# The Birch and Swinnerton-Dyer conjecture explained

TCC course by Raymond van Bommel

May–June 2025

These are notes for a hybrid course I taught as part of the Taught Course Centre (TCC). Comments, questions and suggestions for correction and clarification are always welcome.

## Contents



## 1 Introduction

Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then a famous theorem proved by Mordell in 1922 asserts the abelian group of rational points $E(\mathbb{Q})$ of $E$ is finitely generated, i.e., it is of the shape

$$E(\mathbb{Q}) \cong T \times \mathbb{Z}^r,$$

where $T$ is the finite torsion subgroup and the integer $r$ is called the *(algebraic) rank* of $E$, or $\mathrm{rk}(E)$. Even though it is known exactly which finite groups $T$ can occur as the torsion subgroup (Mazur's theorem), less is known about the rank. It is conjectured, but not proved, that the rank is 0 for 50% of elliptic curves and 1 for another 50% of elliptic curves and greater than 1 for infinitely many but 0% of elliptic curves:

$$\lim_{X\to\infty} \frac{\#\{E \mid H(E) \le X \text{ and } \mathrm{rk}(E) = r\}}{\#\{E \mid H(E) \le X\}} = \begin{cases} \frac{1}{2} & \text{if } r \in \{0,1\} \\ 0 & \text{else} \end{cases},$$

where $H(E) = \max(4|A|^3, 27B^2)$ is the height of the elliptic curve $E\colon y^2 = x^3 + Ax + B$ written in minimal Weierstraß form. There is no consensus on whether there exist a uniform bound for the rank of all elliptic curves over $\mathbb{Q}$. An elliptic curve with rank at least 29 has been found in 2024, breaking the previous record of 28 from 2006. It would actually be very hard to prove that this elliptic curve has rank exactly 29; techniques (descent) to prove such things might be discussed later in this course.

On the other hand, changing the equations of $E$ if needed, we can assume that $A$ and $B$ are integers and minimal, and we can reduce the equation modulo $p$ to obtain a curve $E_p$ over $\mathbb{F}_p$. For all but finitely of the primes $p$, the curve $E_p$ will also be a (smooth) elliptic curve, and $E$ is said to have *good reduction* at $p$. For the other primes, $E$ has either *multiplicative reduction* if $E_p$ has a node, or *additive reduction* if $E$ has a cusp. Moreover, the multiplicative reduction is called *split* if the tangent directions of the curve at the node are rational, and *non-split* otherwise.

Hasse's theorem states that

$$|\#E_p(\mathbb{F}_p) - (p+1)| \le 2\sqrt{p}$$

for all primes $p$ of good reduction. We define $a_p = p + 1 - \#E_p(\mathbb{F}_p)$ and

$$L_p(T) = \begin{cases} 1 - a_pT + pT^2 & \text{if } p \text{ is a prime of good reduction,} \\ 1 - T & \text{if } p \text{ is a prime of split multiplicative reduction,} \\ 1 + T & \text{if } p \text{ is a prime of non-split multiplicative reduction,} \\ 1 & \text{if } p \text{ is a prime of additive reduction.} \end{cases}$$

We then define the $L$-function of $E$ as

$$L(E,s) = \prod_p L_p(p^{-s}).$$

The function $L(E,s)$ extends[1] to an analytic function $\mathbb{C} \to \mathbb{C}$ and it the order of the vanishing at 1 is called the *analytic rank* of $E$, or $\mathrm{rk}_{\mathrm{an}}(E)$.

**Conjecture 1.1** (Birch–Swinnerton-Dyer)**.**

$$\mathrm{rk}(E) = \mathrm{rk}_{\mathrm{an}}(E)$$

The conjecture does not only predict the order of vanishing of the $L$-function at 0, but it also predicts the leading coefficient of the Taylor series at $s = 1$. The version below is the general version for abelian varieties $A$ over a number field $K$.

[1]This is actually very non-trivial to prove and follows from the modularity theorem.

**Conjecture 1.2** (BSD over $\mathbb{Q}$, [HiSi00, Conj. F.4.1.6, p. 462])**.** *Let $A/\mathbb{Q}$ be an abelian variety of dimension $d$ and algebraic rank $r$. Let $L(A,s)$ be its L-function, $A^\vee$ its dual, $R_A$ its regulator, $Ш(A)$ its Tate-Shafarevich group and $P_A$ its period. For each prime $p$, let $c_p$ be the Tamagawa number of $A$ at $p$. Then $L(A,s)$ has a zero of order $r$ at $s=1$ and*

$$\lim_{s\to 1}(s-1)^{-r}L(A,s) = \frac{P_A R_A \cdot |Ш(A)| \cdot \prod_p c_p}{|A(\mathbb{Q})_{\mathrm{tors}}| \cdot |A^\vee(\mathbb{Q})_{\mathrm{tors}}|}. \tag{1.0.1}$$

In this course, we will study the different invariants occurring in the formula, approaches to compute them, and their relation to other important subjects in arithmetic geometry. Sometimes we will focus on the case when $A$ is the Jacobian $J$ of a curve $C$.

# 2 Abelian varieties

The topic of abelian varieties is so vast that one can fill a whole course with it. I will try to highlight some of the things we will need about abelian varieties and refer you to the literature for the full theory. A good source is the unpublished book [EMvdG].

**Definition 2.1** (abelian variety)**.** An *abelian variety* over a field $k$ is a proper/complete variety $A$ over $k$ that also carries a group structure. That is, there is a multiplication $m\colon A\times A\to A$, an identity element $e\colon \{\star\}\to A$ and an inverse $i\colon A\to A$ satisfying the usual group axioms.

**Fact 2.2.** The group structure on an abelian variety is automatically commutative. The proof is omitted.

**Example 2.3** ([EMvdG, Example 1.10])**.** Let $C$ be a (hyperelliptic) curve of genus 2 over $k$. Then $C$ has a hyperelliptic involution $i\colon C\to C$. Consider the surface

$$C^{(2)} \coloneqq (C\times C)/\iota,$$

where $\iota\colon C\times C\to C\times C$ swaps the two coordinates. The antidiagonal

$$\Delta^- \coloneqq \{(P,i(P)) : P\in C\}/\iota \quad \subset \quad C^{(2)}$$

turns out to be a curve of genus 0 with self-intersection $-1$ and by the theory of algebraic surfaces there exists a contraction/blow-down $C^{(2)}\to J$ which contracts $\Delta^-$ to a point and is an isomorphism outside of $\Delta^-$.

On the other hand, it is known for the genus 2 curve $C$ that the divisor $P+i(P)$ is in the canonical divisor class for any $P\in C$. This can be used to construct a map

$$J(k)\to \mathrm{Cl}^0(C)\colon \quad (P,Q)\mapsto [P+Q-K_C],$$

where $\mathrm{Cl}^0(C)$ is the the group of divisors on $C$ of degree 0 modulo principal divisors. It follows from the Riemann-Roch theorem that this map is a bijection, and we can use this bijection to supply $J$ with a group structure and therefore the structure of an abelian variety.

The abelian variety $J$ is the *Jacobian* of $C$.

**Remark 2.4.** More generally, for a curve $C$ of genus $g$, the Jacobian $J$ of $C$, representing the group $\mathrm{Pic}^0(C)$ line bundles of degree 0 on $C$, is an abelian variety, and if $C$ has a $k$-rational point, then $J$ is birational to $C^{(g)}$.

**Definition 2.5** (dual abelian variety)**.** For an abelian variety $A$ the *dual abelian variety* $A^\vee$ is the identity component $\mathrm{Pic}^0(A)$ of the variety $\mathrm{Pic}(A)$ representing the group of isomorphism classes of line bundles on $A$.

In general, the dual abelian variety $A^\vee$ is isogenous to $A$, i.e. there is a surjective map $A \to A^\vee$ with finite kernel. For Jacobians the situation is better.

**Proposition 2.6.** *Let $J$ be the Jacobian of a curve over $k$. Then $J^\vee$ is isormorphic to $J$.*

*Sketch of proof.* Reduce to the case that there is a $k$-rational point $P$ of $C$. Then the image of the map

$$C^{(g-1)} \to C^{(g)} \sim J\colon \quad (P_1, \dots, P_{g-1}) \mapsto (P_1, \dots, P_{g-1}, P)$$

gives a divisor $\Theta \subset J$. Then the map

$$\varphi_\Theta\colon J \to J^\vee\colon \quad x \mapsto t_x^*\Theta \otimes \Theta^{-1},$$

where $t_x\colon J \to J$ is the translation-by-$x$ map, turns out to be an isomorphism.17:31 Details can be found in [EMvdG, Chapter 14] □

**Corollary 2.7.** *If $A$ is the Jacobian of a curve, then the factors $|A(\mathbb{Q})_{\mathrm{tors}}|$ and $|A^\vee(\mathbb{Q})_{\mathrm{tors}}|$ in the BSD formula are equal.*

**Definition 2.8** (Poincaré bundle)**.** The line bundle on $A \times A^\vee$ corresponding to the identity map $A^\vee \to A^\vee$ is called the *Poincaré bundle* $\mathcal{P}$.

For those not aware what this means, you can think like this. Every point $x \in A^\vee$ corresponds to a line bundle $\mathcal{L}$ on $A$. If you restrict $\mathcal{P}$ to $A \times \{x\}$, you get the line bundle $\mathcal{L}$. So the Poincaré bundle is some way to glue all the line bundles on $A$ into a large line bundle.

**Remark 2.9.** The Poincaré bundle can also be used to show that $A^{\vee\vee} \cong A$.

# 3 Models of curves and abelian varieties

The book [Liu02] is a good place to read more about the topic.

Let $K$ be a global or local field, e.g. a number field, or a finite extension of the field $\mathbb{Q}_p$ of $p$-adics. Let $\mathfrak{p}$ be a prime of the ring of integers $\mathcal{O}$ of $K$ and let $\mathcal{O}_\mathfrak{p}$ be the localisation of $\mathcal{O}$ at $\mathfrak{p}$.

The following definition is for people who are familiar with the language of schemes.

**Definition 3.1** (model of a curve)**.** Let $C$ be a curve over $K$. Then *a model of $C$ over $\mathcal{O}_\mathfrak{p}$* is a normal, proper, flat $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$-scheme $\mathcal{C}$, such that all fibres are pure of dimension 1, together with an isomorphism between the generic fibre $\mathcal{C}_\eta$ and the curve $C$.

For those not familiar with this language follows a sketch of what this means. Suppose we start with a curve over $\mathbb{Q}$ and $p$ is a prime. Then to get a model, we need to make sure that the following holds.[2]

- The coefficients of the defining equations of the curve do not have $p$s in the denominators.

[2]These properties are not a formally correct definition, but rather indicate the kind of properties we need.

- When you reduce the equation modulo $p$, you get a curve. This curve can have isolated singularities, but cannot have a whole component that is singular (e.g., $y^2 = p \cdot x$ would not be allowed).
- If you take a point in $C(\mathbb{Q})$, then it can be reduced modulo $p$ to a unique point in $\mathcal{C}(\mathbb{F}_p)$ (also for extensions of $\mathbb{Q}$).

## 3.1 Regular models

**Definition 3.2** (regular points/scheme)**.** Let $X$ be a scheme. Then a point $p \in X$ is called *regular* if the maximal ideal $\mathfrak{m}_p \subset \mathcal{O}_{X,p}$ can be generated by $\dim(\mathcal{O}_{X,p})$ elements, or equivalently when the vector space $\mathfrak{m}_p/\mathfrak{m}_p^2$ has dimension $\dim(\mathcal{O}_{X,p})$.

The scheme $X$ is said to be *regular* is it is regular at every point.

**Fact 3.3.** Under some technical conditions, which are satisfied in the case of models of curves, the non-regular locus is a closed subset of $X$.

**Example 3.4.** Consider the model $\mathcal{C}\colon y^2 = x^5 + x^2 + p^2$ over $\mathbb{Z}_{(p)}$. The point $P = (0,0)$ in the special fibre $\mathcal{C}_{\mathbb{F}_p}$ corresponds to the maximal ideal $\mathfrak{m}_P = (x, y, p)$ in the local ring

$$\left(\mathbb{Z}_{(p)}[x,y]/(y^2 - x^5 - x^2 - p^2)\right)_{(x,y,p)}.$$

The ideal $\mathfrak{m}_P$ cannot be generated by 2 element. The reason is that the elements $\overline{x}, \overline{y}$, and $\overline{p}$ are linearly independent in $\mathfrak{m}_P/\mathfrak{m}_P^2$, because all the terms in the equation lie in $\mathfrak{m}_P^2$. Therefore $\mathcal{C}$ is not regular at $P$.

