M1 internship : Introduction to elliptic curves over finite fields

Hiault Raphaël, under the supervision of Thomas Krämer

Algebraic geometry department
Humboldt University

16 août 2022

Résumé

In this document, I offer a quick overview on a topic in algebraic geometry. More precisely, we will focus on elliptic curves and the arithmetic of these. Our goal is to state and give a reasonable understanding of the proof of Honda-Tate theorem for elliptic curve over finite field and to proove the Weil conjecture for them. To do so we will have to introduce the elliptic curve over a field K and then develop tools over finite fields. This will imply to use our knowledge of galois theory and algebraic curves in particular to count points the point of these curves.

Chapitre 1

Summary of my experience in the lab

To set some context, I did this internship at the Humboldt University (HU) in the algebraic geometry department from february 22 to july 22. My advisor in Paris -Ollivier Benoist- contacted one of his collegue in Berlin -Thomas Krämer- who accepted to be my director. The idea was to get a first taste of what is algebraic geometry today. With that in mind, M.Krämer suggested that I get familiar with the theory of scheme, and then apply that to elliptic curves and abelian varieties. I also did some basic differential geometry, to have more intuition on the kind of object we were trying to build in scheme theory. More precisely, i spent the first half of my internship to work with schemes, and the other half with elliptic curves and some abelian variety and algebraic topology. Given, this I decided to present the elliptic curve part as among those it's the only subject in which I could get a taste of bigger theorems that have a link to some research work. I could've decided to include all of this, but prefer to offer a full immersion in a subject rather than a quick overview of all different kind of topics.
When I arrived in february, the department was not pretty dynamic. Indeed, here the first semestrer was ending and the second debuted only in april, plus covid restrictions were still heavily applied. Nonetheless, I got to meet most of the phD students and get to know better how a doctorate works. After the semester started here, a seasons of weekly conferences on algebraic geometry started at the same time. There were two sessions a week. The first was on more general topics, the second was specialized in arithmetic geometry. This was actually a great surprise : though I could'nt understand most of the material exposed, I got to see I was progressing as some words/concepts started to make more sense.
Concerning the way I was working here : as I had an office there I was coming almost everyday. I would meet my advisor once a month, essentially to get bibliographical advices and see where I was heading. I got to discuss of math quiet often with the other phD students. They were pretty helpful and open to my questions, which sometimes were more interesting than I thought.
Getting back on the mathematical side, I would say that this intership has been a huge step forward the research side of math. Indeed before, I was kind of lost between all the possibilities that were offered to me and could only say that I was interested in algebra, a pretty vague statement. Now I know better where I am trying to go. After working on elliptic curve, I really got to know better what arithmetic geometry looks like. To keep in that direction I would like to get to know better abelian varieties which is a central object in this field. That's why I decided to take-next year- courses around Riemann surface, algebraic topology and number theory to get a better background in order to contextualize more this object.
I really enjoyed this internship. Getting into a research carreer might be scary at first. Indeed, the cultural representation of researcher is that one genius who gets ideas from above or on the other hand he/she can be pictured as the crazy kind. Getting into a math laboratory helped me realised that they were only cliché (even though I knew it before). Also, getting to talk of math with people enjoying the

same subject as me was for me an amazing opportunity. It's complicated to talk of maths sometimes as our studies trained us to get a reasonable understanding of situations only by using a rigourous approach. But here, in this lab, through seminar and discussions, I had the opportunity to talk of math without necesarily having the whole picture in my mind. I do think it's an important skill in research. Today, it's seem unpractical to know everything about a field in math, even a very restricted one. That means, that one need to develop a strong intuition and a great understanding of the concepts they already familiar with. That's then what I want to try to for me in the future as a mathematician.

To finish I would like first to thank M.Krämer to let me do this internship under his direction. His indications and books recomandations were very helpful to me. In addition, I also want to thank all the phD students and other students I met here. The first ones that come to my mind are Waël, Constantin and Jack but also all the others that made me feel welcome here.

Chapitre 2

Elliptic curve

The aim of this document is to provide an overview of what elliptic curves are and which objects they involve. Because they use a lot of different technique coming from algebra, analysis etc we will suppose the reader to be familiar with at least the vocabulary of algebraic variety and Galois theory (including definition of seperabilty through Khäler differential). We will only do a quick overview of the specificities of algebraic curves. For once and for all we use the following notations :
K denotes a perfect field with its algebraic closure K, G will denote the galois group of this extension, C will define an algebraic curve, E will denote an elliptic curve $\mathbb{F}_{p^n}$ is the finite field of cardinal p^n.

2.1 Maps between algebraic curve

We start here by giving a rapid overview of the specific case of algebraic curves which are projective varieties of dimension one (meaning that the function field of the variety over $\overline{K}$ is of degree of transcendance one that is equivalent to having a Zariski tangent space of dimension one for non-singular varieties). As we said, we suppose the reader being familiar with the theory of algebraic variety, mostly regular maps, dimension, projective space etc.
There're two key-facts when it comes to regular functions on a curve :

Theorem 1. *We consider a projective variety V and a rational map $\phi : C \longrightarrow V$. If C is smooth at P, then ϕ is regular at P. As a consequence rational maps from a smooth curve are regular maps*

Theorem 2. *A morphsim of curve is either surjective or constant*

We now explain the link between algebraic curves and galois theory. First, we consider a morphism of curves defined over K, $\phi : C_1 \longrightarrow C_2$. Naturally, it induces a morphism ϕ^* between the function field $K(C_2)$ and $K(C_1)$ that send $f \in K(C_2)$ to $f \circ \phi$. This give a contravariant functor from the category of algebraic curve over K to the one of extension of the field K (maps being the injection given by the extensions). Actually, one can prove there's an equivalence of category. More precisely, we define two categories. The first on being the one of smooth algebraic curves defined over K equipped with the non-constance rational map defined over K. The second one is a subcategory of the category of field. It's composed by the finetly generated extensions of K with degree transcendance one with the field injections fixing K.
Then, one can say that a morphism of curve over K is seperable if and only if, in the category of field we obtain a separable extension and so on. We can also define the degree of a morphism of curve, the degree of separability by using this equivalence of category.

