UNIVERSITÀ DEGLI STUDI DI MILANO
FACOLTÀ DI SCIENZE E TECNOLOGIE

Master's thesis in Mathematics

The Sato-Tate conjecture

Lorenzo Pagani

Thesis advisors:
Prof. Fabrizio Andreatta
Prof. Lenny Taelman

October 2017

Abstract

In this thesis, we explore the connection between Galois representations and the Sato-Tate group. We give an explicit formulation of the Sato-Tate conjecture for smooth and projective varieties over $\mathbb{Q}$ and we see what it concretely implies. We present an approach to this subject following Serre's notes *Lectures on* $N_X(p)$.

We then discuss an example to give the reader a taste of how the proof of the Sato-Tate conjecture works in the case of elliptic curve with complex multiplication.

Acknowledgments

First and foremost, I wish to thank my thesis advisor, Professor Lenny Taelman, for introducing me to this topic, and for all the time he devoted to me, especially during my first days at the University van Amsterdam, and during my first attempts to write this thesis.

Secondly, I wish to thank Professor Fabrizio Andreatta for his help and patience in the conclusive part of this work.

I am also very grateful to Isabella Negrini, a close friend, who encouraged me in taking part in the Erasmus project which allowed me to start working on this thesis with Lenny Taelman.

Finally, I thank my family and all the people who supported me during my studies.

Contents

Introduction

Equidistribution questions arise naturally in number theory, and the Sato-Tate conjecture is one of them. Our goal in this thesis is to present a general framework of the conjecture and its generalizations.

We will introduce the quantity $N_X(p)$ which has a fundamental role in our work. Roughly speaking, one can think about $N_X(p)$ in this way: let X be a family of polynomial equations in finitely many unknowns with integer coefficients, so that it makes sense to reduce them modulo a prime integer p. The function $N_X(p)$ counts the number of solutions modulo p of the given family of equations. For a fixed X, we want to investigate how $N_X(p)$ varies with p; *what is its size? Can it be computed by closed formulae? What can we say about its distribution?*

To (partially) answer these questions we will review some techniques both in algebraic and analytic number theory, étale cohomology and group representations. After reviewing this background we will be able to state the Sato-Tate conjecture in general.

The Sato-Tate conjecture, in its first formulation, concerns elliptic curves. Let E be an elliptic curve over $\mathbb{Q}$. In this setting $N_E(p)$ denotes the number of $\mathbb{F}_p$-points of the reduction of E at p. Define

$$\overline{a_p} = \frac{1 + p - N_E(p)}{\sqrt{p}}.$$

Recall that the Hasse-Weil theorem asserts that $\overline{a_p} \in [-2, 2]$ when E has a good reduction at p. Thus it is natural to investigate their distribution. Furthermore, according to some numerical data this distribution does not seem to be random. The following figures give us examples of this fact.

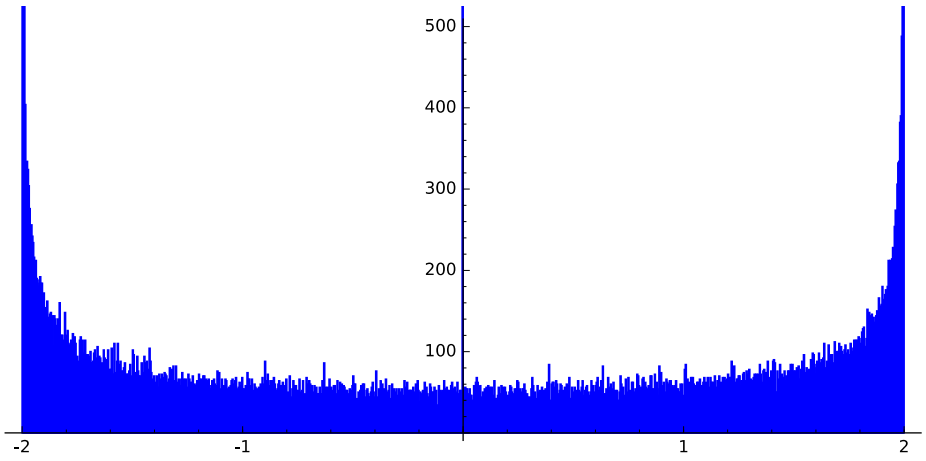

Figure 1: Distribution of $\overline{a_p}$ for the elliptic curve defined by $Y^2 = X^3 - X$ for prime $p \leq 10^6$

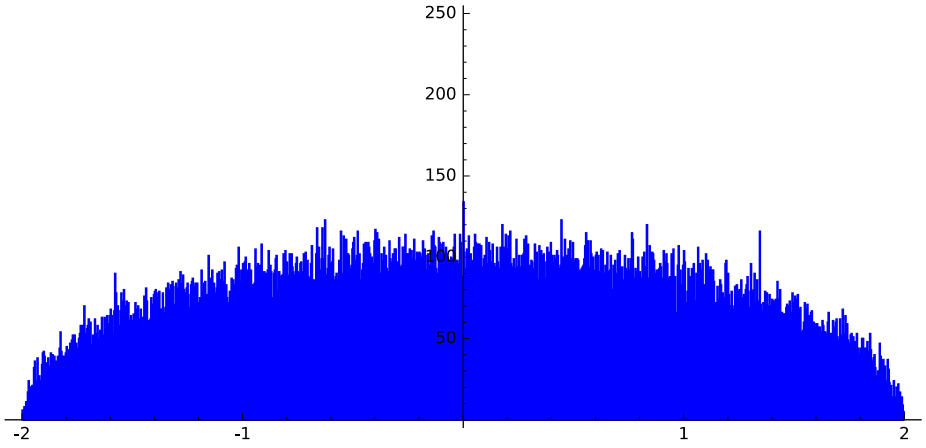

Figure 2: Distribution of $\overline{a_p}$ for the elliptic curve defined by $Y^2 = X^3 + X + 1$ for prime $p \leq 10^6$

We will deduce the analogous of the Hasse-Weil theorem for a generic family of equations X. In particular we will find a formula

$$N_X(p) = \sum_{i=0}^{N} (-1)^i a_{i,p}$$

where $a_{i,p}$ are integers and $|a_{i,p}| \leq n_i p^{i/2}$ for all prime integers except finitely many.

Assuming the Sato-Tate conjecture, we will prove the existence of a measure on the interval $[-n_i, n_i]$ such that the values $\frac{a_{i,p}}{p^{i/2}}$ are equidistributed in the interval with respect to that measure.

The thesis is organized as follows.

Chapter 1 introduces in a formal way the function $N_X(p)$ where X is a scheme of finite type over $\mathbb{Z}$.

Chapter 2 gives us a background in the study of ℓ-adic chomology that will be used later. In particular our main interest is the study of Galois representations induced by the cohomology.

In Chapter 3 we will see the connection between the representations of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ defined in the previous chapters and the function $N_X(p)$. Indeed $N_X(p)$ can be expressed as a virtual character of the Galois group.

Chapter 4 continues the investigation of ℓ-adic representations of the Galois group. This chapter is focused on the size of the eigenvalues of these representations: in particular we will find the formula

$$N_X(p) = \sum_{i=0}^{N} (-1)^i a_{i,p}$$

we present above as the generalization of the Hasse-Weil theorem for elliptic curves.

Chapter 5 describes the Sato-Tate conjecture. In particular we show (in a conjectural way) how the values $a_{i,p}$ that can be defined by ℓ-adic cohomology are related to the distribution of their normalized values in the real interval

$$\frac{a_{i,p}}{p^{i/2}} \in [-n_i, n_i] \quad \text{for every } i.$$

This connection is given by the Sato-Tate group.

In chapter 6 we compute the Sato-Tate group for the elliptic curve $Y^2 = X^3 - X$. Moreover we find a density function describing the distribution in Figure 1.

Chapter 1

What is $N_X(p)$

In this chapter we introduce $N_X(p)$ in a scheme setting. This quantity will be studied in the whole thesis.

1.1 Preliminary definitions

Let R be a commutative ring with unit, we denote with $\underline{\mathrm{Sch}}_R$ the category of R-scheme with R-morphisms.

Definition 1.1 (K-variety)**.** Let K be a field. A K-variety or variety over K is a K-scheme which is separated and of finite type. Denote with $\underline{\mathrm{Var}}_K$ the full subcategory of $\underline{\mathrm{Sch}}_K$ whose objects are K-varieties.

Definition 1.2 (Base change)**.** Let $\alpha : R \to S$ be a morphism of commutative rings with unit. Then α induces the base-change functor:

$$\alpha^* : \underline{\mathrm{Sch}}_R \longrightarrow \underline{\mathrm{Sch}}_S \,.$$

Recall that if $\alpha : R \to S$ is a ring homomorphism and X a R-scheme, then the base changed S-scheme $\alpha^*(X)$ is isomorphic to the fiber product $X \times_R \operatorname{Spec} S$. When the morphism α we are considering is clear, we denote the base changed scheme with X_S instead of $\alpha^*(X)$.

Proposition 1.1. *Let $\alpha : R \to S$ and $\beta : S \to T$ be ring homomorphisms. Then the base change is transitive i.e. if X is a R-scheme then there is a canonical isomorphism $X_T \cong (X_S)_T$.*

Proposition 1.2. *Let $\mathcal{P}$ denote one of the properties between being separated, of finite type, proper and smooth. Let $\alpha : R \to S$ be a morphisms of commutative rings with unit and X a R-scheme. If X has the property $\mathcal{P}$ then X_S has the property $\mathcal{P}$ too.*

Definition 1.3 (K-points)**.** Let X be a variety over K. Define the set of K-points $X(K)$ as the set of K-scheme morphism from $\operatorname{Spec} K \to X$.

Theorem 1.1 (Spreading out)**.** *Let X be a scheme over $\mathbb{Q}$ and let $\mathcal{P}$ denote the properties of being separated, smooth, or proper.*

(i) Suppose X is of finite type over $\mathbb{Q}$. There exist $N \in \mathbb{Z}_{>0}$ and Y a scheme of finite type over $\mathbb{Z}[1/N]$ such that $X \cong Y_{\mathbb{Q}}$.

(ii) Let Y be a scheme of finite type over $\mathbb{Z}$ such that $Y_{\mathbb{Q}}$ has the property $\mathcal{P}$ as a $\mathbb{Q}$-scheme. Then there exist $N \in \mathbb{Z}_{>0}$ such that $Y_{\mathbb{Z}[1/N]}$ has the same property $\mathcal{P}$ as a $\mathbb{Z}[1/N]$-scheme.

Example 1.1. Consider $\mathcal{P}$ to be the property of being smooth.

Let E be a smooth curve over $\mathbb{Q}$ defined by the equation $Y^n = f(X)$ where $f(X) \in \mathbb{Z}[X]$. Let Δ be the discriminant of the polynomial f. The smoothness of E is equivalent to the fact that $f(X)$ has no multiple roots and thus $\Delta \neq 0$. If we consider the reduction modulo a prime $p \in \mathbb{Z}$ the curve is still smooth when $\Delta \neq 0$ in $\mathbb{F}_p$ and p does not divide n. Hence we have smooth reduction for every prime in $\operatorname{Spec} \mathbb{Z}[1/n\Delta]$. So we have a smooth $\mathbb{Z}[1/n\Delta]$-scheme $\mathcal{E}$ defined by the above equation $Y^n = f(X)$. Moreover $\mathcal{E}_{\mathbb{Q}} \cong E$.

1.2 Definition of $N_X(p)$

Consider a scheme X of finite type over $\mathbb{Z}$. For every prime integer p we have the canonical projection $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{F}_p$. Denote with $X_{\mathbb{F}_p}$ the $\mathbb{F}_p$-variety obtained by base change along the map π as in Definition 1.2.

Definition 1.4 ($N_X(p)$)**.** Let X be a scheme of finite type over $\mathbb{Z}$. For every prime p, we define $N_X(p)$ as the cardinality of $X_{\mathbb{F}_p}(\mathbb{F}_p)$.

The definition of $N_X(p)$ makes sense because $X_{\mathbb{F}_p}$ is of finite type over $\mathbb{F}_p$. Indeed, the following proposition assures that $X_{\mathbb{F}_p}(\mathbb{F}_p)$ is finite.

Proposition 1.3. *Let Y be a scheme of finite type over a finite field K. Then $Y(K)$ is a finite set.*

Proof. Since Y is a finite type scheme over K then it can be covered by a finite number of open affine sub-schemes $U = \operatorname{Spec} A$ where A is a finitely generated K-algebra. Consider f a K-point. Since $\operatorname{Spec} K$ topologically is a point there exists a open affine U such that the image of f is in U. So it suffices to prove the proposition in the case Y is affine.

Assume $Y = \operatorname{Spec} A$. In this case $Y(K)$ is in bijection with the set of ring morphisms $\operatorname{Hom}(A, K)$ and it is clearly finite since A is a finitely generated K-algebra and K is a finite field. □

1.2.1 An example: the affine case

In order to have a better understanding of what $N_X(p)$ means, we study the affine case.

Consider X to be an affine scheme of finite type over $\mathbb{Z}$. Thus $X = \operatorname{Spec} A$ with A a finitely generated $\mathbb{Z}$-algebra: namely $A = \mathbb{Z}[T_1, \ldots, T_n]/I$ where I is the ideal generated by a family of polynomials $f_\alpha \in \mathbb{Z}[T_1, \ldots, T_n]$.

Via base change we get $X_{\mathbb{F}_p} = \operatorname{Spec}(A \otimes_{\mathbb{Z}} \mathbb{F}_p)$. Since we are dealing with the affine case we have:

$$X_{\mathbb{F}_p}(\mathbb{F}_p) = \operatorname{Hom}_{\underline{\mathrm{Sch}}}(\operatorname{Spec} \mathbb{F}_p, \operatorname{Spec}(A \otimes_{\mathbb{Z}} \mathbb{F}_p)) \cong \operatorname{Hom}_{\underline{\mathrm{Ring}}}(A \otimes_{\mathbb{Z}} \mathbb{F}_p, \mathbb{F}_p).$$

There is a correspondence between $\operatorname{Hom}_{\underline{\mathrm{Ring}}}(A \otimes_{\mathbb{Z}} \mathbb{F}_p, \mathbb{F}_p)$ and the maximal ideals of $A \otimes_{\mathbb{Z}} \mathbb{F}_p$ with residue field $\mathbb{F}_p$, hence the solutions in $\mathbb{F}_p$ of the polynomials f_α. We conclude that:

$$N_X(p) = \#\{\, (x_1, \ldots, x_n) \in {\mathbb{F}_p}^n \mid \forall \alpha \quad f_\alpha(x_1, \ldots, x_n) = 0 \quad \text{in } \mathbb{F}_p\}.$$

Chapter 2

Some cohomological facts

In this chapter we recall some facts and data about étale cohomology which will be the background for the next chapters. This facts will be presented as in [Se 12] without proving the results. The proofs can be find in [SGA 4], [SGA $4\frac{1}{2}$] and [De 80].

2.1 Étale cohomology and Galois action

Étale cohomology

Fix ℓ a prime integer. There is a functor from the category of schemes to the one of $\underline{\mathbb{Q}_\ell\text{-Mod}}$ for every non-negative integer i:

$$H^i(-_{\acute{e}t}, \mathbb{Q}_\ell) : \underline{\mathrm{Sch}}^{\mathrm{op}} \longrightarrow \underline{\mathbb{Q}_\ell\text{-Mod}} \ .$$

The functor associates to a scheme X the $\mathbb{Q}_\ell$-module $H^i(X_{\acute{e}t}, \mathbb{Q}_\ell)$ called the i-th étale cohomology group of X.

Proposition 2.1. *Let K be an algebraically closed field. If X is a variety over K as in Definition 1.1 and ℓ distinct from* $\operatorname{char} K$ *then $H^i(X_{\text{ét}}, \mathbb{Q}_\ell)$ is a finite dimensional $\mathbb{Q}_\ell$-module. Moreover $H^i(X_{\text{ét}}, \mathbb{Q}_\ell)$ is the zero module when $i > 2 \dim X$.*

In Proposition 2.1 we consider X as a scheme forgetting about the morphism that gives X the structure of a K-variety.

Base-change

Consider K and L algebraically closed fields and $\alpha : K \to L$ a field homomorphism. As in Definition 1.2 the morphism α define a functor:

$$\alpha^* : \underline{\mathrm{Var}}_K \longrightarrow \underline{\mathrm{Var}}_L \ .$$

We are interested in the relation between the cohomology of a K-variety and the one induced by base change.

