K_v,
- $A^\vee/K$ *is the dual variety of* A/K.

Remark 1.6. If A/K is principally polarized (say $A = E$ an elliptic curve or $A = J(C)$ the Jacobian of a curve) then $|A(K)_{tors}||A^\vee(K)_{tors}| = |A(K)_{tors}|^2$.

Known results: BSD has been numerically verified for some elliptic curves over number fields in LMFDB data base, Jacobian of genus 2 curves, and (up to square) for a few Jacobians of higher genus curves (see [6], [10] for details).

1.3. **Consequence of BSD : the parity conjecture.** The BSD conjecture has a very interesting consequence for the computation of the parity of the rank of an abelian variety. This is called the *parity conjecture* and it can be derived from BSD in the following way.

Recall that assuming analytic continuation of $L(A/K, s)$ to $\mathbb{C}$, BSD 1 states that $rk_{an}(A/K) := ord_{s=1}L(A/K, s) = rk(A/K)$. On the other hand, the completed L-function $L^*(A/K, s)$ of $L(A/K, s)$ is conjectured to satisfy the following functional equation (proven for E/$\mathbb{Q}$)

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

where $w \in \{\pm 1\}$ is referred to as the *sign* in the functional equation.

It follows that:

if $w = 1$ then $L(A/K, s)$ is (essentially) symmetric around $s = 1$ so that its order of vanishing is even,

if $w = -1$ then $L(A/K, s)$ is (essentially) antisymmetric around $s = 1$ so that its order of vanishing is odd, i.e. the parity of $rk_{an}(A/K)$ is given by the sign in the functional equation:

$$(-1)^{rk_{an}(A/K)} = w.$$

Assuming BSD this yields that the parity of the (algebraic) rank $rk(A/K)$ is given by the sign in the functional equation:

$$(-1)^{rk(A/K)} = w.$$

Lastly it is also conjectured (and known for $E/\mathbb{Q}$) that w is equal to the global root number W of A/K, defined by

$$W = \prod_{v \in M_K} W_v,$$

where W_v denotes the local root number of A/K at the place v (well defined and computable as a Galois theoretic object).

Conjecture 1.7 (Parity conjecture)**.** *The parity of the (algrebraic) rank $rk(A/K)$ is given by the global root number of A/K :*

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

Remark 1.8. Even though the parity conjecture can be derived from other conjectures, its statement is independent of any other conjecture as it relates well defined objects : the algebraic rank and the global root number.

Example 1.9 (how to make use of the parity conjecture)**.** Consider $E/\mathbb{Q}$: $y^2 + y = x^3 + x^2 - 7x + 5$ with discriminant $\Delta_E = -7 \cdot 13$. Computing root numbers one finds : $W_\infty = -1, W_7 = -1$ (split multiplicative reduction), $W_{13} = -1$ (split multiplicative reduction), so that

$$W = (-1)^3 = -1.$$

Assuming the parity conjecture, one concludes that $rk(E/\mathbb{Q})$ is odd so that $E/\mathbb{Q}$ has at least of point of infinite order (and the associated Diophantine equation has infinitely many solutions).

1.4. **A formula for the parity of the rank.** Thanks to the following result of Cassels, it is possible to compute the parity of $rk(E/\mathbb{Q})$ (assuming finiteness of $Ш(E/\mathbb{Q})$, or the parity of $rk_p(E/\mathbb{Q})$ without any assumption, more on this in Lecture 2).

Theorem 1.10 (BSD-invariance under isogeny, Cassels, 1965)**.** *Assume $Ш(E/\mathbb{Q})$ is finite and let $\varphi : E \to E'$ be an isogeny. Then*

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

Remark 1.11. This result was shortly generalized to abelian varieties by Tate (see [7][Theorem 7.3] and subsequent remarks).

Combined with the following lemma, the BSD-invariance under isogeny result gives a formula for the parity of the rank of $E/\mathbb{Q}$.

Lemma 1.12 (Dokchitser-Dokchitser)**.** *Let $\varphi : E/\mathbb{Q} \to E'/\mathbb{Q}$ be a $\mathbb{Q}$-rational isogeny of degree d. Then*

$$\frac{R(E/\mathbb{Q})}{R(E'/\mathbb{Q})} = d^{rk(E/\mathbb{Q})} \cdot \square_{\mathbb{Q}}.$$

Corollary 1.13. *Let ℓ be a prime and $E/\mathbb{Q}$ be an elliptic curve admitting an isogeny of degree ℓ. Assume that $Ш(E/\mathbb{Q})$ is finite. Then*

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

Proof. It follows from Theorem 1.10 that

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

The result follows from Lemma 1.12. □

The above result relies heavily on the finiteness of $Ш(E/\mathbb{Q})$ and on the fact that if finite, it has square order. In the following lecture, we will explore $Ш(E/\mathbb{Q})$ in more detail in order to derive a similar result without assuming its finiteness. Doing so, we will also give a formula to compute the order, up to square, of the finite part of $Ш(J/K)$ for Jacobians of curves.

1.4.1. *Exercises.*

Exercise 1.14. The *Regulator* of $E/\mathbb{Q}$ is defined as the absolute value of the determinant of the height pairing (see Steffen's lecture):

$$Reg(E/\mathbb{Q}) = |det(< P_i, P_j >)_{i,j}|,$$

where $\{P_i\}$ is any $\mathbb{Z}$-basis for $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.

Use this definition and the hint below to prove Lemma 1.12.

Hint : fix $P \in E, Q \in E'$ and denote $\varphi^\vee$ the dual isogeny. Then

$$< \varphi(P), Q >_{E'} = < P, \varphi^\vee(Q) >_E .$$

Exercise 1.15. 1) Use Corollary 1.13 (and Sage or Magma) to compute the parity of the rank of the following elliptic curves:

(1) $y^2 + xy + y = x^3 - 231x - 442$ (LMFDB 59450.a1, rank 3)
(2) $y^2 + y = x^3 - 7599x + 254970$ (LMFDB 2601.a1, rank 2)

2) Using BSD2 for E/K, compute the parity of the rank of the elliptic curves in the isogeny class 4.1-b over $\mathbb{Q}(\sqrt{89})$ (choose a 5-isogeny)

2. Shafarevich-Tate groups

Main references: [5] Chapter X, [9]. In this section, K denotes first a number field, but becomes a local fields in Proposition 2.23.

2.1. Why does $Ш(E/\mathbb{Q})$ appear in a formula related to the rank of $E/\mathbb{Q}$?

The answer to the above question can be found in the proof of the Mordell-Weil theorem.