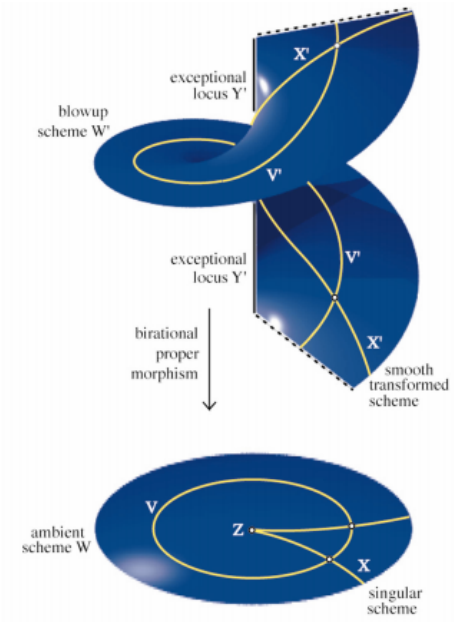


Figure 1: An illustration of a blow up, picture by Hauser

For some of the BSD-invariants of $\mathrm{Jac}(C)$, we need to have a regular model of $C$. Luckily, such models always exist and can be obtained by repeatedly blowing up non-regular points.

**Example 3.5.** In the set-up of Example 3.4, we will blow up $\mathcal{C}$ at the point $P$. We introduce new projective coordinates $U, V$, and $T$ and satisyfing the relations

$$Uy = Vx, \qquad Up = Tx, \qquad Vp = Ty.$$

This blow up has three charts. For the first chart "$U = 1$", we get the relations $y = vx$, and $p = tx$, where $v = \frac{V}{X}$ and $t = \frac{T}{X}$. The equation of the curves changes into

$$x^2v^2 - x^5 - x^2 - x^2t^2 = 0, \qquad p = tx.$$

We will divide by $x^2$, to remove the exceptional locus of the blow up and obtain

$$v^2 - x^3 - 1 - t^2 = 0, \qquad p = tx.$$

In the special fibre of this chart, we already see two components: they are given by $t = 0$ and $x = 0$, respectively. The first component is a smooth curve of genus 1, and the second component is a smooth curve of genus 0. In this chart, the components intersect at $(v, t, x) = (\pm 1, 0, 0)$.

Note that compared to blow-ups of varieties over fields, the number of variables is increasing, as we cannot "replace all $p$ by $tx$".

**Theorem 3.6** (Lipman)**.** *A regular model is obtained after finitely many blow-ups.*

**Remark 3.7.** There are other ways to construct regular models of curves. For example, for hyperelliptic curves cluster pictures can be used, see [HyperUser], and for some plane curves, see [DokT11]. These methods, although way more conceptual and pleasant to use, do not work for all curves.

## 3.2 (Semi-)stable models

**Definition 3.8** ((semi-)stable curve)**.** A curve $C$ is said to be *(semi-)stable* of genus $g \geq 2$ if

- $C$ is geometrically reduced and geometrically connected;
- all singularities of $C$ are nodes / ordinary double points;
- each component of geometric genus 0 meets the other components in at least (two) three points;
- $\dim(H^1(\mathcal{O}_C)) = g$.

A model $\mathcal{C}$ of a smooth curve $C$ of genus at least 2 over $K$ is said to be *(semi-)stable* if its special fibre if semi-stable.

Not every smooth curve has a (semi-)stable model, but this is true after a finite extension.

**Theorem 3.9** (Deligne-Mumford, (semi)-stable reduction theorem)**.** *There exists a finite extension $L$ of $K$ and an extension $\mathfrak{q}$ of the prime $\mathfrak{p}$ such that the base change $C_L$ has a (semi-)stable model over $\mathcal{O}_{L,\mathfrak{q}}$.*

## 3.3 Néron models

A good source to learn more about all the technicalities around Néron models is the book [BLR90].

Let $A$ be an abelian variety over $K$. There does not always exist a model $\mathcal{A}/\mathcal{O}_K$ such that the special fibre $\mathcal{A}_{\mathbb{F}_\mathfrak{p}}$ is also an abelian variety, e.g. take an elliptic curve with bad reduction. The Néron model is in some sense the closest you can get without losing the group structure.

**Definition 3.10** (Néron model)**.** A *Néron model* of $A$ at $\mathfrak{p}$ is a smooth separated $\mathcal{O}_{K,\mathfrak{p}}$-scheme $\mathcal{A}$ that has the following *Néron mapping property*: for any smooth separated $\mathcal{O}_{K,\mathfrak{p}}$-scheme $X$, any morphism $X_K \to A$ on the generic fibre extends uniquely to a morphism $X \to \mathcal{A}$ over $\mathcal{O}_{K,\mathfrak{p}}$.

As a consequence of the definition of a Néron model, the group structure on $A$ given by the multiplication map $m\colon A \times A \to A$, the identity map $e\colon \{\star\} \to A$ and the inverse map $i\colon A \to A$, extends to the Néron model $\mathcal{A}$, giving it a group structure. Another consequence of the defintition is that the Néron model is unique, if it exists.

**Theorem 3.11** (Néron)**.** *Every abelian variety has a Néron model.*

Néron models are typically not proper, as the Néron mapping property is weaker than the valuative criterion for properness. It is does follow from the definition, however, that there is a reduction map on rational points $A(K) \to \mathcal{A}(\mathcal{O}_{K,\mathfrak{p}})$.

**Example 3.12.** Let $E$ be an elliptic curve and $\mathcal{E}$ its minimal regular model (i.e. a regular model on which no components can be contracted). Then the smooth locus of $\mathcal{E}$ is a Néron model of $E$. We consider four cases:

- If $E$ has good reduction, then $\mathcal{E}_{\mathbb{F}_\mathfrak{p}}$ is the reduction of $E$, which is an elliptic curve.
- If $E$ has split multiplicative reduction, then $\mathcal{E}_{\mathbb{F}_\mathfrak{p}}$ is a "circle of $\mathbb{P}^1$s", and the special fibre of the Néron model is of the shape $\mathbb{G}_\mathrm{m} \times \mathbb{Z}/n\mathbb{Z}$ for some integer $n$.
- If $E$ has non-split multiplicative reduction, then it is split multiplicative after an extension. The special fibre of the Néron model consists of copies of $\mathbb{G}_{\mathrm{m},\mathbb{F}_{\mathfrak{p}^2}}$ that are permuted by Galois and non-split tori. Here $\mathbb{F}_{\mathfrak{p}^2}$ denotes the quadratic extension field of $\mathbb{F}_\mathfrak{p}$.
- In the case of additive reduction, the special fibre Néron model is of the shape $\mathbb{G}_\mathrm{a} \times \Phi$, where $\Phi$ is a finite group of order at most 4.

**Fact 3.13.** The Néron model is not stable under base change! Indeed, if an elliptic curve has additive reduction, we know that it will obtain good or multiplicative reduction over some finite extension, so the Néron model must change.

In the case of a curve $C$ over $K$ and its Jacobian $J$, the Néron model $\mathcal{J}$ is related to regular or semi-stable models $\mathcal{C}$ of $C$.

**Theorem 3.14.** *Let $\mathcal{C}$ and $\mathcal{J}$ be as above. Assume (in the case of a regular model), that the greatest common divisor of the multiplicities of the irreducible components in the special fibre is equal to 1. Then the Picard scheme $\mathrm{Pic}^0_{\mathcal{C}/\mathcal{O}_{K,\mathfrak{p}}}$ coincides with the identity component $\mathcal{J}^0$ of $\mathcal{J}$.*

# 4 Period

## 4.1 For abelian varieties

Let $A$ be an abelian variety of dimension $g$ over a number field $K$, and let $\sigma\colon K \hookrightarrow \mathbb{C}$ be an embedding into the complex numbers. Then

$$A_\sigma \coloneqq A \times_\sigma \mathbb{C} \overset{\text{as complex manifold}}{\cong} \mathbb{C}^g/\Lambda$$

for some lattice $\Lambda$.

The periods of $A_\sigma$, i.e. the generators of the lattice $\Lambda$, can be found by integrating a basis of differentials $\underline{\omega} = (\omega_1, \dots, \omega_g)$ of $\Omega^1_A(A)$ inside $\Omega^1_{A_\sigma}(A_\sigma)$ along a set of generators $(\gamma_1, \dots, \gamma_{2g})$ of the homology group $H^1(A_\sigma, \mathbb{Z})$:

$$\Lambda \sim \mathbb{Z}\begin{pmatrix} \int_{\gamma_1} \omega_1 \\ \vdots \\ \int_{\gamma_1} \omega_g \end{pmatrix} \oplus \cdots \oplus \mathbb{Z}\begin{pmatrix} \int_{\gamma_{2g}} \omega_1 \\ \vdots \\ \int_{\gamma_{2g}} \omega_g \end{pmatrix}. \tag{4.1.1}$$

Note that the lattice that you get this way depends on the choice of the basis $\underline{\omega}$ of $\Omega^1_A(A)$. By changing the basis, one changes the $\mathbb{C}$-basis of the vector space $\mathbb{C}^g$.

We first define the complex period.

**Definition 4.1** (local complex period)**.** Suppose that $\sigma$ is a complex place, i.e. that $\sigma$ does not map $K$ into $\mathbb{R}$. Then the *local period of $A$ at $v$ with respect to $\underline{\omega}$* is

$$\Omega_{A,\sigma,\underline{\omega}} = \left| \det\left( \int_{\gamma_i} \omega_j, \overline{\int_{\gamma_i} \omega_j} \right)_{i,j=1}^{i=2g,j=g} \right|.$$

In the real case, the real period measure the size of the lattice $\Lambda \cap \mathbb{R}^g$. Below there are two examples of lattices corresponding to elliptic curves. In the picture, complex conjugation corresponds to reflection through the central horizontal line. The other dotted line in the right hand picture represents the second real component. The real period measures the distance between two nodes on the dotted line (up to a factor 2).

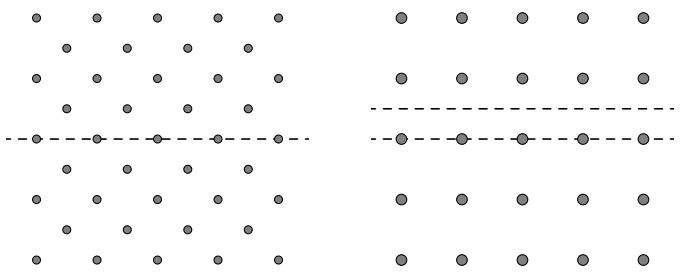

Figure 2: Examples of lattices in $\mathbb{C}$ with one (left) and two (right) real components.

**Definition 4.2** (local real period)**.** Suppose that $\sigma\colon K \hookrightarrow \mathbb{R}$ is a real place. Let $(\gamma_1', \dots, \gamma_g')$ be a basis of $H^1(A_\sigma(\mathbb{C}), \mathbb{Z})^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}$ and let $m_\sigma$ be the number of connected components of $A_\sigma(\mathbb{R})$. Then the *local period of $A$ at $v$ with respect to $\underline{\omega}$* is

$$\Omega_{A,\sigma,\underline{\omega}} = m_v \cdot \left| \det \left( \int_{\gamma_i'} \omega_j \right)_{i,j=1}^{g} \right|.$$

Note that the product

$$\Omega_{A,\underline{\omega}} \coloneqq \prod_{\sigma} \Omega_{A,\sigma,\underline{\omega}}$$

still depends on the choice of $\underline{\omega}$. To resolve this problem and to get a well-defined quantity, we let $\mathcal{A}/\mathcal{O}_K$ be a Néron model of $A$ over $\mathcal{O}_K$.

**Definition 4.3** (period)**.** Suppose $\underline{\omega}$ is an $\mathcal{O}_K$-basis of the module $\Omega^1_{\mathcal{A}/\mathcal{O}_K}(\mathcal{A})$ of global relative differentials on $\mathcal{A}$. Then the *period* of $A$ is defined to be $\Omega_{A,\underline{\omega}}$ as above.

**Remark 4.4.** The sheaf of relative differentials $\Omega^1_{\mathcal{A}/\mathcal{O}_K}$, as defined in [Liu02, Sect. 6.1], is a sheaf that 'glues' the usual sheaves of differentials $\Omega^1_{A/K}$ on the generic fibre and $\Omega^1_{\mathcal{A}_\mathfrak{p}/\mathbb{F}_\mathfrak{p}}$ on the special fibres of $\mathcal{A}$.

The $\mathcal{O}_K$-module $\Omega^1_{\mathcal{A}/\mathcal{O}_K}(\mathcal{A})$ does not need to be a free module (c.f. a non-principal ideal inside $\mathcal{O}_K$ when $K$ has class number greater than 1). The module is only guaranteed to be locally free, and Definition 4.3 can be fixed by taking any $\underline{\omega}$ and measuring how far $\underline{\omega}_\mathfrak{p}$ is from being a basis of $\Omega^1_{\mathcal{A}_\mathfrak{p}/\mathbb{F}_\mathfrak{p}}(\mathcal{A}_\mathfrak{p})$, see also [vB18, Subsect. 1.3.4].