Proposition 2.2. *Let $\alpha : K \to L$ a morphism of algebraically closed fields and let ℓ be a prime distinct from the characteristic of the fields. There is a natural isomorphism between the functors $H^i(-_{\text{ét}}, \mathbb{Q}_\ell)$ and $H^i(-_{\text{ét}}, \mathbb{Q}_\ell) \circ \alpha^*$ i.e. for every X variety over K there is an isomorphism*

$$H^i(X_{\text{ét}}, \mathbb{Q}_\ell) \cong H^i(X_{L,\text{ét}}, \mathbb{Q}_\ell)$$

and it is functorial in X.

Galois action

Let $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ be a functor and let X be an object of the category $\mathcal{C}$. Then $\mathcal{F}$ induces a group homomorphism $\mathrm{Aut}_{\mathcal{C}}(X) \to \mathrm{Aut}_{\mathcal{D}}(\mathcal{F}X)$.

Definition 2.1. Let K a field. Define $\underline{\mathrm{Field}}_K$ the category whose objects are field extension of K, and the morphisms are field homomorphisms that induce the identity map on K. In particular if E is a Galois extension of K, then $\mathrm{Aut}_{\underline{\mathrm{Field}}_K}(E) \cong \mathrm{Gal}(E|K)$.

Definition 2.2 (Galois action)**.** Assume K is a perfect field. For every scheme X over K, and for every prime $\ell \neq \mathrm{char}\, K$, we have the following functor:

$$\begin{aligned} \underline{\mathrm{Field}}_K &\longrightarrow \underline{\mathbb{Q}_\ell\text{-Mod}} \\ L &\longmapsto H^i(X_{L,ét}, \mathbb{Q}_\ell) \end{aligned}$$

Let us consider $\overline{K}$ an algebraic closure of K; the functor above induces a group homomorphism:

$$\mathrm{Gal}(\overline{K}|K) \cong \mathrm{Aut}_{\underline{\mathrm{Field}}_K}(\overline{K}) \longrightarrow \mathrm{Aut}_{\underline{\mathbb{Q}_\ell\text{-Mod}}}(H^i(X_{\overline{K},ét}, \mathbb{Q}_\ell)).$$

Hence the functor defines an action of $\mathrm{Gal}(\overline{K}|K)$ on the cohomology module $H^i(X_{\overline{K},ét}, \mathbb{Q}_\ell)$ for every non-negative i.

Proposition 2.3. *Let K be a perfect field and let X be a K-variety. Then for every prime $\ell \neq \mathrm{char}\, K$ the action*

$$\mathrm{Gal}(\overline{K}|K) \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(H^i(X_{\overline{K},\text{ét}}, \mathbb{Q}_\ell))$$

defined in Definition 2.2 is continuous.

2.2 Finite field

Let $\mathbb{F}_q$ be a finite field with q elements and let X be a $\mathbb{F}_q$-variety. We will denote with $\overline{\mathbb{F}_q}$ an algebraic closure of $\mathbb{F}_q$, and with $X_{\overline{\mathbb{F}_q}}$ the $\overline{\mathbb{F}_q}$-variety obtained via base change.

Arithmetic Frobenius

Definition 2.3 (Arithmetic Frobenius)**.** We call arithmetic Frobenius the element $\sigma_q \in \mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$ that sends an element $x \in \overline{\mathbb{F}_q}$ in its q-th power. Notice that σ_q generates the group $\mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$ as a topological group.

We are interested in the action of the element ${\sigma_q}^{-1}$ on the cohomology group $H^i(X_{\overline{\mathbb{F}_q},\acute{e}t}, \mathbb{Q}_\ell)$ for every non-negative i.

Definition 2.4 (Lefschetz number)**.** Let X be a $\mathbb{F}_q$-variety. We define the Lefschetz number of the arithmetic Frobenius to be:

$$\mathrm{Tr}({\sigma_q}^{-1}|H^\bullet(X_{\overline{\mathbb{F}_q},\acute{e}t}, \mathbb{Q}_\ell) = \sum_i (-1)^i \,\mathrm{Tr}({\sigma_q}^{-1}|H^i(X_{\overline{\mathbb{F}_q},\acute{e}t}, \mathbb{Q}_\ell)$$

By Proposition 2.1, the Lefschetz number is well defined.

The following theorem describes completely the Lefschetz number of the arithmetic Frobenius.

Theorem 2.1 (Grothendieck)**.** *Let X be a proper $\mathbb{F}_q$-variety. Then the Lefschetz number of the arithmetic Frobenius is equal to the number of $\mathbb{F}_q$-points of X.*

$$\mathrm{Tr}({\sigma_q}^{-1}|H^\bullet(X_{\overline{\mathbb{F}_q},\text{ét}}, \mathbb{Q}_\ell) = \#X(\mathbb{F}_q)$$

The full proof can be found in [SGA $4\frac{1}{2}$].

In particular the Lefschetz number, that a priori is in $\mathbb{Q}_\ell$, lies in $\mathbb{Z}$, and moreover it does not depends on ℓ.

Corollary 2.1. *Let X be a proper $\mathbb{F}_q$-variety, and let σ_q be the arithmetic Frobenius. Then for each positive integer r*

$$\mathrm{Tr}({\sigma_q}^{-r}|H^\bullet(X_{\overline{\mathbb{F}_q},\text{ét}}, \mathbb{Q}_\ell) = \#X(\mathbb{F}_{q^r}).$$

Deligne's theorem

Definition 2.5 (p-Weil integer of weight w)**.** Let $p, w \in \mathbb{N}$. We say that an algebraic integer α is a p-Weil integer of weight w if for every embedding $\iota : \mathbb{Q}(\alpha) \to \mathbb{C}$ the absolute value $|\iota(\alpha)|$ is equal to $p^{w/2}$.

Theorem 2.2 (Deligne)**.** *Let X be a proper and smooth $\mathbb{F}_q$-variety. Then the characteristic polynomial of the inverse of the arithmetic Frobenius ${\sigma_q}^{-1}$ acting on $H^i(X_{\overline{\mathbb{F}_q},\text{ét}}, \mathbb{Q}_\ell)$ lies in $\mathbb{Z}[T]$. Moreover it is independent of ℓ and its roots are q-Weil integers of weight i.*

The proof is given in [De 80].

Corollary 2.2. $\mathrm{Tr}({\sigma_q}^{-1}|H^i(X_{\overline{\mathbb{F}_q},\text{ét}}, \mathbb{Q}_\ell)$ *lies in $\mathbb{Z}$ for every non-negative i.*

2.3 Comparison theorems

Specialization map

Proposition 2.4. *Let O_K be a discrete valuation ring with fraction field K and residue field k. Denote an algebraic closure of K with $\overline{K}$. The valuation extends uniquely to $\overline{K}$, let $O_{\overline{K}}$ be the valuation ring and $\overline{k}$ the residue field. Note that $\overline{k}$ is an algebraic closure of k. We have the following maps:*

$$\overline{k} \cong O_{\overline{K}}/\mathfrak{m} \twoheadleftarrow O_{\overline{K}} \hookrightarrow \overline{K}.$$

Let X be a separated and of finite type $O_{\overline{K}}$-scheme and ℓ be a prime distinct from $\operatorname{char} K$*. There exists a linear morphism which is functorial in X:*

$$r_X^i : H^i(X_{\overline{k},\text{ét}}, \mathbb{Q}_\ell) \longrightarrow H^i(X_{\overline{K},\text{ét}}, \mathbb{Q}_\ell)$$

such that if X is proper and smooth the map r_X^i is an isomorphism for every non-negative integer i.

Schemes over $\mathbb{Z}$

We consider now X a separated scheme of finite type over $\mathbb{Z}$. We denote with $\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at the prime p. Notice that $\mathbb{Z}_{(p)}$ is a valuation ring with fraction field $\mathbb{Q}$ and residue field $\mathbb{F}_p$. Using the inclusion of $\mathbb{Z} \to \mathbb{Z}_{(p)}$, we base change X to a separated and finite type scheme $Y = X_{\mathbb{Z}_{(p)}}$ over the localization. Since the base change is transitive we have the following isomorphisms: $Y_{\overline{\mathbb{Q}}} \cong X_{\overline{\mathbb{Q}}}$ and $Y_{\overline{\mathbb{F}_p}} \cong X_{\overline{\mathbb{F}_p}}$.

Applying Proposition 2.4 to the scheme Y over $\mathbb{Z}_{(p)}$ we get a family of linear morphisms $r_p^i : H^i(X_{\overline{\mathbb{F}_p},ét}, \mathbb{Q}_\ell) \to H^i(X_{\overline{\mathbb{Q}},ét}, \mathbb{Q}_\ell)$.

Proposition 2.5. *Let X be a separated scheme of finite type over $\mathbb{Z}$ and r_p^i the maps described above. Let ℓ be a prime integer. Then there exists a finite set of primes S such that for every primes $p \notin S$ the maps r_p^i are isomorphisms. Hence for almost all the primes $H^i(X_{\overline{\mathbb{F}_p},\text{ét}}, \mathbb{Q}_\ell)$ and $H^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell)$ are isomorphic.*

The set S can depend on ℓ.

2.4 Galois compatibility

Let X be a separated scheme of finite type over $\mathbb{Z}$, denote with $X_{\overline{\mathbb{Q}}}$ and with $X_{\overline{\mathbb{F}_p}}$ the variety respectively over $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}_p}$ obtained via base change; by Proposition 2.5 for all but finitely many primes we have an isomorphism $H^i(X_{\overline{\mathbb{F}_p},ét}, \mathbb{Q}_\ell) \cong H^i(X_{\overline{\mathbb{Q}},ét}, \mathbb{Q}_\ell)$. Deligne's Theorem describes the action of the group $\operatorname{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$.

What can we say about the action of $\operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$*?*

Unramified action

Let p be a prime integer and consider the p-adic integer $\mathbb{Z}_p \subset \mathbb{Q}_p$. We extend the valuation to an algebraic closure $\overline{\mathbb{Q}_p}$ and we denote with $\overline{\mathbb{Z}_p}$ the valuation ring and with k the residue field. Hence we have the following diagram:

$$\begin{array}{ccccc} \mathbb{F}_p & \twoheadleftarrow & \mathbb{Z}_p & \hookrightarrow & \mathbb{Q}_p \\ \cap & & \cap & & \cap \\ k & \twoheadleftarrow & \overline{\mathbb{Z}_p} & \hookrightarrow & \overline{\mathbb{Q}_p} \end{array}$$

Definition 2.6 (Unramified action)**.** Let $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$. Choose $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$ an embedding of algebraically closed field, and choose k, the residue field with respect to the p-adic valuation on $\overline{\mathbb{Q}_p}$, as an algebraic closure of $\mathbb{F}_p$. These choices induce the following homomorphisms:

$$\mathrm{Gal}(k|\mathbb{F}_p) \twoheadleftarrow \mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}).$$

We have also the exact sequence

$$1 \to I_p \to \mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p) \to \mathrm{Gal}(k|\mathbb{F}_p) \to 1$$

where I_p is the inertia subgroup at p.

If $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ acts on some space Y, we say that the action is unramified at the prime p if the subgroup $I_p \subset \mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ acts trivially.

Compatibility of the Galois action

Proposition 2.6 (Compatibility of the Galois action)**.** *Let X be a separated scheme of finite type over $\mathbb{Z}$ and let ℓ be a prime. There exists a finite set of primes S such that for every prime $p \notin S$:*

(i) the specialization map $r_p^i : H^i(X_{\overline{\mathbb{F}_p},\text{ét}}, \mathbb{Q}_\ell) \to H^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell)$ as in Definition 2.4 is an isomorphism,

(ii) the action of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ on $H^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell)$ is unramified at p (i.e. the inertia group I_p acts trivially).

Moreover for such p the following actions of group are equivariant:

$$\begin{array}{ccccc} H^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell) & \xleftarrow{\cong} & H^i(X_{\overline{\mathbb{Q}_p},\text{ét}}, \mathbb{Q}_\ell) & \xrightarrow{\cong} & H^i(X_{\overline{\mathbb{F}_p},\text{ét}}, \mathbb{Q}_\ell) \\ \circlearrowright & & \circlearrowright & & \circlearrowright \\ \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) & \longleftarrow & \mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p) \end{array}$$

Notice that the set S depends on ℓ.

Chapter 3

$N_X(p)$ as an ℓ-adic character

From now on we will use the following notations: $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ and $\Gamma_{\mathbb{F}_q} = \mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$ for every finite field. Moreover if S is a finite set of primes we will denote $\mathbb{Q}_S$ the maximal extension $\mathbb{Q} \subset \mathbb{Q}_S \subset \overline{\mathbb{Q}}$ such that it is unramified outside S, and with Γ_S the Galois group $\mathrm{Gal}(\mathbb{Q}_S|\mathbb{Q})$.

The purpose of this chapter is the introduction of a virtual character $h_{X,\ell} : \Gamma_{\mathbb{Q}} \to \mathbb{Q}_\ell$ through the ℓ-adic cohomology. This character will contain all the information about $N_X(p)$ for all the prime but a finite number of exceptions.

For further details about representations of compact group we suggest to see [Vi 89].

3.1 Some facts from representation theory

Definition 3.1 (K-representation)**.** Let G be a topological group and K a topological field such that $\mathrm{char}(K) = 0$. We call K-representation of G a continuous group homomorphism $\rho : G \to \mathbb{GL}(V)$ where V is a finite dimensional K-vector space.

Definition 3.2 (Reducible representation)**.** Let $\rho : G \to \mathbb{GL}(V)$ be a K-representation. We say that ρ is a reducible representation if there exists a non trivial linear subspace $W \subset V$ invariant under the action of G. Hence ρ induces a map $\rho : G \to \mathbb{GL}(W)$. Otherwise we say that ρ is irreducible.

Definition 3.3 (K-character)**.** A map $f : G \to K$ is called a K-character if there exists $\rho : G \to \mathbb{GL}(V)$ a K-representation of G such that for every $g \in G$, we have $f(g) = \mathrm{Tr}(\rho(g))$.

We say that f is irreducible if ρ can be chosen to be irreducible. Moreover in this case ρ is unique.

Proposition 3.1 (Decomposition of character)**.** *Let $f : G \to K$ be a K-character, then f can be written in a unique way as a finite sum of irreducible*

characters of G:

$$f = \sum_{\chi} n_\chi \chi$$

where the χ's are irreducible K-characters of G and each n_χ is a strictly positive integer.

Proof (Sketch). Let $\rho : G \to \mathbb{GL}(V)$ be a representation whose character is f. We see V as a $K[G]$-module and hence we find a composition series

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

such that V_i is a $K[G]$-submodule (and in particular a K vector subspace) and the quotient $S_i = V_{i+1}/V_i$ is simple. The S_i are unique up to isomorphism by the Jordan-Holder's theorem. Hence we have irreducible representations $\rho_i : G \to \mathbb{GL}(S_i)$ for $i = 0, \ldots, n$ and the relative characters χ_i. Since $V \cong \bigoplus_i S_i$ as vector spaces we can prove the claim by the following fact. If $\lambda \in \mathbb{GL}(V)$ is a map such that $W \subset V$ is invariant under the action of λ we can find a subspace $W_1 \cong V/W$ such that

$$\begin{array}{ccccccccc} \{0\} & \longrightarrow & W & \longrightarrow & V & \longrightarrow & W_1 & \longrightarrow & \{0\} \\ & & \downarrow{\scriptstyle \lambda_{|W}} & & \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \bar{\lambda}} & & \\ \{0\} & \longrightarrow & W & \longrightarrow & V & \longrightarrow & W_1 & \longrightarrow & \{0\} \end{array}$$

is a commutative diagram and $\mathrm{Tr}(\lambda) = \mathrm{Tr}(\lambda_{|W}) + \mathrm{Tr}(\bar{\lambda})$. So we can write the character f as a sum of the χ_i's, and the summands are uniquely determined by the S_i hence they are unique. □

Definition 3.4 (Virtual character)**.** We say that a map $f : G \to K$ is a K-virtual character if f can be written as a finite linear combination of irreducible K-characters with coefficient in $\mathbb{Z}$.

In the case that the base field $K = \mathbb{Q}_\ell$ we use the expression ℓ-adic representation or character.

3.2 The cohomology ℓ-adic characters

3.2.1 Definition of $h_{X,\ell}$

The Galois action on the cohomology group gives us a first example of a ℓ-adic character.