Now, we define one of the fundamental map we will study : the frobenius map.
We assume that the caracteristic of the field K is a prime p, and we denote $q = p^r$ for $r \in \mathbb{N}^*$. For a

polynomial $f \in K[X]$, we denote $f^{(q)}$ the polynomial obtained by raising every coefficient to the power q. Then, for a curve C/K, we have a new curve $C^{(q)}/K$ given by the ideal generated by the polynomial $P^{(q)}$ such that $P(C) = 0$. We can now define the q-frobenius (or frobenius if the context is clear), to be :

$$\phi : C \longrightarrow C^{(q)},\ \phi([x_0, ..., x_n]) = [x_0^q, ..., x_n^q]$$

The map takes its value in $C^{(q)}$ as for $f \in I(C)$ (the ideal of polynomial that is zero over C) :

$$\begin{aligned} f^{(q)}([x_0^q, ..., x_n^q]) &= f([x_0, ..., x_n])^q \\ &= 0 \end{aligned}$$

The equality holds because the q^{th}-power frobenius of K is linear over K. The following proposition, not hard to prove just give us the really basics to know about the map ϕ :

Proposition 1. *The map ϕ is of degree q and purely inseparable*

Also, a useful tool when it comes to algebraic curves are divisors :

Definition 1 (divisor group)**.** *The divisor group of a curve C is the free abelian group generated by the points $P \in C$. Then a divisor D is of the form $\sum_{P \in C} n_P(P)$ where the $n_P \in \mathbb{Z}$ and are zero for every but a finite number. The group is denoted $Div(C)$*

A fundamental quantity associated to a divisor $D = \sum_{P \in C} n_P(P)$ is its degree $deg(D) = \sum_{P \in C} n_P$. The divisors of degree 0 form a group denoted $Div^0(C)$.
Divisors are intersting because one can associate to a morphism a divisor :

Definition 2 (divisor of a function)**.** *Considering a smooth curve C and a morphism $f \in K(C)$, we define $div(f)$ to be the divisor $\sum_{P \in C} ord_P(f)(P)$*

Divisors of a morphism are of degree zero. That might seem surprising, but we can see that as an equivalent version of the residue theorem for holomorphic functions over $\mathbb{C}$. On the other hand, not every divisor of degree zero is necessarily the divisor of a morphism. That leads us to the following definition :

Definition 3 (principal divisor)**.** *A divisor $D \in Div(C)$ is said to be principal if there exist $f \in K(C)$ such that $D = div(f)$*

An easy proposition is the following :

Proposition 2. *A principal divisor of a map f is of degree zero if and only f is constant*

Démonstration. We remark that f defines a function from C to $\mathbb{P}^1$ by associated to P the point $[f(P) : 1]$. That map is still of divisor zero, so it is never zero, which means the map is not surjective. Then by 2 it defines a function that is constant, which implies f is too. □

To continue with divisor, we introduce now the Picard Group of a curve, which we will see is going to play an important role :

Definition 4 (Picard Group)**.** *The Picard group of a curve, denoted $Pic(C)$ is defined to be the quotient of the group $Div(C)$ by the subgroup of principal divisor. We also define the degree 0 part of $Pic(K)$ that we denote $Pic^0(C)$ which is the class equivalence of divisor that are of degree zero.*

To finish with divisors here, we set some definitions to state the very useful Riemann-Roch Theorem :

Definition 5. *We consider a divisor D on a curve C. We can associate a vector space of function $f \in \overline{K}(C)^*$ that is $\mathcal{L}(D) = \{f \in \overline{K}(C)^* \text{ such that } div(f) + Div(D) \geq 0\} \cup \{0\}$. The dimension of this $\overline{K}$ vector space is denoted $l(D)$*

This definition play the role of finding the function f that would be holomorphic if multiplied by a function of divisor D for instance. At the same time, an algebraic curve comes equipped with a "canonical" divisor, as the vector space of differential forms is one. What we call the "canonical divisor is :

Definition 6. *A canonical divisor of a curve C is the image of any non-zero derivative in $Pic(C)$. We usually denote it K_C.*

Then we have the Riemann-Roch theorem :

Theorem 3. *Let C be a smooth curve and K_C be a canonical divisor on C. There's an integrer $g \geq 0$ also named the genus of C, such that for any $D \in Div(C)$ we have :*

$$l(D) - l(K_C - D) = deg(D) - g + 1$$

In particular, for a curve of genus one and any $D \in Div(C)$ such that $D \geq 0$, we have $l(D) = deg(D) - g + 1$

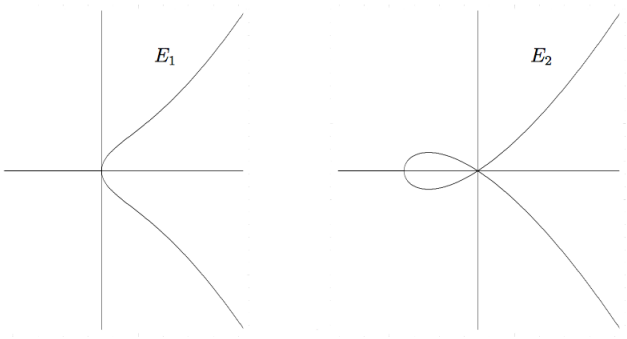
2.2 Elliptic curve through Weirestrass's equations

We are going to introduce the fundamental object of this dissertation. We start by giving a first definition of what is an elliptic curve :

Definition 7 (Elliptic curve)**.** *An elliptic curve is a non-singular projective variety defined in $\mathbb{P}^2$ by the equation $Y^2X + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ with the a_i in $\overline{K}$. We denote E such an elliptic curve and say that the curve is defined over K if $a_i \in K$ and denote it E/K*

The following picture shows that an algebraic variety defined by such an equation can have or not a singualarity but only those without singularities are the elliptic curve :

Two elliptic curves, the first is non-singular, the second has a node



First, one can remark that if $Z = 0$ the only point one obtain on the variety is $[0 : 1 : 0]$ that we denote O and call the distinguished point. But that means, that our projective variety is composed of O and then of the algebraic variety defined by the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

F From now on, we will work with $car(K) \geq 5$. We choose to do so, because in the case of elliptic curve, the caracteristic 2 and 3 are very different, as one cannot make the usual change of variable that we do. Nonetheless, all the proposition here are also true in caracteristic 2 and 3, the proof are just differents and one can rely on "The Arithmetic of Elliptic Curves" by Silvermann to do so.
We can now go back to our suject and by making some change of variables, the equation of an elliptic curve can be put in the more usual and convenient form $y^2 = x^3 - 27c_4x - 54c_6$ where the new coefficients are functions of the a_i. With the change of variable it is easier to define two important quantities of an elliptic curve :

Definition 8 (discriminant and j-invariant)**.** *The discriminant of an ellipitc curve E is the quantity $\Delta = \frac{c_4^3 - c_6^2}{1728}$ (if 1728 is not zero in K, otherwise we put the discriminant to zero. The j-invariant of an ellipitic curve E denoted $j(E)$ is the quantity $\frac{c_4^3}{\Delta}$*

One might ask why are those quantities helpful ? With a bit of calculation one can obtain the two following proposition :

Proposition 3. *A variety defined by the equation $(*)$ is an elliptic curve if the discriminant is non-zero. Two elliptic curves E, E^* are isomorphic over $\overline{K}$ if they have the same j-invariant*

This justify to divide by δ to compute the j-invariant as it's non-zero because the curve is non-singular.