## 4.2 For Jacobians

For a curve $C$ over a number field $K$, it is also possible to obtain the periods of its Jacobian $J$ directly from the curve. Let $\underline{\omega} = (\omega_1, \dots, \omega_g)$ be a basis of differentials of $\Omega^1_C(C)$. For any embedding $\sigma\colon K \hookrightarrow \mathbb{C}$, we can consider these differentials as elements of $\Omega^1_{C_\sigma}(C_\sigma)$ and integrate them along a set of generators $(\gamma_1, \dots, \gamma_{2g})$ of the homology $H^1(C_\sigma, \mathbb{Z})$ and create a lattice as in Equation (4.1.1).

We will now describe which differentials correspond to those in $\Omega^1_{\mathcal{J}/\mathcal{O}_K}(\mathcal{J})$. For this purpose, we introduce the canonical sheaf. The following definitions can also be found in [Liu02, Sect. 6.4].

**Definition 4.5** (determinant)**.** Let $X$ be a scheme, and let $\mathcal{F}$ be a locally free $\mathcal{O}_X$-module of rank $r$. Then we define $\det \mathcal{F}$ to be the line bundle $\wedge^r \mathcal{F}$, i.e. on any affine open $U \subset X$ we let $(\det \mathcal{F})(U) = \wedge^r M$, where $M$ is the $\mathcal{O}_X(U)$-module such that $\mathcal{F}|_U \cong \widetilde{M}$.

The canonical sheaf as defined below is a generalisation of the line bundle $\det \Omega^1_{X/T}$ for smooth schemes $X$ over $T$.

**Definition 4.6** (canonical sheaf)**.** Let $Y/T$ be a quasi-projective locally noetherian scheme that is a local complete intersection (e.g. $Y$ is a semi-stable or regular model of a curve over $T = \mathrm{Spec}(\mathcal{O}_K)$). Let $i\colon Y \to Z$ be an immersion into a smooth scheme $Z/T$ (e.g. projective space). Then the *canonical sheaf* of $Y/T$ is the $\mathcal{O}_Y$-module

$$\omega_{Y/T} \coloneqq \det(i^*(\mathcal{I}/\mathcal{I}^2))^\vee \otimes_{\mathcal{O}_T} i^*(\det \Omega^1_{Z/T}),$$

where $\mathcal{I}$ is the sheaf of ideals defining $Y$ in an open $Z' \subset Z$ containing $Y$ as closed subset.

**Remark 4.7.** This is independent of the choice of $Z$ and $i$, see [Liu02, Sect. 6.4]. Moreover, the canonical sheaf is stable under base change, see [Liu02, Thm. 6.4.9], and for a smooth $Z/T$, it coincides with $\det \Omega^1_Z$, see [Liu02, Cor. 6.4.13].

To get some idea what this canonical sheaf is, we consider the case of a semi-stable curve.

**Theorem 4.8** ([Ols16, Prop. 13.2.9])**.** *Let $C$ be a semi-stable curve over a field $k$ and let $\pi\colon \widetilde{C} \to C$ the normalisation. Let $D = \sum_{y \in \pi^{-1}(C_{\mathrm{sing}})}[y]$ be the divisor on $C'$ consisting of the points that need to be glued on $C'$ to obtain $C$. Then there is an exact sequence*

$$0 \to \omega_{C/k} \to \pi_* \Omega^1_{\widetilde{C}}(D) \to \bigoplus_{P \in C_{\mathrm{sing}}} k(P).$$

*In other words, the sections of $\omega_{C/k}$ correspond to differentials on $\widetilde{C}$ that are allowed to have simple poles at the points in $D$ such that for any $P \in C_{\mathrm{sing}}$ the sum of the residues at the poles corresponding to the two points in $\pi^{-1}(P)$ is zero.*

**Example 4.9.** Take a "nodal elliptic curve" $C$, i.e. glue $\widetilde{C} = \mathbb{P}^1$ at the points 0 and $\infty$. On $\widetilde{C}$, we have $\Omega^1_{\widetilde{C}}([0] + [\infty]) \cong \mathcal{O}_{\widetilde{C}}(2-2) \cong \mathcal{O}_{\widetilde{C}}$. The differential $\frac{1}{x}\,dx$ has simple poles at 0 and $\infty$. The residue at 0 is 1, and writing the differential as $-x\, d\frac{1}{x}$, we see that the residue at $\infty$ is $-1$. Therefore, as their sum is zero[3], the differential gives rise to a global section of $\omega_{C/k}$.

We turn back to the problem of finding the correct differentials for the period.

**Lemma 4.10** ([vB18, Lem. 1.3.5])**.** *Let $\mathcal{C}$ be a regular model[4] of $C$ over $\mathcal{O}_{K,\mathfrak{p}}$, and let $\mathcal{J}$ be a Néron model over $\mathcal{O}_{K,\mathfrak{p}}$ of the Jacobian of $C$. Then there is an isomorphism $\Omega^1_{\mathcal{J}/\mathcal{O}_{K,\mathfrak{p}}}(\mathcal{J}) \cong \omega_{\mathcal{C}/\mathcal{O}_{K,\mathfrak{p}}}(\mathcal{C})$.*

Note that as the canonical sheaf is stable under base change, we have

$$\omega_{\mathcal{C}/\mathcal{O}_{K,\mathfrak{p}}}(\mathcal{C}) \otimes_{\mathcal{O}_{K,\mathfrak{p}}} K \cong \omega_{C/K}(C) \cong \Omega^1_C(C).$$

So we now see that the basis $\underline{\omega}$ of $\Omega^1_C(C)$ that we want to pick in order to find the period of $J$, is one that corresponds to a basis of $\omega_{\mathcal{C}/\mathcal{O}_{K,\mathfrak{p}}}(\mathcal{C})$.

## 4.3 Periods and endomorphisms

Any map $\varphi\colon A \to B$ from an abelian variety to another abelian variety such that $\varphi(0_A) = 0_B$, is automatically also an homomorphism of group varieties, i.e. $\varphi$ respects the group structure.

**Definition 4.11** (isogeny/simple AV/endomorphism algebra)**.** A morphism $\varphi\colon A \to B$ is called an *isogeny* if two of the three following properties hold:

- $\varphi$ is surjective;
- $\dim(A) = \dim(B)$;
- $\ker(\varphi)$ is finite.

[3]The sum of the residues of such a differential is always 0, so in this case it was not necessary to check that. It does become non-trivial when there are more points to glue.

[4]For this theorem, it would actually be enough to consider a model with at most rational singularities.

The abelian varieties $A$ and $B$ are called *isogenous* if such a $\varphi$ exists, and we write $A \sim B$. An abelian variety $A$ is called *simple* if $A \sim B \times C$ can only hold if either $B$ or $C$ is zero-dimensional.

The set of endomorphisms $\mathrm{End}(A)$ is a ring with the composition of endomorphism as multiplication, and the ring

$$\mathrm{End}^0(A) \coloneqq \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is called the *endomorphism algebra* of $A$.

Note that it is possible for an abelian variety $A$ over a field $K$ to be simple, and for $A_{\overline{K}}$ to not be simple. For example, if $L/K$ is a quadratic extension and $B$ is abelian variety over $L$ and $B^\sigma$ its conjugate, then $B \times B^\sigma$ could be isogenous (over $L$) to a simple abelian variety over $K$.

**Theorem 4.12** ([EMvdG, Corollary 12.7])**.** *Let $A$ be an abelian variety such that*

$$A \sim B_1^{e_1} \times \cdots \times B_n^{e_n}$$

*for some simple abelian varieties $B_1, \ldots, B_n$ such that $B_i \not\sim B_j$ if $i \neq j$. Then*

$$\mathrm{End}^0(A) \cong M_{e_1}(D_1) \times \cdots \times M_{e_n}(D_n),$$

*where $D_i \coloneqq \mathrm{End}^0(B_i)$ is a division algebra, and $M_\ell(R)$ denotes the ring of $\ell \times \ell$-matrices with coefficients in $R$.*

There is a more refined classification of the possibilities for the $D_i$ in the theorem above, which is called the Albert classification. There are four possibilities:

- $D$ is a totally real field (type I),
- $D$ split/Hamiltonian quaternion algebra over a totally real field (type II/III),
- $D$ is a central simple algebra over a CM field, i.e. a central simple algebra over a totally imaginary quadratic extension of a totally real field (type IV).

In the case of the Jacobian $J$ of a curve $C$, one can use correspondences to describe an endomorphism $J \to J$.

**Definition 4.13** (correspondence)**.** For (reasonable) varieties $X$ and $Y$, a correspondence between $X$ and $Y$ is a closed subset $R$ of $X \times Y$. For convenience, we will assume that $R$ does not contain subsets of the form $\{x\} \times Y$ or $X \times \{y\}$ for any $x \in X$ or $y \in Y$.

Suppose you have a divisor/correspondence $R \subset C \times C$, then this can describe an endomorphism $J \to J$ as follows. Let $D \in J = \mathrm{Pic}^0(C)$ be some divisor class $\sum_i n_i[P_i]$ on $C$. Then $\{P_i\} \times C$ intersects $R$ in finitely many points $(P_i, Q_{ij})$, with multiplicity if needed, and we can define a map $J \to J$ by

$$D = \sum_i n_i[P_i] \mapsto \sum_{i,j} n_i Q_{ij}.$$

The periods of $A$ can be used to (heuristically) determine the endomorphism ring/algebra of $A$. Indeed, if we arrange the generators of the lattice $\Lambda$ in a $g \times 2g$-matrix $\Pi$ with entries in $\mathbb{C}$, then an endomorphism $A \to A$ gives rise to an equality

$$M\Pi = \Pi R,$$

where $M$ is a $g \times g$-matrix over $\mathbb{C}$, describing a homothety of the lattice, and $R$ is a $2g \times 2g$-matrix over $\mathbb{Z}$, describing the map of lattices. There are commonly used algorithms that solve this problem numerically in order to determine $\mathrm{End}(A)$, see [CMSV19]. It is possible to get certified output, for example in the form of a correspondence of a curve.

# 5 Regulator

## 5.1 Heights on varieties

In this section, we will define the regulator of an abelian variety over a number field. First, we need to discuss some generalities on heights. This is explained well in [Lang83] and [Nér65] (if you don't mind French).

**Definition 5.1** (standard height)**.** Let $K$ be a number field. The *standard height on* $\mathbb{P}^n_K$ is defined by

$$h_{\mathbb{P}^n_K}\colon \mathbb{P}^n_K(\overline{K}) \to \mathbb{R}\colon (x_0 : \cdots : x_n) \mapsto \frac{1}{[L:K]} \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \log \max_{i=0,\ldots,n} \{|x_i|_v\},$$

where $L/K$ is a finite extension containing $x_0, \ldots, x_n$, and $M_L$ is the set of (finite and infinite) places[5] of $L$, and where for all finite places $v$ over the prime $p \in \mathbb{Z}$ the absolute value $|\cdot|_v$ is normalised such that $|p|_v = p^{-1}$.

**Example 5.2.** Over $\mathbb{Q}$, for a rational point $(x_0 : \cdots : x_n)$ with $x_0, \ldots, x_n \in \mathbb{Z}$ coprime, we have

$$h_{\mathbb{P}^n_{\mathbb{Q}}}(x_0 : \cdots : x_n) = \log \max(|x_0|, \ldots, |x_n|).$$

For the rest of this section, let $X/K$ be smooth and projective over a number field $K$.

**Definition 5.3** (naïve height)**.** Let $\mathcal{L}$ be a very ample line bundle on $X$ and let $\mathcal{B}$ be an ordered basis of its global sections, giving rise to an immersion $\varphi\colon X \to \mathbb{P}^n_K$. Then we can define the *naïve global height of* $X$ *at* $\mathcal{L}$ *with respect to* $\mathcal{B}$ as

$$h^{\text{naive}}_{X,\mathcal{L},\mathcal{B}}\colon X(\overline{K}) \to \mathbb{R}\colon P \mapsto h_{\mathbb{P}^n_K}(\varphi(P)).$$

We will now try to extend this definition to work for all line bundles in $A$. For this purpose we will define the following space.

**Definition 5.4** (height function space)**.** Let $\mathrm{Map}(X(\overline{K}), \mathbb{R})$ be the $\mathbb{R}$-vector space of all functions from $X(\overline{K})$ to $\mathbb{R}$. Let $\mathrm{Map}^0(X(\overline{K}), \mathbb{R})$ be the subspace of these functions that are bounded, i.e. the $f\colon X(\overline{K}) \to \mathbb{R}$ for which there exists a $B \in \mathbb{R}$ such that $|f(P)| < B$ for all $P \in X(\overline{K})$. Then the *height function space* of $X$ is

$$\mathcal{H}(X) := \mathrm{Map}(X(\overline{K}), \mathbb{R}) \,/\, \mathrm{Map}^0(X(\overline{K}), \mathbb{R}).$$

Now we can extend the definition of the global height of $X$ to also work at line bundles $\mathcal{L}$, which are not necessarily very ample.