Definition 3.5. Let X be a scheme of finite type over $\mathbb{Z}$. As in Definition 2.2 we have a map $\Gamma_{\mathbb{Q}} \to \mathrm{Aut}(H^i(X_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell))$ and it is continuous. Denote with $h^i_{X,\ell}$ the character associated to this representation.

Recall that if X is of finite type, then $H^i(X_{\overline{\mathbb{Q}},ét}, \mathbb{Q}_\ell)$ is finite dimensional.

Definition 3.6. Let X be a scheme separated and of finite type over $\mathbb{Z}$. Define the virtual character

$$h_{X,\ell} = \sum_i (-1)^i h^i_{X,\ell}$$

where $h^i_{X,\ell}$ are the characters in Definition 3.5.

The fact that X is separated and of finite type over $\mathbb{Z}$ implies that $X_{\overline{\mathbb{Q}}}$ is a variety over an algebraically closed field and by Proposition 2.1 assures us that $h_{X,\ell}$ is well defined.

3.2.2 Main property of $h_{X,\ell}$

Definition 3.7 (Geometric Frobenius)**.** Let S be a finite set of primes and $\mathbb{Q}_S$ the maximal algebraic extension of $\mathbb{Q}$ unramified outside S. Denote with Γ_S its Galois group. for every prime $p \notin S$ choose an embedding $\mathbb{Q}_S \subset \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ and take k the residue field of the p-adic valuation on $\overline{\mathbb{Q}_p}$. We get the following homomorphism:

$$\iota : \Gamma_{\mathbb{Q}_p} \hookrightarrow \Gamma_{\mathbb{Q}} \twoheadrightarrow \Gamma_S$$

and the exact sequence

$$1 \to I_p \to \Gamma_{\mathbb{Q}_p} \to \mathrm{Gal}(k, \mathbb{F}_p) \to 1.$$

Consider $\sigma_p \in \mathrm{Gal}(k, \mathbb{F}_p)$ the arithmetic Frobenius; we can lift it to an element $\hat{\sigma_p} \in \Gamma_{\mathbb{Q}_p}$ and define the geometric Frobenius as $g_p = \iota(\hat{\sigma_p}^{-1})$.

Note that the definition of g_p does not depend on the choice of the lifting $\hat{\sigma_p}$: since $\mathbb{Q}_S$ is unramified at p the map $\iota : \Gamma_{\mathbb{Q}_p} \to \Gamma_S$ factors modulo I_p. Then g_p is well define up to conjugation in Γ_S.

Proposition 3.2. *Let X be a separated scheme of finite type over $\mathbb{Z}$. For every prime ℓ there exists a finite set of primes S such that the action of $\Gamma_{\mathbb{Q}}$ on $H^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell))$ factors to an action $\Gamma_S \to Aut(H^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell))$.*

Proof. By Proposition 2.6 there exists a finite set of primes S such that the action of $\Gamma_{\mathbb{Q}}$ is unramified outside S. Hence the action $\Gamma_{\mathbb{Q}} \to \mathrm{Aut}(H^i(X_{\overline{\mathbb{Q}},ét}, \mathbb{Q}_\ell))$ factors through I_p for every prime $p \notin S$. Hence it factors to a group homomorphism $\Gamma_S \to \mathrm{Aut}(H^i(X_{\overline{\mathbb{Q}},ét}, \mathbb{Q}_\ell))$. □

Theorem 3.1. *Let X be a separated scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is proper. For a fixed prime ℓ there exists a finite set of primes S such that*

$$N_X(p) = h_{X,\ell}(g_p).$$

Proof. Choose S such that satisfies both Proposition 2.6 and Proposition 3.2. Hence for every non-negative i the action of $\Gamma_{\mathbb{Q}}$ factors to an action $\Gamma_S \to \mathrm{Aut}(H^i(X_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell))$. Moreover $H^i(X_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell)) \cong H^i(X_{\overline{\mathbb{F}_p},\acute{e}t}, \mathbb{Q}_\ell))$ and the actions of respectively Γ_S and $\Gamma_{\mathbb{F}_p}$ are compatible. In particular, if $p \notin S$, the geometric Frobenius g_p acts on $H^i(X_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell))$ as the inverse of the arithmetic Frobenius ${\sigma_p}^{-1}$ acts on $H^i(X_{\overline{\mathbb{F}_p},\acute{e}t}, \mathbb{Q}_\ell))$. Hence

$$h^i_{X,\ell}(g_p) = \mathrm{Tr}(g_p | H^i(X_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell))) = \mathrm{Tr}({\sigma_p}^{-1} | H^i(X_{\overline{\mathbb{F}_p},\acute{e}t}, \mathbb{Q}_\ell))).$$

Recall that $X_{\mathbb{Q}}$ is proper, thus we can find a $N \in \mathbb{N}$ such that $X_{\mathbb{Z}[\frac{1}{N}]}$ is proper. Hence if p does not divide N, then $X_{\overline{\mathbb{F}_p}}$ is a proper $\overline{\mathbb{F}_p}$-variety since the property of being proper is stable under base change. So we can apply Theorem 2.1 to deduce that:

$$\mathrm{Tr}({\sigma_p}^{-1} | H^\bullet(X_{\overline{\mathbb{F}_p},\acute{e}t}, \mathbb{Q}_\ell) = \#X_{\mathbb{F}_p}(\mathbb{F}_p)$$

Now combining the two relations we get:

$$\begin{aligned} N_X(p) = \#X_{\mathbb{F}_p}(\mathbb{F}_p) = Tr({\sigma_q}^{-1} | H^\bullet(X_{\overline{\mathbb{F}_p},\acute{e}t}, \mathbb{Q}_\ell) = \\ = \sum_i (-1)^i \,\mathrm{Tr}({\sigma_p}^{-1} | H^i(X_{\overline{\mathbb{F}_p},\acute{e}t}, \mathbb{Q}_\ell))) = \\ = \sum_i (-1)^i h^i_{X,\ell}(g_p) = h_{X,\ell}(g_p) \qquad . \end{aligned}$$

□

Notice that $g_p \in \Gamma_S$ is defined up to conjugation, hence $h^i_{X,\ell}(g_p)$ is uniquely determined for every non-negative i.

Moreover we have that the value of $h_{X,\ell}(g_p)$ does not depend on the choice of ℓ.

Chapter 4

Weight decomposition

In this chapter we are mostly interested in how "big" the value $h^i_{X,\ell}(g_p)$ can be. For this reason we introduce the notion of weight of a character.

We know that for an elliptic curve E and for all the prime of good reduction we can write $N_E(p) = p + 1 - a_p$, where $|a_p| \leq 2\sqrt{p}$; introducing the notion of weight we will be able to "generalize" the idea of weight decomposition for $N_X(p)$.

4.1 The weight of a ℓ-adic character

4.1.1 Weight of effective characters

Definition 4.1. Let ρ be an ℓ-adic representation of $\Gamma_{\mathbb{Q}}$. We say that ρ is unramified outside a finite set of primes S if ρ factors through the group Γ_S. Hence there exists an ℓ-adic representation $\bar{\rho}$ of Γ_S such that:

$$\begin{array}{ccc} \Gamma_{\mathbb{Q}} & \xrightarrow{\rho} & \mathbb{GL}_n(\mathbb{Q}_\ell) \\ \downarrow & \nearrow_{\bar{\rho}} & \\ \Gamma_S & & \end{array}$$

Definition 4.2 (Representation of weight w)**.** Let ρ be an ℓ-adic representation of $\Gamma_{\mathbb{Q}}$ and let $w \in \mathbb{N}_{\geq 0}$. We say that ρ has weight w if:

(i) ρ is unramified outside a finite set of primes S,

(ii) for every $p \notin S$, the eigenvalues of $\rho(g_p)$ are p-Weil integers of weight w as in Definition 2.5.

Definition 4.3. Let $f : \Gamma_{\mathbb{Q}} \to \mathbb{Q}_\ell$ the character of an ℓ-adic representation of $\Gamma_{\mathbb{Q}}$ and let w be a non-negative integer. Then f has weight w if the associated ℓ-adic representation ρ has weight w.

Remark 4.1. The definition above does not depend on the choice of the representation whose character is f. Indeed proceeding as in the proof of Proposition 3.1, we notice that it depends only on the eigenvalues of the irreducible summands and they are uniquely determined.

4.1.2 Weight of virtual characters

We have a definition of weight for an ℓ-adic character; we want to extend this property to virtual characters in order to study the weight of $h_{X,\ell}$.

Definition 4.4 (Character of weight w)**.** Let $f : \Gamma_{\mathbb{Q}} \to \mathbb{Q}_\ell$ be a virtual character. Hence f can be written as a sum of finitely many irreducible characters:

$$f = \sum_{\chi} n_\chi \chi$$

where all the n_χ are non-zero integers. We say that f has weight w if each irreducible summand has weight w in the sense of Definition 4.3.

Remark 4.2. Let $f : \Gamma_{\mathbb{Q}} \to \mathbb{Q}_\ell$ be a ℓ-adic character, then by the unicity of the decomposition of f as sum of irreducible characters it follows that f has weight w if and only if every irreducible summand has weight w. In this sense Definition 4.4 extends Definition 4.3 to virtual characters.

4.2 The character $h_{X,\ell}$ has a weight decomposition

Let X be a separated scheme of finite type over $\mathbb{Z}$; we want to show that if $X_{\mathbb{Q}}$ is smooth and proper, then $h_{X,\ell}$ has a weight decomposition in the sense that it can be written as a sum of distinct characters each with a weight w.

Definition 4.5 (Weight decomposition)**.** Let $f : \Gamma_{\mathbb{Q}} \to \mathbb{Q}_\ell$ be a ℓ-adic virtual character. If there exists a finite number of distinct weights $w_i \in \mathbb{Z}_{\geq 0}$ and ℓ-adic characters f_i such that:

(i) every f_i has weight w_i,

(ii) $f = \sum_i f_i$,

then we say that f has a weight decomposition.

Lemma 4.1. *Let $f : \Gamma_{\mathbb{Q}} \to \mathbb{Q}_\ell$ be a ℓ-adic virtual character. A weight decomposition of f, if it exists, is unique.*

Proof. Let $f = \sum_i f_i$ with f_i characters of distinct weight w_i. By Proposition 3.1 every f_i can be written uniquely as a $\mathbb{Z}$-linear combination of

irreducible characters, and since f_i has weight w_i all these irreducible characters have weight w_i. Hence $f = \sum_\chi n_\chi \chi$ where χ is irreducible with weight w_i for some i, and they are uniquely determined by f. Define

$$W_i = \{\chi \,|\, \chi \text{ irreducible character with weight } w_i \text{ and } n_\chi \neq 0\}.$$

Then it follows that $f_i = \sum_{\chi \in W_i} n_\chi \chi$ and it is uniquely determined by the decomposition in irreducible characters of f. □

Theorem 4.1 (Weight decomposition of $h_{X,\ell}$)**.** *Let X be a separated scheme of finite type over $\mathbb{Z}$. Suppose that $X_\mathbb{Q}$ is proper and smooth over $\mathbb{Q}$. Then $h^i_{X,\ell}$ has weight i, in particular $h_{X,\ell} = \sum_i (-1)^i h^i_{X,\ell}$ is the weight decomposition of $h_{X,\ell}$.*

Proof. The character $h^i_{X,\ell}$ arises from the Galois action on the cohomology group. Denote with $\rho : \Gamma_\mathbb{Q} \to \mathrm{Aut}(H^i(X_{\overline{\mathbb{Q}},ét}, \mathbb{Q}_\ell))$ the ℓ-adic representation that describes this action. Take S_1 as in Proposition 2.6. It follows that for every prime $p \notin S_1$ the group action is unramified hence as in Proposition 3.2 ρ is unramified outside S_1. Moreover if $p \notin S_1$ we have an isomorphism $H^i(X_{\overline{\mathbb{Q}},ét}, \mathbb{Q}_\ell) \cong H^i(X_{\overline{\mathbb{F}_p},ét}, \mathbb{Q}_\ell)$ and the action of the inverse of the arithmetic Frobenius ${\sigma_p}^{-1} \in \Gamma_{\mathbb{F}_p}$ is compatible with the action of the geometric Frobenius $g_p \in \Gamma_{S_1}$.

Since $X_\mathbb{Q}$ is smooth and proper, by Theorem 1.1 we have $N \in \mathbb{Z}_{>0}$ such that $X_{\mathbb{Z}[1/N]}$ is smooth and proper. Consider S_2 the set of primes that divide N, if $p \notin S_2$ we have the canonical projection $\pi : \mathbb{Z}[1/N] \twoheadrightarrow \mathbb{F}_p$. Since being smooth and proper is stable under base change, then $X_{\mathbb{F}_p} \cong (X_{\mathbb{Z}[1/N]})_{\mathbb{F}_p}$ is smooth and proper. Hence we can apply Deligne's theorem (Theorem 2.2) to deduce that the eigenvalues of ${\sigma_p}^{-1}$ are p-Weil integer of weight i.

Finally considering $S = S_1 \cup S_2$ we get that $h^i_{X,\ell}$ has weight i outside S. □

Remark 4.3. In [Se 12] a more general result is shown. Using the *étale cohomology with proper support*, the existence of a weight decomposition is proved in the case X is only a scheme of finite over $\mathbb{Z}$. Anyway, through this decomposition, we can reduce to the case that the variety $X_\mathbb{Q}$ is smooth and projective.

Example 4.1. Let E be an elliptic curve over $\mathbb{Q}$ and p a prime of good reduction *i.e.* the curve obtained by base change $E_{\mathbb{F}_p}$ is an elliptic curve too.

Consider $\ell \neq p$ be a prime. We have an action of $\mathrm{End}(E_{\mathbb{F}_p})$ on the Tate-module $T_\ell E_{\mathbb{F}_p}$. Define F to be the element of $\mathrm{End}(E_{\mathbb{F}_p})$ such that

$$F((x : y : z)) = (x^p : y^p : z^p) \quad .$$

Then F is a root of its characteristic polynomial which, as shown in [Si 86], is in the form $T^2 - a_p T + b_p$ where $b_p = \det(F) = \deg(F) = p$ and $a_p = \mathrm{Tr}(F) =$

$1 + \deg(F) - \deg(1-F)$. In particular we get that $N_E(p) = \#\mathrm{Ker}(1-F) = \deg(1-F) = 1 + p - a_p$ where $a_p = \mathrm{Tr}(F) = F + \bar{F}$ and in the same way we have $N_E(p^n) = 1 - \mathrm{Tr}(F^n) + p^n = 1 + p^n - (F^n + \bar{F}^n)$.

We have found a weight decomposition for $N_E(p)$ which is not the one arising from Galois representation.

Proposition 4.1. *The weight decomposition $N_E(p) = 1+p-a_p$ is the same as the one given by ℓ-adic representations.*

This fact is trivial if someone is familiar with the étale cohomology otherwise it can be shown in the following way.

First of all we need a numerical Lemma.

Lemma 4.2. *Let $\{a_i\}_{i=0}^t$ and $\{b_i\}_{i=0}^s$ be two finite sequences of complex numbers of norm 1 such that*

$$\lim_{n\to+\infty} \left(\sum_{i=0}^{t} a_i^n - \sum_{i=0}^{s} b_i^n \right) = 0$$

then $t = s$ and $a_i = b_i$ for every i up to re-ordering.

