Iwasawa Theory for Elliptic Curves and BSD(p)

Daniele CASAZZA
casazza.daniele@gmail.com

Advised by Prof. Jean GILLIBERT

ALGANT Master Thesis - July 2013
Università degli Studi di Milano and Université Bordeaux 1

Iwasawa Theory for Elliptic Curves and BSD(p)

Daniele Casazza

July 1, 2013

Contents

Introduction

The theory of diophantine equation is about finding integral solution to algebraic equations. Among all these, elliptic curves provide an example in which the elementary request of finding all solution to some equation gives rise to a very rich theory, which had been developed during the last centuries, and provides a motivational task to find new tools that can be used also in other settings.

In our specific case, the goal is simple: given a number field K and two elements $a, b \in K$, we want to find all K-rational points of the elliptic curve given by the cubic equation:

$$E : y^2 = x^3 + ax + b, \quad \text{with } 4a^3 + 27b^2 \neq 0$$

The nice thing is that we can study this object as an algebraic variety over K and so use the tools of algebraic geometry in order to find informations. But the main tool that we have here, is the definition of a group law on the set of K-rational points of the curve. Thanks to the group law one proves the following result:

Theorem 0.0.1 (Mordell-Weil) The group $E(K)$ is finitely generated, hence $E(K)_{\text{tors}}$ is finite and there exists an isomorphism:

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\text{tors}}$$

for some integer $r \geqslant 0$, that ones calls the rank of the curve.

This theorem has a nice consequence: even if the elliptic curve has infinitely many rational points, it is sufficient to know a suitable finite subset of them in order to build them all.

The proof of the Mordell-Weil theorem is not effective. The interesting thing is that if we knew exactly the rank r we could compute $E(K)$. More precisely, using Galois cohomology we have a short exact sequence:

$$0 \to E(K)/mE(K) \to S^m(E/K) \to Ш(E/K)[m] \to 0$$

where $S^m(E/K)$ is the m-Selmer group and $Ш(E/K)$ is the Shafarevich-Tate group (see chapter 2). The m-Selmer is known to be finite, but the problem is that the m-part of the Shafarevich-Tate group is not always zero. Because of this and since it's difficult to see whether an element of the Selmer group goes to zero or not in the Shafarevich-Tate group, we cannot compute exactly r and find the generators of $E(K)$.

Then comes the L-function, denoted by $L(E/K, s)$ which is a complex analytic function. This function was used in order to state the so called Birch and Swinnerton-Dyer conjecture:

Conjecture 0.0.2 (BSD) The function $L(E/K, s)$ has a zero of order equal to the rank of the curve E/K at $s = 1$ and, moreover, we have a formula for the leading term of the expansion of the function at $s = 1$

The beautiful thing of the conjecture is this relation between an analytic object, defined locally, and the rank, a global algebraic invariant. Moreover, the leading term formula contains some of the most important invariant of the curve and provides, in this sense, an analogue to the class number formula for number fields.

Unfortunately this conjecture is only known to hold in very few cases. Results from Kolyvagin and Gross-Zaiger prove the rank part of the conjecture when the order of the zero of $L(E/K, s)$ at $s = 1$ is at most 1. But nothing is known in general or for higher rank curves. This leaded experts to the formulation of a p-adic analogue of the conjecture, that is, replacing the complex L-function by some p-adic L-function. Using Iwasawa theory we can define power series $f_E(T)$ for which we have the following:

Theorem 0.0.3 If the p-adic regulator is non-zero and the p-primary part of $Ш(E/K)$ is finite, then the order of $f_E(T)$ at $T = 0$ is r if p is a good ordinary prime and $r + 1$ if p is split-multiplicative. Moreover the p-adic valuation of the leading term of the expansion of the power series is the same as the valuation of a product of global invariants similar to the ones of conjecture 0.0.2.

The problem of this is that $f_E(T)$ is defined as a generator of the characteristic ideal of the Selmer group, hence it's not canonical. It turns out that we can define analytically a function that we call p-adic L-function attached to E/K and denote by $L_p(E, T)$, which is related to the power series $f_E(T)$ in the sense that:

Conjecture 0.0.4 There exists $u(T) \in \mathbb{Z}_p[[T]]^\times$ such that $L_p(E,T) = and$

$$L_p(E,T) = \begin{cases} \mathfrak{f}_E \cdot u(T), & \text{if } p \text{ is good ordinary;} \\ \mathfrak{f}_E \cdot T \cdot u(T), & \text{if } p \text{ is split-multiplicative.} \end{cases}$$

A positive answer to this conjecture would provide a canonical choice for the generator of the characteristic ideal of the Selmer group. Moreover this would allow to define a p-adic analogue of the Birch and Swinnerton-Dyer conjecture involving an exact formula for the leading term, not just its p-adic valuation.

Chapter 1

Analytic World and Modularity Theorem

The goal of this chapter is to expose in a quick way (as quick as possible) the basic definitions of analytic nature that arises while studying elliptic curves. The main object of the chapter is to provide an exposition of the basic analytical instruments that will be used in this treatment and, specifically, talk about the Tanyiama-Shimura-Weil conjecture, which has been proven joining the contribution of several mathematicians (Wiles, Taylor, Breuil, Conrad, Diamond) and is now known as:

Theorem 1.0.5 (of Modularity) Every elliptic curve over $\mathbb{Q}$ is modular.

This statement is that for every elliptic curve $E/\mathbb{Q}$ we have a rational parametrization given by a surjective rational morphism defined over $\mathbb{Q}$:

$$X_0(N) \longrightarrow E$$

for some N positive integer, where $X_0(N)$ is a the modular curve of level N. In order to give an exposition of these topic, we start recalling the upper half plane, modular forms and all the tools needed for this goal. Most of this chapter can be found, in slight different ways, in basic textbooks on these topics, such as [Sil94], [Dia05]. For some notation we will follow part of [MTT86].

1.1 Upper Half Plane, Modular Group and Quotients

Let us consider:

$$\mathcal{H} := \{z \in \mathbb{C} \mid \mathfrak{Im}(z) > 0\} \subset \mathcal{H}^*$$

we usually refer to points in $\mathcal{H}^* - \mathcal{H}$ as *cusps*. Then $GL_2(\mathbb{Q})^+$ (matrices with positive determinant) acts on $\mathcal{H}^*$ in the following way:

$$Az = \begin{bmatrix} a & b \\ c & d \end{bmatrix} z := \frac{az+b}{cz+d}$$

It is easy to see that it is an action, since $\det A > 0$ and that it sends cusps to cusps. Moreover, if we fix some positive integer k, given a function f on $\mathcal{H}^*$ we can define an action of $GL_2(\mathbb{Q})^+$ by:

$$f \circ [A]_k := \rho(A)^k f(Az), \qquad \rho(A) := \frac{\det(A)^{1/2}}{cz+d} \tag{1.1}$$

Let's now consider $G < \Gamma(1) := SL_2(\mathbb{Z})$ a subgroup of finite index (not excluding $\Gamma(1)$ itself). Then we say that:

Definition 1.1.1 A meromorphic function $f : \mathcal{H}^* \to \mathbb{C}$ is a *weakly modular function of weight* k *for* G if:

$$f \circ [A]_k = f, \quad \forall A \in G$$

i.e. that $f(Az) = (cz+d)^k f(z)$.

Remark 1.1.1 (Fourier Expansion at ∞) $\Gamma(1)$ is generated by the matrices:

$$S := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad T := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Since G is of finite index in $\Gamma(1)$ and S is of finite order, it means that exist a minimal (positive) integer h such that $T^h \in G$, which means that if f is weakly modular for G:

$$f(z+h) = f(z)$$

then, if we call $q_h := e^{2\pi i z/h}$, then we can expand in Fourier series f at ∞ as:

$$\sum_{n \geqslant M} a_n q_h^n$$

for some $M \in \mathbb{Z}$.

Remark 1.1.2 If $r = a/c \in \mathbb{Q}$ is a cusp, then $\exists A \in \Gamma(1)$ such that: $Ar = \infty$.

Definition 1.1.2 We say that a f is holomorphic at a cusp r if the function $f \circ [A]_k$ is holomorphic at ∞, i.e. it has a Fourier expansion for $n \geqslant 0$.

Definition 1.1.3 We say that a weakly modular function f of weight k for G is:

- a *modular form of weight* k *with respect to* G if it is holomorphic on $\mathcal{H}$ and at all cusps; Let's denote the group of these functions as $M_k(G)$;
- a *cusp form of weight* k *with respect to* G if it is a modular form of weight k with respect to G and, moreover, it vanishes at all cusps, i.e. the Fourier expansions are for $n \geqslant 1$; Let's denote the group of these functions as $S_k(G)$.

Of course we have $S_k(G) < M_k(G)$ and since $M_k(G)M_l(G) \subset M_{k+l}(G)$, $S_k(G)M_l(G) \subset S_{k+l}(G)$, we have a structure of graded ring on:

$$M(G) := \bigoplus_{k \in \mathbb{Z}} M_k(G)$$

for which $S(G) := \oplus S_k(G)$ is an ideal.

Let's consider the topology of $\mathcal{H}^*$ given by usual neighborhoods for $z \in \mathcal{H}$, $S_M := \{z \in \mathcal{H} \mid \Im(z) > M\} \cup \{\infty\}$ give neighborhoods of ∞ and for $A \in \Gamma$ such that $A\infty = r \in \mathbb{Q}$, $A(S_M)$ is a neighborhood of r.

Now we consider the quotient of $\mathcal{H}^*$ by the continuous action of G:

$$\pi : \mathcal{H}^* \to G \setminus \mathcal{H}^* =: X(G) \equiv X_G$$

Since the action is totally discontinuous, X_G is a compact Riemann surface. In particular, since a fundamental domain for the action of $\Gamma(1)$ is:

$$\mathcal{D} := \{z = x + iy \in \mathcal{H} \mid |x| < 1/2, |z| \geqslant 1\} \cup \{\infty\}$$

then for a generic finite index subgroup G, if we let $\{M_i\}_{i=1,\dots,e}$ be right coset representatives for G in $\Gamma(1)$, the fundamental domain is: $\cup M_i\mathcal{D}$.

1.2 Diamond Operator, Hecke Operator and Normalized Eingenforms

Definition 1.2.1 Pick $N \in \mathbb{Z}$ positive, we define:

$$\Gamma(N) := \{A \in \Gamma(1) \mid A \equiv 1 \pmod N\}$$

And we say that $G < \Gamma(1)$ is a *congruence subgroup* if $\Gamma(N) \subset G$ for some $N \in \mathbb{Z}$.

From now on we are going to consider the congruence subgroups of Γ denoted by:

$$\Gamma_0(N) := \{A \in \Gamma(1) \mid c \equiv 0 \pmod N\}$$

and:

$$\Gamma_1(N) := \left\{A \in \Gamma(1) \mid A \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod N\right\}$$

if $G = \Gamma_0(N)$ we denote X_G by $X_0(N)$.

Lemma 1.2.1 We have the following short exact sequence:

$$1 \to \Gamma_1(N) \to \Gamma_0(N) \to \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^{\times} \to 1$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d$$

Proof Straightforward. □

This means that for $f \in M_k(\Gamma_1(N))$, the action of $\Gamma_0(N)$ is in fact the action of $(\mathbb{Z}/N\mathbb{Z})^{\times}$, so that we can define the Diamond Operator as:

$$\langle d \rangle f := f \circ [A]_k$$

with:

$$A = \begin{bmatrix} a & b \\ c & \delta \end{bmatrix} \in \Gamma_0(N), \quad \delta \equiv d \pmod N$$

which turns $M_k(\Gamma_1(N))$ into a $\mathbb{C}[(\mathbb{Z}/N\mathbb{Z})^{\times}]-module$ and therefore we can decompose it into:

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})}^{\times}} M_k(N, \chi)$$

The same holds for $S_k(\Gamma_1(N))$. Take then $f \in M_k(N, \chi)$ and define the *Hecke operator* T_p, for p prime, to be:

$$T_p(f) := p^{k/2-1}\left(\sum_{u=0}^{p-1} f \circ \begin{bmatrix} 1 & u \\ 0 & p \end{bmatrix}_k + \chi(p) f \circ \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}_k\right) \tag{1.2}$$

which preserves $M_k(N, \chi)$ (the same for $S_k(N, \chi)$) and whose action commutes with the diamond operator. Moreover, $T_p T_q = T_q T_p$ if p and q are distinct primes. Moreover we can define T_{p^k} inductively and so also $T_{mn} := T_m T_n$, hence T_n, for every n.