**Lemma 5.5** ([Lang83, Thm. 5.1, sect. 4.5, p. 93])**.** *There exists a function*

$$h_{A,\cdot}\colon \mathrm{Pic}(A) \to \mathcal{H}(X)\colon [\mathcal{L}] \mapsto h_{X,[\mathcal{L}]},$$

*having the following properties:*

- *for* $[\mathcal{L}_1], [\mathcal{L}_2] \in \mathrm{Pic}(X)$ *we have* $h_{X,[\mathcal{L}_1]} + h_{X,[\mathcal{L}_2]} = h_{X,[\mathcal{L}_1 \otimes \mathcal{L}_2]}$*;*
- *if* $\mathcal{L}$ *is a very ample line bundle and* $\mathcal{B}$ *an ordered basis of its global sections then* $h_{X,[\mathcal{L}]}$ *is the class of* $h^{\text{naive}}_{X,\mathcal{L},\mathcal{B}}$*.*

*Moreover, this construction is functorial in the following sense. If* $f\colon X \to Y$ *is a morphism of smooth projective schemes over* $K$ *and* $\mathcal{L}$ *is a line bundle on* $Y$*, then* $h_{X,[f^*\mathcal{L}]} = h_{Y,[\mathcal{L}]} \circ f$*.*

[5] Finite place are prime ideals of $\mathcal{O}_L$ and infinite places are embeddings of $L$ into $\mathbb{R}$ or $\mathbb{C}$. Places correspond to the non-trivial absolute values you can put on $K$.

## 5.2 Canonical height on an abelian variety

In case of abelian varieties, for such height functions, there is a canonical representative in the set $\mathrm{Map}(A(\overline{K}), \mathbb{R})$. Just like for elliptic curves (for those who already heard of the height in that situation), the height can be seen as a measure for how many digits you need to write down a point.

**Proposition 5.6** ([Nér65, Thm. 5, sect. II.14, p. 300])**.** *Let $\mathcal{L}$ be a line bundle on an abelian variety $A$ over $K$. Then there exist functions $\ell, q\colon A(\overline{K}) \to \mathbb{R}$, that are linear and quadratic (i.e. $q(P+Q) - q(P) - q(Q)$ is a bilinear form on $A(\overline{K}) \times A(\overline{K})$), respectively, such that $\ell + q$ is in the class $h_{A,[\mathcal{L}]}$.*

*Sketch of proof.* Let $(-1)\colon A \to A$ be the multiplication by $-1$. Let $\mathcal{M} = (-1)^*\mathcal{L}$. Then $[\mathcal{L}]+[\mathcal{M}]$ is a so-called symmetric line bundle, and the limit

$$\lim_{N\to\infty} \frac{h^{\mathrm{naive}}_{X,[\mathcal{L}]+[\mathcal{M}]}(NP)}{N^2}$$

exists, giving rise to the quadratic part $q$. On the other hand, $[\mathcal{L}] - [\mathcal{M}]$ is anti-symmetric, and in this case the limit

$$\lim_{N\to\infty} \frac{h^{\mathrm{naive}}_{X,[\mathcal{L}]-[\mathcal{M}]}(NP)}{N}$$

exists, giving rise to the linear part $\ell$. □

**Remark 5.7.** While the limit in the proof above, gives you a good way to think about the height, this limit does not give a very fast way to compute the height in practice.

**Definition 5.8** (canonical height)**.** For a line bundle $\mathcal{L}$ on an abelian variety $A$ with functions $\ell, q\colon A(\overline{K}) \to \mathbb{R}$ as above, we define the *canonical height of $A$ at $\mathcal{L}$* as

$$\widehat{h}_{A,\mathcal{L}} = \ell + q.$$

**Fact 5.9.** For an ample $\mathcal{L}$, the set $\bigcup_{[L:K]\leq d}\{x \in A(L) : \widehat{h}_{A,\mathcal{L}}(x) \leq B\}$ is finite for any $B$ and $d$ (Northcott property). Moreover, the only points of height 0 are torsion points.

The above definition of height depends on the choice of a line bundle $\mathcal{L}$. To get an even more canonical notion of height, we consider $A \times A^\vee$.

**Definition 5.10** (Néron-Tate height)**.** Let $\mathcal{P}$ be the Poincaré bundle on $A \times A^\vee$. Then the *Néron-Tate height on $A$* is defined as

$$h_{A\times A^\vee,\,\mathrm{NT}} = \widehat{h}_{A\times A^\vee,\mathcal{P}} : A(\overline{K}) \times A^\vee(\overline{K}) \to \mathbb{R}.$$

Now we can define the regulator of $A$.

**Definition 5.11** (regulator)**.** Let $P_1, \ldots, P_{\mathrm{rk}(A)}$ be a basis of the free part of $A(\mathbb{Q})$, Moreover, let $Q_1, \ldots, Q_{\mathrm{rk}(A)}$ be a basis of the free part of $A^\vee(\mathbb{Q})$. Then the *regulator* of $A$ is defined as

$$\left|\det\begin{pmatrix} h_{A\times A^\vee,\,\mathrm{NT}}(P_1,Q_1) & \cdots & h_{A\times A^\vee,\,\mathrm{NT}}(P_{\mathrm{rk}(A)},Q_1) \\ \vdots & \ddots & \vdots \\ h_{A\times A^\vee,\,\mathrm{NT}}(P_1,Q_{\mathrm{rk}(A)}) & \cdots & h_{A\times A^\vee,\,\mathrm{NT}}(P_{\mathrm{rk}(A)},Q_{\mathrm{rk}(A)}) \end{pmatrix}\right|.$$

## 5.3 Canonical height for Jacobians using Arakelov intersection theory

Let $J$ be the Jacobian of a curve $C$ over a number field $K$. Then as $J^\vee \cong J$, the height pairing becomes a function $J(\overline{K}) \times J(\overline{K}) \to \mathbb{R}$. Instead of trying to compute on $J$ directly, it is actually possible to express the heights using arithmetic and geometry information attached to the curve $C$.

**Theorem 5.12** (Faltings-Hriljac)**.** *Let $D, E$ be degree 0 divisors on $C$ with disjoint support. Then the Néron-Tate height can be expressed as a sum*

$$-\sum_{v \in M_K} \langle D, E \rangle_v,$$

*where $M_K$ is the set of finite and infinite places of $K$, and $\langle \cdot, \cdot \rangle_v$ is a local intersection pairing, which we will roughly after this.*

Let us now describe these local intersection pairings. We first consider the case of a finite place, given by a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. Let $\mathcal{C}$ be a regular model of $C$ over $\mathcal{O}_{K,\mathfrak{p}}$. Then $\mathcal{C}$ just behaves like an algebraic surface over a field in the sense that you can do intersection theory on it.

**Definition 5.13** (horizontal/vertical divisors)**.** Let $D \subset \mathcal{C}$ be irreducible of codimension 1. Then $D$ is called *vertical*, if $D$ is contained in the special fibre $\mathcal{C}_\mathfrak{p}$, i.e. if $D$ is an irreducible component of $\mathcal{C}_\mathfrak{p}$. If $D$ is not vertical, then $D$ is called *horizontal*, in which case $D$ consists of a point in the generic fibre $\mathcal{C}_\eta \cong C$ together with the reduction modulo $\mathfrak{p}$ of that point in $\mathcal{C}_\mathfrak{p}$.

Divisors are called horizontal/vertical if their support consists of horizontal/vertical subschemes.

**Definition 5.14** (intersection number)**.** Let $D_1, D_2 \subset \mathcal{C}$ be irreducible and distinct. Then $D_1 \cap D_2$ is finite, and for each point $P \in D_1 \cap D_2$, we can define the intersection multiplicity at $P$ as

$$\iota_P(D_1, D_2) \coloneqq \operatorname{length}_{\mathcal{O}_{\mathcal{C},P}} \left( \frac{\mathcal{O}_{\mathcal{C},P}}{\mathcal{I}_{D_1,P} + \mathcal{I}_{D_2,P}} \right),$$

where $\mathcal{I}_{D_1,P}$ and $\mathcal{I}_{D_2,P}$ are ideals defining $D_1$ and $D_2$ respectively. We then define the *intersection number*

$$\iota(D_1, D_2) \coloneqq \sum_{P \in D_1 \cap D_2} \iota_P(D_1, D_2) \cdot \log |k_P|,$$

where $k_P$ is the (finite) field of definition of $P$. This function can be extended bilinearly to pairs of divisors with disjoint support.

**Remark 5.15.** If you intersect two horizontal irreducibles corresponding to points $P_1, P_2 \in C$, then you are essentially computing the highest power $\mathfrak{p}^i$ of $\mathfrak{p}$ such that $P_1$ and $P_2$ are congruent modulo $\mathfrak{p}^i$. If you intersect a horizontal and a vertical irreducible, corresponding to a point $P \in C$ and a component $D \subset \mathcal{C}_\mathfrak{p}$, you are determining whether the reduction of $P$ lies on $D$.

**Remark 5.16.** There are a lot of subtleties with this intersection pairing. If $D$ is a vertical divisor, and if we consider the whole special fibre $\mathcal{C}_\mathfrak{p}$ as a divisor, then we can extend the intersection pairing by setting $\iota(D, \mathcal{C}_\mathfrak{p}) = 0$, and use this to determine $\iota(D, D)$. Note that this does not hold for horizontal divisors, as $\iota(D, \mathcal{C}_\mathfrak{p}) \neq 0$ in this case, unless $D$ has degree 0 on $C$.

Now we can define the local pairing $\langle D, E \rangle_\mathfrak{p}$.

**Definition 5.17.** Let $D$ and $E$ be divisors on $C$ of degree 0. Let $\overline{D}$ and $\overline{E}$ be the horizontal divisors on $\mathcal{C}$ corresponding to $D$ and $E$. We define

$$\langle D, E\rangle_{\mathfrak{p}} := \iota\big(\overline{D} + \Phi(\overline{D}), \overline{E} + \Phi(\overline{E})\big)\,,$$

where $\Phi(\overline{D})$ (and similarly $\Phi(\overline{E})$) is a vertical divisor such that $\iota(Y, \overline{D} + \Phi(\overline{D})) = 0$ for all vertical divisors $Y$.[6]

For the infinite places $v$ of $K$, the pairing $\langle D, E\rangle_v$ can be defined using the Riemann theta function corresponding to $\mathbb{C}^g/\Lambda$. The details are omitted and can be found in [Lang88, vBHM20].

# 6 Tate-Shafarevich group

## 6.1 Torsors, twists and $H^1$

In arithmetic geometry, there are often situations where two objects are not isomorphic but become isomorphic after base changing to an algebraic closure. Examples of such objects are twists and torsors of abelian varieties. This topic is also discussed in [Silv09, Chap. X].

**Definition 6.1** (twist)**.** Let $A$ and $B$ be abelian varieties over a field $K$. Then $B$ is said to be a *twist* of $A$ if $A_{\overline{K}} \cong B_{\overline{K}}$.

**Definition 6.2** (torsor)**.** Let $A$ be an abelian variety over a field $K$, and let $X$ be a variety over $K$ with an action of $A$ on it, i.e. a map $A \times X \to X$, satisfying the usual properties. Then $X$ is called an *$A$-torsor*, or principal homogeneous space, if $X_{\overline{K}}$ is isomorphic to $A_{\overline{K}}$, as a variety with an action of $A_{\overline{K}}$.

An $A$-torsor $X$ is called *trivial* if $X \cong A$, or equivalently if $X(K) \neq \emptyset$.

**Example 6.3.** Let $C$ be the curve given by $3x^3 + 4y^3 + 5z^3 = 0$ in $\mathbb{P}^2$ over $\mathbb{Q}$. This is a famous example of a genus 1 curve without a rational point. The Jacobian $E$ of $C$ is an elliptic curve, and $E$ carries a natural action $E \times C \to C$. The curve $C$ is an $E$-torsor under that action.

The set of twists or torsors, up to isomorphism over $K$, can be expressed as a cohomology set. We will first state the theorem and then explain it more in the rest of the subsection.

**Theorem 6.4.** *Let $A$ be an abelian variety over a number field $K$. Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of $K$. Then there are isomorphisms*

$$\{\textit{twists of } A\}/_{\cong_K} \cong H^1(G_K, \mathrm{Aut}(A_{\overline{K}})),$$

$$\{A\textit{-torsors}\}/_{\cong_K} \cong H^1(G_K, A_{\overline{K}}).$$

The pattern that you will see is that the group on the right is the automorphism group of the object in question after base changing to $\overline{K}$. Indeed, for $A_{\overline{K}}$ considered as a variety with an action of $A_{\overline{K}}$ on it, the automorphisms consist of translations by points in $A_{\overline{K}}$.