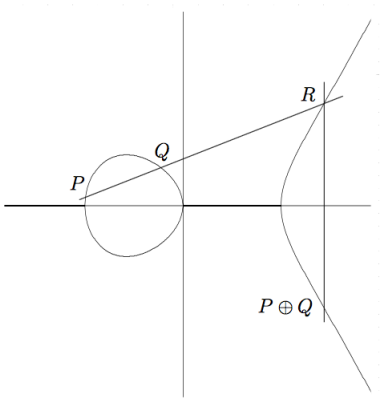
We finish this section by defining the invariant differential of an elliptic curve, which will be a very useful tool to our computations :

Definition 9. *The invariant differential, is the differential $\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$ where Ω_E is the set of differential over E*

2.3 Group structure of an elliptic curve

Here we define from a geometrical point of view the law group that can be put on an elliptic curve. It's spectacular that one can put such a law and in addition having a geometrical description of it. Here we are going to see at the same time how useful it is to work in projective space (mainly Bezout's theorem). Consider two points R, P on the elliptic curve. We look at the line that go through R and P. Because of Bezout's theorem, this line must cross the elliptic curve at another point Q (here Q could be R or P, we speak here from a multiplicity point of view). Then, draw the line from Q to O, it must cross again a third time the elliptic curve, and we denote this point $P + Q$. Here, we picture how it works :

geometrical representation in R of the law group of an elliptic curve



The amazing thing here is that it defines a law group with neutral element O. If one looks for the inverse of a point P, its inverse will be the intersection of line going throught P and O. A picture represent that : I

A remarquable property is that in addition to define a law group, the addition of the point is a morphism meaning is it's a regular map at every point (here we use the fact that an elliptic curve is smooth to state that a rational map is regular). We could give the formula, but it's much more important to know there's one than write it as it can be quite messy.

2.4 Alternative point of view on elliptic curves

The first point of view on elliptic curve is great to compute easily quantities associated to such a curve. However, it might seem weird why the Weierstrass equation is important ? First we give a new definition of what an elliptic curve and proove that the two are equivalent :

Definition 10. *An elliptic curve is a pair (E, O) where E is a non-singular curve of genus one and $O \in E$. It is said to be defined over K if E is so and O is a point with coordinate in K*

Theorem 4. *Let E be an elliptic curve (in the sense of our last definition) defined over K. There exist $x, y \in K(E)$ such that the map : $\phi = [x : y : 1]$ defined from E to $\mathbb{P}^2(K)$ is an isomorphism of E/K to a curve defined by a non-singular Weierstrass equation. Conversly, a smooth curve given by a Weierstrass equations is an elliptic curve in the sense of the definition of this section with $O = [0 : 1 : 0]$.*

We wish here to draw a picture of the proof as it uses the divisors :

Démonstration. The idea is essentially to find a linear relation between the $1, x, x^2, x^3, y, y^2, xy$. To do so, we use the divisor theory. We consider the $\mathcal{L}(n(O))$ for $n \in \mathbb{N}$. Knowing the curve is of genus one, the Riemann-Roch theorem (3) implies that $dim(\mathcal{L}(n(O))) = n$. Then, one can choose $x, y \in K(C)$ such that $\{1, x\}$ is a basis of $\mathcal{L}(2(O))$ and $\{1, x, y\}$ is a basis of $\mathcal{L}(3(O))$. Going on with this idea, we can remark that $\{1, x, y, x^2, x^3, xy, y^2\}$ are in $\mathcal{L}(6(O))$. As the space is of dimension 6, those functions must be linearly dependent. This gives the Weierstrass equation of the curve and allows to define the morphism $\phi = [x : y : 1]$. We need to show it's an isomorphism, which here is equivalent to show that $K(E) = K(x, y)$. To see that, we use the fact that x (*resp.* y) has a double (*resp* triple) pole at O so that the map is of degree 2 i.e $[K(E), K(x)] = 2(resp.\ 3)$. Then $[K(E), K(x, y)] = 1$ as it must be divide 2 and 3. □

Keeping up with a more algebraic approach of elliptic curve, we now see that the law group of an elliptic curve is already coded in the law of the Picard group of the curve. This is the content of the next theorem :

Theorem 5. *Let (E, O) be an elliptic curve*
(a) for every $D \in Div(E)$, there exist a unique point (P) such that $D \sim (O) - (P)$. We then define a map that to such a divisor associate such a point P.
(b) The above map induce a map from $Pic^0(E)$ to E and is actually a bijection. We then obtain the following diagram, that allow to recover the law group already defined over E :

$$\begin{array}{ccc} E \times E & \xrightarrow{\kappa \times \kappa} & Pic^0(E) \times Pic^0(E) \\ {\scriptstyle +}\downarrow & & \downarrow{\scriptstyle +} \\ A_f & \xrightarrow{\kappa} & B_g \end{array}$$

The proof consist more in verifying that the statement are true more than to invent something maybe apart from the first statement that is mostly a consequence of the Riemann-Roch theorem.
This theorem allow to prove instantly a useful criteria to see if a divisor is principal on an elliptic curve :

Proposition 4. *A divisor $D = D = \sum_{P \in C} n_P(P) \in Div(E)$ is principal on elliptic curve if and only if :*
$\sum_{P \in C} n_P = 0$ and $D = \sum_{P \in C} n_P P$ (here we use the law group on E to compute this sum)

2.5 Isogenies

We now introduce a notion of "morphism" specifically for elliptic curve. This is one of the central object we will work with, and we try here to collect informations on their behavior. For once and for all, (E, O_E) and $(E', O_{E'})$ are elliptic curves. First, we begin with a definition :

Definition 11 (isogonies)**.** *An nisogenies is a morphism ϕ from E to E' such that $\phi(O_E) = O_{E'}$. If such an isogeny exist, we say that E and E' are isogenous (and see later it's an equivalence relation). We write $Hom(E, E')$ the group of the isogenies from E to E', and if $E = E'$ it will be denoted $End(E)$ and is a ring using the composotion as our multiplication map.*

The following proposition gives more details on the structure of the ring $Hom(E, E')$:

Proposition 5. *(a) Let E be an elliptic curve defined over K, and $m \in mathbbZ^*$. Then the multiplication map $[m] : EE$ such that $[m](P) = P + ... + P$ (m times) is non-constant*
(b) The group $Hom(E, E')$ is torsion-free
(c) The ring $End(E)$ is torsion-free with no zero divisor.