We can decompose the space of cusp forms into:

$$S_2(\Gamma_1(N)) = S_2(\Gamma_1(N))^{\text{new}} \oplus S_2(\Gamma_1(N))^{\text{old}}$$

where $S_2(\Gamma_1(N))^{\text{old}}$ denotes the space of *oldforms*, the forms of level N which are image of lower level forms and the space $S_2(\Gamma_1(N))^{\text{new}}$ of *newform* (for further details on all of this part, see [Dia05, 5.5]). The Hecke operators respect these subspaces and we have:

Theorem 1.2.2 The space $S_k(\Gamma_1(N))$ admit an orthogonal basis of simultaneous eigenforms for the Hecke operators $\{\langle n\rangle, T_n \mid (n, N) = 1\}$. This is true also for $S_2(\Gamma_1(N))^{\text{old}}$ and $S_2(\Gamma_1(N))^{\text{new}}$ separately. Moreover, for $S_2(\Gamma_1(N))^{\text{new}}$ this holds for every n.

Proof See [Dia05, 5.5.4, 5.6.3, 5.8.2]. □

Definition 1.2.2 Given $f \in M_k(\Gamma_1(N))$ we say that it is an *Hecke eigenform* if it is eigenform for all T_n and $\langle n\rangle$. If, moreover, the first Fourier coefficient satisfies $a_1(f) = 1$ we say that it is a *normalized Hecke eigenform*, or simply *normalized eigenform*. If, moreover, f is in the space of newforms, we simply say that it is a *newform*.

Remark 1.2.3 (Action of T_p on the Fourier coefficients) Take $f \in S_k(N, \chi)$. Then we can expand it as:

$$f(q) = \sum_{n \geqslant 1} a_n(f) q^n$$

where $q = e^{2\pi i z}$. Then, the action of the T_p operators on the coefficients is given by:

$$a_n(T_p f) = a_{np}(f) + \chi(p) p^{k-1} a_{n/p}(f)$$

where $a_{n/p} := 0$ if $p \nmid n$.

In particular, $a_1(T_p f) = a_p(f) \equiv a_p$. This means that if f is a normalized eigenform then we have:

$$T_p f = a_p(f) f \equiv a_p f$$

and so, for all p prime, $a_1(T_p f) = a_p(f)$ is the eigenvalue of f.

1.3 $X_0(N)$ as Algebraic Curve and Modularity Theorem

All the ingredients coming from the previous sections can be interpreted in a different and geometric way. If we consider $G = \Gamma_0(N)$, then we have:

$$Y_0(N) := \Gamma_0(N) \setminus \mathcal{H} \subset X_0(N) := X_{\Gamma_0(N)} = \Gamma_0(N) \setminus \mathcal{H}^*$$

and $X_0(N)$ is a compact Riemann surface. It turns out that we can build $Y_0(N)$ as the data of isomorphism classes of Elliptic Curves over $\mathbb{C}$ (so complex tori) plus a cyclic subgroup of order N, i.e. $y \in Y_0(N)$ can be viewed as:

$$y = (\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \langle 1/N \rangle)$$

where $\tau \in \mathcal{H}$ is any lift of y via the quotient map. In this way, one can also re-interpret the action of Hecke operators and this description carries over to the algebraic context.

Using Serre's GAGA theory (see [Ser56]), one sees that $X_0(N)$ can be defined algebraically over $\mathbb{C}$ and then, by using explicit equation as in [Dia05, 7] one can see that the curve is actually defined over $\mathbb{Q}$ (actually $\mathbb{Z}[1/N]$).

Moreover, if we consider a differential form on $X_0(N)$, we can see that it corresponds, pulling back via the quotient map:

$$\pi : \mathcal{H}^* \to X_0(N)$$

to something of the form $f(z)dz$ and since it must be invariant under the action of $\Gamma_0(N)$ and we have:

$$d(Az) = \rho(A)^{-2} dz$$

we find that f must be a modular function of weight 2. If we ask, moreover, ω to be an holomorphic differential, we can see that $f \in S_2(\Gamma_0(N))$, because:

$$\pi^*(\omega) = f(z)dz$$

with $f \in M_2(\Gamma_0(N))$ and to have it holomorphic also at the cusps we find, from:

$$2\pi i dz = q^{-1} dq$$

that:

$$f dz = \frac{1}{2\pi i} \sum_{n \in \mathbb{Z}} a_n q^n \frac{dq}{q}$$

so that it is holomorphic if and only if $a_0 = 0$, i.e. $f \in S_2(\Gamma_0(N))$. In this sense, the space of holomorphic differentials on $X_0(N)$ can be identified with the space of cusp forms of weight 2.

We have now all the ingredients necessary for the statement of (one version of) the modularity theorem:

Theorem 1.3.1 Let $E/\mathbb{Q}$ be an elliptic curve. For some $N \in \mathbb{N}$ there exist a surjective morphism of curves over $\mathbb{Q}$:

$$\pi : X_0(N) \to E$$

The map π is called *modular parametrization of* E.

Definition 1.3.1 The smallest N for which we have a modular parametrization of E is called the *analytic conductor or* E.

1.4 L-functions attached to Elliptic Curves

We are going to define L-series attached to E/K, with K number field, following the path that can be found in [Sil86]. After this we will only be interested in the case $K = \mathbb{Q}$.

Notation We consider finite places υ of K and we denote by E_υ the reduction of the curve at the residue field k_υ, and with $q_\upsilon = \# k_\upsilon$. We consider the unique extension of degree n of k_υ and denote it by $k_{\upsilon,n}$.

We can define the Z-function of E_υ elliptic curve (i.e. E has good reduction at υ) to be:

$$Z(E_\upsilon/k_\upsilon) := \exp\left(\sum_{n=1}^{\infty} \# E(k_{\upsilon,n}) \frac{T^n}{n}\right)$$

and we know that it is a rational function (Weil conjectures, now proved. See [Sil86, 5]). If we consider the Frobenius: $\phi : E \to E$, sending $(x, y) \mapsto (x^{q_\upsilon}, y^{q_\upsilon})$, then we know that its characteristic polynomial is:

$$X^2 - a_\upsilon X + q_\upsilon$$

where $a_\upsilon = q_\upsilon + 1 - \#E(k_\upsilon)$ and we have the equation:

$$Z(E_\upsilon/k_\upsilon) = \frac{1 - a_\upsilon T + q_\upsilon T^2}{(1-T)(1-q_\upsilon T)}$$

so that we have the local factor for the L-function which is:

$$L_\upsilon(E, T) = 1 - a_\upsilon T + q_\upsilon T^2$$

and we can extend the definition to the bad reduction case as:

$$L_\upsilon(E, T) = \begin{cases} 1, & \text{if } E \text{ has additive reduction at } \upsilon \\ 1 - T, & \text{if } F \text{ has split multiplicative reduction at } \upsilon \\ 1 + T, & \text{if } F \text{ has non-split multiplicative reduction at } \upsilon \end{cases}$$

Definition 1.4.1 We define the L-function attached to E/K to be:

$$L_{E/K}(s) := \prod_{\upsilon \text{ finite}} \frac{1}{L_\upsilon(E, q_\upsilon^{-s})}$$

Remark 1.4.1 If we write it explicitly for the case $K = \mathbb{Q}$, we have the product:

$$L_{E/\mathbb{Q}}(s) \equiv L(E, s) = \prod_{p \text{ good}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \text{ split}} \frac{1}{1 - p^{-s}} \prod_{p \text{ non-split}} \frac{1}{1 + p^{-s}} \tag{1.3}$$

where $a_p = p + 1 - N_p$. What happens if $s = 1$? In that case, the denominators of the components of the product are exactly:

$$L_p(E, p^{-1}) = \frac{\#E^{ns}(\mathbb{F}_p)}{p}$$

so that, somehow, the L-function contains, at $s = 1$, the information about the number of non singular points of each reduction modulo p. In this sense, it contains local informations.

Proposition 1.4.2 The product of $L_{E/K}(s)$ converges for $\mathfrak{Re}(s) > 3/2$.

Consider now the conductor of the curve, an invariant that can be defined using Galois representation. Thanks to the Ogg-Saito theorem, it can be expressed as:

$$N_{E/K} = \prod_{\upsilon \text{ finite}} \mathfrak{p}_\upsilon^{f_\upsilon}$$

where $f_\upsilon = \mathrm{ord}_\upsilon(\Delta) + 1 - m_\upsilon$, where Δ minimal discriminant and m_υ is the number of irreducible components of the special fiber of the minimal Néron model of E at υ. In fact we have, for $p \neq 2, 3$, that:

$$f_\upsilon = \begin{cases} 0 & \text{if } E \text{ has good reduction at } \upsilon \\ 1, & \text{if } F \text{ has multiplicative reduction at } \upsilon \\ 2, & \text{if } F \text{ has additive reduction at } \upsilon \end{cases}$$

the cases $p = 2, 3$ are quite peculiar (see [Sil94, IV, 10] for further details). Take $K = \mathbb{Q}$ and $N_E := N_{E/\mathbb{Q}}$, then we can slightly modify the L-function, in this way:

$$\xi(E, s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$$

where $\Gamma(s)$ denotes the Gamma function. We notice that we added this factor:

$$L_\infty(E, s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)$$

Then we have the following:

Conjecture 1.4.3 The function $L(E, s)$ can be continued analytically to the entire complex plane $\mathbb{C}$ and satisfies the functional equation:

$$\xi(E, s) = \omega\xi(E, 2 - s)$$

with $\omega = \pm 1$.

1.5 L-functions attached to Modular Forms

One can actually find a solution to the last conjecture in the case of a modular curve, i.e. an Elliptic curve having a modular parametrization by some $X_0(N)$. To do this we consider now $f \in S_2(N, \chi)$ to be a normalized Hecke eigenform. Then we can expand it, at ∞, as Fourier series:

$$f(q) = \sum_{n \geqslant 1} c_n q^n$$

with $q = e^{2\pi i z}$, $c_1 = 1$ and c_p is the eigenvalue for the operator T_p as in remark 1.2.3.

Definition 1.5.1 We define the L-series attached to f to be:

$$L(f,s) := \sum_{n\geqslant 1} \frac{c_n}{n^s}$$

Given a dirichlet character ψ we can define the twisted L-function as:

$$L(f,\psi,s) := \sum_{n\geqslant 1} \frac{\psi(n)c_n}{n^s}$$

Proposition 1.5.1 The L-series $L(f,s)$ converges for $\mathfrak{Re}(z) > 2$ and admit an Euler product expansion:

$$L(f,s) = \prod_p \frac{1}{1 - c_p p^{-s} + \chi(p)p^{1-2s}} \tag{1.4}$$

One immediately notice the similarity between (1.4) and (1.3). That is, in fact, a part of the modularity theorem.