Proof (Sketch). Without loss of generality we can assume $a_0 = 1$. If we show that there exists an element b_j such that $b_j = 1$ we can conclude by inductive arguments. From the hypothesis we can deduce that if we fix $N \in \mathbb{N}$ we have that

$$\lim_{n\to+\infty} \frac{\sum_{j=n}^{n+N} (\sum_{i=0}^{t} a_i^j - \sum_{i=0}^{s} b_i^j)}{N} = 0$$

$$\lim_{n\to+\infty} \left(\sum_{i=0}^{t} \frac{\sum_{j=n}^{n+N} a_i^j}{N} - \sum_{i=0}^{s} \frac{\sum_{j=n}^{n+N} b_i^j}{N} \right) = 0$$

Now we recall that if $z \in \mathbb{C}$ is such that $|z| = 1$ and $z \neq 1$ then $\frac{\sum_{j=1}^{N} z^j}{N} \to 0$ when N is large enough. Hence if $a_0 = 1$ and all the b_j are different from 1 we get an absurd in the computation of the last limit. □

Proof (Proposition). We prove a more general statement from which this proposition follows: if we have two different weight decompositions

$$N_E(p) = \sum_{i=0}^{k} \sum_{j=0}^{n_i} a_{ij} p^{i/2} \quad |a_{ij}| = 1$$

$$N_E(p) = \sum_{i=0}^{k} \sum_{j=0}^{m_i} b_{ij} p^{i/2} \quad |b_{ij}| = 1$$

such that for every $n \in \mathbb{N}_{>0}$

$$N_E(p^n) = \sum_{i=0}^{k} \sum_{j=0}^{n_i} a_{ij}^n p^{ni/2} \quad |a_{ij}| = 1$$

$$N_E(p^n) = \sum_{i=0}^{k} \sum_{j=0}^{m_i} b_{ij}^n p^{ni/2} \quad |b_{ij}| = 1$$

then $n_i = m_i$, and $a_{ij} = b_{ij}$. Indeed by the last equality we deduce that

$$\lim_{n \to +\infty} \left(\sum_{j=0}^{n_k} a_{kj}^n - \sum_{j=0}^{m_k} b_{kj}^n \right) = 0.$$

Now we can apply Lemma 4.2 inductively and conclude the proof of the proposition.

□

Chapter 5

Sato-Tate conjecture

In this chapter we want to state the Sato-Tate conjecture and see what it concretely implies for the function $N_X(p)$.

In this chapter X will be a separated scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is a projective and smooth variety. In this case the ℓ-adic character $h_{X,\ell}$ has a weight decomposition

$$h_{X,\ell} = \sum_i (-1)^i h^i_{X,\ell}.$$

Fix a weight i: we denote with S the finite set of prime such that $h^i_{X,\ell}$ has weight i outside S. Namely:

(i) the character $h^i_{X,\ell}$ is afforded by a ℓ-adic representation $\rho : \Gamma_S \to \mathrm{Aut}(H^i(X_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell))$ unramified outside S.

(ii) If $p \notin S$ the eigenvalues of $\rho(g_p)$ are p-Weil integers of weight i.

Let $n_i = \dim_{\mathbb{Q}_\ell} H^i(X_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell)$, for every prime $p \notin S$ we have:

$$|h^i_{X,\ell}(g_p)| = |\operatorname{Tr}(\rho(g_p))| \leq n_i p^{\frac{i}{2}}.$$

We normalize these values by defining $f^i_{X,\ell}(p) \in \mathbb{R}$ as:

$$f^i_{X,\ell}(p) = h^i_{X,\ell}(g_p)/p^{\frac{i}{2}}$$

so that $f^i_{X,\ell}(p)$ lies in the intervall $I = [-n_i, n_i]$ when $p \notin S$ varies.

A question that naturally rises is: *what is the distribution of the $f^i_{X,\ell}(p)$ in the interval I?* The Sato-Tate conjecture gives a (conjectural) answer to this question.

5.1 Equidistribution statements

Before precisely stating the Sato-Tate conjecture, we start by giving an overview of the consequences of it. The propositions in this section will be proved in Theorem 5.1 assuming that the conjecture holds.

5.1.1 Equidistribution

Definition 5.1. A positive measure μ on a closed interval $I \subset \mathbb{R}$ is a linear form on the space of continuous complex valued functions on I with the following property: if φ is a real non-negative valued function then $\mu(\varphi)$ is real and $\mu(\varphi) \geq 0$.

It is customary to denote $\mu(\varphi)$ as $\int_I \varphi \mathrm{d}\mu$.

Definition 5.2. The mass of a measure μ on a real closed interval I is the integral of the constant function 1: $\mu(1) = \int_I \mathrm{d}\mu$ (*i.e.* the measure of the interval I).

Conjecture 5.1. *Let X be a separated scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is a projective and smooth variety. Fix a weight $i \in \mathbb{Z}_{\geq 0}$, and let $I = [-n_i, n_i]$, S and $f^i_{X,\ell}$ be as above. There exists a unique measure μ of mass 1 on the interval I, such that the sequence $f^i_{X,\ell}(p)$ with p a prime outside the finite set S is equidistributed.*

Proof. refer to Theorem 5.1. □

The equidistribution statement means that for every continuous function $\varphi : I \to \mathbb{C}$ we have:

$$\mu(\varphi) = \lim_{x \to +\infty} \frac{1}{\pi(x)} \sum_{\substack{p \leq x, \\ p \notin S}} \varphi(f^i_{X,\ell}(p))$$

where $\pi(x)$ is the function that counts the number of primes $p \leq x$.

This means that picking a random prime p and computing $f^i_{X,\ell}(p)$ is the same thing that picking a number in I which is random according to μ. Hence the probability that $f^i_{X,\ell}(p)$ lies in an open interval $J \subset I$ is proportional to the measure of the interval $\mu(J)$.

5.1.2 Structure of μ

Definition 5.3. A measure μ on a real closed interval I is said to have a density function with respect to the Lebesgue measure, if there exists a continuous function

$$F : I \to \mathbb{R}_{\geq 0}$$

such that:

(i) F is integrable and $\mathcal{C}^\infty$ except for a finite number of point in I,

(ii) For every continuous $\varphi : I \to \mathbb{C}$ we have that $\mu(\varphi) = \int_I \varphi(z)F(z)\mathrm{d}z$.

Definition 5.4. Let μ be a measure on a closed real interval I. The measure μ is discrete if it is a linear combination of Dirac measures δ_n associated to points $n \in D$, with D a finite subset of I.

If the measure μ is both positive and discrete, it has to be a linear combination of finite δ_n with positive coefficients.

Definition 5.5. Let μ be a measure on a closed real interval I. Let $k \in \mathbb{Z}_{\geq 0}$, a k-th moment for μ is the value $\mu(\varphi_k)$, where $\varphi_k : I \to \mathbb{R}$ is defined by $z \mapsto z^k$.

The k-th moments characterize uniquely the measure μ since the polynomials are dense in the space of continuous functions.

Conjecture 5.2. *Let X be a proper and separated scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is a projective and smooth variety. Fix a weight $i \in \mathbb{Z}_{\geq 0}$, and let μ be the measure on $I = [-n_i, n_i]$ defined in Conjecture 5.1. Then μ can be uniquely decomposed in a continuous and in a discrete part; $\mu = \mu^{cont} + \mu^{disc}$ such that:*

(i) μ^{cont} has a density function with respect to the Lebesgue measure,

(ii) μ^{disc} has a finite support contained in $\mathbb{Z} \cap I$. If i is odd the support of μ^{disc} is $\{0\}$ or $\varnothing$.

Moreover the moments of μ lie in $\mathbb{Z}$

Proof. refer to Theorem 5.1. □

Let us recall that in this case the moment can be expressed as:

$$\mu(\varphi_k) = \int_I z^k \mathrm{d}\mu = \lim_{x \to +\infty} \frac{1}{\pi(x)} \sum_{\substack{p \leq x, \\ p \notin S}} f^i_{X,\ell}(p)^k.$$

5.1.3 Density properties

Definition 5.6. Let Q be a set of primes. Consider the functions

$$\pi,\, \pi_Q : \mathbb{R} \longrightarrow \mathbb{Z}_{\geq 0}$$

defined by $\pi(x)$ is the number of primes $p \leq x$ and $\pi_Q(x)$ is the number of prime $p \in Q$ and $p \leq x$. We define:

(i) the lower density of Q as lower-dens$(Q) = \liminf_{x \to +\infty} \dfrac{\pi_Q(x)}{\pi(x)}$,

(ii) the upper density of Q as upper-dens$(Q) = \limsup_{x \to +\infty} \dfrac{\pi_Q(x)}{\pi(x)}$,

(iii) the density of Q, if the limit exists, as dens$(Q) = \lim_{x \to +\infty} \dfrac{\pi_Q(x)}{\pi(x)}$.

Conjecture 5.3. *Let X be a proper and separated scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is a projective and smooth variety. Fix a weight $i \in \mathbb{Z}_{\geq 0}$, and let μ be the measure on $I = [-n_i, n_i]$ defined in Conjecture 5.1. Let $z \in I$ and $J \subset I$ an open interval. Consider the set of primes*

$$P_z = \{p \mid p \notin S \quad f^i_{X,\ell}(p) = z\}$$

$$P_J = \{p \mid p \notin S \quad f^i_{X,\ell}(p) \in J\}.$$

The densities of the sets P_z and P_J in the sense of Definition 5.6 are respectively $\mu(\{z\})$ and $\mu(J)$.

Proof. refer to *Theorem* 5.1. □

The statement of this conjecture is compatible with the measure structure described in Conjecture 5.2. The measure $\mu(\{z\}) \neq 0$ if and only if z lies in the support of μ^{disc} which is contained in $\mathbb{Z}$. As far as P_z is concerned, the facts that $f^i_{X,\ell}(p) = h^i_{X,\ell}(g_p)/p^{\frac{i}{2}}$ and $h^i_{X,\ell}(g_p) \in \mathbb{Z}$ imply that P_z contains at most one point if $z \notin \mathbb{Z}$. Hence when z is not an integer both $\mu(\{z\})$ and P_z are zero.

5.2 The Sato-Tate conjecture

Let X be a separated proper scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is smooth and projective. The Sato-Tate conjecture claims the equidistribution of the $N_X(p)$ when p varies outside a finite set S in term of real measure and real interval. The values of the $N_X(p)$'s are determined by the ℓ-adic cohomology. The crux of the conjecture is to construct a real measure out of ℓ-adic data. The "missing link" between ℓ-adic and real is Lie theory.

5.2.1 Cohomological data

The cohomological data have to contain all the information about $N_X(p)$.

Definition 5.7 (Good reduction)**.** Let Y be a smooth variety over $\mathbb{Q}$ and let $S = \{p_1, p_2, \dots p_r\}$ a finite set of primes. We say that Y has a good reduction if exists a projective and smooth scheme $\mathcal{Y}$ over $\mathbb{Z}[\frac{1}{p_1}, \dots, \frac{1}{p_r}]$ such that the base change $\mathcal{Y}_{\mathbb{Q}}$ is isomorphic as a $\mathbb{Q}$-scheme to Y.

Definition 5.8 (Cohomological data)**.** A set of cohomological data is:

(D_1) a smooth and projective variety Y over $\mathbb{Q}$,

(D_2) a weight $i \in \mathbb{Z}_{\geq 0}$.

Remark 5.1. In this setting, using the spreading out theorem we can find a smooth and projective scheme $\mathcal{Y}$ over $\mathbb{Z}[1/N]$ for some $N \in \mathbb{N}$ such that $\mathcal{Y}_{\mathbb{Q}} = Y$. Then proceeding as in the proof of Theorem 4.1, we can find a set of prime S (including the prime divisor of N) such that the character $h^i_{Y,\ell}$ has weight i outside S and such that for every prime $p \notin S$ we have $H^i(\mathcal{Y}_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell) \cong H^i(\mathcal{Y}_{\overline{\mathbb{F}_p},\acute{e}t}, \mathbb{Q}_\ell)$ and the actions of $\Gamma_{\mathbb{Q}}$ and $\Gamma_{\mathbb{F}_p}$ are compatible.

Remark 5.2. Let S be the set described in the Remark above. Let g_p and σ_p be respectively the geometric and the arithmetic Frobenius. If $p \notin S$, then g_p acts on $H^i(\mathcal{Y}_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell)$ as ${\sigma_p}^{-1}$ acts on $H^i(\mathcal{Y}_{\overline{\mathbb{F}_p},\acute{e}t}, \mathbb{Q}_\ell)$. By Deligne's theorem the characteristic polynomial of g_p lies in $\mathbb{Z}[T]$, and its roots are p-Weil integers of weight i. Denote this polynomial with

$$P_i(p,T) = T^{n_i} - a_1 T^{n_i-1} + a_2 T^{n_i-2} - \dots \quad ,$$

where $n_i = \dim_{\mathbb{Q}_\ell} H^i(Y_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell)$ and $a_1 = \mathrm{Tr}(g_p | H^i(Y_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell))$. Since g_p is defined up to conjugation the polynomial $P_i(p,T)$ is well defined.

We know that all the roots of $P_i(p,T)$ have absolute value $p^{\frac{i}{2}}$; so we define

$$P_i^{\mathrm{norm}}(p,T) = p^{n_i \frac{i}{2}} P_i(p, p^{\frac{i}{2}} T) = T^{n_i} - \frac{a_1}{p^{i/2}} T^{n_i-1} + \frac{a_2}{p^i} T^{n_i-2} - \dots \quad .$$

Denote with $f_i(p)$ the normalized trace:

$$f_i(p) = \frac{a_1}{p^{i/2}} = \frac{\mathrm{Tr}(g_p | H^i(Y_{\overline{\mathbb{Q}},\acute{e}t}, \mathbb{Q}_\ell))}{p^{i/2}}.$$

Since the roots of $P_i^{\mathrm{norm}}(p,T)$ have absolute value 1, we get that $f_i(p)$ lies in the real interval $[-n_i, n_i]$ for all the $p \notin S$.

In particular if we start with X a separated scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is projective and smooth, then for every non-negative i we have the set of cohomological data $(X_{\mathbb{Q}}, i)$. As the Remark 5.1 and 5.2 show, we can recover the set S and the value of $f_i(p) = f^i_{X,\ell}(p)$.

5.2.2 The conjecture

First of all we introduce the counterpart of cohomological data:

Definition 5.9 (Lie group data)**.** A set of Lie group data is:

(ST_1) a compact real Lie group K, the Sato-Tate group,

(ST_2) a smooth linear representation $\rho : K \to \mathbb{GL}_n(\mathbb{C})$ of degree n,

(ST_3) a conjugacy class $s_p \in \mathrm{Cl}(K)$ for every prime outside a finite set S.

Then we have to see how the cohomological and lie group data are related.

Definition 5.10 (Sato-Tate conjecture)**.** We say that a set of cohomological data (Y, i) satisfies the Sato-Tate conjecture if there exists a set of Lie group data $(K, \rho, \{s_p\}_{p \notin S})$ such that the following axioms hold.

(A_1) The set S in the Lie group data has the following properties. Outside S, the $\mathbb{Q}$-variety Y has a good reduction, the Galois action on $H^i(Y_{\overline{\mathbb{Q}}, \acute{e}t}, \mathbb{Q}_\ell)$ is unramified and for every $p \notin S$ the action of g_p is compatible with the action of ${\sigma_p}^{-1}$ (*i.e.* S has the properties stated in Remark 5.1),

(A_2) For every $p \notin S$ the characteristic polynomial of $\rho(s_p)$ is equal to the normalized polynomial $P_i^{\mathrm{norm}}(p, T)$ defined in Remark 5.2. In particular the degree of ρ is n_i and $\mathrm{Tr}(\rho(s_p)) = f_i(p)$.

(A_3) $\rho : K \to \mathbb{GL}_{n_i}(\mathbb{C})$ is injective.

(A_4) The s_p are equidistributed in $\mathrm{Cl}(K)$ with respect to the Haar measure.

Notice that in (A_2) the element $\rho(s_p)$ lies in $\mathrm{Cl}(\mathbb{GL}_{n_i}(\mathbb{C}))$ hence its characteristic polynomial is well defined. By the "Haar measure" on $\mathrm{Cl}(K)$ we mean the pushforward of the the Haar measure μ_K on the compact group K. If we consider the natural projection $\pi : K \to \mathrm{Cl}(K)$, then

$$\mu_{\mathrm{Cl}(K)}(\varphi) = \pi_* \mu_K(\varphi) = \mu_K(\varphi \circ \pi)$$

for every continuous complex function φ on $\mathrm{Cl}(K)$.

5.3 The main theorem

We have introduced the Sato-Tate conjecture, now we want to see what it implies.

Theorem 5.1 (Main Theorem)**.** *Let Y be a projective and smooth variety over $\mathbb{Q}$. Fix a prime ℓ and a weight i. Consider the set of cohomological data (Y, i) and assume that it satisfies the Sato-Tate conjecture i.e. there exists a set of Lie group data $(K, \rho, \{s_p\}_{p \notin S})$ as in Definition 5.10. Hence for every $p \notin S$ the value $f_i(p) = f^i_{Y,\ell}(p)$ lies in the interval $I = [-n_i, n_i]$ where $n_i = \dim_{\mathbb{Q}_\ell} H^i(Y_{\overline{\mathbb{Q}}, \text{ét}}, \mathbb{Q}_\ell)$.*

Then the following statements hold.