Let $E/\mathbb{Q}$ be an elliptic curve. For $n \geq 2$, we have the following exact sequence:

$$0 \to E[n] \to E(\bar{\mathbb{Q}}) \to^{\times n} E(\bar{\mathbb{Q}}) \to 0,$$

which yields the long exact sequence

(2.1)

$$0 \to E(\mathbb{Q})[n] \to E(\mathbb{Q}) \to^{\times n} E(\mathbb{Q}) \to H^1(G_{\mathbb{Q}}, E[n]) \to H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}})) \to^{\times n} H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}}))...$$

It follows that $E(\mathbb{Q})/nE(\mathbb{Q}) \hookrightarrow H^1(G_{\mathbb{Q}}, E[n])$. In order to prove the Mordell-Weil theorem, one first proves that $E(\mathbb{Q})/nE(\mathbb{Q})$ is finite by embedding it into a finite subgroup of $H^1(G_{\mathbb{Q}}, E[n])$. One then argues via a descent argument that the finiteness of $E(\mathbb{Q})/nE(\mathbb{Q})$ implies that $E(\mathbb{Q})$ is finitely generated.

In order to compute $rk(E/\mathbb{Q})$ via this method, one needs to first compute generators for $E(\mathbb{Q})/nE(\mathbb{Q})$. Defined as a subgroup of $H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}}))$, the elements of $Ш(E/\mathbb{Q})$ will interfere with the computation of such generators.

2.2. Definition using principal homogenous spaces.

Main reference for this section is [5] Chapter X.

Definition 2.2. A twist of $E/\mathbb{Q}$ is a smooth curve $C'/\mathbb{Q}$ that is isomorphic to E over $\bar{\mathbb{Q}}$, i.e. there exists an isomorphism $\phi_{\overline{\mathbb{Q}}} : C' \to E$.

If $C_1/\mathbb{Q}$ and $C_2/\mathbb{Q}$ are twists of $E/\mathbb{Q}$ such that $C_1 \simeq_{\mathbb{Q}} C_2$ then we say that C_1 is equivalent to C_2 modulo $\mathbb{Q}$-isomorphisms.

Theorem 2.3. *The twists of $E/\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, are in $1-1$ correspondence with the element of $H^1(G_{\mathbb{Q}}, Isom(E)))$, where $Isom(E)$ denotes the group of $\overline{\mathbb{Q}}$-isomorphisms from E to itself.*

Remark 2.4. $Isom(E)$ contains $Aut(E)$ the group of automorphisms of E which fix $\mathcal{O}_E$ and the translations $\tau_P : E \to E$ such that $\tau_P(Q) = Q + P$ for points $P, Q \in E(\overline{\mathbb{Q}})$.

Proof. Sketch: • Associate to $C'/\mathbb{Q}$ the map $\xi : G_{\mathbb{Q}} \to Isom(E)$ such that $\sigma \mapsto \phi^\sigma \phi^{-1}$.

• Check that ξ is a cocycle i.e. $\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau, \ \forall \sigma, \tau \in G_{\mathbb{Q}}$.

• Denote $\{\xi\}$ the associated cohomology class in $H^1(G_{\mathbb{Q}}, Isom(E)))$ and prove that $\{\xi\}$ is determined by the $\mathbb{Q}$-isomorphism class of C' and is independent of the choice of ϕ.

• Prove that the map $C' \mapsto \{\xi\}$ is a bijection. □

We now restrict to the twists of $E/\mathbb{Q}$ that arise from the translations $Isom(E)$ via the above bijection. These are genus 1 curves on which E acts via an algebraic group action **defined over** $\mathbb{Q}$ (the fact that the action is defined over $\mathbb{Q}$ comes precisely from the correspondence to a translation in $Isom(E)$).

Definition 2.5. A principal homogenous space (PHS) for $E/\mathbb{Q}$ is a smooth curve C/K together with a simply transitive algebraic group action of E on C defined over $\mathbb{Q}$ i.e. there exists a morphism $\mu : C \times E \to C$ **defined over** $\mathbb{Q}$ satisfying

- $\mu(p, \mathcal{O}) = p, \forall p \in C$,
- $\mu(\mu(p, P), Q) = \mu(p, P + Q) \forall p \in C; P, Q \in E$,
- $\forall p, q \in C$ there is a unique $P \in E$ such that $\mu(p, P) = q$.

The latter property allows us to define a subtraction map on C

$$\nu : C \times C \to E; p, q \mapsto P,$$

where P is the unique point satisfying $\mu(p, P) = Q$.

Remark 2.6. When working with PHS's it is understood that $+, -$ refer to μ, ν.

Proposition 2.7. *Let $C/\mathbb{Q}$ be a PHS for $E/\mathbb{Q}$. Fix a point $p_0 \in C$ and define a map*

$$\theta : E \to C; P \mapsto p_0 + P \quad (= \mu(p_0, P)).$$

Then θ is an isomorphism defined over $\mathbb{Q}(p_0)$. In particular, $C/\mathbb{Q}$ is a twist of $E/\mathbb{Q}$.

Definition 2.8. Two PHSs $C/\mathbb{Q}$ and $C'/\mathbb{Q}$ for $E/\mathbb{Q}$ are *equivalent* if there is an isomorphism $\theta : C \to C'$ defined over $\mathbb{Q}$ 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.

The equivalence class containing $E/\mathbb{Q}$ acting on itself by translation is the trivial class.

The collection of equivalence classes of PHS for $E/\mathbb{Q}$ is called the *Weil-Châtelet* group for $E/\mathbb{Q}$, denoted $WC(E/\mathbb{Q})$.

Remark 2.9. One can define several structures of PHS for $E/\mathbb{Q}$ on a single curve $C/\mathbb{Q}$ via the natural action of $Aut(E)$ on $WC(E/\mathbb{Q})$. Let $\alpha \in Aut(E)$ and define $\{C/\mathbb{Q}, \mu\}^\alpha = \{C/\mathbb{Q}, \mu \circ (1 \times \alpha)\}$. Then $\{C/\mathbb{Q}, \mu \circ (1 \times \alpha)\}$ and $\{C/\mathbb{Q}, \mu\}$ are not in the same equivalence class of $WC(E/\mathbb{Q})$ by Definition 2.8.