Démonstration. (a) To prove (a), we first need to show that [2] is not the zero-map. To do so, we just use the duplication formula that gives the coordinates of $2P$ knowing P and verify it is not constant (which, in the details is a consequence of having $\delta \neq 0$. Now using the fact that $[m] \circ [n] = [mn]$, that allows us to prove by induction that $[m] \neq [0]$ for m even. For the case of odds number, we show that there's is alway a non-trivial point P_0 that is of order two that is $2P_0 = 0$. To do so, one use again the duplication formula and because they're quotient of polynomials can find a zero to these functions (to do so, we use again that $\delta \neq 0$). In the end $[2m + 1](P_0) = P_0 \neq 0$.
(b) Here we need to verify that for $\phi \in Hom(E, E')$, and $m \in \mathbb{Z}^*$ we have $[m] \circ \phi \neq 0$. Indeed, if such an equality hold, then $deg(m)deg(\phi) = 0$ but $deg(m) \neq 0$ by (a), so $deg(\phi) = 0$ which means $\phi = 0$.
(c) It's the same proof. □

Naturally, as the m-multipilcation map is not 0, one might be intrested by its kernel as a morphism of group :

Definition 12. *We define the m-torsion group of an elliptic curve as the sub-group $E(m)$ of E such that $E(m) = \{P \in E \text{ such that } [m]P = 0\}$. The torsion sub-group of E denoted E_{tors} is the union of the m-torsion subgroups for every integrer $m \geq 1$*

We now see that these m-torsion groups are finite :

Proposition 6. *Let ϕ be a non-zero isogeny from E to E' then, $\phi^{-1}(O_{E'})$ is a finite group*

Here we skip the proof, but it's not a complicated one.
Going back to isogenies themselves, an important property is that they're morphsim of group :

Proposition 7. *An isogeny ϕ from E to E' is a group morphism*

Démonstration. This proposition is a consequence of the following diagramm :

$$\begin{array}{ccc} E & \xrightarrow{\kappa} & Pic^0(E) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E' & \xrightarrow{\kappa'} & Pic^0(E') \end{array}$$

where the κ, κ' are the isomorphism of group and ϕ_* is the induced morphism of group by ϕ (which is possible as ϕ fixes the distinguished point of the elliptic curves).
We know interpret the galois theory for elliptic curve :

Proposition 8. *Let ϕ from E to E' be a non-zero isogeny.*
(a) For every $P \in E$ $Q \in E'$, $card(\phi^{-1}(Q)) = deg_s(\phi)$ and $e_\phi(P) = deg_i(\phi)$
(b) The map :$ker(\phi) \longrightarrow Aut(\hat{K}(E)/\phi^* K(\hat{E'})$ such that $T \mapsto \tau_T^*$ is an isomorphism.
(c) Suppose that ϕ is separable, the ϕ is unramified and so : $ker(\phi) = deg(\phi)$ and $\hat{K}(E)$ is a galois extension of $\phi^* K(\hat{E'})$

The proof of this statement is more or less a use of Galois theory so we don't give it. We give two useful propositions that are consequences of it :

Proposition 9. *Let $\phi : E \longrightarrow E'$, $\psi : E :\longrightarrow E'$, be two non-constant isogenies with ϕ separable. If $ker(\phi) \subset ker(\psi)$, then there exist a unique isogeny $\lambda : E' \longrightarrow E$ such that, $\psi = \lambda \circ \phi$*

Démonstration. Application of the last proposition using the equivalence of category between fields and elliptic curve □

Proposition 10. *Let Φ be a finite subgroup of the elliptic curve E, there are a unique elliptic curve E and a separable isogeny $\phi : E \longrightarrow E'$ such that $ker(\phi) = \Phi$.*

□

2.6 The invariant differential

We now go back to the invariant differential as defined at the begining. To set the situation again, we consider an elliptic curve E defined over K with a Weirestrass equation : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then, the invariant differential ω is the differential $\frac{dx}{2y+a_1x+a_3} \in \Omega_E$. We justify the terminology "invariant" and see that it is useful to linearize some problem we might encounter.

Proposition 11. *Let $Q \in E$ and the Q-translation map τ_Q that to P associate $P + Q$ on E. Then : $\tau_Q^*\omega = \omega$*

Two strategies are avaible to proove this proposition : one can simply compute $\tau_Q^*\omega$ or one can use some differential theory to avoid it. We choose the second option :

Démonstration. First, we know that Ω_E is one dimensional $K(E)$ vector-space. Then that implies that there exist $a_Q \in K(E)$ such that $\tau_Q^*\omega = a_Q\omega$. We compute now the divisor of a_Q :
$div(a_Q) = div(\omega) - div(\tau_Q^*\omega) = div(\omega) - div(\omega)$ The next step is to show that $a_Q = 1$. To do so, we show that a_Q is constant. Indeed the non-surjectivity of the map $[a_Q : 1]$ misses $[1 : 0]$ implies then that a_Q. Then, $a_Q = a_O = 1$ which concludes the proof. □

Theorem 6. *Let E and E' be two elliptic curves, and ω by the invariant differential on E. Let ϕ, ψ two isognies from E to E'. Then, $\phi^* + \psi^*(\omega) = \phi^*\omega + n\psi^*\omega$.*

The proof will be skipped as it is much more technical than intresting, but one not afraid of computation will see it's true. A simple induction, shows that $[m]^*\omega = m\omega$. Then we have the following propositions :

Proposition 12. *The multiplication map $[m]$ is separable if and only $m \neq 0$ in K*

The next proposition will be useful when we will start to work on finite field :

Proposition 13. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of caracteristic p, and let ϕ be the froebenius map. Then, the map $m + n\phi$ is seperable if and only if $m \neq 0$ in $\mathbb{F}_q$*

Démonstration. A simple computation show that $(m + n\phi)^*(\omega) = m^*\omega + n\phi^*\omega = m\omega$, so that its non-zero if and only if $m \neq 0$ in $\mathbb{F}_q$ □

2.7 The dual isogeny

As we said in the definition of isogeny, the relation on elliptic curve of being isogenous is a relation of equivalence. This section show that this is true by defining the dual isogeny of an isogeny and will -for instance- enable to compute the torsion group of an elliptic curve.
Let's $\phi : E \longrightarrow E'$ be an isogeny. We show how one can construct what we call the dual isogeny of ϕ. Once again the idea is to use the Picard group of the elliptic curve. Indeed, ϕ induce a morphism of group from $Pic^0(E')$ to $Pic^0(E)$ that we denote ϕ^*. More precisely, $\phi^*((P)) = \sum_{Q \in E, \phi(Q)=P} e_\phi(Q)$. Then, because we have the following sequence, one has an isogeny from E' to E :

$$E' \xrightarrow{\kappa'} Pic^0(E') \xrightarrow{\phi^*} Pic^0(E) \xrightarrow{\kappa} E$$

where the κ, κ' are the isomorphism of group we introduced previously. This isogeny will be denoted $\hat{\phi}$.
The next theorem states the uniqueness of this isogeny :