Definition 1.5.2 (Mellin Transform) The Mellin Transform of f is defined to be:

$$\text{Mel}(f)(s) := \int_0^\infty f(it)t^s \frac{dt}{t}$$

When $f \in S_2(N,\chi)$ it turns out that we have:

$$\text{Mel}(f)(s) = (2\pi)^s\Gamma(s)L(f,s) \tag{1.5}$$

Considering the involution $f(z) \mapsto f(-1/Nz)$ we can divide the space of weight 2 cusps as:

$$S_2(N,\chi) = S_2(N,\chi)^+ \oplus S_2(N,\chi)^-$$

and we have the following:

Proposition 1.5.2 $L(f,s)$ can be continued analytically to the entire $\mathbb{C}$ and if we write:

$$\Lambda(f,s) := N^{s/2}\text{Mel}(f)(s) = N^{s/2}(2\pi)^s\Gamma(s)L(f,s)$$

we have:

$$\Lambda(f,2-s) = \varepsilon\Lambda(f,s)$$

where $f \in S_2(N,\chi)^\varepsilon$, $\varepsilon = \pm 1$.

This implies that for modular elliptic curves E we have actually a functional equation which relates $L(E,s)$ and $L(E,2-s)$ as we expressed in the conjecture. Actually, if we restrict our attention to curves over $\mathbb{Q}$, we can restate the Modularity Theorem in this way:

Theorem 1.5.3 (Modularity Theorem) Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E, $L(E,s) = \sum_{n \geqslant 1} c_n n^{-s}$ the L-series expansion of the product, let $f(z) \equiv f_E(z) := \sum c_n q^n$ be the inverse of the Mellin transform of $L(E,s)$. Then:

- $f(z) \in S_2(\Gamma_0(N_E))$ is a normalized Hecke eigenform (moreover, a newform);

- Let ω_E be the invariant differential of $E/\mathbb{Q}$. There exists a finite morphism over $\mathbb{Q}$:
$$\pi : X_0(N_E) \to E$$
such that: $\pi^*(\omega_E) = c_\pi 2\pi i f(z) dz$. c_π is called the *Manin constant* and it is conjectured to be equal to 1;

- $L(f,s) = L(E,s)$, so that $f \in S_2(N_E, 1_{N_E})$, with 1_{N_E} the trivial character of conductor N_E.

Chapter 2

Algebraic World and BSD(∞)-conjecture

On Elliptic Curves we can put several different structures. The main structure is the group law and a lot of job can be done thanks to this, by applying group cohomology and finding invariants of the curve which allows us also to do computations. In this chapter we sketch some important result in this direction and expose the classical version Birch and Swinnerton-Dyer conjecture, which we denote by BSD or, in the following chapters, BSD(∞) to distinguish it from the p-adic version.

2.1 Finiteness of the Selmer Group

We introduce now the 2 main algebraic structures attached to an elliptic curve that will be deeply involved in the following treatment, the Selmer and the Shafarevich-Tate group. We will also provide the main steps of the proof of the finiteness of the Selmer group, following Milne ([Mil96]). We'll not go into the details of this but we are going to introduce the ingredients that are in fact used in the proof, because the same objects are involved into the BSD conjecture. Let's consider now a number field K and let be $\bar{K}$ it's algebrac closure. We have the following lemma:

Lemma 2.1.1 The following sequence is exact:

$$0 \to E(\bar{K})[n] \to E(\bar{K}) \xrightarrow{n} E(\bar{K}) \to 0$$

Let us denote $G_k = Gal(\bar{K} \mid K)$ and the Galois cohomology by $H^n(G_k, -) = H^n(K, -)$. Thanks to the lemma we obtain a long exact sequence in cohomology:

$$0 \to E(K)[n] \to E(K) \to E(K) \to H^1(K, E(\bar{K})[n]) \to H^1(K, E(\bar{K})) \xrightarrow{n} H^1(K, E(\bar{K}))$$

From which we can extract the following short exact sequence, denoting for simplicity $E \equiv E(\bar{K})$:

$$0 \to E(K)/nE(K) \to H^1(K, E[n]) \to H^1(K, E)[n] \to 0$$

Since this holds also for local fields we can consider the map induced by $K \to K_v$ and so we get the localization diagram:

$$\begin{tikzcd}
0 \arrow[r] & E(K)/nE(K) \arrow[r] \arrow[d] & H^1(K, E[n]) \arrow[r] \arrow[d] & H^1(K, E)[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K_v)/nE(K_v) \arrow[r] & H^1(K_v, E[n]) \arrow[r] & H^1(K_v, E)[n] \arrow[r] & 0
\end{tikzcd}$$

where we denote, with abuse of notation, E to be the elliptic curve on the algebraically closed field.

Definition 2.1.1 We call n-*Selmer Group* and *Shafarevich-Tate group* of E/K respectively the groups which makes these sequences exact:

$$0 \to S^n(E/K) \to H^1(K, E[n]) \to \prod_v H^1(K_v, E)[n]$$

$$0 \to Ш(E/K) \to H^1(K, E) \to \prod_v H^1(K_v, E)$$

Proposition 2.1.2 One has the following short exact sequence:

$$0 \to E(K)/nE(K) \to S^n(E/K) \to Ш(E/K)[n] \to 0$$

Proof Apply the kernel-cokernel sequence to:

$$H^1(K, E[n]) \to H^1(K, E)[n] \to \prod_v H^1(K_v, E)[n]$$

□

Proposition 2.1.3 For $L \mid K$ Galois extension the kernel:

$$\Phi := \ker\left(S^n(E/K) \to S^n(E/L)\right)$$

is finite.

Proof We have the diagram:

$$\begin{tikzcd}
0 \arrow[r] & \Phi \arrow[r] \arrow[d] & S^n(E/K) \arrow[r] \arrow[d, hook] & S^n(E/L) \arrow[d, hook] \\
0 \arrow[r] & H^1(Gal(L/K), E[n]) \arrow[r] & H^1(K, E[n]) \arrow[r] & H^1(L, E[n])
\end{tikzcd}$$

so that $\Phi \subset H^1(Gal(L \mid K), E[n])$, and the latter finite, because $Gal(L \mid K)$ and $E[n]$ are both finite. □

In order to prove finiteness of Selmer Group is then sufficient to consider $L \mid K$ finite, large enough so that $E[n] \subset E(L)$. Using the Weil pairing one can show that $\mu_n \subset L$, i.e. the ground field contains all n-roots of unity and we can use Kummer sequence, which implies:

Lemma 2.1.4 We have an isomorphism (*Kummer theory*):

$$L^\times/(L^\times)^n \xrightarrow{\sim} H^1(L, \mu_n)$$

given by: $x \mapsto (\sigma \mapsto \sigma(x)/x)$, which gives the isomorphism:

$$H^1(L, E[n]) \simeq \frac{L^\times}{(L^\times)^n} \times \frac{L^\times}{(L^\times)^n}$$

Proof For the first part, apply group cohomology for the sequence:

$$1 \to \mu_n \to \bar{L}^\times \xrightarrow{n} \bar{L}^\times \to 1$$

For the second part, notice that chosen a basis we can write $E[n] \simeq \mu_n \times \mu_n$ with the trivial action and cohomology commutes with products. □

Remark 2.1.5 From elementary algebraic number theory for a number field L with ring of integers R, units U and ideal class group C, we have the exact sequence:

$$1 \to U \to L^\times \xrightarrow{x \mapsto v(x)} \bigoplus_{v} \mathbb{Z} \to C \to 0$$

with U finitely generated (Dirichlet Unit Theorem, see [Jan96], [Mil]) and C finite (finiteness of the ideal class group, see [Jan96], [Mil]). If we consider a finite set of places T, write R_T for the ring of T-integers of R:

$$R_T := \{x \in K(R) \mid v(x) \leqslant 1, \forall v \notin T\}$$

and denote by C_T its ideal class group, we find the following exact sequence:

$$1 \to U_T \to L^\times \xrightarrow{x \mapsto v(x)} \bigoplus_{v \notin T} \mathbb{Z} \to C_T \to 0$$

with U_T finitely generated and C_T finite (use kernel-cokernel sequence, see [Mil96, 4]).

Lemma 2.1.6 For T finite set of places containing the infinite places, let be Θ such that:

$$1 \to \Theta \to L^\times/(L^\times)^n \xrightarrow{x \mapsto v(x) \pmod{n}} \bigoplus_{v \notin T} \mathbb{Z}/n\mathbb{Z}$$

Then there is an exact sequence:

$$1 \to U_T/U_T^n \to \Theta \to C_T[n]$$

so that Θ is finite.

Proof Double the sequence of the previous remark, connect the two with multiplication by n and apply the snake lemma (see [Mil96, 4]). □

Lemma 2.1.7 The Selmer Group $S^n(E/K)$ is finite.

Proof After passing to a suitable extension $L \mid K$, pick $T := \{v \mid 2n\Delta\}$ where Δ is the discriminant of E/L and then one prove that $S^n(E/L) \subset \Theta$, because it is unramified outside T ([Mil96, prop. 3.6]). □

Corollary 2.1.8 (Weak Mordell-Weil Theorem) For K number field, $m \in \mathbb{N}$, $E(K)/mE(K)$ is finite.

Before going on with some remark in the technics used to prove the Mordell-Weil theorem, we remark just a couple of result concerning the Shafarevich-Tate group. As always, K is a number field:

Proposition 2.1.9 $Ш(E/K)$ is a torsion abelian group and $Ш(E/K)[m]$ is finite for every $m > 1$.

Proof The fact that it is torsion directly follows by the definition, since:

$$Ш(E/K) \subset H^1(K, E)$$

and the latter is the cohomology of a profinite group, hence it is obtained as limit from finite quotients, hence is torsion. The finiteness of the m-torsion part comes from the exact sequence in proposition 2.1.2. □

Conjecture 2.1.10 $Ш(E/K)$ is finite.

This is of crucial importance for the BSD conjecture that we are about to formulate, because the cardinality of the Shafarevich-Tate group plays a role in that formula. After this, a theorem of Cassels asserts that:

Theorem 2.1.11 (Cassels) If $\#Ш(E/K)$ is finite, then it is a perfect square.

2.2 Mordell-Weil Theorem

Theorem 2.2.1 (Descent Theorem) Let $A \in$ **Ab**. Suppose there exists a *Height Function*:

$$h : A \to \mathbb{R}$$

such that:

(i) Let $Q \in A$, then $\exists C_1 = C_1(A, Q)$ such that:

$$h(P+Q) \leqslant 2h(P) + C_1, \quad \forall P \in A$$

(ii) $\exists n \geqslant 2$ and $C_2 = C_2(A)$ such that:

$$h(nP) \geqslant n^2 h(P) - C_2, \quad \forall P \in A$$

(iii) $\forall C_3$ constant, the set:

$$\{P \in A \mid h(P) \leqslant C_3\}$$

is finite

Suppose further that for the integer n of (ii) we have A/nA finite, then A is finitely generated.

Then to prove that $E(K)$ is finitely generated it is sufficient to find a height function which satisfies the hypothesis of the descent theorem above. We are not going to analyze the details of the proof, but we'll define here the height function needed and talk about the canonical height.

Definition 2.2.1 We call *local degree at* υ the number: $m_\upsilon := [K_\upsilon : \mathbb{Q}_\upsilon]$.

Proposition 2.2.2 For $L \mid K$ number field extension we have:

$$\sum_{\substack{\omega \in L \\ \omega \mid \upsilon}} m_\omega = [L : K] m_\upsilon$$

Proof See [Lan94]. □

Proposition 2.2.3 (Product Formula) If $x \in K^\times$ then we have:

$$\prod_{\upsilon} |x|_\upsilon^{m_\upsilon} = 1$$

Proof See [Lan94]. □

Definition 2.2.2 Let $P = [x_0, \ldots, x_N] \in \mathbb{P}^N(K)$, with $x_i \in K$, we define the *height of* P *relative to* K to be:

$$H_K(P) := \prod_{v} \max_i\{|x_i|_v\}^{n_v}$$

The previous proposition allow us to give the following:

Definition 2.2.3 We define the *absolute height* of $P \in \mathbb{P}^N(\bar{Q})$ to be:

$$H(P) := H_K(P)^{1/[K:\mathbb{Q}]}$$

for K such that $P \in \mathbb{P}^N(K)$ ($H(P) \geqslant 1$).