Proposition 2.10. *Let $C/\mathbb{Q}$ be a PHS for $E/\mathbb{Q}$. Then $C/\mathbb{Q}$ is in the trivial class if and only if $C(\mathbb{Q})$ is not the empty set.*

Proof. This is Proposition 2.7 with $p_0 \in C(\mathbb{Q})$ (hence θ is a $\mathbb{Q}$-isomorphism). □

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

$$\{C/\mathbb{Q}\} \mapsto \{\sigma \mapsto p_0^\sigma - p_0\},$$

for a fixed $p_0 \in C$.

Proof. • show that $\sigma \mapsto p_0^\sigma - p_0$ is a cocycle.

• show that two equivalent PHS map to two cohomologous cocycles.

• show that the above map is injective: assume that the cocycles corresponding the $C/\mathbb{Q}$ and $C'/\mathbb{Q}$ are cohomologous. Prove that for $p, p_0 \in C, p_0' \in C', P_0 \in E$ the map $\theta : C \to C';\ p \mapsto p_0' - (p - p_0) + P_0$ is a $\mathbb{Q}$-isomorphism.

• show that the above map is surjective: let $\xi : G_\mathbb{Q} \to E$ be a 1-cocycle representing an element in $H^1(G_\mathbb{Q}, E)$. View E as the set of translations in $Isom(E)$ so that ξ can be viewed as an element of $H^1(G_\mathbb{Q}, Isom(E))$. By Theorem 2.3 there exist a curve $C/\mathbb{Q}$ and a $\overline{\mathbb{Q}}$-isomorphism $\phi : C \to E$ such that for all $\sigma \in G_\mathbb{Q}$, $\phi^\sigma \circ \phi^{-1} =$ translation by ξ_σ. Define a map

$$\mu : C \times E \to E; (p, P) \mapsto \phi^{-1}(\phi(p) + P).$$

Check that μ is simply transitive, defined over $\mathbb{Q}$ and compute the cohomology class associated to $C/\mathbb{Q}$ to show that it is ξ_σ. □

Recall from equation 2.1 that we have the Kummer sequence for $E/\mathbb{Q}$:

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

Understanding $\mathrm{Im}(E(\mathbb{Q})/nE(\mathbb{Q})) \in H^1(G_\mathbb{Q}, E[n])$ boils down to understanding $\ker(H^1(G_\mathbb{Q}, E[n]) \to H^1(G_\mathbb{Q}, E))$. By Theorem 2.11 and Proposition 2.10, this is equivalent to finding rational points on certain genus 1 curve.

This is as difficult as determining the rank of $E/\mathbb{Q}$. On the other hand, fixing a place v and using Hensel's Lemma, the same question is more accessible for $E(\mathbb{Q}_v)/nE(\mathbb{Q}_v)$. Namely consider:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \xrightarrow{\delta} & H^1(G_\mathbb{Q}, E[n]) & \longrightarrow & WC(E/\mathbb{Q})[n] & \longrightarrow & 0 \\
 & & & & \downarrow Res & & \downarrow Res & & \\
0 & \longrightarrow & E(\mathbb{Q}_v)/nE(\mathbb{Q}_v) & \xrightarrow{\delta_v} & \prod_v H^1(G_{\mathbb{Q}_v}, E[n]) & \longrightarrow & \prod_v WC(E/\mathbb{Q}_v)[n] & \longrightarrow & 0
\end{array}$$

Definition 2.12. The n-Selmer group of $E/\mathbb{Q}$ is the subgroup of $H^1(G_\mathbb{Q}, E[n])$ defined by

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

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

$$Ш(E/\mathbb{Q}) := \ker\{WC(E/\mathbb{Q}) \to \prod_v WC(E/\mathbb{Q}_v)\}.$$

Remark 2.13. One proves that $Sel^n(E/\mathbb{Q})$ is finite and fits in the following exact sequence

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

By definition $Ш(E/\mathbb{Q})$ can be thought of as the group of PHS for $E/\mathbb{Q}$ that are everywhere locally trivial (i.e. possess a $\mathbb{Q}_v$-rational point at all places v).

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

Proposition 2.14. *The Weil-Chatelet group, and hence* $Ш(E/\mathbb{Q})$*, is torsion. In particular, we may write*

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

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

Moreover for each $n \geq 2$*,* $Ш(E/\mathbb{Q})[n]$ *is finite. It follows that*

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

with $\delta_p \in \mathbb{Z}_{\geq 0}$*,* T_p *a finite abelian* p*-group.*

The subgroup $\oplus_p(\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p}$ *is called the infinitely divisible subgroup of* $Ш(E/\mathbb{Q})$*, denoted* $Ш_{div}(E/\mathbb{Q})$*.*

Definition 2.15. Fix a pime p and define the p^∞-Selmer group as the direct limit

$$\lim_{\to n} Sel_{p^n}(E/\mathbb{Q}).$$

Moreover define the p^∞-Selmer rank, denoted $rk_p(E/\mathbb{Q})$ as

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

Remark 2.16. The advantage of defining the p^∞-Selmer rank comes from the fact that $Ш(E/\mathbb{Q})$ is conjectured to be finite. In this case, $\delta_p = 0$ for all p and $rk_p(E/\mathbb{Q}) = rk(E/\mathbb{Q})$.

The key point is that one can reformulate Theorem 1.10 and Lemma 1.12 in terms of Selmer groups and give an unconditional formula for the parity of $rk_p(E/\mathbb{Q})$ (More on this in Lecture 4, also see [8] for a detailed exposition of this approach).

Recall that to prove Corollary 1.13 we used that if finite, $Ш(E/\mathbb{Q})$ has square order. This is true for elliptic curves but not true in general. It comes from the following pairing on $Ш(E/\mathbb{Q})$ (and more generally on $Ш(A/K)$).

2.4. **Cassels-Tate pairing.** Let A/K be an abelian variety over a number field and denote $A^\vee/K$ its dual.