Theorem 7. *Let $\phi : E \longrightarrow E'$ be a non-constant isogeny of degree m. There exist a unique map $\hat{\phi}$ $E' \longrightarrow E$ such that $\hat{\phi} \circ \phi = [m]$*

Now we give some usefeul properties of the dual :

Proposition 14. *Let $\phi : E \longrightarrow E'$ of degree m then :*
(a) $\phi \circ \hat{\phi} = [m]$ on E
(b) Let $\lambda : E' \longrightarrow E''$ then : $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$
(c) Let $\psi : E \longrightarrow E'$, then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$
(d) $\hat{[m]} = [m]$ and $deg[m] = m^2$
(e) $deg(\hat{\phi}) = deg(\phi)$ and the dual isogeny of $\hat{\phi}$ is ϕ

As there're lot of properties we choose not to prove them all. But once you proved the linearity of the dual-isogeny, then its a matter of a simple induction to show the property of the m-multiplication map. It's those properties that allows us to compute the m- torsion group of an elliptic curve :

Proposition 15. *Let E be an elliptic curve, and $m \in \mathbb{Z}$ non-zero. Then :*
(a) If $m \neq 0$ in K, then $E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$
(b) If $car(K) = p$ then $E[p^e]$ is either 0 or $\frac{\mathbb{Z}}{p^e\mathbb{Z}}$

Démonstration. We first proove the proposition (a) by remarking that we know that $card(ker[m]) = m^2$ as the degree of $[m]$ is m^2 and that $[m]$ is a separable map because $m \neq 0$ in K. Then, because for every d dividing m we have $card(E[d]) = d^2$, it's a group theory fact that $E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$.
Now to proove (b), one can simply see that : $card(E[p^e]) = deg_s([p^e]) = deg(\hat{\phi} \circ \phi^e) = deg_s(\hat{\phi}^e)$. Then, as $deg(\hat{\phi}) = deg(\phi) = p$, the degree of seperability is either p or 1. Then, again writing the group as a product of cyclic group, one obtain the wanted isomorphism. □

2.8 Tate Module

We know introduce the Tate-Module. We try to motivate the introduction of such an object. The context is the following : our field K is a field of caracteristic non-zero and our elliptic curve is defined over K. We just proved that the m-torsion of an elliptic curve is non-trivial as soon as m is prime to $car(K)$. But, the group $E[m]$ has more structure, for instance the galois group $G_{\overline{K}/K}$ act on it that is to say we have a representation : $G_{\hat{K}/K} \longrightarrow GL_2(\frac{\mathbb{Z}}{m\mathbb{Z}})$. That said, here the situation is not the best as that implies to do linear algebra in caracteristic non-zero. One can introduce the Tate-module to avoid this problem :

Definition 13. *For an elliptic curve E over a field K of caracteristic non-zero, we define the l-adic Tate Module $T_l(E)$ (with l a prime number prime to $car(K)$) to be $\underset{n}{colim} E[l^n]$, with the map between $E[l^{n+1}]$ and $E[l^n]$ being $[l]$.*

Because we know how to compute the torsion-groups, the following proposition holds immediatly :

Proposition 16. *As $\mathbb{Z}_l$, the tate-module is $\mathbb{Z}_l \times \mathbb{Z}_l$ if $l \neq p$, and is the zero or $\mathbb{Z}_l$ if $l = p$.*

As our elliptic curve is defined over K, the multliplication map are morphism whose coefficients are in K and then commute with the action of the galois group. Because of that, we have an induced representation $G_{\hat{K}/K} \longrightarrow Aut(T_l(E))$. This time, we work in caracteristic zero as $car(\mathbb{Z}_l) = 0$. We will see soon that working in $\mathbb{Z}_l$ will be a huge advantage. We now are close to present the Honda-tate conjecture. As we are going to see, we can get a better understanding of isogenies through the

Tate-Module. Indeed, an isogeny $\phi : E \longrightarrow E'$ induces a $\mathbb{Z}_l$-linear map between $T_l(E)$ and $T_l(E)$ as the being a morphism group allows ϕ to commute with the multiplication map. We denote ϕ_l the map we just defined. Then we just defined a map from $Hom(E, E')$ to $Hom(T_l(E), T_l(E'))$. We enounce a pretty easy statement that capture a lot of information on $Hom(E, E')$:

Proposition 17. *The map $Hom(E, E') \otimes \mathbb{Z}_l \longrightarrow Hom(T_l(E), T_l(E))$ $\phi \mapsto \phi_l$ is injective*

Démonstration. We first enounce a lemma using some topology :

$$\text{Let } M \subset Hom(E, E') \text{ be a finitely generated subgroup, and define}$$
$$M^{div} := \{\phi \in Hom(E, E'), [m] \circ \phi \in M\}. \text{ Then, } M^{div} \text{ is a finitely generated group.}$$

Now, consider $\phi \in Hom(E, E') \otimes \mathbb{Z}_l$ such that ϕ_l. Consider a subgroup M of $Hom(E, E')$ finitely generated such that $\phi \in M \otimes \mathbb{Z}_l$. By our lemma, M^{div} is finitely generated. In addition to that, we know it's a free $\mathbb{Z}$-module. Then, we have a basis of M^{div} that denote $\psi_1, ..., \psi_n$ $inHom(E, E')$. Then we know that for some $\alpha_1, ..., \alpha n$, $\phi = \alpha_1\psi_1 + \ldots + \alpha_n\psi_n$. Choosing some $a_i = \alpha_i$ $mod[l^n]$, the hypothesis implies that $a_1\psi_1 + ... + a_n\psi_n$ is zero on $E[l^n]$. Denoting ψ the morphism, that means it can factorized through $[l^n]$ i.e that we have $\lambda \in Hom(E, E'), suchthat, \psi = [l^n] \circ \lambda$. As a conclusion, $\lambda \in M^{div}$ so that it can decomposed on the base $\psi_1, ..., \psi_n$. But as $\psi = [l^n] \circ \lambda$, this means, the $\alpha_i = 0$ $mod[l^n]$, which is what we wanted to show. □

A simple consequence of it, is that $Hom(E, E')$ is at most of rank 4 as a $\mathbb{Z}$. Indeed, it is clear that $End(T_l(E), T_l(E'))$ is of rank 4 at most (as $End(T_l(E), T_l(E')) = GL_2(\mathbb{Z}_l)$).
Now one can ask, is this map an isomorphism ? We are going to see that in the case of finite field it's true, that is the Honda-Tate conjecture :

Theorem 8. *The map $Hom(E, E') \otimes \mathbb{Z}_l \longrightarrow Hom(T_l(E), T_l(E))$ $\phi \mapsto \phi_l$ is an isomorphism if K is a finite field*

Usually, proof of this require a good knowledge of abelian varieties. Here, we present a proof that don't require such knowledge. The only drawback to this approach will be that, the material it covers is broad. Then the objective of the next sections is to get familiar with more of the concepts needeed. By lack of time, we could'nt get all the material covered, and a part of the proof we'll be skipped.