(i) There exists a unique measure μ of mass 1 on the interval I, such that the sequence of the $f_i(p)$'s is equidistributed,

(ii) μ can be uniquely decomposed in a continuous and in a discrete part; $\mu = \mu^{cont} + \mu^{disc}$ such that: μ^{cont} has a density function with respect to the Lebesgue measure, and μ^{disc} has support contained in $I \cap \mathbb{Z}$, the support is contained in $\{0\}$ when the weight i is odd. Moreover the moments of μ lie in $\mathbb{Z}$,

(iii) The densities of the set $P_z = {f_i}^{-1}(\{z\})$ and $P_J = {f_i}^{-1}(J)$ are respectively equals to $\mu(\{z\})$ and $\mu(J)$ when $z \in I$ and $J \subset I$ is an open interval,

Remark 5.3. Let X be a separated scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is a projective and smooth variety. If we assume that the Sato-Tate conjecture holds for the set of cohomological data $(X_{\mathbb{Q}}, i)$ then Conjecture 5.1, Conjecture 5.2 and Conjecture 5.3 hold.

5.3.1 Proof of the main theorem

Definition of μ and equidistribution

Let $\psi = \mathrm{Tr}(\rho)$ be the character of the representation ρ of K. Since $\psi : K \to \mathbb{C}$ is a smooth character it factors to a smooth map $\bar{\psi} : \mathrm{Cl}(K) \to \mathbb{C}$. Applying the axiom (A_2) we get that for every $p \notin S$

$$\bar{\psi}(s_p) = \mathrm{Tr}(\rho(s_p)) = f_i(p) \in I\,.$$

Since the s_p are equidistributed in $\mathrm{Cl}(K)$ with respect to the Haar measure, they form a dense subset of $\mathrm{Cl}(K)$. We conclude that $\bar{\psi} : \mathrm{Cl}(K) \to I$. So we can lift the Haar measure of $\mathrm{Cl}(K)$ to the interval I or equivalently lift the Haar measure of K via $\psi : K \to I$. Define

$$\mu = \mu_I = \bar{\psi}_* \mu_{\mathrm{Cl}(K)} = \psi_* \mu_K.$$

By the equality $\bar{\psi}(s_p) = f_i(p)$ and the equidistribution of s_p in $\mathrm{Cl}(K)$ we get that $f_i(p)$ are equidistributed in I according to μ.

Compute the mass of this measure μ:

$$\mu(I) = \int_I 1 \mathrm{d}\mu = \int_K 1 \circ \psi \mathrm{d}\mu_K = \int_K 1 \mathrm{d}\mu_K = 1.$$

Hence we have a measure μ on I of mass 1 and such that the sequence of $f_i(p)$ is equidistributed. The uniqueness follows from the fact that by the equidistribution we can write

$$\mu(\varphi) = \lim_{x \to +\infty} \frac{1}{\pi(x)} \sum_{\substack{p \leq x, \\ p \notin S}} \varphi(f_i(p))$$

for every $\varphi : I \to \mathbb{C}$ continuous function.

k-th moments

Proposition 5.1. *Let K be a topological compact group with μ its Haar measure. Consider a complex character $\theta : K \to \mathbb{C}$; it can be decompose as a sum of irreducible complex characters χ's*

$$\theta = \sum_{\chi} n_\chi \chi$$

such that all the n_χ are positive integer. Consider χ an irreducible character and denote with $\overline{\chi}$ the complex conjugate character then

$$n_\chi = \int_K \theta \overline{\chi} \mathrm{d}\mu.$$

Proof. The proof can be found in [Vi 89] in the case of finite groups. To deduce the compact case, the integration replaces the average summation over the elements of the group. A crucial feature of the Haar measure is the invariance by left multiplication. □

The k-th moment $\mu(\varphi_k)$ is defined as $\int_I z^k \mathrm{d}\mu = \int_I \psi^k \mathrm{d}\mu_K$. Consider the complex irreducible character χ_0 given by the trivial representation $K \to \mathbb{C}^* \cong \mathbb{GL}_1(\mathbb{C})$ that send all the elements of K to 1. Recall that since ψ is a complex character of K also ψ^k is a character. Let n_{χ_0} be the coefficient of χ_0 in the expansion of the character ψ^k as a $\mathbb{Z}_{\geq 0}$-linear combination of irreducible characters. Then by *Proposition* 5.1

$$n_{\chi_0} = \int_K \psi^k \overline{\chi_0} \mathrm{d}\mu_K = \int_K \psi^k \mathrm{d}\mu_K = \mu(\varphi_k)$$

in particular the k-th moment is an integer.

Structure of μ

Consider K_0 the identity connected component of K. It is a normal open and closed subgroup. Moreover since K is compact the quotient group K/K_0 is finite; let N be its cardinality. For every σ in the quotient group we have $K_\sigma = \sigma K_0$ the corresponding K_0-coset. The subspace K_σ is a connected compact submanifold of K. Let μ_{K_σ} be the restriction of the Haar measure of K on K_σ. Since the Haar measure is invariant by left multiplication by elements of the group K, we get that μ_{K_σ} has total mass $\frac{1}{N}$. Denote $\mu_\sigma = \psi_* \mu_{K_\sigma}$; we have the following relation:

$$\mu = \psi_* \mu_K = \psi_* \sum_\sigma \mu_{K_\sigma} = \sum_\sigma \psi_* \mu_{K_\sigma} = \sum_\sigma \mu_\sigma$$

Let D be the subset of K/K_0 defined by:

$$D = \{\sigma \in K/K_0 \quad | \quad \psi \text{ is constant on } K_\sigma\}$$

Define μ^{disc} and μ^{cont} as follow:

$$\mu^{\mathrm{disc}} = \sum_{\sigma \in D} \mu_\sigma \qquad \mu^{\mathrm{cont}} = \sum_{\sigma \notin D} \mu_\sigma$$

and clearly $\mu = \mu^{\mathrm{disc}} + \mu^{\mathrm{cont}}$.

Properties of $\mu^{\mathbf{disc}}$

If $\sigma \in D$, let n_σ be the constant value of ψ on K_σ; then the measure μ_σ is clearly a Dirac measure of the form $\frac{1}{N}\delta_{n_\sigma}$. This suffices to show that μ^{disc} is a discrete measure.

Lemma 5.1. *If $\sigma \in D$, and let n_σ be the constant value of ψ on K_σ then n_σ lies in $\mathbb{Z}$. Moreover if the weight i is odd, $n_\sigma = 0$.*

Proof. Let $\pi : K \twoheadrightarrow \mathrm{Cl}(K)$ the canonical projection, and let $C_\sigma = \pi(K_\sigma)$. Note that C_σ is open and closed in $\mathrm{Cl}(K)$ since the same properties hold for $K_\sigma \subset K$. The classes s_p are equidistributed in $\mathrm{Cl}(K)$ and in particular they are dense in $\mathrm{Cl}(K)$. Hence there exists two distinct prime q_1 and q_2 outside S such that the respective classes s_{q_1} and s_{q_2} lie in C_σ, so we have

$$n_\sigma = \bar{\psi}(s_{q_1}) = \frac{h^i_{X,\ell}(q_1)}{{q_1}^{i/2}} = \bar{\psi}(s_{q_2}) = \frac{h^i_{X,\ell}(q_2)}{{q_2}^{i/2}}.$$

In particular we get the equation

$$h^i_{X,\ell}(q_1){q_2}^{i/2} = h^i_{X,\ell}(q_2){q_1}^{i/2}.$$

Assume that i is even: since $h^i_{X,\ell}$ and $h^i_{X,\ell}$ lie in $\mathbb{Z}$ the equation above implies that ${q_1}^{i/2}$ divides $h^i_{X,\ell}(q_1)$ hence $n_\sigma \in \mathbb{Z}$.

Otherwise if i is odd and $n_\sigma \neq 0$, by the equation above we get that $(\frac{p}{q})^{1/2} \in \mathbb{Q}$ which leads to an absurd. Hence if i is odd the only possibility is $n_\sigma = 0$. □

Properties of $\mu^{\mathbf{cont}}$

First of all we recall an important result of Lie groups. For further information about the following fact we suggest to see the proof in [Kn 02].

Proposition 5.2. *Each Lie group admits the structure of a real analytic manifold in one and only one way such that both multiplication and inverse are analytic maps.*

Lemma 5.2. *Let $g : Y \to \mathbb{R}$ be a $\mathcal{C}^\infty$-function on a compact differential oriented real manifold of dimension N. Let C be the set of critical points of g i.e. the $y \in Y$ such that $dg = 0$, and let $V = g(C)$ be the set of critical value of g. Let α be a $\mathcal{C}^\infty$-differential form of degree N over Y. Assume that α induces a positive measure such that the measure of C is zero and assume that the set V is finite. Then the measure on $\mathbb{R}$ induced by α through g has a density.*

The hypotheses of the Lemma are fulfilled by $\psi : K_\sigma \to I$ when $\sigma \notin D$. Indeed, the Lie group K has a natural real analytic structure. Since ψ is not

constant on K_σ then the set of critical point C has empty interior; since C is closed, analytic (*i.e.* it can be defined as the zeros of an analytic function), with empty interior, then its Haar measure is zero. Moreover since ψ is constant on every connected component of C, and C is compact with empty interior then the image $\psi(C)$ consists of a finite number of points.

Proof (Sketch). For the proof we outline the main steps done in [De 09].

Let $Y_0 = Y \setminus g^{-1}(V)$ and let $g_0 : Y_0 \to \mathbb{R} \setminus V$ the restriction of g to Y_0. g_0 is a $\mathcal{C}^\infty$-function. We can apply the "integration over the fiber process". Let z be a point of $\mathbb{R} \setminus V$, denote with Y_z the preimage ${g_0}^{-1}(z)$. If $y \in Y_z$ we can choose a local system of coordinates $(t_1, \ldots, t_N)$ such that the last coordinate is given by $g - z$. In a neighborhood of y, we write α as $a(t_1, \ldots, t_N)\mathrm{d}t_1 \wedge \cdots \wedge \mathrm{d}t_N$ where a is a a smooth function. Consider on Y_z the $(N-1)$-differential form $\alpha_z = a(t_1, \ldots, t_{N-1}, 0)\mathrm{d}t_1 \wedge \cdots \wedge \mathrm{d}t_{N-1}$. The orientation of Y induces a orientation on Y_z hence α_z define a measure on Y_z such that for every φ continuous function with compact support on Y_0 we have:

$$\int_{y \in Y_0} \varphi(y)\alpha(y) = \int_{z \in \mathbb{R} \setminus V} \left(\int_{y \in Y_z} \varphi(y)\alpha_z(y) \right) \mathrm{d}z.$$

(The proof of this fact is based on local computation, based on the Lebesgue-Fubini theorem). Define the function $F(z) = \int_{Y_z} \alpha_z$. It is $\mathcal{C}^\infty$ function on $\mathbb{R} \setminus V$ and if we denote with α_0 the measure induced by α on Y_0 we get that for every continuous real valued map φ on $\mathbb{R} \setminus V$

$$\begin{aligned} g_*\alpha_0(\varphi) = \alpha_0(\varphi \circ g) = \int_{y \in Y_0} \varphi(g(y))\alpha(y) = \\ = \int_{z \in \mathbb{R} \setminus V} \left(\int_{y \in Y_z} \varphi(g(y))\alpha_z(y) \right) \mathrm{d}z = \\ \int_{z \in \mathbb{R} \setminus V} \varphi(z)F(z)\mathrm{d}z = \int_{z \in \mathbb{R}} \varphi(z)F(z)\mathrm{d}z \quad . \end{aligned}$$

The function F is $\mathcal{C}^\infty$ on $\mathbb{R}$ outside a finite set of points, is positive and integrable since its integral is equal to the mass of α_0. In conclusion the measure $g_*\alpha_0$ on $\mathbb{R}$ has a density.

Consider $\beta = g_*\alpha - g_*\alpha_0$. It is a measure on a compact subset of $\mathbb{R}$. We know that β is the null measure on $\mathbb{R} \setminus V$, moreover V has measure 0 with respect to $g_*\alpha$ by hypothesis and it is clearly 0 for $g_*\alpha_0$. Hence β is the null measure. We conclude that $g_*\alpha$ and $g_*\alpha_0$ coincide as measures and in particular $g_*\alpha$ has a density. □

Density properties

Lemma 5.3. *If A is any subset of I, let P_A be the set of primes $p \notin S$ such that $f_i(p) \in A$. Then*

(i) if A is open then lower-dens$(P_A) \geq \mu(A)$,

(ii) if A is closed then upper-dens$(P_A) \leq \mu(A)$.

Proof. Let A be an open subset of I. By definition $\mu(A)$ is the upper bound of $\mu(\varphi)$ for every positive continuous function $\varphi \leq 1$ that vanish outside A. Consider one of this φ, since $\mathrm{supp}(\varphi) \subset A$ we get that for every positive real number x:

$$\sum_{p \leq x} \varphi(f_i(p)) \leq \sum_{\substack{p \leq x, \\ p \in A}} 1 = \pi_A(x)$$

Applyng the fact that the $f_i(p)$ are equidistributed, we conclude that for every φ with the properties above

$$\mu(\varphi) = \lim_{x \to +\infty} \frac{1}{\pi(x)} \sum_{p \leq x} \varphi(f_i(p)) \leq \text{lower-dens}(P_A)\,.$$

Since $\mu(A)$ is the upper bound of $\mu(\varphi)$ we get the thesis.

When A is closed the proof is similar. □

Lemma 5.4. *Let A be a finite subset of I and let P_A be the set of primes $p \notin S$ such that $f_i(p) \in A$. Then dens$(P_A) = \mu(A)$.*

Applying the Lemma to $A = \{z\}$ it follows that $\mathrm{dens}(P_z) = \mu(\{z\})$.

Proof. We define D and K_σ as in the previous paragraphs.

Let $K_A \subset K$ be the inverse image via ψ of the finite set A; we have that $p \in P_A$ if and only if $s_p \subset K_A$.

We split K as $K = K' \sqcup K''$; where $K' = \bigsqcup_{\sigma \in D} K_\sigma$ and $K'' = \bigsqcup_{\sigma \notin D} K_\sigma$. Then intersecting with K_A we have the decomposition $K_A = K'_A \sqcup K''_A$ and similarly $P_A = P'_A \sqcup P''_A$.

The set K'_A is the union of K_0-coset on which ψ is constant and this constant value lies in A. Notice that K'_A is open and closed hence measurable. By Lemma 5.3 it follows that $\mathrm{dens}(P'_A) = \mu_K(K'_A) = \mu^{\mathrm{disc}}(A)$. On the other hand K''_A is closed, analytic with empty interior since K has a real analytic structure. So it follows that $\mathrm{dens}(P''_A) = \mu_K(K''_A) = 0$. Thus we have $\mathrm{dens}(P_A) = \mathrm{dens}(P'_A) = \mu^{\mathrm{disc}}(A) = \mu(A)$.

□

Lemma 5.5. *Let $A \subset I$ be an open interval. Then P_A has density equal to $\mu(A)$.*

Proof. Denote with $\overline{A}$ the topological closure of A in I and with ∂A the boundary of A. From the previous lemmas we know that

$$\text{lower-dens}(P_A) \geq \mu(A)\,,$$

$$\text{upper-dens}(P_{\overline{A}}) \leq \mu(\overline{A})\,,$$
$$\text{dens}(P_{\partial A}) = \mu(\partial A)\,.$$

Since $\text{upper-dens}(P_A) = \text{upper-dens}(P_{\overline{A}}) - \text{dens}(P_{\partial A})$ we can conclude that

$$\text{upper-dens}(P_A) \leq \mu(\overline{A}) - \mu(\partial A) = \mu(A)\,.$$

Using the following relation

$$\mu(A) \leq \text{lower-dens}(P_A) \leq \text{upper-dens}(P_A) \leq \mu(A)\,;$$

we get that P_A has a density and $\text{dens}(P_A) = \mu(A)$. □

Chapter 6

Example of a chosen elliptic curve with CM

The Sato-Tate conjecture holds in the case we are considering elliptic curves with complex multiplication. In order to understand how this has been proved, we investigate an example.

In this chapter we will consider the elliptic curve E defined by the polynomial $Y^2 = X^3 - X$ and we want to find the Sato-Tate group for this curve.

The general proof proceed in two main steps.