Proposition 2.17. *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 each side is exactly $Ш_{div}(A/K)$ *and* $Ш_{div}(A^\vee/K)$ *respectively.*

In particular if $Ш(A/K)$ *is finite then the Cassels-Tate pairing is non-degenerate.*

Remark 2.18. Consider a principally polarized abelian variety A/K and let $\lambda : A \to A^\vee$ be a principal polarization. We define

$$\langle ., . \rangle_\lambda : Ш(A/K) \times Ш(A/K) \to \mathbb{Q}/\mathbb{Z},$$

by

$$\langle a, a' \rangle_\lambda = \langle a, \lambda a' \rangle.$$

2.4.1. *Definition of the Cassels-Tate pairing via PHS.*

Take $a \in Ш(A/K)$ and denote X/K the associated locally trivial PHS for A/K. Denote by $K^{sep}(X)$ the function field of $X \otimes_K K^{sep}$. The following exact sequence

$$0 \to K^{sep\times} \to K^{sep}(X)^\times \to K^{sep}(X)^\times/K^{sep\times} \to 0$$

yields

$$\begin{array}{ccccccc} Br(K) & \longrightarrow & H^2(G_K, K^{sep}(X)^\times) & \longrightarrow & H^2(G_K, K^{sep}(X)^\times/K^{sep\times}) & \longrightarrow & 0 \\ \downarrow Res & & \downarrow Res & & \downarrow Res & & \\ 0 \longrightarrow \prod_v Br(K_v) & \longrightarrow & \prod_v H^2(G_{K_v}, K^{sep}(X)^\times) & \longrightarrow & \prod_v H^2(G_{K_v}, K^{sep}(X)^\times/K^{sep\times}) & & \end{array}$$

On the other hand from the exact sequence

$$0 \to K^{sep}(X)^\times/K^{sep\times} \to Div^0(X \otimes_K K^{sep}) \to Pic^0(X \otimes_K K^{sep}) \to 0$$

we have

$$H^1(G_K, Div^0(X \otimes K^{sep})) \to H^1(G_K, Pic^0(X \otimes_K K^{sep})) \to H^2(G_K, K^{sep}(X)^\times/K^{sep\times}) \to ...$$

Now over K^{sep}, $A \otimes K^{sep} \simeq X \otimes K^{sep}$ hence $Pic^0(A \otimes K^{sep}) \simeq Pic^0(X \otimes K^{sep})$ and one gets a map

(2.19)

$$H^1(G_K, A^\vee) = H^1(G_K, Pic^0(A \otimes K^{sep})) \to H^2(G_K, K^{sep}(X)^\times/K^{sep\times}).$$

Let $a' \in Ш(A^\vee/K)$ and denotes b' its image in $H^2(G_K, K^{sep}(X)^\times/K^{sep\times})$ via the above map. Then b' lifts to an element $f' \in H^2(G_K, K^{sep}(X)^\times)$, which maps to an element $Res(f') \in \prod_v H^2(G_{K_v}, K^{sep}(X)^\times)$. Lastly $Res(f')$ lifts to $(c_v) \in \prod_v Br(K_v)$ (this can be seen from considering the equivalent version of (2.19) over local completions. Since a' represents a locally trivial

PHS, it maps vertically to 0 in the product of completions, and hence is 0 in $\prod_v H^2(G_{K_v}, K^{sep}(X)^\times/K^{sep\times}))$ and we define $\langle a, a'\rangle = \Sigma_v inv_v(c_v) \in \mathbb{Q}/\mathbb{Z}$ (recall $0 \to Br(K) \to \prod_v Br(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$.)

Exercise 2.20. Prove that if λ comes from a rational divisor then the above pairing is alternating.

Proposition 2.21. *Let A/K be a principally polarized abelian variety with principal polarization λ. Assume that $Ш(A/K)$ is finite. If λ is given by a rational divisor then $|Ш(A/K)| = \square$.*

Proof. By Exercise 2.20 if λ is given by a rational divisor then the pairing is alternating. If moreover $Ш(A/K)$ is finite then it is non-degenerate. The result follows since a finite abelian group equipped with a bilinear non-degenerate alternating pairing can be shown to have square order. $\square$

In order to numerically verify BSD (up to square), one needs to compute whether $|Ш(A/K)| = \square$ or $2\square$. In case of $A = J(C)$ the Jacobian of a curve C/K, Poonen and Stoll in [9] Corollary 12, give the following formula:

Definition 2.22. Let C be a curve of genus g over a local field K_v. Then C is deficient if it has no K_v-rational divisor of degree $g-1$.

Proposition 2.23. *Let J/K be the Jacobian of a smooth curve C/K and assume that $Ш(J/K)$ is finite. Then $|Ш(J/K)| = \square$ if C/K has an even number of deficient places, and $|Ш(J/K)| = 2\square$ if C/K has an odd number of deficient places.*

The following Proposition gives an explicit criterion for a curve to be deficient.

Proposition 2.24. *Let $K/\mathbb{Q}_p$ be a finite extension and C/K be a hyperelliptic curve of genus g. Denote k the residue field of K. The following are equivalent:*

1) C is deficient 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.

Proof. Remark 1 after Lemma 16 in [9]. $\square$

2.5. **Exercises.**

Exercise 2.25. This exercise leads you through a 2-descent procedure and exhibit PHS's in $Sel^2(E/\mathbb{Q})$.

Let $E/\mathbb{Q} : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ with $\alpha, \beta, \gamma \in \overline{\mathbb{Q}}$ distinct.

(1) Let $P = (x_0, y_0)$ with $x_0 \neq \alpha, \beta, \gamma$.
Prove that the map $E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, which sends $P \mapsto (x_0 - \alpha, x_0 - \beta, x_0 - \gamma)$ is an injective homomorphism.

Note: replace $(x_0 - \alpha)$ by $(x_0 - \beta)(x_0 - \gamma)$ if $x_0 = \alpha$ etc.. and $\mathcal{O} \mapsto (1, 1, 1)$.

(2) Prove that a triple a, b, c with $abc \in \mathbb{Q}^{\times 2}$ lies in the image if and only if it is in the image of $E(\mathbb{Q})[2]$, or

$$cz_3^2 - \alpha + \gamma = az_1^2 \quad cz_3^2 - \beta + \gamma = bz_2^2$$

is soluble with $z_i \in \mathbb{Q}^\times$.

Note: -in this case $P = (az_1^2 + \alpha, \sqrt{abc}z_1z_2z_3) \mapsto (a, b, c)$ so that it is possible to explicitly find points on E via this method.

-Each triple a, b, c defines a PHS as the intersection of the two quadrics above.

The following exercise yields a version of Corollary 1.13 for abelian varieties without assuming finiteness of Ш.

Exercise 2.26. Let $\varphi : A/K \to B/K$ be an isogeny of abelian varieties defined over K such that $\varphi\varphi^\vee = [p]$. Let

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

Show that

$$\frac{Q(\varphi^\vee)}{Q(\varphi)} \equiv p^{rk_p(A/K)} \mod \mathbb{Q}^{\times 2}$$

You may use that $Q(\varphi \circ \varphi^\vee) = Q(\varphi)Q(\varphi^\vee)$.