2.9 The Weil Pairing

This section can be skipped during the first reading. We show how one can realise the m- groupe torsion of an elliptic curve equipped with its Galois group. That allows to proove a link between the degree of a map ϕ of E and the determinant of the associated map on the Tate-module that is the following statement :

Proposition 18. *Let $\phi \in End(E)$ and ϕ_l the induced map of Tate-module. Then*

$$det(\phi_l) = deg(\phi) \text{ and } tr\phi_l 1 + deg(\phi) - deg(1 - \phi)$$

So we consider E/K an elliptic curve, and we fix an integrer $m \geq 2$ that is prime to the caracteristic of K (if the caracteristic is non-zero). We are gonna achieve a pariring of the group $E[m]$ with galois invariance by using the m^{th}- root of unity. We want our construction to be intrinsical. To do so, we are gonna use the divisors of E. One consider $T \in E[m]$. Then, because of 4, we know there's $f \in K(E)$ such that :

$$div(f) = m(T) - m(O)$$

Taking a point $T' \in E$ so that $[m]T' = T$, we have then $g \in \overline{K}(E)$ so that :

$$div(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R)$$

One can check that $f \circ [m]$ and g^m have the same divisor so that, scaling f by a constant $f \circ [m] = g^m$. Then, for any $S \in E[m]$ and $X \in E$, we have :

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$$

As a conclusion, the quotient $g(X+S)/g(X)$ takes its value in the m^{th} root of unity, so it's constant. Then, we define the pairing :

$$\begin{gathered} e_m : E[m] \times E[m] \longrightarrow \mu_m \\ \text{with } e_m(S,T) = \frac{g(X+S)}{g(X)} \end{gathered}$$

This pairing enjoy a lot of useful properties, that we sum up in the following proposition :

Proposition 19. *The pairing defined sooner has the following properties :*
(a) $e_m(S+S',T) = e_m(S,T)e_m(S',T)$ *and* $e_m(S,T+T') = e_m(S,T)e_m(S,T')$
(b) $e_m(T,T) = 1$ *and* $e_m(S,T)^{-1} = e_m(T,S)$
(c) It's non-degenerate, meaning if $e_m(S,T) = 1$ *for all* $S \in E[m]$ *then* $T = O$
(d) The galois invariance : $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$ *for* $\sigma \in G$
(e) $e_{mm'}(S,T) = e_m([m']S,T)$ *for* $S \in E[mm'], T \in E[m]$

The proof consist mainly of just some computation and playing with the divisors so we skip it. We see now the dual isogeny is the adjoint/dual in the sense of the Weil pairing :

Proposition 20. *Let* $\phi : E \longrightarrow E'$ *be an isogeny. Then, for* $S \in E[m]$ *and* $T \in E'[m]$ *we have* $e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$

Démonstration. To do so, we consider the same function f and g we defined at the begining of the section and we recall that $div(f) = m(T) - m(O)$ with $f \circ [m] = g^m$. Be defintion, $e_m(\phi(S), T) = \frac{g(X+\phi(S))}{g(X)}$ The trick here is to consider a function $h \in \overline{K}$ such that $\phi^*((T)) - \phi^*((O)) = (\hat{\phi}(T)) - (O) + div(h)$ which is possible thanks to criteria 4. We can then compute $div(\frac{f \circ \phi)}{h^m} = m(\hat{\phi}(T)) - m(O)$ and knowing $\frac{g \circ \phi}{h \circ [m]}^m = \frac{f \circ \phi}{h^m} \circ [m]$ we can finish our computation :

$$\begin{aligned} e_m(S, \hat{\phi(T)} &= \frac{(g \circ (\phi/h) \circ [[m]])(X+S)}{(g \circ (\phi/h) \circ [[m]])(X)} \\ &= \frac{g(\phi X + \phi S)}{g(\phi X} \frac{h([mX]}{h([m]X + [m]S} \\ &= e_m(\phi(S), T) \end{aligned}$$

□

We give now a more geometric point of view about the Weil pairing. To do we consider the group of the l^n-root of unity in K for any integrer $n \geq 0$ and prime l and denote the associated group μ_{l^n}. We know that $\mu_{l^{n+1}} \cong \mathbb{Z}/l^{n+1}\mathbb{Z}$, and the l-power map defines a morphism from $\mu_{l^{n+1}} \longrightarrow \mu_{l^n}$ so we can take the colimit of the corresponding diagramm which give us a corresponding version of the tate module that we denote $T_l(\mu)$. We know combine the Weil-pairing $e_{l^{n+1}} : E[l^{n+1}] \times E[l^{n+1}] \longrightarrow \mu_{l^n}$

we already constructed. To define a map from the tate module $T_l(E)$ to $T_l(\mu)$ we need to show that they're compatible that is to say : $e_{l^{n+1}}(S,T)^l = e_{l^n}([l]S,[l]T$. That is done very quickly by remarking using 19 $e_{l^{n+1}}(S,T)^l = e_{l^{n+1}}(S,[lT]) = e_{l^n}([l]S,[l]T)$. So our map is now defined.
We now go back to the heart of the subject and show that this pairing allows us to proove two formula that are going to be pretty useful to count the point over the finite fields. To start with the proof of 18, we take a $\mathbb{Z}_l$-basis of $T_l(E)$ that we denote $\{v_1, v_2\}$ and write $\phi_l(v_1) = av_1 + cv_2$, $\phi_l(v_2) = bv_1 + dv_2$. Then, we have :

$$\begin{aligned} e(v_1,v_2)^{deg(\phi)} &= e(deg(\phi)v_1, v_2) \\ &= e(\hat{\phi_l}\phi v_1, v_2) \\ &= e(\phi_l v_1, \phi_l v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1,v_2)^{ad-bc} \\ &= e(v_1,v_2)^{det(\phi_l)} \end{aligned}$$

Because of the nondegenerecense of the pairing we conclude that $deg(\phi) = det(\phi_l)$. The trace formula is easy to proove as one knows the relation $tr(A) = 1 + det(A) - det(1-A)$.