Definition 2.2.4 We call the *logarithmic height of* P the map:

$$\begin{aligned} h : \mathbb{P}^N(\bar{Q}) &\to \mathbb{R} \\ P &\mapsto h(P) := \log H(P) \end{aligned}$$

Let's be given a surjective morphism $f \in \bar{K}(E)$:

$$\begin{aligned} f : E &\to \mathbb{P}^1 \\ P &\mapsto \begin{cases} [1,0], & \text{if } P \text{ is a pole for } f \\ [f(P),1], & \text{otherwise} \end{cases} \end{aligned}$$

Definition 2.2.5 We call the *height on* E *relative to* f the function:

$$h_f(P) := h(f(P))$$

Theorem 2.2.4 Let be f an even function, i.e. invariant via the multiplication of $[-1]$ on E, then the height function h_f respects the hypothesis of the descent theorem.

Proof See [Sil86, VIII.6]. □

Corollary 2.2.5 (Mordell-Weil Theorem) The group $E(K)$ is finitely generated, hence there exists an isomorphism:

$$E(K) \simeq \mathbb{Z}^r \oplus E(K)_{\text{tors}}$$

where $r \equiv r(E/K)$ is called the *algebraic rank*, or simply rank, of the curve E/K and $E(K)_{\text{tors}}$ is finite.

Proof Use the weak version and then chose a non-constant even function on E, for example the x-coordinate function, then apply the theorem. □

2.3 Canonical Height and Regulator

Proposition 2.3.1 Let $f \in K(E)$ be a non-constant even function, $P \in E(\bar{K})$. Then the limit:

$$\widehat{h}_f(P) := \frac{1}{\deg f} \lim_{N \to infty} 4^{-N} h_f([2^N]P)$$

exists and it is independent on the choice of f

Proof Prove it is Cauchy for the existence. □

Definition 2.3.1 The *canonical* or *Néron-Tate height* on E/K is the function:

$$\widehat{h} \equiv \widehat{h}_E : E(\bar{K}) \to \mathbb{R}$$

defined by the previous limit.

Theorem 2.3.2 (Néron-Tate) Let be $\widehat{h}$ the canonical height on E/K, then:

(a) $\forall P, Q \in E(\bar{K})$ we have the parallelogram law:

$$\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$$

(b) $\forall P \in E(\bar{K}), m \in \mathbb{Z}$ we have:

$$\widehat{h}([n]P) = n^2 \widehat{h}(P)$$

(c) $\widehat{h}$ is a quadratic form on $E(K)$, i.e. $\widehat{h}$ even and gives a bilinear pairing:

$$\langle -, - \rangle : E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}$$

defined by $\langle P, Q \rangle = \widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)$.

(d) $\widehat{h}(E(\bar{K})) \subset \mathbb{R}^+$ and $\widehat{h}(P) = 0$ if and only if $P \in E(\bar{K})_{\text{tors}}$.

(e) Given $f \in K(E)$ even, then:

$$(\deg f)\widehat{h} = h_f + C$$

for some constant $C \equiv C(E, f)$.

Moreover, if $\widehat{h}'$ is any other function satisfying (e) for some f and (b) for some $m \geqslant 2$, then $\widehat{h}' = \widehat{h}$, i.e. it is

Proof It is just computational, using the definitions of h_f and $\widehat{h}$. □

Remark 2.3.3 This provide a correction to the h_f height which is bilinear up to constant, so not really bilinear. In this way we find moreover something which is independent on the choice of f. Furthermore, one can easily see that we can define as the only map for which (e) and (b) hold for some f and m.

Remark 2.3.4 Thanks to the Mordell-Weil theorem, $E(K) \otimes \mathbb{R}$ is finite dimensional over $\mathbb{R}$ and $\widehat{h}$ extends uniquely from the lattice $E(K)_{\text{free}}$ to the whole $E(K) \otimes \mathbb{R}$ and provide a bilinear form which is, indeed, positive definite. Then we can compute the volume of the lattice using $\widehat{h}$.

Definition 2.3.2 We call *elliptic regulator of* E/K, denoted by $\mathcal{R}_{E/K}$ the volume of the lattice $E(K)_{\text{free}}$ in $E(K) \otimes \mathbb{R}$ computed using $\widehat{h}$. Then it is equal to:

$$\mathcal{R}_{E/K} = \det\left(\langle P_i, P_j \rangle\right)$$

where $P_1, \ldots, P_r$ are generators for $E(K)_{\text{free}}$ ($= 1$ if $r = 0$).

2.4 Classical BSD conjecture

Let's consider now $E/\mathbb{Q}$ and denote by $E/\mathbb{Z}$ it's Néron model. Then it's minimal Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

provide the Néron differential:

$$\omega_E = \frac{dx}{2y + a_1x + a_3}$$

If we denote with $E(\mathbb{C})^{\pm}$ the ± 1-eigen-subgroups of $E(\mathbb{C})$ under the action of the complex conjugation involution, we define:

$$\Omega_E^{\pm} := \int_{E(\mathbb{C})^{\pm}} \omega_E$$

to be the positive *real* and *imaginary* periods. Denote by m_l the Tamagawa numbers of E, i.e. the number of connected $\mathbb{F}_l$-rational components of the Néron fiber. Moreover call:

$$L^{(k)}(E) = \frac{1}{k!}\frac{d^k}{ds^k}L(E,s)\mid_{s=1}$$

Then we have the following:

Conjecture 2.4.1 (Birch and Swinnerton-Dyer) We have $L^{(k)}(E) = 0$ for $k < r = r(E/\mathbb{Q})$ and:

$$L^{(r)}(E) = \#Ш(E/\mathbb{Q}) \cdot \frac{\mathcal{R}_{E/\mathbb{Q}}}{\#E(\mathbb{Q})^2_{\text{tors}}} \cdot \big(\prod_{l} m_l\big) \cdot \Omega_E^+$$

Chapter 3

Modular Symbol and BSD(p)

In this chapter we are going to describe a p-adic Birch and Swinnerton-Dyer conjecture when p is either a good prime or a prime of multiplicative reduction. In fact it should be better to say that we are going to state the Mazur-Tate-Teitelbaum conjecture, from the paper [MTT86], which provide a p-adic analogue to the classical version.

In particular, this chapter provide a detailed treatment of the p-adic L-function attached to the elliptic curves, viewed as in [MTT86]. This approach seems to be artificial, not natural at all and somehow magic, but we'll see in the next chapter that it is in fact just an expression of a more canonical machinery.

For this chapter we basically follow the treatment of [MTT86], showing some result in a very specific case, which is the one that really interest us for the BSD(p).

3.1 Modular Symbols and Complex L-functions

In this section we present a special case of some result of Mazur-Tate-Teitelbaum (see [MTT86]). Let's write $S_2 = \sum_{N,\chi} S_2(\Gamma_1(N), \chi)$. Remember the action of $GL_2(\mathbb{Q})$ on f defined as in (1.1) and simplify notation with $f \mid A := f \circ [A]_2$, then:

$$(f \mid A)(z)dz = f(Az)d(Az)$$

Definition 3.1.1 (Modular Integral) We can define:

$$\begin{aligned} \phi : S_2 \times \mathbb{P}^1(\mathbb{Q}) &\longrightarrow \mathbb{C} \\ (f, r) &\longmapsto \phi(f, r) \end{aligned}$$

given by:

$$\phi(f,r) = 2\pi i \int_{\infty}^{r} f(z)dz = \begin{cases} 2\pi \int_0^{\infty} f(r+it)dt, & \text{if } r \in \mathbb{Q}; \\ 0, & \text{if } r = \infty \end{cases}$$

Proposition 3.1.1 We have:

- $\phi(f,r)$ is linear in f, $\forall r \in \mathbb{P}^1(\mathbb{Q})$;
- $\phi(f \mid A, r) = \phi(f, Ar) - \phi(f, A\infty)$.

Proof First part is obvious from the definition, since the integral is linear in f. For the second part we have:

$$\phi(f \mid A, r) = 2\pi i \int_{\infty}^{r} (f \mid A)(z)dz = 2\pi i \int_{\infty}^{r} f(Az)d(Az) = 2\pi i \int_{A\infty}^{Ar} f(z)dz =$$
$$= 2\pi i \int_{\infty}^{Ar} f(z)dz - 2\pi i \int_{\infty}^{A\infty} f(z)dz = \phi(f, Ar) - \phi(f, A\infty)$$

where the split of the integral can be done since $\mathcal{H}^*$ is simply connected. □

Definition 3.1.2 Call $L_f := \phi(f, \mathbb{P}^1(\mathbb{Q}))$ the *module of values of* f.

Proposition 3.1.2 L_f is finitely generated as $\mathbb{Z}[\chi]$-module. A set of generators is given by:

$$\phi(f, A_j\infty) - \phi(f, A_j 0) \tag{3.1}$$

where A_j provide a set of representatives for $\Gamma_0(N)$ in $\Gamma(1) = SL_2(\mathbb{Z})$.

Proof Let first of all $f \in S_2(N, \chi)$, then pick:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$$

and call $\chi(A) := \chi(d)$, then $f \mid A = \chi(A)f$, then by proposition 3.1.1 we have that:

$$\chi(A)\phi(f,r) = \phi(f \mid A, r) = \phi(f, Ar) - \phi(f, A\infty)$$

which proves that L_f is a $\mathbb{Z}[\chi]$-module.

Now let denote by $L_f^0 \subset L_f$ the $\mathbb{Z}[\chi]$-module generated by the quantities (3.1). If $a, m \in \mathbb{Z}$, $m \geqslant 0$, $(a, m) = 1$, we must show, for the reverse inclusion, that:

$$\phi(f, a/m) \in L_f^0$$

In order to do that, we proceed by induction on m. If $m = 0$ then $\phi(f, a/m) = 0$. Let's take $m > 0$, and suppose $m' \in \mathbb{Z}$ such that $am' \equiv 1 \pmod{m}$ and $0 \leqslant m' < m$. Let be $a' := (am' - 1)/m$, then define:

$$A := \begin{bmatrix} a & a' \\ m & m' \end{bmatrix}$$

Then we have $A = BA_j$ for some of the chosen representatives A_j, $B \in \Gamma_0(N)$. Then we have:

$$\begin{aligned}\phi(f, a/m) - \phi(f, a'/m') = \phi(f, A\infty) - \phi(f, A0) = \phi(f, BA_j\infty) - \phi(f, BA_j0) = \\ = \chi(B)[\phi(f, A_j\infty) - \phi(f, A_j0)]\end{aligned}$$

and by induction hypothesis, $\phi(f, a'/m') \in L_f^0$, hence $\phi(f, a/m) \in L_f^0$, so that $L_f^0 = L_f$.

If now $f \in S_2$, then it is a finite sum of eigenforms, so that L_f is again finitely generated. □

Definition 3.1.3 (Modular Symbols) Let $a, m \in \mathbb{Q}$, $m > 0$. We set the *modular symbol* to be the mapping:

$$\lambda(f; a, m) \equiv \lambda_f(a, m) := \phi(f, -a/m) = 2\pi i \int_{\infty}^{-\frac{a}{m}} f(z)dz = \phi\left(f \circ \begin{bmatrix} 1 & -a \\ 0 & m \end{bmatrix}_2 ; 0\right)$$

Remark 3.1.3 Obviously the modular symbol is homogeneous in a and m, in the sense that $\forall t \in \mathbb{Q}^+$ we have:

$$\lambda_f(ta, tm) = \phi(f, ta/tm) = \phi(f, a/m) = \lambda_f(a, m)$$

Proposition 3.1.4 For fixed f, for $a, m \in \mathbb{Z}$, $m > 0$, then $\lambda_f(a, m)$ takes values in L_f and it only depends on the class of $a \pmod{m}$.