Exercise 2.27. Prove that if λ comes from a rational divisor then the Cassels-Tate pairing is alternating.

3. Tamagawa Numbers

In this section, K denote a finite extension of $\mathbb{Q}_p$ for some prime p. Sometimes, p is required to be odd.

We now explore another arithmetic invariant of abelian varieties that appear in BSD2, the Tamagawa number. It is well tabulated for elliptic curves over number fields, and under some conditions, can be computed for Jacobians of curves.

Fix a prime p, let $K/\mathbb{Q}_p$ be a finite extension and A/K be an abelian variety.

Recall from Adam's lecture 2 that the group $A(K)/A_0(K)$ is finite, where $A_0(K)$ denotes the set of points reducing to the connected component of the identity of the Neron model of A/K.

Definition 3.1. The *Tamagawa number* $c(A/K) = |A(K)/A_0(K)|$. Alternatively $c(A/K) = |\tilde{\mathcal{A}}/\tilde{\mathcal{A}}^0(\bar{k})^{\mathrm{Gal}(\bar{k}/k)}|$, where k denotes the residue field of K and $\tilde{\mathcal{A}}, \tilde{\mathcal{A}}^0$ denote the reduction of the abelian variety and the reduction of the identity component of the Neron model respectively.

We first look at Tamagawa numbers of elliptic curves over K.

3.1. **Elliptic curves.** In this case we need to compute $E(K)/E_0(K)$ where $E_0(K)$ is defined by the following exact sequence

$$0 \to E_1(K) \to E_0(K) \to^{\pi} \tilde{E}_{ns}(k) \to 0.$$

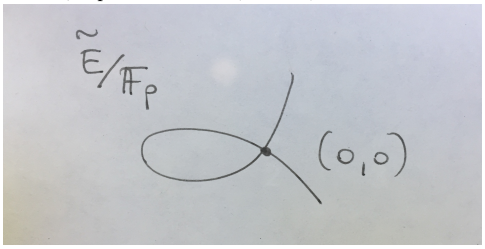
Namely, $E_0(K)$ denotes the points $P \in E(K)$ that reduce to non-singular points $\tilde{P} \in \tilde{E}_{ns}(k)$.

Note that the surjectivity of the reduction map π above depends crucially on the fact that we can use Hensel's lemma to lift non-singular points.

Example 3.2. Let $p > 3$.

(1) Consider $E/\mathbb{Z}_p : y^2 = x(x-1)(x-2)$. Reducing $\bmod p$ gives $\tilde{E}/\mathbb{F}_p : \tilde{y}^2 = \tilde{x}(\tilde{x}-1)(\tilde{x}-2)$, which defines an elliptic curve over $\mathbb{F}_p$.
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 $c(E/\mathbb{Q}_p) = 1$.
This shows that if $E/\mathbb{Q}_p$ has good reduction then $c(E/\mathbb{Q}_p) = 1$. This is reassuring since BSD2 involves $\prod_p c(E/\mathbb{Q}_p)$. This infinite product now makes sense since it is 1 for all but finitely many p.

(2) Consider $E/\mathbb{Z}_p : y^2 = (x+1)(x-p^2)(x+p^2)$. Reducing $\bmod p$ gives $\tilde{E}/\mathbb{F}_p : \tilde{y}^2 = \tilde{x}^2(\tilde{x}+1)$.



In this case, $\tilde{E}/\mathbb{F}_p$ is a nodal curve with singularity at $(0,0)$, i.e. $\tilde{E}_{ns}(\mathbb{F}_p) = \tilde{E}(\mathbb{F}_p)\setminus(0,0)$ and Hensel's lemma is inconclusive at $(0,0)$. From this model $E/\mathbb{Z}_p$, it is not possible to compute $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ because we don't know whether points reducing to $(0,0)$ comes from $\mathbb{Q}_p$-points.

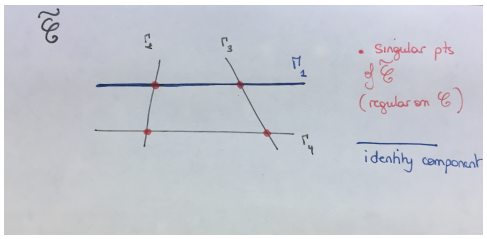
To solve the problem of Example 3.2.2 above we need to consider a "better" model for E. In particular, this model should be such that only the non-singular points of its special fiber can be lifted to points over $\mathbb{Q}_p$ (as opposed to the node above which may or may not lift to $\mathbb{Q}_p$-points). This is achieved by the minimal regular model of $E/\mathbb{Z}_p$.

Proposition 3.3. *Let $\mathcal{C}/\mathbb{Z}_p$ be a proper model for E. If $\mathcal{C}$ is regular (as a scheme) then*

$$E(\mathbb{Q}_p) = \mathcal{C}(\mathbb{Z}_p) = \mathcal{C}^0(\mathbb{Z}_p),$$

where $\mathcal{C}^0 = \mathcal{C}\setminus\{$singular points$\}$.

Example 3.4. Continuing on with Example 3.2.2 above, we construct the special fiber of a minimal regular model for $E/\mathbb{Z}_p$.



Assume first that all components are defined over $\mathbb{F}_p$ (this is the case when E has split multiplicative reduction). By Proposition 3.3, all points $P \in \Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$ away from their intersections can lift to $\mathbb{Q}_p$-points. Moreover, intersection points will not lift to $\mathbb{Q}_p$-points. We entirely determined $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, i.e. $|E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)| = 4$.

In the general case, if some components are not defined over $\mathbb{F}_p$, one needs to consider only components defined over $\mathbb{F}_p$. As Γ_1 is defined over $\mathbb{F}_p$ ($\mathcal{O}$ maps to it), and since the special fibre as a whole is itself defined over $\mathbb{F}_p$, the only possibility is for Γ_2 and Γ_3 to be permuted by Frob. This is the case of E having non-split multiplicative reduction, and in this case $|E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)| = 2$.

3.2. **Jacobians of curves.** In this section we consider a curve C/K and its Jacobian J. Denote $\mathcal{O}_K$ the ring of integers of K, k its residue field and $\bar{k}$ the algebraic closure of k.

We wish to compute Tamagawa numbers for J and hence we need to compute $|J(K)/J_0(K)|$. Models for Jacobians are difficult to construct while on the other hand, models of curves are relatively easy to handle. It would therefore be preferable to compute Tamagawa numbers of J via the minimal regular model of C. As we've seen in Adam's second lecture, Theorem 2.30, it is possible to do so if C is semistable.