2.10 Endomorphism ring of an elliptic curve : general case

This very short section has for main objective to get to know better the endomorphism ring of an elliptic curve. The main work has already be done. Indeed, what we know so far is that $End(E)$ is a ring of caracteristic 0, with no torsion, it comes equipped with an anti-involution (the dual isogeny), so that $\hat{\phi}\phi$ is a non-negative integrer (for $\phi \neq 0$). In addition to that, we know it's of rank 4 at most as a $\mathbb{Z}$-module. But first, we introduce some vocabulary :

Definition 14. *We consider a $\mathbb{Q}$-algebra κ finitely generated over $\mathbb{Q}$. Then, we say that a subring R of κ is an order in κ if, $R \otimes \mathbb{Q} = \kappa$.*

We can now state our theorem :

Theorem 9. *The endomorphism of an elliptic curve E defined over K is either $\mathbb{Z}$ or an order in an imaginary quadratic field or in a quaternion algebra. In the case $car(K) = 0$ the two first are the only possible*

The proof relies on a much general statement that any ring verifying some properties as $End(E)$ (having an anti-involution, caracteristic 0 etc) are exactly of this form. It's not difficult, but not the subject here. One can still check "The Arithmetic of elliptic curve" for more informations. We wish already to bring the attention to a fact that will occupy us at the end of this work. We know that $End(E)$ contains $\mathbb{Z}$ (the multiplication map), but it can be bigger as tell us 9. In particular in caracteristic non-zero it can be much bigger (at least when tensorized it can be the quaternion algebra or an imaginary quadratic field). The elliptic curve such that $End(E) \otimes \mathbb{Q}$ is the quaternion algebra are called supersingular. We give a quick warning about this name : those elliptic cure have-definition-no singular point. The name comes from the surprise of mathematician when they saw that $End(E)$ could be much bigger than $\mathbb{Z}$ and not being an imaginary quadratic field. This can be historically explained by the fact that those curve appears only in caracteristic non-zero while elliptic curves were historically studied over $\mathbb{C}$.

2.11 Some elliptic curve over finite fields

We now get more focused on the case where our field is a finite one of caracteristic p. A natural question that comes up, is to count the number of point of an elliptic curve over a finite field. In his thesis, Hasse showed the following result :

Theorem 10. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then :*

$$|card(E(\mathbb{F}_q) - q - 1 \leq 2\sqrt{q}|.$$

Démonstration. If we denote ϕ the Frobenius of the elliptic curve E, we show that : $card(E(\mathbb{F}_q)) = deg(1-\phi)$. Indeed, as we know that the galois group of the $\hat{F}_q\mathbb{F}_q$, is generated by the Frobenius, we know that a point $P \in E$ is in $\mathbb{F}_q$ if and only if $\phi(P) = P$. Then $ker(1-\phi) = E(\mathbb{F}_q)$, and as $1-\phi$ is separable (from 13), we know that $card(ker(1-\phi)) = deg(1-\phi)$. To conclude, as the degree is a non-degenerate quadratic form over the endormophism ring, one can apply a version of Cauchy-Schwarz to have the inequality. □

Now to get a better understanding of our elliptic curve, we collect some informations on the Frobenius :

Proposition 21. *Let E be an elliptic curve over $\mathbb{F}_q$ equipped with its frobenius ϕ and let's denote a the quantity $q + 1 - E(\mathbb{F}_q)$. We have the following statement :*
(a) If α, β are the complex roots of $T^2 - aT + q$. Then α, β are complex conjugate of absolute value $\sqrt{q}$ and for every integrer $n \geq 1$ we have $card(E(\mathbb{F}_{p^n})) = q^n + 1 - \alpha^n - \beta^n$.
(b) The frobenius verfies $\phi^2 - a\phi + q$.

Démonstration. First we need to show we have complexe conjugate roots. But, one might remark that $T^2 - aT + q$ is caracteristic polynomial of ϕ_l. Indeed, $det(\phi_l) = deg(\phi) = q$ and $tr(\phi_l) = 1 + deg(\phi) - deg(1-\phi) = 1 + Q + card(E(\mathbb{F}_q)) = a$ and we know that ϕ is a morphism of a two-dimensional -$\mathbb{Z}_l$ vector space. That being said, $det(T - \phi_l) = (T-\alpha)(T-\beta)$ Now we show that α, β are two conjugate complex numbers. To do so, we use a density idea, as for every rational number $\frac{m}{n}$ we can see that $det(\frac{m}{n} - \phi_l) = \frac{det(m-n\phi_l}{n^2} = \frac{deg(m-n\phi)}{n^2} \geq 0$
Then, we have two possibilities : either a double real root, or two complex conjugate roots. But as we know, $\alpha\beta = det(\phi_l) = q$ and $|\alpha| = |\beta| = \sqrt{q}$. Then, the only option for a double root is $\sqrt{q}$ which is not possible.
The second part of the proposition (a) is almost instantaneous as soons as we remark that the q^n-power of Frobenius verify $card(E(\mathbb{F}_{q^n}) = deg(1-\phi^n)$.
(b) For the second statement, one already knows the caracteristic polynomial of ϕ_l is $T^2 - aT + q$. Then : $deg(\phi^2 - a\phi + q) = det(\phi_l^2 - a\phi_l + q) = det(0) = 0$. □

2.12 The endomorphism ring of an elliptic curve over a finite field

We first set our context : we consider a finite field K of caracteristic p and an elliptic curve E defined over this field,. We know that the p-group torsion of E is either 0 or $\mathbb{Z}$ $p\mathbb{Z}$. We show that the isomorphism class of $E(p)$ is actually related to the structure of the ring $End(E)$.

Theorem 11. *For each integrer $r \geq 1$ let ϕ_r be the ϕ^r-power Frobenius.*
(a) The following proposition are equivalent :

(i) One (so all of them) of the torsion group $E(p^r)$ is trivial
(ii)The dual of ϕ^r is purely inseparable for one (all) value of r

(iii) The p-multplication map $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$
(iv) $End(E)$ is an order in a quaternion algebra.

(b) If the conditions in (a) does not hold, then with the hypothesis $j(E) \in \bar{\mathbb{F}}_l$ (meaning it's not transcendantal) then $End(E)$ is an order of a quadratic imaginary field.