There are other examples of this phenomenon. For example, line bundles, which become trivial when you look at small enough open subsets, are classified by $H^1(X, \mathbb{G}_{\mathrm{m}})$ or $H^1(X, \mathcal{O}_X^*)$. In this

[6] It is not a priori clear that this vertical divisor $\Phi(\overline{D})$ exists, see [Lang88, vBHM20].

case, $\mathbb{G}_{\mathrm{m}}$ is the automorphism group of a trivial line bundle. Another example is that of central simple algebras, which can be classified using cohomology sets like $H^1(G_K, \mathrm{PGL}_n)$.

The general setup for $H^1(G, A)$ is that $G$ is a group acting on a group $A$. In our case, $G$ is the absolute Galois group acting on the automorphisms over $\overline{K}$ by acting on the coefficients occurring in the automorphisms.

The reason $H^1(G, A)$ exists, is because the functor $A \mapsto A^G$ mapping the group to its invariance, is not exact. If $A$ is abelian, then there is a whole theory of homological algebra, which will give cohomology sets $H^n(G, A)$ with long exact sequences, et cetera. For this course, I will only give a definition for $H^1(G, A)$ that also works for non-abelian $A$, and you will have to consult other sources for more background on the general theory, e.g. [Silv09, App. B]. Note that $H^1(G, A)$ will not be a group, but only a pointed set, unless $A$ is abelian.

**Definition 6.5.** Let $G$ be a group acting on another group $A$, we will denote this action by ${}^g a$ for $g \in G$ and $a \in A$. A *cross morphism* is a map $f\colon G \to A$ such that

$$f(g_1 g_2) = f(g_1) \cdot {}^{g_1} f(g_2), \qquad \text{for all } g_1, g_2 \in G.$$

Two cross morphisms $f_1$ and $f_2$ are called *cohomologous* if there is an $a \in A$ such that

$$f_2(g) = a^{-1} \cdot f_1(g) \cdot {}^g a, \qquad \text{for all } g \in G.$$

The *cohomology set* $H^1(G, A)$ is the set of cross morphisms modulo the equivalence of cohomologous cross morphisms.

*Idea of proof of Theorem 6.4.* Consider an $A$-torsor $X$ over $K$ (the situation of twists is analogous). Let $i\colon A_{\overline{K}} \to X_{\overline{K}}$ be an isomorphism. For any $\sigma \in G_K$, the composite map

$$A_{\overline{K}} \xrightarrow{{}^\sigma i} X_{\overline{K}} \xrightarrow{i^{-1}} A_{\overline{K}},$$

where ${}^\sigma i$ is the isomorphism you get by applying $\sigma$ to the coefficients of $i$, is translation by an element $a_\sigma$. You can now check that the map $\sigma \mapsto a_\sigma$ is a cross morphism.

The other way around, if you are given a cross morphism $f$, then this can be used to construct a torsor. The idea is to consider the variety $A$ over $K$ as a variety over $\overline{K}$ with the action of $\mathrm{Gal}(\overline{K}/K)$ on it, and change this action action of the Galois group. More specifically, any element $\sigma \in \mathrm{Gal}(\overline{K}/K)$ gives rise to a map $\sigma_A\colon A_{\overline{K}} \to A_{\overline{K}}$ (over $K$, not over $\overline{K}$). This action of Galois can be twisted by replacing $\sigma_A$ with $f(\sigma) \circ \sigma_A$. Then one can use descent on $A_{\overline{K}}$ with this new Galois action to get another variety $X$ over $K$, the $A$-torsor. □

We will demonstrate the construction for twists by the means of an example.

**Example 6.6.** Let $E\colon y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$. Let

$$f\colon \mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big) \to \mathrm{Gal}\Big(\mathbb{Q}\left(\sqrt{d}\right)/\mathbb{Q}\Big) \to \mathrm{Aut}\big(E_{\overline{\mathbb{Q}}}\big)$$

be the cross morphism that maps the non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ to the automorphism $-1\colon (x, y) \mapsto (x, -y)$, and the identity to the identity. Then the twisted Galois action on $E$ is given by

$$\left(a + b\sqrt{d}\right) \cdot x \quad \mapsto \quad \left(a - b\sqrt{d}\right) \cdot x,$$

$$\left(a + b\sqrt{d}\right) \cdot y \quad \mapsto \quad \left(-a + b\sqrt{d}\right) \cdot y.$$

The ring of invariants under this action is generated by $x' = x$ and $y' = \sqrt{d} \cdot y$, and we see that they will satisfy the relation $y'^2 = d \cdot f(x')$. In other words, we get the quadratic twist.

**Remark 6.7.** Note that the quadratic twist could be isomorpic to $E$ itself. This may happen if $\mathrm{Aut}(E_{\overline{\mathbb{Q}}})$ has more than 2 elements, and the cross morphism will actually become homologous to the cross morphism mapping everything to the identity.

## 6.2 Local-global principle for torsors

Now we are ready to define the Tate-Shafarevich group.

**Definition 6.8** (Tate-Shafarevich group)**.** Let $A$ be an abelian variety over a number field $K$. Let $M_K$ be the set of places of $K$. Then the *Tate-Shafarevich group* of $A$ is the group

$$Ш(A/K) \coloneqq \bigcap_{v \in M_K} \ker\left(H^1(G_K, A_{\overline{K}}) \to H^1(G_{K_v}, A_{\overline{K_v}})\right),$$

where $K_v$ is the completion of $K$ at $v$, and $\ker(\cdots)$ is the set of elements mapping to the trivial torsor.

In other words, $Ш(A/K)$ is the set of torsors $X$ of $A$ such that $X$ has a point over $K_v$ for all places $v$, up to isomorphism over $K$. These are torsors that have point everywhere locally, but not necessarily globally. You could say that $Ш(A/K)$ measures the failure of the local-global principle for torsors of abelian varieties.

**Example 6.9.** The torsor from Example 6.3 corresponds to a non-trivial element of the Tate-Shafarevich group of the Jacobian $E$ occurring in that example. This element turns out to have order 3.

**Remark 6.10.** While it is conjectured that $Ш(A/K)$ is finite, this is not proved. It is known that $Ш(A/K)[n]$ is finite, but that doesn't exclude the possibility of $Ш(A/K)$ containing some infinite divisible group like $\mathbb{Q}$.

If $Ш(A/K)_{\mathrm{div}}$ is the maximal divisible subgroup of $Ш(A/K)$, then it has been believed for a long time that $|Ш(A/K)/Ш(A/K)_{\mathrm{div}}|$ would be a square. The reason for that is that there is a pairing, called the *Cassels-Tate pairing*

$$\langle \cdot, \cdot \rangle \colon Ш(A/K) \times Ш(A^\vee/K) \to \mathbb{Q}/\mathbb{Z},$$

and this pairing was believed to be alternating after mapping $Ш(A/K)$ to $Ш(A^\vee/K)$ through some polarisation, i.e. $\langle x, x \rangle = 0$. If the polarisation is principal, the pairing can be shown to be antisymmetric, i.e. $\langle x, y \rangle = -\langle y, x \rangle$, which is a weaker property. It turns out that the pairing is not alternating in general and even for Jacobians $J$ the order $|Ш(J/K)/Ш(J/K)_{\mathrm{div}}|$ can also be two times a square, see also [PoSt99].

## 6.3 Descent and Selmer groups

### 6.3.1 Setup

This subsection gives an introduction to descent and Selmer groups. For a more complete picture of the theory, you could read [CFOSS08] or [Silv09, Chap. X]. Let us start with the elliptic curve

$$E\colon y^2 = x(x-a)(x-b) \text{ over } \mathbb{Q}.$$

For a rational point $(x,y) \in E(\mathbb{Q})$, the numbers $x, x-a$, and $x-b$ do not need to be squares, but their product should be. Let us do a substitution

$$x = d_1x_1^2, \quad x-a = d_2x_2^2, \quad x-b = d_1d_2x_3^2, \quad y = d_1d_2d_3x_1x_2x_3.$$

This naturally leads to the curve

$$C_{d_1,d_2}\colon \quad d_1x_1^2 = d_2x_2^2 + a = d_1d_2x_3^2 + b.$$

There is a natural map

$$\varphi_{d_1,d_2}\colon C_{d_1,d_2} \to E\colon \quad (x_1,x_2,x_3) \mapsto (d_1x_1^2, d_1d_2d_3x_1x_2x_3).$$

Any rational point on $E(\mathbb{Q})$ must come from a rational point on $C_{d_1,d_2}(\mathbb{Q})$ for some choice of $d_1$ and $d_2$. So suppose you want to find generators of the Mordell-Weil group $E(\mathbb{Q})$, then it could be useful to study rational points on $C_{d_1,d_2}$.

### 6.3.2 Covers as twists

The cover $\varphi_{d_1,d_2}$ is unramified, and $\mathrm{Aut}(C_{d_1,d_2}/E) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong E[2]$, given by the maps

$$(x_1,x_2,x_3) \mapsto (\pm x_1, \pm x_2, \pm x_3)$$

with an even number of plus signs. Note that different curves $C_{d_1,d_2}$ and $C_{d_1',d_2'}$ become isomorphic over $\overline{\mathbb{Q}}$: they are twists. In this case, the group $\mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$ classifies these twists. In light of what we learned before, it would not be hard to believe the following more general statement.

**Proposition 6.11.** *The $E[2]$-covers of $E$ are classified by the group $H^1(G_{\mathbb{Q}}, E[2])$.*

Note that any point $(x,y) \in E(\mathbb{Q})$ is the image of a rational point on some $C_{d_1,d_2}$. Indeed, we need $d_1 = x \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ and $d_2 = x-a \in \mathbb{Q}^*/\mathbb{Q}^{*2}$. This gives a natural map

$$\rho\colon E(\mathbb{Q}) \to H^1(G_{\mathbb{Q}}, E[2]) : (x,y) \mapsto C_{d_1,d_2}.$$

**Remark 6.12.** Another way to get this map is by taking the long exact sequence of group cohomology for the exact sequence of algebraic groups $0 \to E[2] \to E \xrightarrow{\cdot 2} E \to 0$. Doing it this way, you'll see that $\rho$ factors through $E(\mathbb{Q})/2E(\mathbb{Q})$.

### 6.3.3 Local-global principle again

If you want to know if $C_{d_1,d_2}$ has rational points, you might as well first consider if $C_{d_1,d_2}$ has points everywhere locally, i.e. over every completion $\mathbb{Q}_v$ of $\mathbb{Q}$. It turns out that the curve $C_{d_1,d_2}$ only has points everywhere locally for finitely many of the possible values of $d_1$ and $d_2$.

We want to determine these $d_1$ and $d_2$. For our $C_{d_1,d_2}$, it turns out that $d_1$ and $d_2$ are only allowed to have prime factors that occur in $2ab(a-b)$ if we want $C_{d_1,d_2}(\mathbb{Q}_v) \neq \emptyset$ for all places $v$. For the general case, this motivates the following definition.

**Definition 6.13** (Selmer group)**.** Let $A$ be an abelian variety over a number field $K$ and let $n$ be an integer[7]. Then the *$n$-Selmer group* $\mathrm{Sel}_n(A)$ is the subgroup of those $H^1(K, A[n])$ whose restriction to $H^1(K_v, A[n])$ lies in the image of the local map $\rho_v \colon A(K_v) \to H^1(G_{K_v}, A[n])$ for every place $v$ of $K$.

In other words, the Selmer groups classifies $A[n]$-covers of the abelian variety that have points everwhere locally. As we know, having points everywhere locally is not a guarantee for having a point globally. The failure is again measured by the Tate-Shafarevich group.

**Lemma 6.14.** *There is an exact sequence*

$$0 \to A(K)/nA(K) \to \mathrm{Sel}_n(A) \to Ш(A/K)[n] \to 0.$$

*Proof.* The proof is omitted, but follows from an analysis of a bunch of long exact sequences. □

**Fact 6.15.** The Selmer group is finite and, in principle, effectively computable. The idea is that group $H^1(K, E[n])$ can be embedded in $R^*/R^{*,n}$, where $R$ is a product of fields over which the points in $E[n]$ are defined. The most difficult step in computing the Selmer group is the computation of the class and unit groups of these fields. Again, see [CFOSS08] for more background.

As a consequence of this fact, the Selmer group can be used to bound the rank of $E$ and $Ш(E/K)[n]$. If you believe that $Ш(E/K)$ is finite, then there must be an $n$ for which the right term of the sequence is 0, and you will actually find a sharp upper bound of the rank. On the other hand, there is no unconditional algorithm known to compute the rank of an elliptic curve.

# 7 Tamagawa number

Let $\mathcal{A}$ be a Néron model over $\mathcal{O}_{K,\mathfrak{p}}$ of an abelian variety $A$ over a number field $K$ at a prime $\mathfrak{p}$ of $K$. The special fibre $\mathcal{A}_\mathfrak{p}$ over the residue field $k_\mathfrak{p}$ does not need to be connected. The connected component containing the identity element $\mathcal{A}^0_\mathfrak{p}$ is a subgroup, and the quotient $\Phi \coloneqq \mathcal{A}_\mathfrak{p}/\mathcal{A}^0_\mathfrak{p}$ is called the component group.