Proof Use the definition 3.1.3 to see that it takes values in L_f. For the second part, notice that:

$$f \mid \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = f, \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -a \\ 0 & m \end{bmatrix} = \begin{bmatrix} 1 & -a+m \\ 0 & m \end{bmatrix}$$

so that, again using 3.1.3:

$$\lambda_f(a, m) = \phi\left(f \mid \begin{bmatrix} 1 & -a \\ 0 & m \end{bmatrix}, 0\right) = \phi\left(f \mid \begin{bmatrix} 1 & -a+m \\ 0 & m \end{bmatrix}, 0\right) = \lambda_f(a - m, m)$$ □

Proposition 3.1.5 Given $f \in S_2(N, \chi)$ and a prime number p, we have:

$$\lambda(T_p(f); a, m) = \sum_{u=0}^{p-1} \lambda(f; a - um, pm) + \chi(p)\lambda(f; a, m/p)$$

and so $L_{T_p(f)} \subset L_f$.

Proof Straightforward, using the definition of the operator T_p given in equation (1.2), the linearity of λ in f. □

The first link with the classical L-function is an interpolation property given by the easy:

Proposition 3.1.6 $L(f, 1) = \lambda_f(0, 1) = \phi_f(0)$

Proof Using Mellin transform (definition 1.5.2) and, in particular, the result of equation (1.5) with $s = 1$, you get the result, simply noticing that:

$$\mathrm{Mel}(f, 1) = \phi_f(0)$$ □

Remark 3.1.7 As was said at the beginning of the section, the paper of Mazur, Tate and Teitelbaum provide a more general definition of modular symbol which can be used to evaluate L-function attached to cusps of weight k in the points $0 \leqslant j \leqslant k - 2$. For further details, see [MTT86, I.7].

3.2 Twists

Let be ψ a Dirichlet character modulo m.

Definition 3.2.1 (Gauss sums) For $n \in \mathbb{Z}$ we define the Gauss sums:

$$\tau(n, \psi) := \sum_{a \pmod m} \psi(a) e^{2\pi i n a/m}$$

$$\tau(\psi) := \tau(1, \psi)$$

Proposition 3.2.1 If $(n, m) = 1$ and ψ any character modulo m:

$$\tau(n, \psi) = \overline{\psi}(n)\tau(\psi)$$

Proof We have:

$$\tau(n,\psi) = \sum_{a[m]} \psi(a)e^{2\pi i n a/m} = \overline{\psi(n)} \sum_{na[m]} \psi(na)e^{2\pi i n a/m} =$$
$$= \overline{\psi(n)} \sum_{a[m]} \psi(a)e^{2\pi i a/m} = \overline{\psi(n)}\tau(\psi)$$

where the last passage holds because $(n, m) = 1$. □

Lemma 3.2.2 Let ψ be a Dirichlet character of conductor m, $n \mid m$, then we have:

$$\sum_{\substack{a[m] \\ a\equiv b[n]}} \psi(a) = 0$$

for every $b \in \mathbb{Z}/n\mathbb{Z}$.

Proof If $(b, m) \neq 1$, then there is nothing to prove. If $(b, m) = 1$ then we can find $1 \neq t \in \mathbb{Z}/m\mathbb{Z}$ such that $t \equiv 1 \pmod n$. For this t, we have that $\psi(t) \neq 1$, otherwise its conductor would be $< m$. Then we find:

$$\psi(t) \sum_{\substack{a[m] \\ a\equiv b[n]}} \psi(a) = \sum_{\substack{a[m] \\ a\equiv b[n]}} \psi(at) = \sum_{\substack{a[m] \\ a\equiv b[n]}} \psi(a)$$

which implies that the sum is 0. □

Proposition 3.2.3 $\tau(n, \psi) = \overline{\psi(n)}\tau(\psi)$, for every $n \in \mathbb{Z}$ if and only if ψ is primitive modulo m. Moreover we have:

$$|\tau(\psi)|^2 = \psi(-1)\tau(\psi)\tau(\overline{\psi})$$

Proof For the first part we divide in cases. If ψ is primitive modulo m and $(m, n) = 1$, then we are done by proposition 3.2.1. If $(m, n) = d \neq 1$, then we have $\overline{\psi}(n) = 0$ then we have to prove that $\tau(n, \psi) = 0$. In order to do that we see that we can suppose that $n \mid m$, since:

$$\sum_{a[m]} \psi(a)e^{2\pi i a n/m} = \overline{\psi(n/d)} \sum_{a[m]} \psi(a)e^{2\pi i a d/m}$$

Then, if $n \mid m$, say $m = nk$ we find:

$$\sum_{a[m]} \psi(a)e^{2\pi i a/(k)} = \sum_{b[k]} e^{2\pi i a/k} \sum_{\substack{a[m] \\ a\equiv b[k]}} \psi(a)$$

and the latter is zero by the lemma 3.2.2.

To prove the converse, i.e. that if $\tau(n,\psi) = \overline{\psi(n)}\tau(\psi)$ holds for every $n \in \mathbb{Z}$ then ψ is primitive modulo m, simply notice that if it's not primitive, the last computation is non-zero for some $n \mid m$, then $\tau(n,\psi) \neq 0$ but $\overline{\psi(n)} = 0$.

For the last equality use the first with $n = -1$. □

Definition 3.2.2 Given $f(z) = \sum_{n\geqslant 1} a_n e^{2\pi i n z} \in S_2$ and ψ character modulo m, we define:

$$f_\psi(z) = \sum_{n\geqslant 1} \psi(n) a_n e^{2\pi i n z}$$

Remark 3.2.4 Notice that we have:

$$L(f_\psi, s) = L(f, \psi, s)$$

Lemma 3.2.5 (Birch's Lemma) For $f \in S_2$, ψ primitive character modulo m, we have:

$$f_{\overline{\psi}}(z) = \frac{1}{\tau(\psi)} \sum_{a[m]} \psi(a) f\Big(z + \frac{a}{m}\Big)$$

Proof Using the proposition 3.2.3, we find:

$$\begin{aligned} f_{\overline{\psi}}(z) &= \sum_{n\geqslant 1} \overline{\psi(n)} a_n e^{2\pi i n z} = \sum_{n\geqslant 1} \frac{\tau(n,\psi)}{\tau(\psi)} a_n e^{2\pi i n z} = \\ &= \frac{1}{\tau(\psi)} \sum_{n\geqslant 1} \sum_{a[m]} \psi(a) e^{2\pi i n a/m} a_n e^{2\pi i n z} = \\ &= \frac{1}{\tau(\psi)} \sum_{a[m]} \psi(a) \sum_{n\geqslant 1} a_n e^{2\pi i n (z+a/m)} = \frac{1}{\tau(\psi)} \sum_{a[m]} \psi(a) f\Big(z + \frac{a}{m}\Big) \end{aligned}$$ □

Corollary 3.2.6 For $f \in S_2$, ψ primitive character modulo m, we have the twisting rule for the modular integral:

$$\phi(f_{\overline{\psi}}, r) = \frac{1}{\tau(\psi)} \sum_{a[m]} \psi(a) \phi(f, r + a/m)$$

Proof Substitute the expression of Birch lemma 3.2.5 in the modular integral and use linearity in the first variable and the fact that:

$$\phi\Big(f \mid \begin{bmatrix} 1 & a/m \\ 0 & 1 \end{bmatrix}, r\Big) = \phi(f, a/m)$$

□

Corollary 3.2.7 For $f \in S_2$, ψ primitive character modulo m, we have the twisting rule for the modular symbol:

$$\lambda_{f_{\overline{\psi}}}(b,n) = \frac{1}{\tau(\psi)} \sum_{a[m]} \psi(a)\lambda_f(mb - na, mn)$$

In particular, for $b = 0$ and $n = 1$ we find that:

$$\lambda_{f_{\overline{\psi}}}(0,1) = \frac{1}{\tau(\psi)} \sum_{a[m]} \psi(a)\lambda_f(-a,m) = \frac{\tau(\overline{\psi})}{m} \sum_{a[m]} \psi(a)\lambda_f(a,m)$$

Proof It is the last corollary, with $r = b/n$ and use the relation of proposition 3.2.3: □

Proposition 3.2.8 For $f \in S_2$, ψ primitive character modulo m, we have the interpolation property:

$$L(f,\overline{\psi},1) = L(f_{\overline{\psi}},1) = \frac{\tau(\overline{\psi})}{m} \sum_{a[m]} \psi(a)\lambda_f(a,m)$$

Proof Using the proposition 3.1.6 and the corollary relation of 3.2.7 with $b = 0$, $n = 1$, we find:

$$L(f_{\overline{\psi}},1) = \lambda_{f_{\overline{\psi}}}(0,1) = \frac{1}{\tau(\psi)} \sum_{a[m]} \psi(a)\lambda_f(-a,m)$$

then again using the relation of proposition 3.2.3 we find:

$$\frac{\tau(\overline{\psi})}{m}\psi(-1) \sum_{a[m]} \psi(a)\lambda_f(-a,m) = \frac{\tau(\overline{\psi})}{m} \sum_{a[m]} \psi(a)\lambda_f(a,m) \qquad \square$$

3.3 p-adic Distributions, Measures and L-functions

Given our elliptic curve $E/\mathbb{Q}$, we use the modularity theorem (see 1.5.3) to find the associated newform $f \in S_2(N, 1_N)$, so that $T_p f = a_p f$, $\pi^*(\omega_E) = c_\pi 2\pi i f(z)dz$ and $L(E,s) = L(f,s)$ for ψ Dirichlet character. Consider now the polynomial:

$$g_p(X) = X^2 - a_p X + 1_N(p)p$$

which is, again for the modularity theorem, the minimal polynomial of the Frobenius at p (remember that we denote by 1_{N_E} the trivial character of conductor $N_E = N$). Let $\upsilon = \upsilon_p$ denote the p-adic valuation normalized such that $\upsilon(p) = 1/p$ and pick $\alpha \neq 0$ a root of g_p such that $\upsilon(\alpha) < 1$, then:

Definition 3.3.1 We define:

$$\mu_{f,\alpha}(a;m) := \frac{1}{\alpha^{\upsilon(m)}}\lambda_f(a,m) - \frac{1_N(p)}{\alpha^{\upsilon(m)+1}}\lambda_f(a,m/p)$$

Proposition 3.3.1 (Distribution Relation) For $a, m \in \mathbb{Z}$, $m > 0$ we have:

$$\mu_{f,\alpha}(a,m) = \sum_{\substack{b \in \mathbb{Z}/pm\mathbb{Z} \\ b \equiv a \pmod m}} \mu_{f,\alpha}(b,pm)$$

Thanks to the theorem of Vishik, Amice-Vélu (see [MTT86, I.11]), if we pick α such that $\upsilon_p(\alpha) \leqslant 1$ we can define a measure ν on $\mathbb{Z}_p$ such that for $p \nmid a$ we have:

$$\nu_{f,\alpha}(a + p^k\mathbb{Z}) = \mu_{f,\alpha}(a,p^k) = \frac{1}{\alpha^k}\lambda(f;a,p^k) - \frac{1_N(p)}{\alpha^{k+1}}\lambda(f;a,p^{k-1})$$

against which we can integrate locally analytic function on $\mathbb{Z}_p^\times$. With abuse of notation we will denote both the distribution and the measure as $\mu_{f,\alpha}$. The distribution relation provide the fact that the so defined $\mu_{f,\alpha}$ is in fact a measure (additivity on the set of integration).

Definition 3.3.2 We define a p-adic character to be a continuous homomorphism:

$$\psi : \mathbb{Z}_p^\times \to \mathbb{C}_p^\times$$

where $\mathbb{C}_p$ denotes the completion of the algebraic closure of $\mathbb{Q}_p$.