Theorem 3.5. *Let C/K be a semistabe curve, $\mathcal{C}/\mathcal{O}_K$ be a minimal regular model for C and $\mathcal{J}/\mathcal{O}_K$ the Neron model of J. Consider $\bar{\mathcal{C}} = \mathcal{C} \times_{\mathcal{O}_K} \bar{k}$ (i.e. the base change to $\bar{k}$ of the special fiber of $\mathcal{C}$). Let $I = \{\Gamma_1, .., \Gamma_n\}$ denote the irreducible components of $\bar{\mathcal{C}}$ and let d_i denote their multiplicities.*

Define the map $\alpha : \mathbb{Z}^I \to \mathbb{Z}^I$ by

$$\Gamma_i \mapsto \sum_j (\Gamma_i.\Gamma_j)\Gamma_j,$$

where $\Gamma_i.\Gamma_j$ is the intersection number of Γ_i and Γ_j, and extend by linearity.

Define the map $\beta : \mathbb{Z}^I \to \mathbb{Z}$ by $\Gamma_i \to d_i$, and extend by linearity.

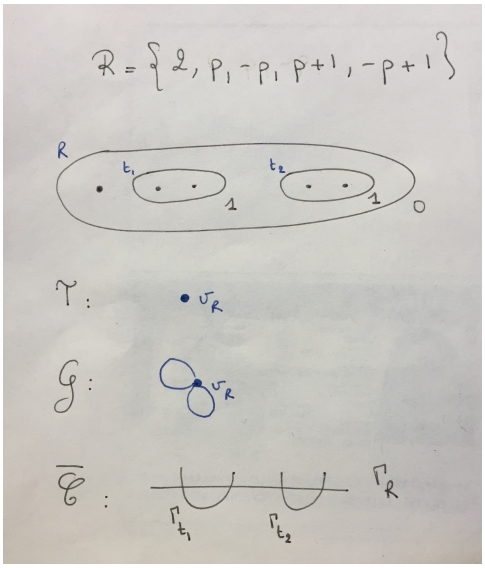
Then $\mathrm{Im}(\alpha) \subseteq \ker(\beta)$ and

$$\mathcal{J}/\mathcal{J}^0(\bar{k}) \simeq \ker(\beta)/\mathrm{Im}(\alpha).$$

The isomorphism above is equivariant for the action of $\mathrm{Gal}(\bar{k}/k)$.

Example 3.6. Let $p > 3$ and consider $C/\mathbb{Q}_p$ be the hyperelliptic curve

$$C : y^2 = (x-2)((x-1)^2 - p^2)(x^2 - p^2).$$



We have $I = \{\Gamma_R, \Gamma_{t_1}, \Gamma_{t_2}\}$ and all components have multiplicity 1. Computing intersection numbers one finds: $\Gamma_R.\Gamma_{t_1} = \Gamma_R.\Gamma_{t_2} = 2$, $\Gamma_R.\Gamma_R = -4$, $\Gamma_{t_1}.\Gamma_{t_1} = \Gamma_{t_2}.\Gamma_{t_2} = -2$ and $\Gamma_{t_1}.\Gamma_{t_2} = 0$.

It follows that $\ker \beta = \{n_R\Gamma_R + n_{t_1}\Gamma_{t_1} + n_{t_2}\Gamma_{t_2} \mid n_R + n_{t_1} + n_{t_2} = 0\}$, and $\mathrm{Im}(\alpha)$:

$[\Gamma_R] = -4\Gamma_R + 2\Gamma_{t_1} + 2\Gamma_{t_2}$

$[\Gamma_{t_1}] = 2\Gamma_R - 2\Gamma_{t_1}$

$[\Gamma_{t_2}] = 2\Gamma_R - 2\Gamma_{t_2}$.

So that $\ker(\beta)/\mathrm{Im}(\alpha) =< \Gamma_{t_1}, \Gamma_{t_2} \mid 2\Gamma_{t_1} = 2\Gamma_{t_2} = 0 > \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

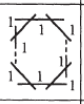
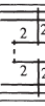
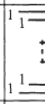
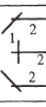
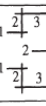
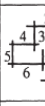
If Γ_{t_1} and Γ_{t_2} are defined over $\mathbb{F}_p$, this yields $c(J/K) = 4$, if they are permuted by Frob then $c(J/K) = 2$.

Remark 3.7. For odd semistable places, there exists an algorithm due to A. Betts which computes Tamagawa numbers of Jacobians of hyperelliptic curves.

Based on the function RegularModel in Magma, R. VanBommel implemented an algorithm to compute Tamagawa numbers of Jacobians of curves (it will return a value if Magma is able to compute a regular model).

3.3. **Exercises.**

Exercise 3.8. Compute the possible Tamagawa numbers of elliptic curves using the following table.

Kodaira symbol	I_0	I_n $(n \geq 1)$	II	III	IV	I_0^*	I_n^* $(n \geq 1)$	IV^*	III^*	II^*
Special fiber $\tilde{\mathcal{C}}$ (The numbers indicate multiplicities)										
$m =$ number of irred. components	1	n	1	2	3	5	$5+n$	7	8	9
$E(K)/E_0(K)$ $\cong \tilde{\mathcal{E}}(k)/\tilde{\mathcal{E}}^0(k)$	(0)	$\frac{\mathbb{Z}}{n\mathbb{Z}}$	(0)	$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$\frac{\mathbb{Z}}{3\mathbb{Z}}$	$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$	$\frac{\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}}{n \text{ even}}$ $\frac{\mathbb{Z}}{4\mathbb{Z}}$ n odd	$\frac{\mathbb{Z}}{3\mathbb{Z}}$	$\frac{\mathbb{Z}}{2\mathbb{Z}}$	(0)
$\tilde{\mathcal{E}}^0(k)$	$\tilde{E}(k)$	k^*	k^+	k^+	k^+	k^+	k^+	k^+	k^+	k^+
Entries below this line only valid for $\mathrm{char}(k) = p$ **as indicated**										
$\mathrm{char}(k) = p$			$p \neq 2,3$	$p \neq 2$	$p \neq 3$	$p \neq 2$	$p \neq 2$	$p \neq 3$	$p \neq 2$	$p \neq 2,3$
$v(\mathcal{D}_{E/K})$ (discriminant)	0	n	2	3	4	6	$6+n$	8	9	10
$f(E/K)$ (conductor)	0	1	2	2	2	2	2	2	2	2
behavior of j	$v(j) \geq 0$	$v(j) = -n$	$\tilde{j} = 0$	$\tilde{j} = 1728$	$\tilde{j} = 0$	$v(j) \geq 0$	$v(j) = -n$	$\tilde{j} = 0$	$\tilde{j} = 1728$	$\tilde{j} = 0$

Note : the numbers in the description of the minimal regular model indicate the multiplicity of the components. In particular a component with multiplicity higher than 1 is singular.