**Definition 7.1** (Tamagawa number)**.** The *Tamagawa number* of $A$ at $\mathfrak{p}$ is defined to be

$$c_\mathfrak{p} \coloneqq \#\Phi(k_\mathfrak{p}).$$

Let $K_\mathfrak{p}$ be the completion of $K$ at $\mathfrak{p}$. For elliptic curves $E$ with a minimal Weierstraß equation, the Tamagawa number is sometimes also defined as $\#(E(K_\mathfrak{p})/E(K_\mathfrak{p})^0)$ where $E(K_\mathfrak{p})^0$ is the subgroup of points whose reduction is a smooth point (on the reduction of the minimal Weierstraß model). The lemma below explains why this is the same.

[7] Instead of integers, it is also possible to use other endomorphisms of $A$, in the case $\mathrm{End}(A) \neq \mathbb{Z}$.

**Lemma 7.2.** *There is an equality*

$$c_{\mathfrak{p}} = \#\big(\mathcal{A}(K_{\mathfrak{p}})/\mathcal{A}^0(K_{\mathfrak{p}})\big)\,.$$

*Proof.* Let $R$ be the ring of integers in $K_{\mathfrak{p}}$. By the Néron mapping property $\mathcal{A}(K_{\mathfrak{p}}) = \mathcal{A}(R)$. This also induces a reduction map $\mathcal{A}(K_{\mathfrak{p}}) \to \mathcal{A}(R) \to \mathcal{A}_{\mathfrak{p}}(k_{\mathfrak{p}})$. This reduction map is surjective, because $\mathcal{A}$ is smooth and $K_{\mathfrak{p}}$ is complete (Hensel's lemma). Moreover, as $\mathcal{A}^0$ is open, the reduction maps $\mathcal{A}^0(K_{\mathfrak{p}})$ into $\mathcal{A}^0_{\mathfrak{p}}(k_{\mathfrak{p}})$, and the kernel of $\mathcal{A}(K_{\mathfrak{p}}) \to \Phi(k_{\mathfrak{p}})$ is $\mathcal{A}^0(K_{\mathfrak{p}})$. □

Note that the Tamagawa number is 1 for all primes of good reduction. In particular, only finitely many of the $c_{\mathfrak{p}}$ are not equal to 1.

**Remark 7.3.** There is a different notion of Tamagawa numbers for reductive algebraic groups. While this notion shows similarity to the one for abelian varieties, they should not be considered the same. In fact, historically, the Tamagawa numbers for elliptic curves have been called fudge factors. The exact definition of these fudge factors was determined later, see for example [Tate75].

## 7.1 For Jacobians

In the case of a Jacobian $J$ of a curve $C$ over a number field $K$, the Tamagawa number $c_{\mathfrak{p}}$ can be determined using intersection theory on regular model $\mathcal{C}$ over $\mathcal{O}_{K,\mathfrak{p}}$.

Let $I$ be the set of geometrically irreducible components of the special fibre $\mathcal{C}_{k_{\mathfrak{p}}}$. Let $L$ be an unramified extension of $K$ over, and let $\mathfrak{q}$ be a prime of $L$ extending $\mathfrak{p}$, such that all components in $I$ are defined over $k_{\mathfrak{q}}$. We define the intersection of two such components $D$ and $E$ as

$$\langle D, E\rangle = \iota(D, E)/\log(k_{\mathfrak{q}}),$$

where $\iota$ is as in Def. 5.14, so that $\langle D, E\rangle \in \mathbb{Z}$. The component group of $\Phi$ can now be related to the intersections on the regular model as follows.

**Theorem 7.4** ([BoLi99, Thm. 1.1])**.** *There is an exact sequence of* $\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$*-modules*

$$0 \to \mathrm{im}(\alpha) \to \ker(\beta) \to \Phi(k_{\mathfrak{q}}) \to 0,$$

*where* $\alpha\colon \mathbb{Z}^I \to \mathbb{Z}^I$ *is the linear map which maps a component* $D \in I$ *to* $\sum_{E\in I}\langle D, E\rangle \cdot E \in \mathbb{Z}^I$*, and* $\beta\colon \mathbb{Z}^I \to \mathbb{Z}$ *is the linear map mapping a component* $D \in I$ *to its multiplicity in* $\mathcal{C}_{k_{\mathfrak{q}}}$*.*

*Proof sketch.* The Néron model $\mathcal{J}$ of $J$ is almost equal to the subfunctor of $\mathrm{Pic}_{\mathcal{C}/\mathcal{O}_{k_{\mathfrak{q}}}}$ consisting of divisor classes of total degree 0. If you take a divisor $D$ of total degree 0 and some component $E \in I$, then $\langle D, E\rangle$ does not need to be 0, but the weighted sum of the $\langle D, E\rangle$ must be 0, as $\mathcal{C}_{k_{\mathfrak{q}}}$ has intersection number 0 with every other divisor of total degree 0. In other words, we get a map $\mathrm{Div}^0_{\mathcal{C}/\mathcal{O}_{k_{\mathfrak{q}}}} \to \ker(\beta)$. Moreover, the principal divisors correspond exactly to those in $\mathrm{im}(\alpha)$. So we actually get a map $\mathcal{J} \to \ker(\beta)/\mathrm{im}(\alpha)$.

The identity component $\mathcal{J}^0_{\mathfrak{p}}$ corresponds to those line bundles that have degree 0 on each component in $I$. So now we have a map $\mathcal{J}_{\mathfrak{p}}/\mathcal{J}^0_{\mathfrak{p}} \to \ker(\beta)/\mathrm{im}(\alpha)$. One then needs to show that this map is surjective, and respects the action of the Galois structure. This is all a bit technical and can be found in [BoLi99, BLR90]. □

# 8 L-function

## 8.1 Definitions

Let $A$ be an abelian variety over a number field $K$ of dimension $g$. Let $G = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of $K$. We first define the Tate module as follows.

**Definition 8.1** (Tate module)**.** For a prime $\ell$, the *Tate-$\ell$-module* is the $G$-module defined by

$$T_\ell(A) = \lim_{n \in \mathbb{Z}_{>0}} A[\ell^n](\overline{K}),$$

i.e., its elements are sequences $(t_1, t_2, \ldots)$ of $t_i \in A[\ell^i](\overline{K})$ such that $\ell \cdot t_i = t_{i-1}$ for all $i \geq 2$.

Because $A[\ell^n](\overline{K}) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, there is an isomorphism $T_\ell(A) \cong \mathbb{Z}_\ell^{2g}$ of groups. We define $V_\ell$ to be the $G$-module $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. The dual $\mathrm{Hom}(V_\ell(A), \mathbb{Q}_\ell)$ also has a $G$-module structure:

$$g \cdot \varphi(-) = \varphi(g^{-1} \cdot -), \quad \text{for } \varphi \in \mathrm{Hom}(V_\ell(A), \mathbb{Q}_\ell).$$

Let $\mathfrak{p}$ be a prime of $K$ coprime to $\ell$ and fix an extension $\mathfrak{q}$ of $\mathfrak{p}$ to $\overline{K}$. Let $I_\mathfrak{q} \subset G$ be the inertia group, i.e. the subgroup of $\sigma \in G$ fixing $\mathfrak{q}$ and acting trivially on the residue field $k_\mathfrak{q}$. The Frobenius element of $\mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p})$ lifts to an element $\mathrm{Frob}_\mathfrak{q}$ in $G$, which is only unique up to elements in $I_\mathfrak{q}$.

**Definition 8.2** (Euler factor)**.** We define the *Euler factor* of $A$ at $\mathfrak{p}$ to be

$$P_\mathfrak{p} \coloneqq \det\big(1 - \mathrm{Frob}_\mathfrak{q} \cdot T \mid \mathrm{Hom}(V_\ell(A), \mathbb{Q}_\ell)^{I_v}\big) \in \mathbb{Q}_\ell[T].$$

**Remark 8.3.** The coefficients of this polynomial turn out to lie in $\mathbb{Z}$, and the polynomial does not depend on the choice of $\mathfrak{q}$, $\ell$ or $\mathrm{Frob}_\mathfrak{q}$, as long as $\ell$ is coprime to $\mathfrak{p}$.

The $L$-function can now be defined in terms of these Euler factors.

**Definition 8.4** (L-function)**.** The *$L$-function* of $A$ is defined by

$$L(A, s) = \prod_\mathfrak{p} P_\mathfrak{p}\big((\#k_\mathfrak{p})^{-s}\big)^{-1}.$$

A priori, one can show relatively easy that this gives rise to a holomorphic function on the space $\{z \in \mathbb{C} : \mathrm{Im}(z) > \frac{3}{2}\}$. It is expected that it extends to a holomorphic function on $\mathbb{C}$.

**Conjecture 8.5.** *The $L$-function can be continued to an a holomorphic function $\mathbb{C} \to \mathbb{C}$. Moreover, let*

$$\Lambda(A, s) = \mathrm{Norm}(N)^{s/2} \cdot \big((2\pi)^{-s}\,\Gamma(s)\big)^{g \cdot [K:\mathbb{Q}]} \cdot |\Delta(K)|^{g \cdot s} \cdot L(A, s),$$

*where $N$ is the conductor of $A$ (to be defined later), $\Gamma(s)$ is the usual $\Gamma$-function, and $\Delta(K)$ the discriminant of $K$. Then we have*

$$\Gamma(A, 2 - s) = \varepsilon \cdot \Gamma(A, s) \quad \textit{for all } s \in \mathbb{C}$$

*where $\varepsilon \in \{\pm 1\}$ is the root number of $A$, i.e. $(-1)^{\mathrm{rk}(A) \bmod 2}$.*

One could say that the (norm of the) conductor is the integer that makes the functional equation work; this is what people sometimes call the *analytic conductor*. There is also an algebraic definition of the conductor (and conjecturally this is the same).

**Definition 8.6** (Conductor, [BrKr94])**.** Let $A$ be an abelian variety over a number field $K$. Let $\mathfrak{p}$ be a prime of $K$ and let $\ell$ be a prime of $\mathbb{Z}$ coprime to $\mathfrak{p}$. Consider $V_\ell(A)$ with the action of $\mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p})$. Then the *tame conductor exponent* of $A$ at $\mathfrak{p}$ is

$$\varepsilon(A,\mathfrak{p}) \coloneqq 2g - \dim\bigl(V_\ell(A)^I\bigr)\,,$$

where $I$ is the inertia subgroup.

Moreover, if $L = K_\mathfrak{p}(A[\ell])$, then the *wild/Swan conductor exponent* of $A$ at $\mathfrak{p}$ is

$$\delta(A,\mathfrak{p}) \coloneqq \sum_{i=1}^{\infty} \frac{|G_i|}{|G_0|} \dim\bigl(A[\ell]/A[\ell]^{G_i}\bigr)\,.$$

Here $G_i \subset \mathrm{Gal}(L/K_\mathfrak{p})$ is the $i$-th ramification group

$$G_i \coloneqq \{\sigma \in \mathrm{Gal}(L/K_\mathfrak{p}) : v_L(\sigma(\pi_L) - \pi_L) \geq i+1\},$$

where $\pi_L$ is a uniformiser of $L$ and $v_L$ is the discrete valuation on $L$.

The *conductor exponent* of $A$ at $\mathfrak{p}$ is defined as $f_\mathfrak{p} \coloneqq \varepsilon(A,\mathfrak{p}) + \delta(A,\mathfrak{p})$, and the *conductor* of $A$ is then defined to be the ideal $\prod_\mathfrak{p} \mathfrak{p}^{f_\mathfrak{p}}$.

**Fact 8.7.** If the residue characteristic $p$ of $\mathfrak{p}$ is greater than $2g+1$, then the wild conductor exponent $\delta(A,\mathfrak{p})$ is equal to 0.

**Remark 8.8.** It is also possible to define the Euler factors and the conductor using $H^1(A_{\overline{K}}, \mathbb{Z}_\ell)$ instead of $T_\ell(A)$, as there is a duality between the two groups, see [EMvdG, Chap. 10].

## 8.2 For Jacobians

Let $C$ be a curve over a number field $K$ and let $J$ be its Jacobian. Because $H^1(J_{\overline{K}}, \mathbb{Q}_\ell)$ is isomorphic to $H^1(C_{\overline{K}}, \mathbb{Q}_\ell)$, the computation of the Euler factors can also be done on the curve. Consider a prime $\mathfrak{p}$ of good reduction and let $C_\mathfrak{p}$ be the reduction. Then by the Néron-Ogg-Shafarevich criterion, the action of inertia on $H^1(J_{\overline{K}}, \mathbb{Q}_\ell)$ is trivial, and we need to compute the characteristic polynomial of Frobenius. This essentially comes down to computing the numerator of the zeta function

$$Z(C_\mathfrak{p}, T) \coloneqq \exp\left(\sum_{n=1}^{\infty} \#C_\mathfrak{p}(k_{\mathfrak{p},n}) \cdot \frac{T^n}{n}\right),$$

where $k_{\mathfrak{p},n}$ is the degree $n$ extension field of the residue field $k_\mathfrak{p}$. Because of the functional equation that the zeta function satisfies, it is sufficient to count points in $C_\mathfrak{p}(k_{\mathfrak{p},n})$ for $n = 1, \ldots, g$.