Remark 3.3.2 For $x \in \mathbb{Z}_p^\times$ we have a unique decomposition as:

$$x = \omega(x)\langle x \rangle$$

where $\omega(x)$ is a $p-1$ root of unity and:

$$\langle x \rangle \in \begin{cases} 1 + p\mathbb{Z}_p, & \text{if } p \text{ odd} \\ 1 + 4\mathbb{Z}_2, & \text{if } p = 2 \end{cases}$$

And both are characters on $\mathbb{Z}_p$.

Definition 3.3.3 For a p-adic character ψ we define:

$$F_p(f,\alpha,\psi) := \int_{\mathbb{Z}_p^\times} \psi d\mu_{f,\alpha}$$

If now we set:

$$\psi_s(x) := \langle x\rangle^s = \exp(s\log\langle x\rangle) = \sum_{j=0}^{\infty} \frac{s^j}{j!}(\log\langle x\rangle)^j$$

We can define:

Definition 3.3.4 The p-adic L-function associated to α is:

$$L_p(f,\alpha,s) := F_p(f,\alpha,\psi_{s-1}) = \int_{\mathbb{Z}_p^\times} \langle x\rangle^{s-1} d\mu_{f,\alpha}$$

The p-adic L-function associated to α twisted by ψ is defined to be:

$$L_p(f,\alpha,\psi,s) = F_p(f,\alpha,\psi\psi_{s-1})$$

Proposition 3.3.3 $L_p(f,\alpha,\psi,s)$ is a locally analytic function in s defined for $s \in \mathbb{Z}_p$ and for ψ of conductor p^k we have:

$$L_p(f,\alpha,\psi,s) = \sum_{j=0}^{\infty} \frac{(s-1)^j}{j!} \sum_{a[p^k]} \psi(a) \int_{D(a,k)} (\log(x))^j$$

where $D(a,k) = a + p^k\mathbb{Z}_p$.

Proof See [MTT86, I.13.2]. □

Definition 3.3.5 Given a character ψ of conductor p^k, we define the p-adic multiplier to be:

$$\epsilon_p(\alpha,\psi) := \frac{1}{\alpha^k}\left(1 - \frac{\bar{\psi}(p)1_N(p)}{\alpha}\right)\left(1 - \frac{\psi(p)}{\alpha}\right)$$

In particular, in case of ψ trivial character, we have:

$$\epsilon_p(\alpha) = \left(1 - \frac{1_N(p)}{\alpha}\right)\left(1 - \frac{1}{\alpha}\right)$$

of course it depends on f, since $f \in S_2(N,\chi)$, and χ encode the bad reduction with its conductor.

Remark 3.3.4 We notice that we can distinguish the cases:

$$\epsilon_p(\alpha) = \begin{cases} \left(1 - \frac{1}{\alpha}\right)^2, & \text{if } p \text{ is a good reduction prime;} \\ 0, & \text{if } p \text{ is split multiplicative;} \\ 2, & \text{if } p \text{ is non-split} \end{cases}$$

Proposition 3.3.5 (Interpolation Property) We have this interpolation property, for a character ψ of conductor p^k:

$$L_p(f, \alpha, \psi, 1) = \epsilon_p(\alpha, \psi)\frac{p^k}{\tau(\bar{\psi})}L(f, \bar{\psi}, 1)$$

and, in particular, for the trivial character (no twist):

$$L_p(f, \alpha, 1) = \epsilon_p(\alpha)L(f, 1)$$

Proof Suppose first of all that $k \geqslant 1$, i.e. p divides the conductor of ψ. Then we can compute, splitting the integral:

$$L_p(f, \alpha, \psi, 1) = \int_{\mathbb{Z}_p^\times} \psi(x)d\mu_{f,\alpha} = \sum_{a[p^k]} \int_{D(a,k)} \psi(x)d\mu_{f,\alpha}$$

but here $D(a, k) = a + p^k\mathbb{Z}_p$, hence for $c \in D(a, k)$, we have $c - a \in p^k\mathbb{Z}_p$, then $\psi(c) = \psi(a), \forall c \in D(a, k)$, then we find:

$$\begin{aligned}\sum_{a[p^k]} \psi(a) \int_{D(a,k)} d\mu_{f,\alpha} &= \sum_{a[p^k]} \psi(a)\mu_{f,\alpha}(a, p^k) = \\ &= \sum_{a[p^k]} \psi(a) \left(\frac{1}{\alpha^k}\lambda_f(a, p^k) - \frac{1_N(p)}{\alpha^{k+1}}\lambda_f(a, p^{k-1})\right) = \\ &= \frac{1}{\alpha^k} \sum_{a[p^k]} \psi(a)\lambda_f(a, p^k) - \frac{1_N(p)}{\alpha^{k+1}} \sum_{a[p^k]} \psi(a)\lambda_f(a, p^{k-1})\end{aligned}$$

Now, the second sum, by proposition 3.1.4, can be seen as:

$$\sum_{a[p^k]} \psi(a)\lambda_f(a, p^{k-1}) = \sum_{b[p^{k-1}]} \left(\sum_{\substack{a[p^k] \\ a \equiv b[p^{k-1}]}} \psi(a) \right) \lambda(b, p^{k-1}) = 0$$

where the last equality holds because the some in the large brackets is zero because of lemma 3.2.2. Then only the first sum is non-zero and since in this case $\epsilon_p(\alpha, \psi) = 1/\alpha^k$, we find that:

$$\begin{aligned}L_p(f, \alpha, \psi, 1) &= \epsilon_p(\alpha, \psi)\frac{p^k}{\tau(\overline{\psi})}\frac{\tau(\overline{\psi})}{p^k} \sum_{a[p^k]} \psi(a)\lambda_f(a, p^k) = \\ &= \epsilon_p(\alpha, \psi)\frac{p^k}{\tau(\overline{\psi})}\lambda_{f_{\overline{\psi}}}(0, 1) = \epsilon_p(\alpha, \psi)\frac{p^k}{\tau(\overline{\psi})}L(f, \overline{\psi}, 1)\end{aligned}$$

where the last two passages are true thanks to corollary 3.2.7 and the proposition 3.1.6.

The case $k = 0$ comes as follows: if we consider an integer a such that $p \nmid a$, then we have:

$$\mathbb{Z}_p^\times = \coprod_{b[p]} D(b,1) \setminus D(0,1)$$

so all the balls of radium p except the one centered in zero. Moreover, $D(0,1) = D(ap,p)$. Then we find, by distribution relation (proposition 3.3.1) we find:

$$\int_{\mathbb{Z}_p^\times} d\mu_{f,\alpha} = \mu_{f,\alpha}(a,1) - \mu_{f,\alpha}(pa,p) =$$

$$= \lambda_f(a,1) - \frac{1_N(p)}{\alpha}\lambda_f(a,1/p) - \frac{1}{\alpha}\lambda_f(ap,p) + \frac{1_N(p)}{\alpha^2}\lambda_f(ap,1)$$

then using homogeneity of the modular symbol and $ap \equiv a \pmod 1$ we find that the latter is equal to:

$$\left(1 - \frac{1_N(p)}{\alpha} - \frac{1}{\alpha} + \frac{1_N(p)}{\alpha^2}\right)\lambda_f(a,1) = \epsilon_p(\alpha)\lambda_f(a,1) = \epsilon_p(\alpha)L(f,1)$$

□

Remark 3.3.6 The paper of Mazur, Tate and Teitelbaum provide a more technical approach on the part of integration which makes them able to hold also the case of characters of conductor $m = p^k M$, $p \nmid M$. A general proof of the last proposition in the case of character of conductor m, where $p \nmid M$, can be found in their paper (see [MTT86, I.14]), but it follows basically the same reasoning that we did in this specific case.

At this point we would like to state the p-adic version of the Birch and Swinnerton-Dyer conjecture, for which we need more instruments. Before doing this we provide a conjecture of which relates the order of vanishing of the p-adic L-function to the order of vanishing of the classical L-function which comes naturally after the last proposition:

Conjecture 3.3.7 For ψ Dirichlet character of conductor p^k we have that:

- $\mathrm{ord}_{s=1} L_p(f,\alpha,\psi,s) = \mathrm{ord}_{s=1} L(f,\psi,1)$ if $\epsilon_p(\alpha,\psi) = 0$;
- $\mathrm{ord}_{s=1} L_p(f,\alpha,\psi,s) = \mathrm{ord}_{s=1} L(f,\psi,1) + 1$ if $\epsilon_p(\alpha,\psi) \neq 0$.

In particular, if ψ is the trivial character of conductor 1, i.e. we are not twisting, the second case happens exactly if and only if p is split multiplicative (remark 3.3.4)

Notice that this conjecture related with the classical BSD conjecture would provide a p-adic version divided in two cases. This comes along with the last proposition, since the p-adic multiplier is zero in the case of split multiplicative reduction.

3.4 The BSD(p)-conjecture

If we consider the modular function j in terms of Fourier expansion $q = e^{2\pi i z}$, we have:

$$j = q^{-1} + A + Bq + \dots$$

and we can invert the formula to get:

$$q = q(j) = \sum_{n=1}^{\infty} B_n j^{-n}$$

Let $K \mid \mathbb{Q}_p$ finite, E/K with non-integral j-invariant $j(E)$. Evaluating $q(j(E)) \equiv q(E)$, the *multiplicative period of* E, we have:

$$\upsilon_p(q(E)) = -\upsilon_p(j(E)) > 0$$

Definition 3.4.1 Let $\lambda : K^\times \to \mathbb{Q}_p$ be a continuous homomorphism. We call $\mathcal{L}$ *invariant* the quantity:

$$\mathcal{L}_\lambda(E) := \frac{\lambda(q(E))}{\upsilon_p(q(E))} \in \mathbb{Q}_p$$

In particular, if λ is the composition:

$$K^\times \xrightarrow{N_{K|\mathbb{Q}_p}} \mathbb{Q}_p^\times \xrightarrow{\log_p} \mathbb{Q}_p$$

we call it $\mathcal{L}_p(E) \equiv \mathcal{L}_\lambda(E)$.

And we have the following:

Conjecture 3.4.1 If $j(E)$ is algebraic, then $\mathcal{L}_p(E)$ does not vanish.

Now we have to introduce the p-adic version of the regulator. It can be defined in terms of σ-functions or in terms of biextensions. In both case we need quite technical arguments which we'll not explore here in details.

We just say the strict needed to expose the p-adic version of the BSD conjecture. In particular, it turns out that we can define, as it's expressed in [MTT86] a p-adic height which provides a bilinear pairing:

$$\begin{aligned}(E^{\dagger}(K) \otimes \mathbb{Q}_p) \times (E^{\dagger}(K) \otimes \mathbb{Q}_p) &\to \mathbb{Q}_p \\ (P, Q) &\to \langle P, Q \rangle_{\lambda}\end{aligned}$$

called the λ-height pairing, where $E^{\dagger}(K)$ denote the extended Mordell-Weil group, which fits into the exact sequence:

$$1 \to \mathbb{Z}^N \to E^{\dagger}(K) \to E(K) \to 1$$

And with this, one can give the following:

Definition 3.4.2 The λ-*sparsity* of E/K to be:

$$\mathcal{S}_{\lambda}(E/K) := \mathcal{R}_{\lambda}(E/K)/\#E(K)^2_{\text{tors}}$$

where $\mathcal{R}_{\lambda}(E/K)$ is the volume of the lattice $E(K)_{\text{free}}$ in $E(K) \otimes \mathbb{Q}_p$, computed with the λ-height pairing.

The *Schneider* λ*-height* can be defined as a slight modification of the previous one using the λ-pairing and provide a regulator $\mathcal{R}^{\text{Sch}}_{\lambda}$ for which holds the following:

Proposition 3.4.2

$$\mathcal{S}_{\lambda}(E/K) = C\frac{\mathcal{R}^{\text{Sch}}_{\lambda}(E/K)}{\#E(K)^2_{\text{tors}}}$$

where C is some term depending on the q_v for v such that the Néron model is split multiplicative at v and $\lambda_v(q_v)$ is non zero.