Exercise 3.9. Let $p > 5, n, m > 0 \in \mathbb{Z}$ and consider $C/\mathbb{Q}_p$ be the hyperelliptic curve

$$C : y^2 = (x-1)(x-2)(x-3)(x-p^{n/2})(x+p^{n/2})(x-4-p^{m/2})(x-4+p^{m/2})$$

Compute the possible Tamagawa numbers of J at p.

4. Explicit computations of parity of rank

In this section, K is a number field and we consider its completions K_v at places v.

From what we have seen so far, it is possible to compute some invariants involved in BSD2 under certain conditions. If a hyperelliptic curve C over a number field is semistable at all odd places and has good reduction at places above 2, then we can compute the Tamagawa numbers for its Jacobian. In this case we can also compute whether the order of its Shafarevich-Tate group is a square or twice a square by Proposition 2.24. It is not enough to yet be able to numerically verify BSD2. For more details on how one can do that, see for example [6] or [10] where verifications up to squares are performed for higher genus curves.

However, we now know enough to compute the parity of the rank of J under certain conditions. This last lecture will describe how to do so in the case of some Jacobians of genus 2 curves.

4.1. parity of $rk_p(A/K)$.

In this section we generalize Theorem 1.10 (the invariance of the BSD quotient under isogenies) to abelian varieties and remove the assumption on the finiteness of Shafarevich-Tate groups.

Fix p a prime and a number field K.

Let $\varphi : A/K \to B/K$ be an isogeny of abelian varieties defined over K such that $\varphi\varphi^\vee = [p]$. Recall the following definition (see Exercise 1.15).

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

Proposition 4.1. *Keeping notation as above and fixing non-zero global exterior forms ω_A, ω_B for A, B we have*

$$\frac{Q(\varphi^\vee)}{Q(\varphi)} = \frac{|B(K)_{tors}||B^\vee(K)_{tors}|\Omega_A \prod_{v\nmid\infty} c(A/K_v)|\frac{\omega_A}{\omega^0_{A,v}}|_v}{|A(K)_{tors}||A^\vee(K)_{tors}|\Omega_B \prod_{v\nmid\infty} c(B/K_v)|\frac{\omega_B}{\omega^0_{B,v}}|_v} \frac{|Ш_0(A)[p^\infty]|}{|Ш_0(B)[p^\infty]|},$$

where $Ш_0(A/K)$ denotes $Ш(A/K)$ modulo its divisible part (hence it is finite) and

$$\Omega_X = \prod_{v|\infty_{\mathbb{R}}} \int_{A(K_v)} |\omega_A| \cdot \prod_{v|\infty_{\mathbb{C}}} 2^{\dim A} \int_{A(K_v)} |\omega_A \wedge \overline{\omega}_A|$$

Proof. Theorem 4.3 in [11] □

Note that Proposition 4.1 combined with Exercise 2.25, which proves that

$$\frac{Q(\varphi^\vee)}{Q(\varphi)} \equiv p^{rk_p(A/K)} \mod \mathbb{Q}^{\times 2},$$

gives a formula for the parity of $rk_p(A/K)$ provided that A admits an isogeny defined over K.

Remark 4.2. 1) If both A and B are principally polarized then $A \simeq A^\vee$ and similarly for B. In particular this is the case if A is the Jacobian of a genus 2 curve admitting a Richelot isogeny.

In this case, if J/K is semistable at odd places (+ some extra conditions at places above 2), we can compute Tamagawa numbers and the order of the finite part of the Shafarevich-Tate groups up to square.

To then compute the parity of $rk_2(J)$, it remains to compute the Tamagawa numbers at places above 2 and the real period contributions.

2) For p odd, Coates, Fukaya, Kato, Sujatha prove that the parity of $rk_p(A/K)$ of an abelian variety admitting a p-cyclic isogeny is given by the root number of A (plus technical constraints, see [14] Theorem 2.1)

Following this remark, we compute $rk_2(J/K)$ for semistable (with extra constraints at places above 2) Jacobian of genus 2 curves admitting a Richelot isogeny (degree 4, generalization of a 2-isogeny for elliptic curves).

Let C/K be a genus 2 curve such that its Jacobian J admits a Richelot isogeny φ. Denote $\hat{J}$ and $\hat{C}$ the isogenous Jacobian and its underlying curve respectively. In this case Proposition 4.1 and Exercise 2.25 gives

$$(-1)^{rk_2(J/K)} = (-1)^{\mathrm{ord}_2}\Big(\frac{\Omega_J \prod_{v\nmid 2\infty} c(J/K_v) \prod_{v|2} c(J/K_v) |\frac{\omega_J}{\omega^0_{J,v}}|_v |Ш_0(J)[2^\infty]|}{\Omega_{\hat{J}} \prod_{v\nmid 2\infty} c(\hat{J}/K_v) \prod_{v|2} c(\hat{J}/K_v) |\frac{\omega_{\hat{J}}}{\omega^0_{\hat{J},v}}|_v |Ш_0(\hat{J})[2^\infty]|}\Big)$$

4.2. **Infinite places.** We start with the computation of $\mathrm{ord}_2(\frac{\Omega_J}{\Omega_{\hat{J}}})$. Thanks to the following Proposition, it is enough to work with real and complex roots of C.

Proposition 4.3. *Let J/K be a Jacobian admitting a Richelot isogeny φ over a number field K. Let $\omega_{\hat{J}}$ be a choice of exterior form for $\hat{J}$ and choose $\omega_J = \varphi^*\omega_{\hat{J}}$ as an exterior form for J. Then*

$$\frac{\Omega_J}{\Omega_{\hat{J}}} = \prod_{v|\infty} \frac{n(\hat{J}(K_v))}{|\ker(\varphi^0)| n(J(K_v))},$$

where

$n(J(K_v)), n(\hat{J}(K_v))$ denote the number of connected components of $J(K_v)$ and $\hat{J}(K_v)$ respectively,

φ^0 denote the map induced by φ on $J(K_v)^0$ (restrict the map induced by φ to the connected component of the identity).