**Remark 8.9.** For elliptic curves, Schoof's algorithm can be used to count points in runtime that is polynomial in $\log(\#k_\mathfrak{p})$. For higher genus curves, there is no practical algorithm that does this in polynomial time. However, if you want to compute the Euler factors for all $p \leq N$ at the same time, there are algorithms that can do that in average polynomial time, see for example [HaSu14].

For the bad primes, there have been several strategies:

- try guessing the conductor exponents and Euler factors until you find a guess that satisfies the functional equation of the $L$-function;
- compute the Euler factors on a regular model of $C$;
- compute the Euler factors on the (semi)stable reduction of $C$.

We will go into more detail on the last two approaches. A good place to read more about this is [BoWe17].

**Lemma 8.10** ([BoWe17, Prop. 2.8])**.** *Suppose that $\mathcal{C}$ is a regular or (semi-)stable model of $C$ over $\mathcal{O}_{K,\mathfrak{p}}$. Suppose that the greatest common divisor of the multiplicities of the components in the special fibre $\mathcal{C}_{k_\mathfrak{p}}$ is 1. Then there is an isomorphism*

$$H^1(C_{\overline{K}}, \mathbb{Q}_\ell)^{I_K} \cong H^1(\mathcal{C}_{\overline{k}_\mathfrak{p}}, \mathbb{Q}_\ell).$$

It then turns out to be possible to determine the Euler factor by point counting on $\mathcal{C}_{\overline{k}_\mathfrak{p}}$, as the Euler factor is essentially the zeta function of $\mathcal{C}_{k_\mathfrak{p}}$.

As a regular model always exists without needing to extend the base field $K$, this method can always be applied in this case. However, a regular model can be computationally expensive to compute. There is also a way to use the stable reduction, even if $C$ does not have stable reduction over $K$.

Suppose that $L/K$ is a Galois extension, such that $C$ has stable reduction over $L$. Let $\mathfrak{q}$ a prime of $L$ extending $\mathfrak{p}$, and let $\mathcal{C}$ be a stable model of $C$ over $\mathcal{O}_{L,\mathfrak{q}}$. In [BoWe17, Thm. 2.4], it is proved that

$$H^1(C_{\overline{K}}, \mathbb{Q}_\ell)^{I_K} \cong H^1(\mathcal{C}_{\overline{k}_\mathfrak{q}}, \mathbb{Q}_\ell)^{I_K} \cong H^1(\mathcal{C}_{\overline{k}_\mathfrak{q}}/I_K, \mathbb{Q}_\ell).$$

The Euler factor can now be determined by counting points on $\mathcal{C}_{k_\mathfrak{q}} / \operatorname{Gal}(L/K)$. Moreover, the tame part of the conductor is

$$2 \cdot \operatorname{genus}(C) - \operatorname{genus}_{\text{arith}}(\mathcal{C}_{\overline{k}_\mathfrak{q}}/I_K) - \operatorname{genus}_{\text{geom}}(\mathcal{C}_{\overline{k}_\mathfrak{q}}/I_K).$$

For the wild part of the conductor, you also need to compute the genera of the curves $\mathcal{C}_{\overline{k}_\mathfrak{q}}/G_i$, where $G_i \subset I_K$ is the $i$-th ramification group, see also [BoWe17, Thm. 2.9].

# 9 What is known about BSD?

The most prominent result on the Birch and Swinnerton-Dyer conjecture is the statement that the conjecture holds for elliptic curves of analytic rank 0 and 1. The proof, which is the accumulation of work by Gross-Zagier, Kolyvagin, and others, uses modularity, Heegner points, and Euler systems. While there is not enough time in the course to discuss these in full detail, I will make an attempt to convey some of the ideas behind them.

There are also some other things known about the conjecture. For example, it is known that the conjecture holds for an abelian variety $A$ over a number field $K$, if and only if it holds for an $K$-isogenous abelian variety, or in the case of a field extension $K/L$ for the Weil restriction $\operatorname{Res}_{K/L} A$ of $A$. In certain cases, there are also things known about the parity (odd/even) of the rank of an elliptic curve. Finally, the conjecture can be viewed as a special case of the Bloch-Kato conjecture.

## 9.1 Modularity

Let $N$ be an intgeer. There is an algebraic curve $Y_0(N)$ over $\mathbb{Z}[1/N]$ whose points correspond to pairs $(E, \varphi\colon E \to E')$ of an elliptic curve $E$ together with an $N$-isogeny $\varphi$. Complex analytically this corresponds to the quotient $\mathcal{H}/\Gamma_0(N)$, where $\mathcal{H}$ is the upper half plane $\{\mathrm{im}(z) > 0\}$, and

$$\Gamma_0 = \left\{ M \in \mathrm{SL}_2(\mathbb{Z}) : M \equiv \begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix} \mod N \right\}.$$

This curve can be compactified into a projective curve $X_0(N)$ by also allowing "generalised elliptic curves", which are isomorphic to an $n$-gon of $\mathbb{P}^1$s.

**Theorem 9.1** (modularity theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with conductor $N$. Then there exists a surjective map $X_0(N) \to E$.*

The modularity theorem, or Shimura-Taniyama conjecture, was proved first for semi-stable curves by Wiles and Taylor in 1995, as part of the proof of Fermat's last theorem, and later in full generality by Breuil, Conrad, Diamond, and Taylor in 2001. As a consequence of the modularity theorem, the $L$-function of $E$ will be equal to the $L$-function of a certain modular form of weight 2, and we get the following.

**Corollary 9.2.** *The $L$-function of $E$ extends to an analytic function $\mathbb{C} \to \mathbb{C}$.*

## 9.2 Heegner points

Let $N$ be the conductor of an elliptic curve $E$ over $\mathbb{Q}$. Let $K$ be an imaginary quadratic number field, such that every prime $p \mid N$ splits in $\mathcal{O}_K$. Then there exists an ideal $\mathfrak{N}$ such that

$$\mathcal{O}_K/\mathfrak{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

Embedding $K$ into $\mathbb{C}$, we get an $N$-isogeny of elliptic curves over $\mathbb{C}$:

$$\varphi\colon \mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{N}^{-1}.$$

By the theory of complex multiplication the curves $\mathbb{C}/\mathcal{O}_K$ and $\mathbb{C}/\mathfrak{N}^{-1}$, and the map $\varphi$ can be defined over the *Hilbert class field* $H$ of $K$. This field $H$ is the maximal abelian unramified extension of $K$ and the Galois group $\mathrm{Gal}(H/K)$ is isomorphic to the class group of $\mathcal{O}_K$.

The pair $(\mathbb{C}/\mathcal{O}_K, \varphi)$ now corresponds to a point $x_1 \in X_0(N)(H)$. Under the map $X_0(N) \to E$, this point maps to a point $y_1 \in E(H)$. Let $y := \mathrm{tr}_{H/K}(y_1) \in E(K)$.

**Theorem 9.3** (Gross-Zagier)**.** *Let $\omega$ be a minimal differential on $E$. Let $c$ be the Manin constant of $E$.*[8]

$$L'(E/K, 1) = \frac{2\left(\int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}\right) h_{\mathrm{NT}}(y)}{c^2 \cdot |\mathcal{O}_K^*/\{\pm 1\}| \cdot \sqrt{|\Delta_K|}}.$$

This means that if the analytic rank of $E$ over $K$ is 1, then we just found a point of infinite order, and a relation between its Néron-Tate height, some periods and the leading coefficient of the $L$-function at $s = 1$.

[8] This constant is known to be an integer and is conjectured to always be 1.

**Theorem 9.4** ([Mil11, Thm. 4.4])**.** *If* $\mathrm{rk}_{\mathrm{an}}(E) \leq 1$*, then we can choose* $K$ *in such a way that* $\mathrm{rk}_{\mathrm{an}}(E_K) = 1$*.*

*Proof idea.* If $E'$ is the $K$-quadratic twist of $E$, then $\mathrm{rk}_{\mathrm{an}}(E_K) = \mathrm{rk}_{\mathrm{an}}(E) + \mathrm{rk}_{\mathrm{an}}(E')$. The $L$-function of $E'$ can be obtained from the $L$-function of $E$ by multiplying its coefficients with the values of a quadratic character $\chi$. This twisted $L$-function is then studies in work of Waldspurger for $\mathrm{rk}_{\mathrm{an}} = 1$ and work of Bump, Friedberg, and Hoffstein for $\mathrm{rk}_{\mathrm{an}} = 0$ to show that $K$ exists. □

In case $\mathrm{rk}_{\mathrm{an}}(E) = 1$, it then turns out that the point $y$ actually descends to a point in $E(\mathbb{Q})$ up to torsion, see [Dar04, Prop. 3.11], so we can now use this to find a point in $E(\mathbb{Q})$ of infinite order.

## 9.3 Euler systems

Recall that the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is the subgroup of torsors in $H^1(G_{\mathbb{Q}}, E_{\overline{Q}})$ that have points everywhere locally. Moreover, we have an exact sequence

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

The way to show that $E$ has rank 0 or 1 equal to the analytic rank, and that $Ш(E/\mathbb{Q})$ is finite is by showing that $\mathrm{Sel}_\ell(E) \cong (\mathbb{Z}/\ell\mathbb{Z})^{\mathrm{rk}_{\mathrm{an}}(E)}$ for all but finitely many primes $\ell$, and by giving bounds for $n = p^n$ for the finitely many previously excluded primes $p$.

The construction of the Heegner point above can be generalised by replacing the maximal order $\mathcal{O}_K$ by the order $\mathcal{O}_{k,n} \coloneqq \mathbb{Z} + n\mathcal{O}_K$. This gives rise to a sequence of points $y_n \in E(H_n)$, where $H_n$ is a so-called *ring class field* of $\mathcal{O}_{k,n}$; it is a Galois extension of $H$.

Now, for any finite Galois module $T$ and any place $v$, there is a pairing induced by the cup product

$$\langle \cdot, \cdot \rangle_v \colon H^1(G_{\mathbb{Q}_v}, T) \times H^1(G_{\mathbb{Q}_v}, T^*) \to H^2(G_{\mathbb{Q}_v}, \mathbb{G}_{\mathrm{m}}) \cong \mathbb{Q}/\mathbb{Z}.$$

The (very rough) idea to bound the Selmer group is to use the Heegner points $y_n$ to find elements $h \in H^1(G_{\mathbb{Q}}, E[n])$ which have the property that

$$\sum_v \langle h_v, \sigma_v \rangle_v = 0,$$

for all $\sigma \in \mathrm{Sel}_n(E)$. This relation can then be used to bound the order of $\mathrm{Sel}_n(E)$. To learn more about this, I can recommend [Dar04] or [Rub00].

## 9.4 BSD is invariant under isogeny

The Birch and Swinnerton-Dyer conjecture is invariant under isogeny. The full proof for the following theorem can be found in [Mil06].

**Theorem 9.5** ([Mil06, Thm. 7.3])**.** *Let* $A$ *and* $B$ *be two* $K$*-isogenous abelian varieties. Then BSD holds for* $A$ *if and only if it holds for* $B$*.*

*Proof.* Let $f \colon A \to B$ be an isogeny. For any $\ell$ coprime to $\deg(f)$ the Tate-$\ell$-modules $V_\ell(A)$ and $V_\ell(B)$ are isomorphic, so the $L$-functions of $A$ and $B$ are the same. The map

$$f(K) \colon A(K) \to B(K)$$

has finite kernel and cokernel, so the algebraic ranks of $A$ and $B$ are also the same. Finally the kernel of $Ш(f)\colon Ш(A) \to Ш(B)$ is contained in the image of the map

$$H^1(G_K, \ker(f)) \to H^1(G_K, A),$$

coming from the long exact sequence coming from $0 \to \ker(f) \to A \to B \to 0$. As $H^1(G_K, \ker(f))$ is finite, this implies that $Ш(A)$ is finite if $Ш(B)$ is, and vice verse considering the dual isogeny $f^\vee$. The order of $Ш(A)$ and $Ш(B)$ need not be equal, and differ by a factor

$$\frac{|\ker(Ш(f))|}{|\mathrm{coker}(Ш(f))|} = \frac{|\ker(Ш(f))|}{|\ker(Ш(f^\vee))|}.$$

Careful analysis of the interaction of the Néron-Tate height pairing with the isogeny $f$ will show that

$$\frac{R_A}{|A_{\mathrm{tors}}(K)| \cdot |A^\vee_{\mathrm{tors}}(K)|} = \frac{|\ker(f(K))| \cdot |\mathrm{coker}(f^\vee(K))|}{|\ker(f^\vee(K))| \cdot |\mathrm{coker}(f(K))|} \cdot \frac{R_B}{|B_{\mathrm{tors}}(K)| \cdot |B^\vee_{\mathrm{tors}}(K)|}.$$

Finally, the period and Tamagawa numbers change as follows:

$$P_A \cdot \prod_p c_p(A) = \prod_v \frac{|\ker(f(K_v))|}{|\mathrm{coker}(f(K_v))|} \cdot P_B \cdot \prod_p c_p(B).$$

Finally, using a large commutative diagram and group cohomology, one finally shows that

$$\prod_v \frac{|\ker(f(K_v))|}{|\mathrm{coker}(f(K_v))|} \cdot \frac{|\ker(Ш(f))|}{|\ker(Ш(f^\vee))|} = \frac{|\ker(f(K))| \cdot |\mathrm{coker}(f^\vee(K))|}{|\ker(f^\vee(K))| \cdot |\mathrm{coker}(f(K))|},$$

which finishes the proof. □

## 9.5 BSD and Weil restriction

Let $L/K$ be a finite extension of number fields.