(i) Construction of a Hecke character ψ defined on the ideals of the CM-field such that for every prime $p \in \mathbb{Z}$ we have that

$$a_p = \psi(\mathfrak{p}) + \overline{\psi(\mathfrak{p})}$$

where $\mathfrak{p}$ is a prime ideal in the CM-field over p. Hence we can write the L-function of the elliptic curve as an L-function of a number field.

(ii) Deduce the equidistribution of the values $\frac{a_p}{p^{1/2}}$ studying the analytic properties of the L-function.

6.1 Multiplicative characters

In this section we want to give a framework of multiplicative characters of a finite field, and see some applications of them in order to count solutions of equations modulo prime integers. We will mainly follow [IR 82] as reference.

Finally we introduce the quartic residue character for a prime ideal $\mathfrak{p} \subset \mathbb{Z}[i]$.

6.1.1 Basic properties of multiplicative characters

Definition 6.1. A multiplicative character on $\mathbb{F}_p$ is a group homomorphism $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$. We denote with $\hat{\mathbb{F}_p}$ the group of multiplicative characters on $\mathbb{F}_p$.

Clearly $\hat{\mathbb{F}_p}$ is a group by means of the following definitions:

(i) if χ and λ are two characters, then $\chi\lambda$ is the map that takes $a \in \mathbb{F}_p^*$ to $\chi(a)\lambda(a)$,

(ii) if χ is a character, then χ^{-1} is the map that takes $a \in \mathbb{F}_p^*$ to $\chi(a)^{-1}$,

(iii) let ϵ the unitary character defined by $\epsilon(a) = 1$ for every $a \in \mathbb{F}_p^*$.

Proposition 6.1. *The group $\hat{\mathbb{F}_p}$ is cyclic of order $p-1$.*

Proof. We know that $\mathbb{F}_p^*$ is a cyclic group, let denote with g a generator. A character χ is uniquely determined by the value $\chi(g)$; since this value is a $(p-1)$-th root of unity, there are at most $p-1$ multiplicative characters.

Define the character λ by $\lambda(g) = e^{\frac{2\pi i}{p-1}}$. We conclude the proof noticing that $\epsilon, \lambda, \lambda^2, \ldots, \lambda^{p-2}$ are all distinct since they differ on the element g. □

Characters are useful in counting solutions of equations as explained in the following propositions. For our purpose we extend the character over $\mathbb{F}_p$ setting $\chi(0) = 0$ if $\chi \neq \epsilon$ and $\epsilon(0) = 1$.

Lemma 6.1. *Let a be an element of $\mathbb{F}_p^*$ and n be a divisor of $p-1$. Assume $X^n = a$ is not solvable in $\mathbb{F}_p$, then there exists a character $\chi \in \hat{\mathbb{F}_p}$ such that:*

(i) $\chi^n = \epsilon$,

(ii) $\chi(a) \neq 1$.

Proof. Let g be a generator of $\mathbb{F}_p^*$. Define χ setting $\chi(g) = e^{\frac{2\pi i}{n}}$. Then it is clear that $\chi^n = \epsilon$ and $\chi(a) \neq 1$. Indeed if we write $a = g^m$ then $\chi(a) = e^{\frac{2\pi i m}{n}}$; this value is equal to 1 if and only if $n|m$ but this is not possible, otherwise $g^{m/n}$ would be a solution of $X^n = a$. □

Proposition 6.2. *Let $N(X^n = a)$ be the number of solutions in $\mathbb{F}_p$ of the equation $X^n = a$. If $n|p-1$ then*

$$N(X^n = a) = \sum_{\substack{\chi \in \hat{\mathbb{F}_p} \\ \chi^n = \epsilon}} \chi(a).$$

Proof. First of all we study the case $a = 0$. The equation $X^n = 0$ has only one solution for $X = 0$. It is clear that $\sum_{\chi^n=\epsilon} \chi(0) = 1$ since $\epsilon(0) = 1$ and $\chi(0) = 0$ for $\chi \neq \epsilon$.

If $X^n = a$ is solvable and $a \neq 0$, then $X^n = a$ has exactly n solution. Indeed, if b is a solution and g is a generator of $\mathbb{F}_p^*$ then all the elements $bg^{\frac{k(p-1)}{n}}$ for $k = 0, 1, \ldots, n-1$ are distinct solutions. Moreover the characters, whose order divides n, are exactly n; they are generated as a cyclic group by the character ρ such that $\rho(g) = e^{\frac{2\pi i}{n}}$. Notice that for all the χ appearing in the sum $\chi(a) = \chi(b^n) = \epsilon(b) = 1$ and so $\sum_{\chi^n=\epsilon} \chi(a) = n$.

If $X^n = a$ is not solvable, we denote $T = \sum_{\chi^n=\epsilon} \chi(a)$ and denote with ρ the character described in Lemma 6.1. Then

$$\rho(a)T = \sum_{\chi^n=\epsilon} \rho(a)\chi(a) = \sum_{\chi^n=\epsilon} \rho\chi(a) = T$$

since the group of characters of order dividing n form a group. Since $\rho(a) \neq 1$ we get $T = 0$. □

6.1.2 Gauss and Jacobi sums

Definition 6.2 (Gauss sum)**.** Let χ be a character on $\mathbb{F}_p$ and let a be an element of $\mathbb{F}_p^*$. A Gauss sum belonging to χ is

$$G_a(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta^{at}$$

where $\zeta = e^{\frac{2\pi i}{p}}$.

Lemma 6.2. *If $\chi \neq \epsilon$, then $|G_1(\chi)| = \sqrt{p}$.*

Proof. First we notice that

$$\chi(a)G_a(\chi) = \chi(a) \sum_t \chi(t)\zeta^{at} = \sum_t \chi(at)\zeta^{at} = G_1(\chi).$$

It follows that

$$G_a(\chi)\overline{G_a(\chi)} = \chi(a^{-1})\overline{\chi(a^{-1})}G_1(\chi)\overline{G_1(\chi)} = |G_1(\chi)|^2.$$

On the other hand,

$$G_a(\chi)\overline{G_a(\chi)} = \sum_t \sum_s \chi(t)\overline{\chi(s)}\zeta^{at-as}.$$

We recall that $\sum_{t=0}^{p-1} \zeta^{at}$, by simple computation, is equal to p if $a \equiv 0$ and 0 otherwise. Thus we get

$$(p-1)|G_1(\chi)|^2 = \sum_{a\in\mathbb{F}_p^*} G_a(\chi)\overline{G_a(\chi)} = \sum_t \sum_s \sum_a \chi(t)\overline{\chi(s)}\zeta^{at-as} = p(p-1).$$

□

Definition 6.3 (Jacobi sum)**.** Let χ and λ be characters of $\mathbb{F}_p$ define the Jacobi sum as

$$J(\chi,\lambda)=\sum_{\substack{a,b\in\mathbb{F}_p\\ a+b\equiv 1}}\chi(a)\lambda(b).$$

Proposition 6.3. *Let χ and λ be non trivial characters of $\mathbb{F}_p$ then:*

(i) $J(\epsilon,\epsilon)=p$,

(ii) $J(\epsilon,\chi)=0$,

(iii) $J(\chi,\chi^{-1})=-\chi(-1)$,

(iv) if $\chi\lambda\neq\epsilon$, *then* $J(\chi,\lambda)=\frac{G_1(\chi)G_1(\lambda)}{G_1(\chi\lambda)}$.

Proof. Part *(i)* is trivial.

To prove *(ii)* we notice that $\sum_{a\in\mathbb{F}_p}\chi(a)=0$. Indeed, if $T=\sum_{a\in\mathbb{F}_p}\chi(a)$ and $b\in\mathbb{F}_p$ such that $\chi(b)\neq 1$, then

$$\chi(b)T=\sum_{a\in\mathbb{F}_p}\chi(ba)=T$$

and hence $T=0$. By this fact it follows immediately *(ii)*.

Part *(iii)* follows by a simple computation:

$$J(\chi,\chi^{-1})=\sum_{a+b\equiv 1}\chi(a)\chi^{-1}(b)=\sum_{\substack{a+b\equiv 1\\ b\neq 0}}\chi(ab^{-1})=\sum_{a}\chi(a(1-a)^{-1})$$

The map $a\mapsto a(1-a)^{-1}$ gives a bijection between $\mathbb{F}_p\setminus\{1\}$ and $\mathbb{F}_p\setminus\{-1\}$. Thus

$$J(\chi,\chi^{-1})=\sum_{a\neq -1}\chi(a)=-\chi(-1)$$

due to the fact used in part *(ii)*.

To prove part *(iv)* notice that

$$G_1(\chi)G_1(\lambda)=\sum_{a,b}\chi(a)\lambda(b)\zeta^{a+b}=\sum_{t}\left(\sum_{a+b\equiv t}\chi(a)\chi(b)\right)\zeta^t.$$

If $t=0$, since $\chi\lambda\neq\epsilon$ we have

$$\sum_{a+b\equiv 0}\chi(a)\lambda(b)=\sum_{a}\chi(a)\lambda(-a)=\lambda(-1)\sum_{a}\chi\lambda(a)=0=\chi\lambda(0)J(\chi,\lambda).$$

If $t\neq 0$, we get

$$\sum_{a+b\equiv t}\chi(a)\lambda(b)=\sum_{a+b\equiv 1}\chi(ta)\lambda(tb)=\chi\lambda(t)J(\chi,\lambda).$$

In the end by a simple substitution we get

$$G_1(\chi)G_1(\lambda) = \sum_t \chi\lambda(t)J(\chi,\lambda)\zeta^t = G_1(\chi\lambda)J(\chi,\lambda).$$

□

Corollary 6.1. *If χ, λ and their product $\chi\lambda$ are non trivial characters, then $|J(\chi,\lambda)| = \sqrt{p}$.*

Proof. Combine part *(iv)* of Proposition 6.3 and Lemma 6.2. □

6.1.3 The quartic residue symbol

In this section we will denote with K the field $\mathbb{Q}(i)$, where i is a solution of the equation $X^2 + 1 = 0$ and with O_K the ring of integer $\mathbb{Z}[i]$. We recall that $\mathbb{Z}[i]$ is a principal ideal domain.

Remark 6.1. Let $p \in \mathbb{Z}$ be a prime integer: according to how the polynomial $X^2 + 1$ decomposes in $\mathbb{F}_p$ we deduce that:

(i) if $p \equiv 1 \pmod 4$ the the ideal $pO_K = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p} = (\pi)$ and $\overline{\mathfrak{p}} = (\overline{\pi})$ and the residue fields have cardinality p,

(ii) if $p \equiv 3 \pmod 4$ the ideal pO_K is still a prime ideal and the residue field has cardinality p^2,

(iii) if $p = 2$ the ideal $2O_K$ decomposes as $\mathfrak{p}^2$ where $\mathfrak{p} = (i+1)O_K$.

Moreover we will denote with $\mathcal{N}$ the norm function: where the norm of an ideal is the cardinality of the residue field. It is a well known fact that the norm is a multiplicative function (as a consequence of the Chinese remainder theorem). Furthermore $\mathcal{N}(aO_K) = a\overline{a}$.

Irreducible and primary elements

Definition 6.4 (Irreducible element)**.** An element $\pi \in O_K$ is irreducible if the ideal πO_K is prime.

We already know the irreducible elements by Remark 6.1.

Definition 6.5 (Primary element)**.** A non-unit $\alpha \in O_K$ is primary if $\alpha \equiv 1 \pmod{\mathfrak{q}^3}$, where $\mathfrak{q} = (i+1)O_K$.

Lemma 6.3. *Let $\alpha \in O_K$ be a non unit and let $\mathfrak{q} = (i+1)O_K$. If $\alpha \notin \mathfrak{q}$, then there exists a unique unit u such that $u\alpha$ is primary.*

First of all we recall that the units in O_K are in $\{1, -1, i, -i\}$.

Since $\alpha \notin \mathfrak{q}$ it follows that if $\alpha = a + ib$, then a and b have different parity.

Notice that $\mathfrak{q} = (2 + 2i)O_K$. The condition α primary is equivalent to

$$\frac{\alpha - 1}{2 + 2i} = \frac{a + b - 1}{4} + i\frac{b - a + 1}{4} \in \mathbb{Z}[i]$$

and hence equivalent to $a + b \equiv 1 \pmod 4$ and $a - b \equiv 1 \pmod 4$. This happens when $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$ or $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$. Since a and b have different parity we can find a unit u such that $u\alpha$ is primary. The uniqueness of this unit follows from the fact that all the units in O_K are still distinct modulo $\mathfrak{q}^3$.

The quartic symbol

Definition 6.6. Let $\mathfrak{p}$ be a prime ideal in O_K such that $\mathcal{N}(\mathfrak{p}) \neq 2$ we define the quartic residue character $\chi_\mathfrak{p} : O_K/\mathfrak{p}^* \to \mathbb{C}^*$ as follow: $\chi_\mathfrak{p}(\alpha) = i^j$ such that $\alpha^{(\mathcal{N}(\mathfrak{p})-1)/4} \equiv i^j \pmod{\mathfrak{p}}$.

This character is well defined since $\alpha^{(\mathcal{N}(\mathfrak{p})-1)/4}$ is a solution of the equation $X^4 - 1 = 0$ modulo $\mathfrak{p}$. Since $\mathcal{N}(\mathfrak{p}) \neq 2$ and hence $\mathfrak{p} \neq (i + 1)O_K$ it implies that $1, i, -1, -i$ are distinct in the residue field and so they are the only solutions of the equation $X^4 - 1 = 0$.

Proposition 6.4. *Let p be a prime $p \equiv 1 \pmod 4$. Let $\mathfrak{p}$ a prime ideal in O_K such that $\mathcal{N}(\mathfrak{p}) = p$. Consider the quartic residue character $\chi_\mathfrak{p} : O_K/\mathfrak{p}^* \cong \mathbb{F}_p^* \to \mathbb{C}^*$, then the value $-\chi_\mathfrak{p}(-1)J(\chi_\mathfrak{p}, \chi_\mathfrak{p})$ is the only primary generator of $\mathfrak{p}$.*

Proof. First we notice that $-\chi_\mathfrak{p}(-1)J(\chi_\mathfrak{p}, \chi_\mathfrak{p})$ is primary. Indeed,

$$J(\chi_\mathfrak{p}, \chi_\mathfrak{p}) = 2\sum_{t=2}^{\frac{p-1}{2}} \chi_\mathfrak{p}(t)\chi_\mathfrak{p}(1 - t) + \chi_\mathfrak{p}\left(\frac{p + 1}{2}\right)^2.$$

Any unit in O_K is congruent to 1 modulo $(1+i)O_K$. Thus, modulo $(2+2i)O_K$ we get

$$J(\chi_\mathfrak{p}, \chi_\mathfrak{p}) \equiv 2\left(\frac{p - 3}{2}\right) + \chi_\mathfrak{p}\left(\frac{p + 1}{2}\right)^2.$$

Since $p \equiv 1 \pmod 4$, then $p \equiv 1 \pmod{2 + 2i}$. Furthermore we have that

$$\chi_\mathfrak{p}\left(\frac{p + 1}{2}\right)^2 = \chi_\mathfrak{p}(2)^{-2} = \chi_\mathfrak{p}(2)^2 = \chi_\mathfrak{p}(-i(1 + i)^2)^2 = \chi_\mathfrak{p}(-1)$$

It follows that:

$$J(\chi_\mathfrak{p}, \chi_\mathfrak{p}) \equiv -2 + \chi_\mathfrak{p}(-1).$$

Thus

$$-\chi_{\mathfrak{p}}(-1)J(\chi_{\mathfrak{p}},\chi_{\mathfrak{p}}) \equiv 2\chi_{\mathfrak{p}}(-1) - 1 \equiv 1$$

where the last congruence holds since $\chi_{\mathfrak{p}} = \pm 1$.

Secondly we prove that $-\chi_{\mathfrak{p}}(-1)J(\chi_{\mathfrak{p}},\chi_{\mathfrak{p}}) \equiv 0$ modulo $\mathfrak{p}$. Let g be a generator for $\mathbb{F}_p^*$. Then modulo $\mathfrak{p}$ we get

$$J(\chi_{\mathfrak{p}},\chi_{\mathfrak{p}})) \equiv \sum_{t=1}^{p-1} (t)^{\frac{p-1}{4}} (1-t)^{\frac{p-1}{4}} = \sum_{k=0}^{p-1} \left(g^{\frac{k(p-1)}{4}} - g^{\frac{k(p-1)}{2}} \right).$$

Denote $x = g^{\frac{p-1}{4}}$ and $y = g^{\frac{p-1}{2}}$; notice both x and y are not 1. Thus

$$\sum_{k=0}^{p-1} x^k + \sum_{k=0}^{p-1} y^k \equiv 0$$

since this value is already congruent to zero modulo p.