Proposition 4.4. *Keeping notation as above, we have $n(J(\mathbb{R})) = 2^{n(C(\mathbb{R}))-1}$ if $n(C(\mathbb{R})) > 0$, and $n(J(\mathbb{R})) = 1$ otherwise.*

Proof. Proposition 3.2.2 and 3.3 in [12] □

Remark 4.5. Exercise 4.7 computes $n(\hat{J}(K_v))$ and $|\ker(\varphi^0)|$.

4.3. **2-adic places.** Let $K/\mathbb{Q}_2$ be a finite extension. Consider the following family of curves

$$\mathcal{F} : y^2 = G_1(x)G_2(x)G_3(x) = (x^2 - (4t_1)^2)(x^2 + t_2x + t_3)(x^2 + t_4x + t_5),$$

where

$$t_1 \in \mathcal{O}_K, \quad t_2 \equiv 1 \mod 2, \quad t_3 - \frac{1}{4} \equiv 0 \mod 2, \quad t_4 \equiv -2 \mod 8, \quad t_5 \equiv 1 \mod 8.$$

Proposition 4.6. *Keeping notation as above, suppose that $C \in \mathcal{F}$ and that both $G_2(x)$ and $G_3(x)$ are irreducible in K. Then*

$$(-1)^{\mathrm{ord}_2\left(\prod_{v|2} \frac{c(\hat{J}/K_v)|\frac{\omega_{\hat{J}}}{\omega^0_{\hat{J},v}}|_v}{c(J/K_v)|\frac{\omega_J}{\omega^0_{J,v}}|_v}\right)} = 1$$

Proof. Every curve in $\mathcal{F}$ has totally split toric reduction. The Proposition follows from a result of A. Morgan in the appendix of [13]. □

4.4. **Exercises.** The first exercise computes $n(\hat{J}(K_v))$ and $|\ker(\varphi^0)|$. The second is an explicit computation of the parity of $rk_2(J/K)$.

Exercise 4.7. Let K be a number field. The Jacobian J of a genus 2 curve $C/K : y^2 = f(x)$ admits a Richelot isogeny if and only if $\mathrm{Gal}(f(x)) \subseteq C_2^3 \rtimes S_3$. This is equivalent to $f(x)$ admitting the following factorization over K:

$$f(x) = f_1(x)f_2(x)f_3(x),$$

where $deg(f_i(x)) \leq 2$.

For a fixed such factorization, write α_i, β_i for the roots of $f_i(x)$ and let $P_i = (\alpha_i, 0), Q_i = (\beta_i, 0)$ be the corresponding points on C.

Define the kernel of the Richelot isogeny on J to be the following Galois stable subgroup of 2-torsions:

$$\{\mathcal{O}, [P_1, Q_1], [P_2, Q_2], [P_3, Q_3]\}.$$

Write $\hat{C} : y^2 = g(x) = g_1(x)g_2(x)g_3(x)$ (it is easy to show that $\hat{C}$ also admits such a quadratic factorization).

1) Assume that all quadratic factors of $f(x)$ are individually defined over K. Give a formula for the number of real roots of $g(x)$ in terms of the roots of $f(x)$. By Proposition 4.3 this is enough to compute $n(\hat{J}(K_v))$.

Hint: for $i = 1, 2, 3$ we have

$$Disc(g_i(x)) = (\alpha_{i+1} - \alpha_{i+2})(\alpha_{i+1} - \beta_{i+2})(\beta_{i+1} - \alpha_{i+2})(\beta_{i+1} - \beta_{i+2}),$$

for some non-zero constant c.

2) Prove the following Proposition:

Proposition 4.8. *A divisor $D_i = [P_i, Q_i] \in \ker \varphi$ is in $\ker \varphi^0$ if and only if the points $P_i, Q_i \in C$ satisfy either*

i) $P_i = \bar{Q}_i$, or

ii) P_i, Q_i lie in the same connected component of $C(\mathbb{R})$.

Exercise 4.9. Let $C/\mathbb{Q} : y^2 = (x^2-16)(x^2+x+\frac{17}{4})(x^2-2x+9)$. Compute the parity of $rk_2(J)$. Hint : The corresponding curve is given by $C'/\mathbb{Q}$: $y^2 = \frac{-131}{2}(-3x^2+\frac{19}{2}x+\frac{35}{2})(2x^2-50x+32)(x^2+\frac{81}{2}x+16)$.

References

[1] A. Betts, On the computation of Tamagawa numbers and Néron component groups of semistable hyperelliptic curves, Preprint (2016).

[2] T. Dokchitser, V. Dokchitser, C. Maistret, A. Morgan, Arithmetic of hyperelliptic curves over local fields, preprint (2017).

[3] J. Tate, On the conjecture of Birch and Swinnerton-Dyer and a geometric analog, Seminaire N. Nourbaki, 1964-1966, exp. 306, p. 415-440

[4] H. Darmon, Rational Points on Modular Elliptic Curves, CBMS Regional Conference Series in Mathematics Volume: 101; 2004; p.129

[5] J.H. Silverman, The Arithmetic of Elliptic Curves, 2nd Edition, Springer

[6] E.V. Flynn, F. Leprévost, E. F. Shaeffer, W.A. Stein, M. Stoll, J.L. Wetherell, Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves, Mathematics of Computation.

[7] J.S. Milne, Arithmetic Duality Theorems, 2nd Edition.

[8] T. Dokchitser, Notes on the parity conjecture, September 2010, CRM Barcelona Advanced Courses in Mathematics "Elliptic Curves, Hilbert Modular Forms and Galois Deformations", Birkhauser, 2013.

[9] B. Poonen, M. Stoll, The Cassels-Tate pairing on polarized abelian varieties, Annals of Mathematics, **150**, 1999, 1109-1149.

[10] R. Van Bommel, Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over Q up to squares, arXiv:1711.10409.

[11] T. Dokchitser, V.Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, Annals of Mathematics, Second Series, Vol 172, 2010.

[12] B. H. Gross, J. Harris, Real algebraic curves, Annales scientifiques de l'E.N.S, 4. Serie, tome 14, p 157-182, 1981

[13] C. Maistret, Parity of ranks of Jacobian of hyperelliptic curves of genus 2, PhD Thesis, 2017.

[14] J. Coates, T. Fukaya, K. Kato, R. Sujatha, Root numbers, Selmer groups, and noncommutative Iwasawa theory, J. Algebraic Geometry, 2009