Proof See [MTT86, II.6]. □

In both cases, we substitute the index λ with p when it comes from the p-adic logarithm as explained before.

Conjecture 3.4.3 (Schneider) The p-adic regulator is non-zero.

Consider the real and the complex period of the elliptic curve Ω^+_E and Ω^-_E and denote by m_l the Tamagawa numbers. Denote now:

$$L^{(k)}_p(E, \psi) = \frac{1}{k!}\frac{d^k}{ds^k} L_p(E, \psi, s) \mid_{s=1}$$

and $L^{(k)}_p(E)$ if $\psi = 1$ (so the k-th coefficient in the expansion of the L-function at $s = 1$. Then Mazur, Tate and Teitelbaum stated the following:

Conjecture 3.4.4 (BSD(p)) If we consider an elliptic curve $E/\mathbb{Q}$ then:

- If $\alpha \neq 1$, i.e. E has good ordinary or non-split multiplicative reduction at p, then $L_p^{(k)} = 0$, for $k < r = r(E/\mathbb{Q})$ and we have:

  $$L_p^{(r)}(E) = \left(1 - \frac{1}{\alpha}\right)^b \cdot \#\text{Ш}(E/Q) \cdot \mathcal{S}_p(E/\mathbb{Q}) \cdot \big(\prod_l m_l\big) \cdot \Omega_E^+$$

  where $b = 2$ if p is good ordinary and $b = 1$ if p is non-split multiplicative (the term is in fact the p-adic multiplier $\epsilon_p(\alpha)$);

- If $\alpha = 1$, i.e. E has split multiplicative reduction at p, then $L_p^{(k)}(E) = 0$, for $k < r + 1$ and we have:

  $$L_p^{(r+1)}(E) = \#\text{Ш}(E/\mathbb{Q}) \cdot \mathcal{S}_p(E/\mathbb{Q}) \cdot \big(\prod_l m_l\big) \cdot \Omega_E^+$$

Chapter 4

Iwasawa Theory for Elliptic Curves

Iwasawa theory provides, as it was said also in the previous chapter, a way to link the algebraic objects attached to the elliptic curves with p-adic L-functions. The artificial p-adic L-functions previously defined using p-adic analysis become extremely natural objects attached to the Pontryagin dual of the Selmer group, consideres as a Λ-module (where Λ denotes the Iwasawa algebra). More precisely, it is possible to associate to this Λ-module an ideal of Λ, and it is conjectured that the p-adic L-function is in relation with this ideal, after some algebrization step that will be developed in the following chapter.

We first recall the basics of Iwasawa theory for elliptic curves.

4.1 Iwasawa Algebra and Λ-modules

Let be $\mathcal{O} = \mathbb{Z}_p$ the *coefficient ring* (we can take other ring than $\mathbb{Z}_p$, but in fact that's all we need here). For a infinite cyclotomic extension K_∞, denote by $\Gamma \equiv G_\infty$ its Galois group and by G_n the Galois group of the n-th intermediate field K_n, such that:

$$\Gamma = \varinjlim_{n} G_n$$

Then:

Definition 4.1.1 We call *Iwasawa Algebra* the completed group ring:

$$\Lambda := \varprojlim_{n} \mathcal{O}[G_n]$$

Proposition 4.1.1 Pick a generator $\gamma \in \Gamma$. Then we have an isomorphism:

$$\begin{aligned} \Lambda &\to \mathcal{O}[[T]] \\ \gamma &\mapsto T+1 \end{aligned}$$

Proof Using Weierstrass preparation theorem. □

Consider now $X_n \in \mathbf{Ab}$ such that G_n acts on it. If the X_n's create a system, with some *norm map* $X_{n+1} \to X_n$ compatible with the action of the G_n's then:

$$X := \varprojlim_n X_n$$

is a compact Λ-module.

Proposition 4.1.2 (Structure Theorem for Finitely Generated Λ-Modules) Let X be a finitely generated Λ-module. Then there exist integers r, s, t, m_i, n_j, irreducible distinguished polynomials f_j and a morphism of Λ modules:

$$X \to \Lambda^r \oplus \bigoplus_{i=1}^{s} \frac{\Lambda}{p^{m_i}\Lambda} \oplus \bigoplus_{j=1}^{t} \frac{\Lambda}{f_j^{n_j}\Lambda}$$

with finite kernel and cokerel (a *quasi-isomorphism*).

Remark 4.1.3 We have the following invariants attached to X:

- $\mathrm{rank}_\Lambda(X) = r$, the *rank* of X;
- $\mu(X) = \sum_{i=1}^{s} m_i$, the μ-*invariant* of X;
- $\lambda(X) := \sum_{j=1}^{t} n_j \deg f_j$, the λ-*invariant* of X;
- $\mathrm{char}(X) = p^{\mu(X)} \prod_{j=1}^{t} f_j^{n_j}\Lambda$, the *characteristic ideal* of X.

Moreover, if $r = 0$, i.e. X it is a torsion λ-module (i.e. $r = 0$), $s \leqslant 1$ and f_j coprime, than:

$$X \to \frac{\Lambda}{\mathrm{char}(X)}$$

is a quasi-isomorphism.

Denote by X_{Γ_n} the largest quotient of X on which $\Gamma_n = \mathrm{Gal}(K_\infty \mid K_n)$ acts trivially. Then we have a characterization lemma for Λ-module which can be used in proofs:

Lemma 4.1.4 Let X be a Λ-module, then:

(a) X is finitely generated if and only if X is compact and X_Γ finitely generated over $\mathbb{Z}_p$;

(b) If X is finitely generated Λ-module, than it is Λ-torsion ($r = 0$) if and only if X_{Γ_n} has bounded $\mathbb{Z}_p$-rank;

(c) If X_{Γ_n} is finite $\forall n$, than there are constants ν and n_0 such that $\#X_{\Gamma_n} = p^{e_n}$, where $e_n = \mu(X)p^n + \lambda(X) + \nu$, $\forall n > n_0$.

Remark 4.1.5 So it's sufficient to consider a Λ-module to get information in this way! In particular, in Iwasawa theory for number fields, we are used to consider cyclotomic extensions and as Λ-module the p-primary part of the class group, so that $X_n = C(K_n)[p]$.

In our case of elliptic curves it's natural to use the Selmer groups, somehow, to get informations on the rank and, as we'll see, on the p-adic L-functions.

4.2 Selmer Groups and Iwasawa Theory

Let τ be the set of bad places for E/K plus the infinite places. Then Selmer group is unramified outside τ, hence we have the short exact sequence:

$$0 \to S^n(E/K) \to H^1_\tau(K, E[m]) \to \bigoplus_{v \in \tau} H^1(K_v, E)[m]$$

where by $H^1_\tau(K, -)$ we denote the cohomology of the Galois group of the maximal extension of K which is unramified outside τ.

Fix now a prime p and take now the group:

$$\mathcal{S}(E/K) := \varinjlim_k S^{p^k}(E/K) \subset H^1_\tau(K, E[p^\infty])$$

Since we have the exact sequence given in the proposition 2.1.2, passing to the direct limit we obtain the exact sequence:

$$0 \to \varinjlim_k \frac{E(K)}{p^k E(K)} \to \mathcal{S}(E/K) \to Ш(E/K)[p^\infty] \to 0$$

moreover, the first term is equal to:

$$\varinjlim_k \frac{E(K)}{p^k E(K)} = \varinjlim_k E(K) \otimes \frac{\mathbb{Z}}{p^k \mathbb{Z}} = E(K) \otimes \varinjlim_k \frac{\mathbb{Z}}{p^k \mathbb{Z}} = E(K) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$$

so that the sequence become the following:

Proposition 4.2.1 We have the following exact sequence:

$$1 \to E(K) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \to \mathcal{S}(E/K) \to Ш(E/K)[p^\infty] \to 1$$

Proof See the steps above. □

As one can see, since $\mathbb{Q}_p/\mathbb{Z}_p$ is divisible, the tensor kills the torsion part of $E(K)$ and hence the first term is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$, with $r = r(E/K)$.

A crucial step is now to handle the p-Selmer group. It happens that the beheaviour of the Pontryagin dual of this group in a Z_p-extension of K is well understood.

More precisely, let us consider a Z_p-extension $K_\infty = \cup_n K_n$ and let:

$$X := \mathcal{S}\widehat{(E/K_\infty)} = \mathrm{Hom}_{\mathbb{Z}}(\mathcal{S}(E/K), \mathbb{Q}/\mathbb{Z})$$

be the Pontryagin dual of the p-Selmer over K_∞. Then we have that:

$$X = \varprojlim_n S\widehat{(E/K_n)}$$

where all the maps are induced by the natural inclusions $E(K_n) \subset E(K_{n+1})$. We have the following:

Lemma 4.2.2 The group X is a finitely generated Λ-module for any $\mathbb{Z}_p$-extension $K_\infty \mid K$.

Consider the cyclotomic extension $K_\infty \mid K \mid \mathbb{Q}$, K number field, then:

Theorem 4.2.3 (Kato, [Kat04]) If $E/\mathbb{Q}$ has good ordinary reduction at p and $K \mid \mathbb{Q}$ is an abelian extension, then X is a torsion Λ-module.

This result support the following:

Conjecture 4.2.4 (Mazur, [Maz72]) If E has good reduction at all places of K above p, then X is a torsion Λ-module.

and in fact it is true under the assumption that both $E(K)$ and $Ш(E/K)[p^\infty]$ are finite, by a result of Mazur (see [Maz72]).

Chapter 5

Evidences for the BSD($\mathfrak{p}$)

We are going to see some evidences in support of BSD(p) conjecture and why it is good to treat it, computationally, instead of the classical version. We also connect the conjecture to Iwasawa Main Conjecture which provides a theoretical evidence in this direction. From now on we suppose p to be an odd prime.

5.1 p-adic L-functions again: Algebrization

Let $E/\mathbb{Q}$ be an elliptic curve. As we have seen using the language of modular symbols, we have that:

$$\phi_f(0) = \lambda_f(0,1) = L(f,1)$$

where f denote the newform associated to E by modularity theorem and $L(f,1)$ the complex L-function attached to the cusp form f. Now we want to deal with Iwasawa theory, so we want L-function to be, somehow, algebraic objects.

For that, we can symmetrize and antisymmetrize the modular symbols in the way that we now explain (see [MTT86]). Consider L_f, the module of value, as defined in definition 3.1.2 and set $L_f^+ := L_f \cap \mathbb{R}$ and $L_f^- := L_f \cap i\mathbb{R}$. Then we have:

Lemma 5.1.1 $L_f^{\pm}\mathbb{Q} = \Omega_E^{\pm}\mathbb{Q}$

Proof It is a theorem of Manin (see [Man72]) that $L_f \subset Z_E/t$ for some $t \subset \mathbb{Z}$, $t \geqslant 1$, where Z_E is the image of $H^1(E(\mathbb{C}), \mathbb{Z})$ via the map:

$$\int \omega_E : H^1(E(\mathbb{C}), \mathbb{Z}) \to \mathbb{C}$$

$$\gamma \mapsto \int_\gamma \omega_E$$

So there exists a basis of $H^1(E(\mathbb{C}), \mathbb{Z}) = \langle \gamma^+, \gamma^- \rangle$ such that, up to scalar in $\mathbb{Q}$, $\int_{\gamma^\pm} \omega_E$ is equal to $\Omega_E^\pm$. □

Definition 5.1.1

$$\lambda_E^\pm(a, m) := \frac{1}{2}\big(\lambda_f(a, m) \pm \lambda_f(-a, m)\big)$$

Remark 5.1.2 Notice that now we still have the interpolation property as in proposition 3.1.6:

$$\lambda_E^+(0) = L(f, 1)$$

while $\lambda_E^-(0) = 0$.