Now we deduce the thesis by Corollary 6.1. Indeed $-\chi_{\mathfrak{p}}(-1)J(\chi_{\mathfrak{p}},\chi_{\mathfrak{p}})$ has absolute value p. □

6.1.4 Local computation on the elliptic curve

In this section we want to compute the number of points of the elliptic curve E defined by $Y^2 = X^3 - X$ over the residue field $\mathbb{F}_p$. The discriminant of E is 2^6 and so we will avoid the prime $p = 2$.

The number of points of the curve over $\mathbb{F}_p$ is $N_E(p) = 1 + N_p$ where 1 stands for the infinity point, and N_p for the number of "affine" solutions hence the solution in $\mathbb{F}_p$ of $Y^2 = X^3 - X$. First of all, in order to make the character's theory applicable, we transform our curve into the one defined by $U^2 = V^4 + 4$. The following maps

$$T(U,V) = \left(\frac{1}{2}(U + V^2)\,,\, \frac{1}{2}V(U + V^2) \right)$$

$$S(X,Y) = \left(2X - \frac{Y^2}{X^2}\,,\, \frac{Y}{X} \right)$$

give a bijection between

$$\{\text{solutions of} \quad Y^2 = X^3 - X\} \setminus \{(0,0)\} \underset{T}{\overset{S}{\rightleftarrows}} \{\text{solutions of} \quad U^2 = V^4 - 4\}$$

Hence we have $N_E(p) = 2 + M_p$ where M_p are the number of solutions of the equation $U^2 = V^4 - 4$.

Case $p \equiv 3 \pmod 4$

We notice that every element in $\mathbb{F}_p$ is in the form $\pm w^2$. Indeed, consider the map $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ that sends $a \mapsto a^2$, since $\mathbb{F}_p^* \cong \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$ we have the following diagram:

$$\begin{array}{ccc} \mathbb{F}_p^* & \xrightarrow{\varphi} & \mathbb{F}_p^* \\ \cong\downarrow & & \cong\downarrow \\ \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} & \xrightarrow{m_2} & \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \end{array}$$

where the map m_2 is the multiplication by 2. Since $p \equiv 3 \pmod 4$, we have that $p-1 = 2k$ with k odd and hence $\frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{k\mathbb{Z}}$. The multiplication by 2 induces an automorphism of $\frac{\mathbb{Z}}{k\mathbb{Z}}$, thus we conclude that $\mathbb{F}_p^*/\varphi(\mathbb{F}_p^*) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \{\pm 1\}$.

From this fact it follows that every square in $\mathbb{F}_p^*$ is a fourth power. Thus M_p is equals to the number of solution of the equations $U^2 = V^2 - 4$.

We use Proposition 6.2 to count the number of solutions.

$$M_p = \sum_{a+b=4} N(U^2 = a)N(V^2 = -b) = \sum_{a+b=4} (\epsilon(a) + \chi(a))(\epsilon(-b) + \chi(-b))$$

where χ is the non trivial character on $\mathbb{F}_p$ of order 2. Since $\sum_{a\in\mathbb{F}_p} \chi(a) = 0$, we get that

$$M_p = p + \sum_{a+b=4} \chi(a)\chi(-b) = p + \chi(-1)\chi^2(4)J(\chi,\chi).$$

Since $\chi = \chi^{-1}$, Proposition 6.3 tells us that $J(\chi,\chi) = -\chi(-1)$ and hence $M_p = p - 1$. We conclude that $N_E(p) = 2 + p - 1 = p + 1$.

Remark 6.2. Knowing the relation $N_E(p) = 1 + p - a_p$ we get that $a_p = 0$ for every prime $p \equiv 3 \pmod 4$.

Case $p \equiv 1 \pmod 4$

Let χ be a character of order 4 of $\mathbb{F}_p$ and set $\lambda = \chi^2$ the non trivial character of order 2. In this case we compute M_p as follow:

$$M_p = \sum_{a+b=4} N(U^2 = a)N(V^4 = -b) =$$

$$= \sum_{a+b=4} (\epsilon(a) + \lambda(a))(\epsilon(-b) + \chi(-b) + \lambda(-b) + \chi^{-1}(-b)).$$

Via simple manipulation, we find out

$$M_p = p + \chi(-4)\lambda(4)J(\chi,\lambda) + \lambda(-4)\lambda(4)J(\lambda,\lambda) + \chi^{-1}(-4)\lambda(4)J(\chi^{-1},\lambda)$$

Now notice that since 4 and -4 are both square in $\mathbb{F}_p$ then $\lambda(4) = \lambda(-4) = 1$. Moreover by Proposition 6.3 we have that $J(\lambda, \lambda) = -\lambda(-1) = -1$. Thus

$$M_p = p - 1 + \chi(-4)J(\chi, \lambda) + \chi^{-1}(-4)J(\chi^{-1}, \lambda)$$

Lemma 6.4. *Let p be an odd prime, let λ a character of order 2 and η any non trivial character of $\mathbb{F}_p$. Then*

$$J(\lambda, \eta) = \eta(4)J(\eta, \eta).$$

Proof. First of all we recall that by Proposition 6.3 we have that $J(\epsilon, \eta) = 0$. Thus

$$J(\lambda, \eta) = J(\epsilon, \eta) + J(\lambda, \eta) = \sum_{a+b=1} (\epsilon(a) + \lambda(a))\eta(b) =$$

$$= \sum_{a+b=1} N(t^2 = a)\eta(b) = \sum_t \eta(1 - t^2) =$$

$$\eta(4) \sum_t \eta\left(\frac{1-t}{2}\right) \eta\left(\frac{1+t}{2}\right) = \eta(4)J(\eta, \eta).$$

□

From the lemma it follows that $\chi(-4)J(\chi, \lambda) = \chi(-1)\chi(2^4)J(\chi, \chi) = \chi(-1)J(\chi, \chi)$ and since χ^{-1} coincides with the character obtained from χ by conjugation, we get

$$M_p = p - 1 + \chi(-1)J(\chi, \chi) + \overline{\chi(-1)J(\chi, \chi)}$$

and hence

$$N_E(p) = 1 + p + \chi(-1)J(\chi, \chi) + \overline{\chi(-1)J(\chi, \chi)}.$$

Remark 6.3. When $p \equiv 1 \pmod 4$ we have found that $a_p = -\chi(-1)J(\chi, \chi) - \overline{\chi(-1)J(\chi, \chi)}$, where χ is a character of order 4.

We conclude this section with the following theorem.

Theorem 6.1. *Suppose p a prime integer and $p \neq 2$. Consider the elliptic curve E over $\mathbb{Q}$ then*

(i) if $p \equiv 3 \pmod 4$ then $a_p = 0$,

(ii) if $p \equiv 1 \pmod 4$ then $a_p = \pi + \overline{\pi}$ where π is the primary generator of the prime ideal $\mathfrak{p} \subset O_K$ lying over p.

Proof. The case $p \equiv 3 \pmod 4$ follows by Remark 6.2. For the case $p \equiv 1 \pmod 4$, it suffices to choose the quartic residue character $\chi_\mathfrak{p}$ of Definition 6.6 as character of order 4 over $\mathbb{F}_p$, then by Remark 6.3 combined with Proposition 6.4 we deduce that

$$a_p = 1 + p - N_E(p) = -\chi_\mathfrak{p}(-1)J(\chi_\mathfrak{p}, \chi_\mathfrak{p}) - \overline{\chi_\mathfrak{p}(-1)J(\chi_\mathfrak{p}, \chi_\mathfrak{p})} = \pi + \overline{\pi}$$

□

6.2 The L-function attached to an elliptic curve

Definition 6.7. Let E be an elliptic curve over $\mathbb{Q}$ and Δ its discriminant. Then we define the L-function of E as the Euler product

$$L(E,s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

6.2.1 A Hecke charcter

Definition 6.8 (Hecke character)**.** Let $\mathbb{Q} \subset L$ be a number field. Let $O_L \subset L$ be the ring of integer and $M \subset O_L$ an ideal. A Hecke character modulo M is a map χ from the ideals of O_L to the complex number with the following properties:

(i) $\chi(O_L) = 1$,

(ii) $\chi(I) \neq 0$ iff there are no common prime ideal dividing I and M,

(iii) $\chi(IJ) = \chi(I)\chi(J)$

Since we know that every ideal of O_L can be uniquely written as a product of prime ideals it suffices to define χ only on prime ideals coprime with M.

Definition 6.9. Define $\chi_{\mathbb{Z}[i]}$ to be the Hecke character modulo $4\mathbb{Z}[i]$ on the field $K = \mathbb{Q}(i)$ as the multiplicative map determined by $\chi_{\mathbb{Z}[i]}(\mathfrak{p}) = \pi$ where π is the only primary generator of the prime ideal $\mathfrak{p}$.

Remark 6.4. By the definition we have that: if $p \equiv 3 \pmod 4$ and hence pO_K is a prime ideal we have $\chi_{\mathbb{Z}[i]}(pO_K) = -p$.

Moreover we have that for every ideal $A \subset O_K$ the absolute value $|\chi_{\mathbb{Z}[i]}(A)| = \mathcal{N}(A)^{1/2}$. Indeed, if A is a prime ideal, this fact is trivial, then the general statement follows since both the norm and the character are multiplicative functions.

Remark 6.5. If $\alpha \in O_K$ is such that $\alpha \equiv 1 \pmod 4$, then $\chi_{\mathbb{Z}[i]}(\alpha O_K) = \alpha$.

Proposition 6.5. *Let E be the elliptic curve over $\mathbb{Q}$ defined by the equation $Y^2 = X^3 - X$ and $\chi = \chi_{\mathbb{Z}[i]}$ the character defined as in Definition 6.9. Then $L(E,s) = L(\chi, s)$.*

Proof. First of all recall that

$$L(\chi, s) = \prod_{\mathfrak{p} \nmid 4O_K} (1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s})^{-1}.$$

Then applying Theorem 6.1 we have that: if $p \equiv 1 \pmod 4$, we decompose $pO_k = \mathfrak{p}\overline{\mathfrak{p}}$, and we get

$$1 - a_p p^{-s} + p^{1-2s} = (1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s})(1 - \chi(\overline{\mathfrak{p}})\mathcal{N}(\overline{\mathfrak{p}})^{-s}).$$

On the other hand, when $p \equiv 3 \pmod 4$ and hence pO_K is a prime ideal we have

$$1 - a_p p^{-s} + p^{1-2s} = 1 + p^{1-2s} = 1 - \chi(pO_K)\mathcal{N}(pO_K)^{-s}$$

So the factors of the Euler products that define both $L(E, s)$ and $L(\chi, s)$ are the same. Furthermore, they coincide as holomorphic functions where they converge. □

6.3 The equidistribution statement

In this section we give an idea of how the analytic properties of L functions associated to a character are related to statements about equisdistribution.

We will state the an important theorem without giving a proof, followed by the main steps that lead to it.

First of all we need to recall some definitions and properties of Ideles. They can be found in [La 86].

Definition 6.10. Let $\{v\}$ be a set of indexes, and for each v, let G_v be a locally compact topological group. For all but a finite number of v let H_v be a compact open subgroup of G_v. Then the restricted product of the G_v, with respect to H_v, is the subgroup G of the direct product consisting of elements all but a finite number of whose components lie in H_v.

Definition 6.11. Let K be a number field. Let $\{\mathrm{v}\}$ be the set of finite and infinite places of K. Denote with k_v the completion of K at the place v and O_v the valuation ring when v is finite. Then the restricted product of K_v^* with respect to the units O_v^* is called the Ideles group of K, by convention we set $O_v^* = K_v^*$ when v is real or complex. We will denote it with J_K.

Remark 6.6. On the Idele group of K we define a norm. For each finite place v, corresponding to a prime ideal $\mathfrak{p}$ in the ring of integer, we have the $\mathfrak{p}$-adic norm. While for the infinite places we consider the usual absolute value if v is a real place, or the square of the absolute value if v is complex.

Now if $a = (a_v)_v \in J_K$ we define the norm in this way:

$$||a|| = \prod_v |a_v|_v$$

This definition makes sense since $|a_v|_v = 1$ for all but finitely many v.

Remark 6.7. The norm induces a continuous group homomorphism

$$||\cdot|| : J_K \longrightarrow \mathbb{R}^+$$

We denote with J_0 the kernel of this map. Furthermore if we embed K^* in J_K via the diagonal immersion we have that $K^* \subset J_0$. Indeed it follows from the product formula.

Definition 6.12. A cycle $\mathfrak{c}$ for K is a formal product of places of K with respective multiplicity $m(v)$

$$\mathfrak{c} = \prod_v v^{m(v)}$$

such that: if v is finite $m(v)$ is a positive integer, if v is an infinite place then $m(v) \in \{0, 1\}$. Moreover $m(v) = 0$ for all but finitely many places.

In the case $m(v) \neq 0$ only for finite places, we can identify the cycle $\mathfrak{c}$ with the ideal $\prod_{v \text{ finite}} \mathfrak{p}_v^{m(v)} \subset O_K$ where $\mathfrak{p}_v$ is the prime ideal corresponding to the place v.

We want to extend the notion of being congruent to 1 modulo a cycle.

Definition 6.13. Let $\mathfrak{c}$ be a cycle of K. We say that an idele $a = (a_v)_v$ is congruent to 1 modulo $\mathfrak{c}$ when:

(i) for every finite places v such that $v|\mathfrak{c}$ (i.e. $m(v) > 0$) then $a_v \equiv 1$ modulo $\mathfrak{p}_v^{m(v)}$,

(ii) if $v|\mathfrak{c}$ and v is real then $a_v > 0$.

We denote with $J_\mathfrak{c} \subset J_K$ the subgroup of ideles congruent to 1 modulo $\mathfrak{c}$.

Remark 6.8. Letting $\prod'$ denote the restricted product, then

$$J_\mathfrak{c} \cong \prod_{v|\mathfrak{c}} W_\mathfrak{c}(v) \times \prod_{v \nmid \mathfrak{c}}{}' K_v^*$$

where $W_\mathfrak{c}(v)$ is defined as:

(i) If v finite, corresponding to the prime $\mathfrak{p}$, then $W_\mathfrak{c}(v) = 1 + \mathfrak{p}^{m(v)}$,

(ii) If v is real $W_\mathfrak{c}(v) = \mathbb{R}^+$,

(iii) If v is complex $W_\mathfrak{c}(v) = \mathbb{C}^*$.

Proposition 6.6. *For each cycle $\mathfrak{c}$ we define $K_\mathfrak{c} = J_\mathfrak{c} \cap K^*$ where K^* is embedded in J_K via the diagonal immersion. Then*

$$J_\mathfrak{c}/K_\mathfrak{c} \cong J/K^*$$

Proof. We have the following diagram.

$$\begin{array}{ccc} J_\mathfrak{c} & \longrightarrow & J_K \\ \cup & & \cup \\ K_\mathfrak{c} & \longrightarrow & K^* \end{array}$$

It easily follow the injectivity. While the surjectivity is a consequence of approximation theorem. □

6.3.1 Equidistributed sequences

We recall the definition of equidistribution.

Definition 6.14 (Equidistribution)**.** Let $F = \bigcup_r F_r$ be a set which is the union of finite set F_r, with $r = 1, 2, 3, \ldots$ such that $F_r \subset F_{r+1}$. Let G a compact group with a measure μ defined on it. Let $\lambda : F \to G$ a map. We shall say that F is λ-equidistributed if for every continuous function $\varphi : G \to \mathbb{C}$ we have

$$\lim_{r \to +\infty} \frac{1}{\#F_r} \sum_{f \in F_r} \varphi(\lambda(f)) = \int_G \varphi \mathrm{d}\mu.$$

Theorem 6.2. *Let $\mathcal{P}$ be the set of prime ideals of a number field K. Let $\tau : \mathcal{P} \to J_K$ be the map defined as: for each prime $\mathfrak{p}$, select an element $\pi_\mathfrak{p} \in K_\mathfrak{p}^*$ with $\mathfrak{p}$-adic norm 1, and let $\tau(\mathfrak{p})$ having component 1 at all v except $v_\mathfrak{p}$ at which it has component $\pi_\mathfrak{p}$. We view $\mathcal{P}$ as filtered by the sets P_r consisting of those $\mathfrak{p}$ such that $\mathcal{N}(\mathfrak{p}) \leq r$. Let G be an abelian compact group, and let $\sigma : J_K \to G$ be a continuous homomorphism such that $\sigma(J_0) = G$, and whose kernel contains K^*. Let $\lambda = \sigma \circ \tau$, then $\mathcal{P}$ is λ-equidistributed in G with respect to its Haar measure.*

For the proof of this theorem we suggest to see [La 86].