**Definition 9.6** (Weil restriction)**.** Let $X$ be a scheme over $L$, then the *Weil restriction* or *restrictions of scalars* $\mathrm{Res}_{L/K}(X)$ is a scheme over $K$ for which

$$\mathrm{Res}_{L/K}(X)(T) = X(T \times_K L)$$

for any $K$-scheme $T$.

**Example 9.7.** Let $\mathbb{G}_{\mathrm{m}} = Z(xy-1) \subset \mathbb{A}^2_{\mathbb{Q}(i)}$ be the multiplicative group over $\mathbb{Q}(i)$. To determine $\mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{G}_{\mathrm{m}})$, we introduce new variables $x_1, x_i, y_1, y_i$ and we substitute $x = x_1 + i \cdot x_i$ and $y = y_1 + i \cdot y_i$. The relation then becomes

$$1 + i \cdot 0 = (x_1 + i \cdot x_i)(y_1 + i \cdot y_i).$$

Then $\mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{G}_{\mathrm{m}})$ is the subscheme $Z(x_1y_1 - x_iy_i - 1, x_1y_i + x_iy_1)$ of $\mathbb{A}^4_{\mathbb{Q}}$.

**Theorem 9.8** ([Mil72, Thm. 1])**.** *Let $A$ be an abelian variety over $L$. Then BSD holds for $A$ if and only if BSD holds for* $\mathrm{Res}_{L/K}(A)$.

**Corollary 9.9.** *Suppose $L/K$ is quadratic*[9] *and $A$ is an abelian variety over $K$. Then BSD holds for $A_L$ if and only if BSD holds for both $A$ and the $L$-quadratic twist $A'$ of $A$.*

*Proof.* BSD holds for $A_L$ if and only if it holds for $\mathrm{Res}_{L/K}(A_L)$. Because $\mathrm{Res}_{L/K}(A_L)$ is isogenous to $A \times A'$, the result now follows. □

[9] A similar statement can be made for larger extensions, but then the 'twists' involved could actually be abelian varieties of higher dimension.

## 9.6 Parity

The parity conjecture is all about the sign $\varepsilon(A/K)$ occurring in the conjectural functional equation of the $L$-function. There is a conjecture of what this sign should be, and this is denoted by $w(A/K)$ and is called the *global root number of $A$ over $K$*. This sign is defined as a product $\prod_v w(A/K_v)$ of local root numbers. The exact definition for these local root numbers is too complicated for this lecture, see [DokT13].

**Fact 9.10.** For a elliptic curve $E$ with semi-stable reduction, the local root number is 1 if $v$ is non-archimedean and $E$ has good or non-split multiplicative reduction, and $-1$ if $v$ is either archimedean, or $E$ has split multiplicative reduction.

If you believe in the BSD conjecture, then you will also believe the following.

**Conjecture 9.11** (Parity conjecture)**.**

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

Similarly, one can define the $p^\infty$-Selmer rank $\mathrm{rk}_p(A/K)$ as the dimension of the vector space

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{\mathbb{Z}_p}\Big(\lim_n \mathrm{Sel}_{p^n}(A/K), \mathbb{Q}_p/\mathbb{Z}_p\Big).$$

If Ш is finite, then $\mathrm{rk}_p(A/K)$ is equal to $\mathrm{rk}(A/K)$.

**Conjecture 9.12** ($p$-parity conjecture)**.**

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

**Theorem 9.13** (Dokchitser-Dokchitser)**.** *The $p$-parity conjecture is true for all elliptic curves over $\mathbb{Q}$ and all primes $p$.*

The following example demonstrates how you can get the parity of the rank of an elliptic curve, assuming finiteness of Ш, from local computations. Similar methods can be used for the $p^\infty$-Selmer rank.

**Example 9.14** ([DokT13, Subsect. 1.3])**.** Consider two elliptic curves $E$ and $E'$ over $\mathbb{Q}$ with Cremona labels 91b1 and 91b2. There exists a 3-isogeny $\varphi\colon E \to E'$ between them. Assume that $Ш(E/\mathbb{Q})$ and $Ш(E'/\mathbb{Q})$ is finite. Even if we don't know if BSD holds for $E$ and $E'$, we actually do know that the quotient of the terms on the right hand side of the BSD formula (1.0.1) is 1, see subsection 9.4.

$$\frac{R_E}{R_{E'}} = \frac{P_{E'}}{P_E} \cdot \frac{\prod_p c_p(E')}{\prod_p c_p(E)} \cdot \frac{|Ш(E'/\mathbb{Q})|}{|Ш(E/\mathbb{Q})|} \cdot \frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2}{|E'(\mathbb{Q})_{\mathrm{tors}}|^2}. \tag{9.6.1}$$

It is relatively easy to compute $\frac{P_E}{P_{E'}}$ and all $c_p(E)$ and $c_p(E')$. Moreover, the other two factors on the right hand side of (9.6.1) are squares. Doing this, we find that

$$\frac{R_E}{R_{E'}} \in 3 \cdot \mathbb{Q}^{*2}.$$

On the other hand, let $\varphi^\vee$ be the dual isogeny and $P_1, \dots, P_{\mathrm{rk}(E)}$ be generators of the free part of $E(\mathbb{Q})$. Then

$$\begin{aligned} 3^{\mathrm{rk(E)}} \cdot R_E &= \det(\langle 3P_i, P_j\rangle)_{i,j} = \det(\langle \varphi^\vee\varphi(P_i), P_j\rangle)_{i,j} \\ &= \det(\langle \varphi(P_i), \varphi(P_j)\rangle)_{i,j} = R_{E'} \cdot [E'(\mathbb{Q})_{\mathrm{free}} : \varphi(E(\mathbb{Q})_{\mathrm{free}})]^2. \end{aligned}$$

Altogether, we deduce from this that $\mathrm{rk}(E) = \mathrm{rk}(E')$ must be odd.

## 9.7 Relation with Bloch-Kato

What follows here is a very rough interpretation of what is written in [LoZe23]. Consult this source and other sources for more complete information.

The Bloch-Kato conjecture is some very general conjecture relating the $L$-function $L(V^*(1), s)$ to a so-called Bloch-Kato Selmer group $H^1_f(G_K, V)$ associated to some geometric representation $V$ (e.g. $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p(n))$ for some smooth projective variety $X/K$):

$$\dim(H^1_f(G_K, V)) - \dim(H^0(G_K, V)) = \text{ord}_{s=0}(L(V^*(1), s).$$

**Example 9.15.** Let $V = \mathrm{Q}_p(1)$. In this case it turns out that $\text{ord}_{s=0}(L(V^*(1), s)) = r_1 + r_2 - 1$, where $r_1$ and $r_2$ are the number of real and complex places of $K$. Moreover, we also get that $\dim(H^0) = 0$ and $\dim(H^1_f) = \text{rk}(\mathcal{O}_K^*)$. So the Bloch-Kato conjecture becomes Dirichlet's unit theorem.

**Example 9.16.** Take $V = V_p(E)$. Then $\dim(H^0) = 0$, and $H^1_f$ is a certain Selmer group whose rank is equal to $\text{rk}(E)$ if $Ш(E/K)[p^\infty]$ is finite. Finally $\text{ord}_{s=0}(L(V^*(1), s)) = \text{ord}_{s=1}L(E/K, s)$, which demonstrates that Bloch-Kato is a variant of the BSD conjecture.

# References


[HyperUser] Alex J. Best; Alexander L. Betts, Matthew Bisatt, Raymond van Bommel, Vladimir Dokchitser, Omri Faraggi, Sabrina Kunzweiler, Céline Maistret, Adam Morgan, Simone Muselli, Sarah Nowell, A user's guide to the local arithmetic of hyperelliptic curves, *Bull. Lond. Math. Soc.* **54** (2022), no. 3, 825–867.

[vB18] Raymond van Bommel, *Models of curves: the Birch and Swinnerton-Dyer conjecture & ordinary reduction.* PhD thesis.

[vBHM20] Raymond van Bommel, David Holmes, J. Steffen Müller, Explicit arithmetic intersection theory and computation of Néron-Tate heights, *Math. Comp.* **89** (2020), no. 321, 395–410.

[BoLi99] S. Bosch, Q. Liu, Rational points of the group of components of a Néron model. *Manuscripta Math.* **98** (1999), no. 3, 275–293.

[BLR90] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models.* Springer-Verlag, Berlin, 1990.

[BoWe17] Irene I. Bouw, S. Wewers, Computing $L$-functions and semistable reduction of superelliptic curves, *Glasg. Math. J.* **59** (2017), no. 1, 77–108.

[BrKr94] Armand Brumer, Kenneth Kramer, The conductor of an abelian variety, *Compositio Math.* **92** (1994), no. 2, 227–248.

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, John Voight, Rigorous computation of the endomorphism ring of a Jacobian, *Math. Comp.* **88** (2019), 1303–1339.

[CFOSS08] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, M. Stoll, Explicit $n$-descent on elliptic curves. I. Algebra, *J. Reine Angew. Math.* **615** (2008), 121–155.

[Dar04] Henri Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, 101, Conf. Board Math. Sci., Washington, DC, 2004 Amer. Math. Soc., Providence, RI, 2004.

[DokT11] Tim Dokchitser, Models of curves over discrete valuation rings, *Duke Math. J.* **170** (2021), no. 11, 2519–2574.

[DokT13] Tim Dokchitser, Notes on the parity conjecture, in *Elliptic curves, Hilbert modular forms and Galois deformations*, 201–249, Adv. Courses Math. CRM Barcelona, Birkhäuser/Springer, Basel, 2013.

[EMvdG] Bas Edixhoven, Ben Moonen, Gerard van der Geer. *Abelian varieties.* `http://van-der-geer.nl/~gerard/AV.pdf`

[HaSu14] David Harvey, Andrew V. Sutherland, Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, *LMS J. Comput. Math.* **17** (2014), 257–273.

[HiSi00] M. Hindry, J. H. Silverman. *Diophantine geometry. An introduction.* Springer-Verlag, New York, 2000.

[Lang83] S. Lang, *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[Lang88] Serge Lang, *Introduction to Arakelov theory.* Springer-Verlag, New York, 1988.

[Liu02] Qing Liu, *Algebraic Geometry and Arithmetic Curves.* Oxford University Press, Oxford, 2002. Translated by R. Erné.

[LoZe23] David Loeffler, Sarah Livia Zerbes, Euler systems and the Bloch-Kato conjecture for automorphic Galois representations, in *ICM—International Congress of Mathematicians. Vol. 3. Sections 1–4*, 1918–1939, EMS Press, Berlin, 2023.

[Mil11] Robert L. Miller, Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one, *LMS J. Comput. Math.* **14** (2011), 327–350.

[Mil72] J. S. Milne, On the arithmetic of abelian varieties, *Invent. Math.* **17** (1972), 177–190.

[Mil06] J. S. Milne, *Arithmetic duality theorems*, second edition, BookSurge, Charleston, SC, 2006.

[Nér65] A. Néron, Quasi-fonctions et hauteurs sur les Variétés abéliennes. *Ann. of Math.* **82** (1965), no. 2, 249–331.

[Ols16] Martin Olsson, *Algebraic spaces and stacks*, American Mathematical Society Colloquium Publications, 62, Amer. Math. Soc., Providence, RI, 2016.

[PoSt99] Bjorn Poonen, Michael Stoll, The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)* **150** (1999), no. 3, 1109–1149.

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies Hermann Weyl Lectures. The Institute for Advanced Study, 147, Princeton Univ. Press, Princeton, NJ, 2000

[Silv09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second edition, Grad. Texts in Math., 106, Springer, Dordrecht, 2009.

[Tate75] J. T. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pp. 33–52, Lecture Notes in Math., Vol. 476, Springer, Berlin-New York.