We can write:

$$\lambda_f(a, m) = \lambda_E^+(a, m) + \lambda_E^-(a, m)$$

Recall from section 3.3 that the p-adic L-function was defined to be:

$$L_p(f, \alpha, \psi, s) := \int_{\mathbb{Z}_p^\times} \psi(x)\langle x\rangle^{s-1} d\mu_{f,\alpha}$$

where $\mu_{f,\alpha}$ was the measure defined by:

$$\mu_{f,\alpha}(a + p^k\mathbb{Z}_p) = \frac{1}{\alpha^k}\lambda_f(a, p^k) - \frac{1_N(p)}{\alpha^{k+1}}\lambda_f(a, p^{k-1})$$

whenever $f \in S_2(N, 1_N)$ and α is an allowable root of the polynomial $X^2 - a_pX + 1_N(p)p$. Similarly we can define:

$$\mu_{f,\alpha}^\pm(a + p^k\mathbb{Z}_p) = \frac{1}{\alpha^k}\lambda_f^\pm(a, p^k) - \frac{1_N(p)}{\alpha^{k+1}}\lambda_f^\pm(a, p^{k-1}) \tag{5.1}$$

And we can define, moreover:

$$\mu_\alpha^\pm := \frac{\mu_{f,\alpha}^\pm}{\Omega_E^\pm}$$

Remark 5.1.3 The same measures $\mu_\alpha^\pm$ can be defined using:

$$[r]^\pm := \frac{\lambda_E^\pm(r,1)}{\Omega_E^\pm} \in \mathbb{Q}$$

For which the interpolation property become:

$$[0]^+ = L(f,1)/\Omega_E^+$$

and $[0]^- = 0$. So that we can recover the measures as:

$$\mu_\alpha^\pm(a + p^k\mathbb{Z}_p) = \frac{1}{\alpha^k}[a/p^k]^\pm - \frac{1_N(p)}{\alpha^{k+1}}[a/p^{k-1}]^\pm$$

Lemma 5.1.4 We have that:

$$\mu_{f,\alpha} = \mu_{f,\alpha}^+ + \mu_{f,\alpha}^-$$
$$\mu_{f,\alpha} = \mu_\alpha^+\Omega_E^+ + \mu_\alpha^-\Omega_E^-$$

Proof Comes from the above discussion. □

We can define, in this way, a new measure which can be proven to be a measure using the distribution property:

Definition 5.1.2 We call $\mu_E := \mu_\alpha^+ + \mu_\alpha^-$ and we define the p-adic L-function associated to E, twisted by ψ Dirichlet character, to be the following:

$$L_p(E,\psi,s) \equiv L_\alpha(E,\psi,s) := \int_{\mathbb{Z}_p^\times} \psi(x)\langle x\rangle^{s-1} d\mu_E$$

If we twist by the trivial character, we simply denote it by: $L_p(E,s)$.

Remark 5.1.5 While twisting by an even character it turns out that the μ_α^- part of the measure do not give any contribution and viceversa while twisting by an odd character. Then, since we are going to deal just with the not-twisted version of the BSD(p), in our case $\mu_E = \mu_\alpha^+$.

Remark 5.1.6 Having taken the quotient we have made things much more algebraic than before, as we'll see with Iwasawa main conjecture. So this point is of central importance in our treatment. Moreover notice that we divided basically for Ω_E^+, which appears in the BSD(p). Thanks to this, it will disappear in the modified version of the conjecture.

5.2 Iwasawa Theory for Elliptic Curves and p-adic L-functions

We did some change in the definition of the L-function. We go ahead with this, by turning the L-function into a power series, since the goal is in fact the main conjecture, which relate the p-adic L-function with the characteristic ideal of $X(E/\mathbb{Q}_\infty)$. Fix our generator γ of $\Gamma = Gal(\mathbb{Q}_\infty \mid \mathbb{Q})$. Then writing $\kappa : \Gamma \to 1 + p\mathbb{Z}_p^\times$ for the usual character (via $\Gamma \simeq \mathbb{Z}_p$) we define:

$$T := \kappa(\gamma)^{s-1} - 1$$

then we can change the variables and so:

$$L_p(E, s) := \int_{\mathbb{Z}_p^\times} \langle x \rangle^{\frac{\log(T+1)}{\log \kappa(\gamma)}} d\mu_E = \int_{\mathbb{Z}_p^\times} (T+1)^{\frac{\log\langle x \rangle}{\log \kappa(\gamma)}} d\mu_E \in \mathbb{Q}_p(\alpha)[[T]]$$

where α is our root of the characteristic polynomial of the Frobenius at p.

Consider now the p-adic regulator and normalize it in this way, with $r = r(E/\mathbb{Q})$:

$$\mathcal{R}_\gamma(E/\mathbb{Q}) := \frac{\mathcal{R}_p(E/\mathbb{Q})}{(\log \kappa(\gamma))^r}$$

we can then restate the BSD(p) in the following:

Conjecture 5.2.1 (Mazur, Tate, Teitelbaum) Let $E/\mathbb{Q}$ be an elliptic curve with either good ordinary or multiplicative reduction at p. Then:

- The order of vanishing of $L_p(E, T)$ at $T = 0$ is equal to r if p is good ordinary or non-split multiplicative and $r + 1$ if p is split multiplicative;

- The leading term of the series is:

  $$L_p^{(r)}(E) = \epsilon(\alpha) \frac{\prod_l m_l \cdot \#Ш(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{\text{tors}}} \mathcal{R}_\gamma(E/\mathbb{Q})$$

  if p is good ordinary or non-split multiplicative, and it is:

  $$L_p^{(r+1)}(E) = \frac{\mathcal{L}_p}{\log \kappa(\gamma)} \frac{\prod_l m_l \cdot \#Ш(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{\text{tors}}} \mathcal{R}_\gamma(E/\mathbb{Q})$$

Going back to Iwasawa theory, to link the objects, we have the following result, as a special case of the theorem 4.2.3:

Theorem 5.2.2 Assume that $E/\mathbb{Q}$ has either good ordinary or multiplicative reduction at p. Then $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module.

Then, if we denote by f_E to be a generator of the characteristic ideal (see remark 4.1.3) we have that $f_E \in \mathbb{Z}_p[[T]]$ and it is well defined, up to units in $\mathbb{Z}_p[[T]]^\times$.

Theorem 5.2.3 (Schneider, Perrin-Riou, Jones)

- The order of vanishing of $f_E(T)$ at $T = 0$ is at least equal to the rank $r(E/\mathbb{Q})$.
- It is equal to the rank if and only if the p-adic height is non-degenerate (conjecture 3.4.3) and $Ш(E/\mathbb{Q})[p]$ is finite (conjecture 2.1.10), then the leading term of the series f_E is:

$$\Upsilon \frac{\prod_l m_l \cdot \#Ш(E/\mathbb{Q})[p]}{\#E(\mathbb{Q})[p]^2} \mathcal{R}_\gamma(E/\mathbb{Q})$$

where $\Upsilon = \epsilon(\alpha)$ if p is good ordinary or non-split multiplicative and $\Upsilon = \mathcal{L}_p / \log \kappa(\gamma)$ if p is split multiplicative.

Conjecture 5.2.4 (Main Conjecture of Iwasawa Theory for Elliptic Curves) If $E/\mathbb{Q}$ has good or non-split multiplicative reduction at p, then:

$$\langle L_p(E,T)\rangle = \mathrm{char}(X) \quad (= \langle f_E(T)\rangle)$$

If p is split multiplicative, then:

$$\langle L_p(E,T)\rangle = T \cdot \mathrm{char}(X) \quad (= \langle T f_E(T)\rangle)$$

So we see that this conjecture provide an evidence and a possible direction in order to prove the BSD(p), if combined with the theorem 5.2.3.

5.3 Numerical Evidences

The paper [GJP+09] and [Mil11] treat the numerical verification for the BSD(p) conjecture for elliptic curves of conductor less or equal, respectively, 1000 and 5000, with rank less or equal than 1, using the Euler systems results of Kato and Kolyvagin.

Recall that the action of G_K on $E(\bar{K})$ restricts to $E[p]$ and it provides a mod p representation:

$$\rho_{E,p} : G_K \to \mathrm{Aut}(E[p]) \cong GL_2(\mathbb{F}_p)$$

Serre proved that this representation is surjective for all but finitely many primes, whenever the curve doesn't admit complex multiplication (see [Ser71]). Then we have the following:

Theorem 5.3.1 (Grigorov, Jorza, Patrikis, Stein, Tarniţă-Pătraşcu) Suppose that $E/\mathbb{Q}$ is a non-CM elliptic curve of rank $\leqslant 1$, conductor $N \leqslant 1000$ and p prime. If p is odd, assume further that the mod p representation $\rho_{E,p}$ is irreducible and p does not divide any Tamagawa number of E. Then BSD(p) is true.

Theorem 5.3.2 (Miller) Suppose that $E/\mathbb{Q}$ is an elliptic curve of conductor $N < 5000$ and (analytic) rank at most one. If p is a prime such that $E[p]$ is irreducible, then BSD(p) holds. If $E[p]$ is reducible and the pair (E, p) is not one of the eleven pairs appearing in Table 10 (see [Mil11]), then BSD(p) holds.

This is very good and interesting in the direction of the conjecture, but it's a limit in terms of rank! As one can see, it only works for the case of rank $\leqslant 1$. The paper of Stein and Wuthrich (see [SW13]) describes an algorithm which uses Iwasawa theory in order to compute Ш and prove the conjecture under specific hypothesis, but killing the one of rank $\leqslant 1$. In fact it is complementary in the sense that provides algorithms for a large scale verification of the conjecture in the case of rank $\geqslant 2$. In particular, the main result is:

Theorem 5.3.3 (Stein, Wuthrich, see [SW13]) For elliptic curves $E/\mathbb{Q}$ without complex multiplication, of rank $\geqslant 2$, conductor $N \leqslant 30000$ and $p \geqslant 5$ good ordinary prime for E, $p < 1000$ such that the mod p representation is surjective we have that $Ш(E/\mathbb{Q})[p] = 0$.

Bibliography

[Dia05] Diamond, Fred and Shurman, Jerry, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer, New York, 2005.

[GJP$^+$09] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William Stein, and Corina Tarniţă, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Mathematics of Computation **78** (2009), no. 268, 2397–2425.

[Jan96] Gerald J Janusz, *Algebraic number fields*, vol. 7, Ammath. Soc, 1996.

[Kat04] Kazuyra Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), no. ix, 117–290.

[Lan94] Serge Lang, *Algebraic number theory*, Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[Man72] Ju I. Manin, *Parabolic points and zeta-functions of modular curves*, Mathematics of the USSR-Izvestiya **6** (1972), no. 1, 19.

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Inventiones Mathematicae **18** (1972), 183–266.

[Mil] James S. Milne, *Algebraic number theory*, `http://www.jmilne.org/math/CourseNotes/ANT.pdf`.

[Mil96] J.S. Milne, *Elliptic curves*, `http://www.jmilne.org/math/Books/ectext5.pdf` (1996).

[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., 2011, pp. 327–350.

[MTT86] Barry Mazur, John Tate, and Jeremy Teitelbaum, *On* p*-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Inventiones Mathematicae **84** (1986), no. 1, 1–48.

[Ser56] Jean-Pierre Serre, *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier **6** (1956), no. 19554956, 14–2.

[Ser71] ______, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae **15** (1971), no. 4, 259–331.

[Sil86] Silverman, Joseph H., *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[Sil94] ______, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[SW13] William Stein and Christian Wuthrich, *Algorithms for the arithmetic of elliptic curves using Iwasawa theory*, Mathematics of Computation **82** (2013), 1757–1792.