Anyway, we want to illustrate the main reasons that lead to the theorem. First of all, we have that instead of considering all the continuous function $\varphi : G \to \mathbb{C}$ we can reduce to the case where φ is an irreducible character of G. Indeed the irreducible characters of G generates a dense subgroup of the complex valued continuous function.

Then we know the value of $\int_g \chi$ with respect to the Haar measure. We have that $\int_g \chi = 0$ for every irreducible character but the trivial one; in this case $\int_g \chi = 1$. The proof of this fact uses the invariance of the Haar measure by multiplication by element of G.

The crux of this theorem is the relation between the λ equidistribution of $\mathcal{P}$ and the fact that for every non trivial character χ of the group G we have that

$$\lim_{r \to +\infty} \frac{1}{\#P_r} \sum_{\mathfrak{p} \in P_r} \chi(\lambda(\mathfrak{p})) = 0.$$

This link lies in the L function of the Hecke character $\chi \circ \lambda$. Indeed, the statement above is implied by the fact that $L(\chi \circ \lambda, s)$ is holomorphic on $\Re(s) \geq 1$ except for $s = 1$ where it can have a pole, and it has no zero on the line $1 + it$. This analytic property of this L function was proved by Hecke.

6.3.2 Application of the equidistribution statement

Let χ be the Hecke character defined in Definition 6.8. We want to apply Theorem 6.2 to deduce the equidistribution of the sequence $\left\{ \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^{1/2}} \right\}_\mathfrak{p}$ in

the circle S^1 when $\mathfrak{p}$ varies in the set of primes $\mathcal{P}$ of $\mathbb{Z}[i]$.

Proposition 6.7. *Let χ be the Hecke character defined in Definition 6.8. Then the sequence $\left\{\frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p}^{1/2})}\right\}_{\mathfrak{p}}$ when $\mathfrak{p}$ varies in the set of primes $\mathcal{P}$ of $\mathbb{Z}[i]$, is equidistributed in circle S^1 with respect to the filtration given by norm.*

Proof. Consider the cycle of $\mathbb{Q}(i)$ defined by $\mathfrak{c} = \mathfrak{q}^4 \times v_\infty$ where $\mathfrak{q}$ is the ideal over the prime 2 and v_∞ is the only complex place of $\mathbb{Q}(i)$. Notice that $\mathfrak{q}^4 = 4O_k$, and this exactly the modulus of the Hecke character. Let τ be the map described in the hypotesis of Theorem 6.2; we want to define a map $\sigma : J_{\mathfrak{c}} \to S^1$ such that if $\mathfrak{p} \neq \mathfrak{q}$ we have

$$\sigma\tau(\mathfrak{p}) = \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^{1/2}}.$$

Moreover we require that $\sigma(J_0 \cap J_{\mathfrak{c}}) = G$. Let $J^{\mathfrak{c}}$ be the ideles subgroup

$$J^{\mathfrak{c}} = \prod_{v \nmid \mathfrak{c}} O_K^* \times \{1\} \times \cdots \times \{1\},$$

we require that both $K_{\mathfrak{c}}$ and $J^{\mathfrak{c}}$ are contained in the kernel of σ.

Indeed, if such σ exists, we can define a map $\sigma' : J_K \to S^1$ in this way

$$\sigma' : J_K \twoheadrightarrow \frac{J_K}{K^*} \cong \frac{J_{\mathfrak{c}}}{K_{\mathfrak{c}}} \xrightarrow{\sigma} S^1.$$

Notice that, when $\mathfrak{p} \neq \mathfrak{q}$, we have $\sigma' \circ \tau(\mathfrak{p}) = \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^{1/2}}$. Then applying Theorem 6.2 we prove the equidistribution.

It remains to prove the existence of such σ. The request that σ is trivial on $J^{\mathfrak{c}}$ define uniquely σ at the place $v \nmid \mathfrak{c}$. Indeed we have

$$\frac{J_{\mathfrak{c}}}{J^{\mathfrak{c}}} \cong \prod_{v \nmid \mathfrak{c}}{}' \frac{K_v^*}{O_K^*} \times W_{\mathfrak{c}}(\mathfrak{q}) \times W_{\mathfrak{c}}(v_\infty).$$

Let v be the place corresponding to a prime $\mathfrak{p}$. Recall that every element of $K_{\mathfrak{p}}^*$ can be written as $u\pi_{\mathfrak{p}}^r$ for some $u \in O_K^*$ and $r \in \mathbb{Z}$. Then σ is uniquely determined at the place v by the value that it assumes in $\tau(\mathfrak{p})$, hence by the condition $\sigma \circ \tau(\mathfrak{p}) = \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^{1/2}}$.

Furthermore we define σ trivially on the component $\mathfrak{q}$. We have to define σ for element in $W_{\mathfrak{c}}(v_\infty) \cong \mathbb{C}^*$. If $\alpha \in \mathbb{C}^*$ we define $\sigma_\infty(\alpha) = |\alpha|\alpha^{-1}$. Thus for every idelic element $a = (a_v)_v$ we have $\sigma(a) = \prod \sigma_v(a_v)$.

The fact that $\sigma(J_0 \cap J_{\mathfrak{c}}) = G$ is a consequence of the definition of σ at the place v_∞. Furthermore, if $\alpha \in K_{\mathfrak{c}}$ we have that

$$\sigma(\alpha) = \frac{\chi(\alpha O_K)}{\mathcal{N}(\alpha O_K)^{1/2}} \alpha^{-1}|\alpha|$$

where in this case we are extending the Hecke character multiplicatively to fractional ideal. Combining the fact that $\alpha \in K_{\mathfrak{c}}$ and Remark 6.5 we get that $\chi(\alpha) = \alpha$ and hence $K_{\mathfrak{c}}$ is contained in the kernel. This conclude the proof. □

Let j be the complex conjugation restricted to element in S^1. Let p be a prime such that $p \equiv 1 \pmod 4$. By the definition of the character χ it is clear that if $pO_K = \mathfrak{p}\overline{\mathfrak{p}}$, then $j(\chi(\mathfrak{p})) = \chi(\overline{\mathfrak{p}})$.

Corollary 6.2. *Let P_1 be the set of prime integers with the property $p \equiv 1 \pmod 4$. Let j be the restriction of the complex conjugation on S^1 and let $\lambda : P_1 \to S^1/\{Id_{S^1}, j\}$ be the map defined by $\lambda(p) = \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^{1/2}}$ where $\mathfrak{p}$ is a prime in $\mathbb{Z}[i]$ lying over p. Then P_1 is λ-equidistributed with respect to filtered set $Q_r = \{p \in P_1 \,|\, p \leq r\}$.*

Proof. Keep the notation of Proposition 6.7. Let $\mathcal{P}_3$ be the subset of $\mathcal{P}$ such that the element are those prime ideal lying over the integer prime $p \equiv 3 \pmod 4$. Then the density of $\mathcal{P}_3$ in $\mathcal{P}$ is 0. Indeed let $\mathcal{Q}_r$ be filtration in $\mathcal{P}$ given by the norm $\mathcal{Q}_r = \{\mathfrak{p} \in \mathcal{P} \,|\, \mathcal{N}(\mathfrak{p}) \leq r\}$ then

$$\operatorname{dens}(\mathcal{P}_3) = \lim_{r\to+\infty} \frac{\#(\mathcal{P}_3 \cap \mathcal{Q}_r)}{\#\mathcal{Q}_r} = \lim_{r\to+\infty} \frac{\pi(\sqrt{r})}{2\pi(r)} = 0$$

where $\pi(r)$ is the function that counts the prime integers lesser equal than r. So by Proposition 6.7 we have that the set $\mathcal{P} \setminus \mathcal{P}_3$ is equidistributed in S^1.

Let $\tau : S^1 \to S^1/\{\mathrm{Id}_{S^1}, j\}$ the quotient map and let $\varphi : S^1/\{\mathrm{Id}_{S^1}, j\} \to \mathbb{C}$ a continuous function. Then

$$\int_{S^1/\{\mathrm{Id}_{S^1},j\}} \varphi = \int_{S^1} \varphi \circ \tau = \lim_{r\to+\infty} \frac{1}{\#\mathcal{Q}_r} \sum_{\substack{\mathfrak{p}\in\mathcal{P}\setminus\mathcal{P}_3 \\ \mathfrak{p}\in\mathcal{Q}_r}} \varphi \circ \tau \left(\frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^{1/2}}\right) =$$

$$= \lim_{r\to+\infty} \frac{1}{2\pi(r)} \sum_{p\in P_1} 2\varphi \circ \lambda(p) = \lim_{r\to+\infty} \frac{1}{\pi(r)} \sum_{p\in P_1} \varphi \circ \lambda(p).$$

Thus we get the equidistribution. □

6.4 The Sato-Tate group

Finally we are able to determine the Sato-Tate group related to the elliptic curve E over $\mathbb{Q}$ defined by the equation $Y^2 = X^3 - X$. In this case by Sato-Tate group we mean the tern $(K, \rho, \{s_p\}_{p\notin S})$ defined in Definition 5.10 related to the set of cohomological data $(E, 1)$.

Compact group Define U to be the subgroup of $\mathbb{SU}_2(\mathbb{C})$ whose elements are in the form $x_\alpha = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix}$ for $\alpha \in \frac{\mathbb{R}}{2\pi\mathbb{Z}}$. Then define K to be the normalizer of U inside $\mathbb{SU}_2(\mathbb{C})$. Thus

$$K = \left\langle U, \gamma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

Notice that K as topological group, has two connected component: U and the element of the form γU. Both of them are compact real Lie group of dimension 1 hence isomorphic to S^1.

Remark 6.9. We are looking at $\mathbb{SU}_2(\mathbb{C})$ as a compact real Lie group. Hence K has a natural induced real Lie group structure.

Linear representation As linear representation we consider the natural embedding

$$\rho : K \hookrightarrow \mathbb{SU}_2(\mathbb{C}) \subset \mathbb{GL}_2(\mathbb{C})$$

Conjugacy classes We notice that the space $\mathrm{Cl}(K)$ consists of the following elements:

(i) $K \setminus U$ make up a unique class with mass $\frac{1}{2}$ with respect to the Haar measure. A representative of this class is the element γ,

(ii) the conjugacy classes of U in K can be represent by diagonal matrices x_α with $\alpha \in [0, \pi]$ since x_α and $x_{-\alpha}$ are conjugate. The Haar measure on such classes is $\frac{1}{2\pi}\mathrm{d}\alpha$; its mass is $\frac{1}{2}$.

To define the s_p we distinguish two cases: when $p \equiv 3 \pmod 4$ (*i.e.* when p is inhert in $\mathbb{Z}[i]$) we put $s_p = [\gamma]$. On the other hand, when $p \equiv 1 \pmod 4$ (*i.e.* when p completely splits in $\mathbb{Z}[i]$) we use the character χ defined in Definition 6.8, setting

$$s_p = \left[\begin{pmatrix} \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^{1/2}} & 0 \\ 0 & \frac{\overline{\chi(\mathfrak{p})}}{\mathcal{N}(\mathfrak{p})^{1/2}} \end{pmatrix} \right]$$

where $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[i]$ lying over p. Notice that if we choose the other prime over p we get the same conjugacy class.

Axioms We recall some notation: let g_p be the geometric Frobenius of Definition 3.7, let $h^1_{E,\ell}$ be the ℓ-adic character given by the first cohomology group of E. For all the prime integers but finitely many, we have that $h^1_{E,\ell}(g_p) = a_p$. Thus by Theorem 6.1, we get that $\frac{a_p}{p^{1/2}} = \mathrm{Tr}(\rho(s_p))$. Indeed, when $p \equiv 3 \pmod 4$ we have that

$$\frac{a_p}{p^{1/2}} = 0 = \mathrm{Tr}(\gamma) = \mathrm{Tr}(\rho(s_p)),$$

while when $p \equiv 1 \pmod 4$, if we denote with $\mathfrak{p}$ a prime ideal in $\mathbb{Z}[i]$ lying over p, we get

$$\frac{a_p}{p^{1/2}} = \frac{\chi(\mathfrak{p}) + \overline{\chi(\mathfrak{p})}}{\mathcal{N}(\mathfrak{p})^{1/2}} = \mathrm{Tr}(x_p) = \mathrm{Tr}(\rho(s_p)).$$

To show that K is exactly the Sato-Tate group of E we need to show the equidistribution of the classes s_p.

Proposition 6.8. *The conjugacy classes $\{s_p\}_p$ are equidistribuited in $\mathrm{Cl}(K)$ with respect to tha Haar measure.*

Proof. We denote with P the set of prime integers, with P_3 the set of prime integers $p \equiv 3 \pmod 4$ and with P_1 the ones such that $p \equiv 1 \pmod 4$. Since $\mathrm{dens}(P_3) = \frac{1}{2}$ and for each element of P_3 the conjugacy class s_p is the class of $[\gamma]$ whose Haar measure has mass exactly $\frac{1}{2}$, it suffices to show that the classes $[x_p]$ for $p \in P_1$ are equidistributed in $\mathrm{Cl}_K(U)$. It follows from the Corollary 6.2.

Indeed we have a diffeomorphism $S^1 \to U$; if we see S^1 as the subgroup of $\mathbb{C}^*$ made up of elements of norm 1 the diffeomorphism sends an element $a \in S^1$ in the matrix $\begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix}$. Since the action by conjugation by $\gamma \in U$ is defined by

$$\gamma^{-1} \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix} \gamma = \begin{pmatrix} \overline{a} & 0 \\ 0 & a \end{pmatrix}$$

then the equidistribution of the s_p for $p \in \mathrm{Cl}_K(U)$ is equivalent to the equidistribution of the element $\frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^{1/2}}$ in $S^1/\{\mathrm{Id}_{S^1}, j\}$ with respect to the Haar measure induced by S^1 where with j we denote the restriction of the complex conjugation to S^1. □

Corollary 6.3. *Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation $Y^2 = X^3 - X$. Then the sequence $\{a_p/p^{1/2}\}_p$ when p varies in the primes of good reduction for E, is equidistributed in $[-2, 2]$ with respect to the measure $\mu = \frac{1}{2}\delta_0 + \frac{1}{2}\mu^{\mathrm{cont}}$ where μ^{cont} is defined by*

$$\mu^{\mathrm{cont}}(f) = \int_{[-2,2]} f(x) \frac{1}{2\pi\sqrt{4 - x^2}}\, dx.$$

Proof. We know that K is the Sato-Tate group of E. Then it suffices to show that μ is the pushforward of the Haar measure on $\mathrm{Cl}(K)$ via the map given by the trace. Then using the equidistribution of the classes $\{s_p\}_p$ in $\mathrm{Cl}(K)$ we get our claim. □

References

[De 80] Deligne, P, *La Conjecture de Weil II*, Publ. Math. IHES 52 (1980). 137-252.

[De 09] Demailly, J P, *Complex Analytic and Differential Geometry*, Open Content Book, Univ. Grenoble (2009).

[IR 82] Ireland, K, Rosen, M, *A Classical Introduction to Modern Number Theory*, GTM 84, Springer-Verlag, New York (1982). 306-311

[Kn 02] Knaap, A W, *Lie Groups Beyond an Introduction*, II ed., Birkhauser (2002). 98-99

[La 86] Lang, S, *Algebraic Number Theory*, GTM 111, Springer-Verlag, New York (1986). 303-322

[Se 12] Serre, J P, *Lectures on* $N_X(p)$, Research Notes in Mathematic 11, CRC Press, (2012).

[SGA 4] Artin, M, Grothendieck, A, Verdier, J L, *Théorie des Topos et Cohomologie Étale des Scémas*, 3 vol., Springer Lect. Notes 269, 270, 305 (1972-1973).

[SGA $4\frac{1}{2}$] Deligne, P, *Cohomologie Étale*, Springer Lect. Note 569 (1977)

[Si 86] Silverman, J H, *Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York, 1986. 140-144.

[Vi 89] Vinberg, E B, *Linear Representations of Groups*, Modern Birkahuser Classics (1989).