Before we go into more details, the elliptic curve that satisfies (a) are named supersingular. The reader might ask you ? First, such elliptic curve does not exist in the case $\mathbb{C}$ In addition to that, even among the case of elliptic curve, they're few of them with such an endomorphism ring (one can observe that with the condition $j(E) \in \mathbb{F}_{p^2}$ which implies ther're a finite number)

Démonstration. (a) We see first that the proposition (i) and (ii) are equivalent pretty easily as $deg_s(\hat{\phi_r} = deg_s([p^r]) = (deg_s[p])^r = deg_s(\hat{\phi})^r)$ which implies : $card(E(p^r) = deg_s(\hat{\phi})^r$ and so gives the wanted result.
Now we show $(ii) \Longrightarrow (iii)$. It's pretty easy to see that $[p]$ is purely inseparable as $\hat{\phi}, \phi$ are and $[p] = \hat{\phi} \circ \phi$. We need then to show that $j(E) \in \mathbb{F}_{p^2}$. To do so, one can use the fact $\hat{\phi}$ is purely inseparable (by hypothesis) so that we have the diagramm :

$$\begin{array}{ccc} E^{(p)} & \xrightarrow{\hat{\phi}} & E \\ {\scriptstyle \phi'}\downarrow & & \downarrow{\scriptstyle inclusion} \\ E^{(p^2)} & \xrightarrow{\psi} & E \end{array}$$

where ϕ' is the p^{th}-power frobenius and ψ is of degree one. Then, we have that ψ is an isomomorphism, which implies $j(E) = j(E^{p^2}) = j(E)^{p^2}$ which implie that $j(E) \in \mathbb{F}_{p^2}$.
Now we prove that $(iii) \Longrightarrow (iv)$. If $End(E)$ is not an order in a quaternion algebra, we have that $\kappa = End(E) \otimes \mathbb{Q}$ is a number field.
Then consider E' any elliptic curve isogenous to E, that is we have $\psi : E \longrightarrow E'$. As p multiplication map in E is purely inseparable, it's the same in E' (because $\psi \circ [p] = [p] \circ \psi$). We deduce then that p-group torsion is trivial (from our precedent equivalence) and $j(E') \in \mathbb{F}_{p^2}$. As a conclusion, ther're a finite number of elliptic curve isogenous to E.
Now we try to obtain a condtradiction. To do so, we choose a prime $l \in \mathbb{Z}$ that is still a prime in $End(E')$ for E' isogenous to E (which we can do as there's a finite number of them). Then, because of we choose l we know that $E(l^i) \cong \mathbb{Z}/l^i\mathbb{Z} \times \mathbb{Z}/l^i\mathbb{Z}$, so take a sequence $\Phi_1 \subset \Phi_2 \subset ... \subset E$ so that $\Phi \cong \mathbb{Z}/l^i\mathbb{Z}$. We denote $E_i = E/\Phi_i$ which comes with an isogeny $E \longrightarrow E_i$ of kernel Φ_i. But as we know, there can be only finitely many distinct E_i (because they're isogenous to E), then for some integrer m, n, we know that E_m and E_{m+n} are isomorphic, so we have $\lambda : E_m \longrightarrow E_{m+n} \cong E_m$ an isomorhism whose kernel is cyclic $ker(\lambda) = \phi_{m+n}/\phi_m$. The problem comes now, as l is a prime in $End(E_m)$ the kernel of $[l^{n/2}]$ can't be cyclic but a degree comparison shows $\lambda = u \circ [l^{n/2}]$ for some $u \in Aut(E_m)$. Then, κ can't be a number field, which conclude the proof.
Now it's only left to see $(iv) \Longrightarrow (ii)$. To do so, we suppose that (ii) here is false meaning, $\hat{\phi}_r$ is separable for all $r \geq 1$. We show that $End(E)$ must be commutative, which is a contradiction as $End(E)$ is suppose to be an order in a quaternion algebra. To do so, we remark that $End(E) \longrightarrow End(T_p(E))$ is an injective map. Suppose that $\psi \in End(E)$ is zero in $End(T_p(E))$. We know, then because of the construction of $T_p(E)$ that ψ is zero on every p^r torison group. Then, $ker(\hat{\phi_r}) \subset \phi_r(ker(\psi))$ as $[p^r] = \phi_r \circ \hat{\phi}_r$. Then, because ϕ_r is surjective we deduce that $card(ker(\psi)) \geq card(ker\hat{\phi}_r) = deg(\phi^r) = p^r$. Then, ψ must be zero. So, $End(E)$ is a subring of the comutative ring $End(T_p(E))$, which is a contradiction.
To complete the proof, we need to prove the point (b). So, having the conditions in (a) are not satisfied means the torsion group is not trivial. Using the fact that $j(E)$ is not transcendental, we find an elliptic curve E' defined over $\mathbb{F}_{p^r}$ isomorphic to E. Suppose then, that $\hat{\phi}_r \in \mathbb{Z} \subset End(E')$. By degree comparison, $\hat{\phi}_r = [p^{r/2}]$ or is $[-p^{r/2}]$. But that means that $E[p^{r/2}]$ is trivial as those map are not

separable. Conclusion, the frobenius is not in $\mathbb{Z}$, which means $End(E') = End(E)$ is an order in an imaginary quadratic field. □

That being proved, we here have more knowledge on the endomorphism ring.

2.13 Reduction of elliptic curve

Reduction of elliptic curve is a pretty natural thing to do. For instance one can consider an elliptic curve defined over $\mathbb{Z}$ and look at the equation whose coefficient are reduced module a prime p. We will see that is pretty useful, as it enables to make a link between caracteristic 0 (typically in $\mathbb{C}$ of which we have a great knowledge) and non-zero (where the picture might blurry). The idea to keep in mind here is the reduction module a prime, but we give here a more general context : we consider a local ring K with a respect to a discrete valuation v with the ring of integrer $R = \{x \in K, v(x) \geq 0\}$. The ring R is local, of maximal ideal $M = \{x \in K, v(x) \geqslant 0\}$. Naturally, as local ring, we can get a uniformizer π meaning $\pi R = M$, and the residue field $k = R/M$ where the reduction will take place. Then, reducing an elliptic curve defined over K is simply to map the coefficient of the equation that defined E in k. The litterature on this subject is pretty broad for instance "The arithmetic of elliptic curve" dedicate a whole chapter to it as Lang does in "Ellptic function". We just state here the theorem we will use in the Honda-Tate proof :

Theorem 12 (Deuring's lifting theorem)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve and $\phi \in End(E)$. There exists an elliptic curve E^* over a number field L with $\phi^* \in End(E^*)$ such that there's a good reduction module a prime p so that the reduction module p of E^* and ϕ^* is E with ϕ*

2.14 The Honda-Tate theorem

This section is now dedicated to a summary of the proof of the Honda-Tate theorem. First we recall the statement :

Theorem 13. *The map $Hom(E, E') \otimes \mathbb{Z}_l \longrightarrow Hom(T_l(E), T_l(E))$ $\phi \mapsto \phi_l$ is an isomorphism if K is a finite field*

This theorem is actually a restricted version to a more general statement. The Honda-Tate theorem says that this is actually an isomorphism even in the case of abelian varieties. To quicky explain what is abelian variety, one can think of them as generalisation of elliptic curve in higher dimension, meaning an algebraic variety/scheme equipped with a group structure. Then, the usual proof of this theorem require a good knowledge of abelian variety. Here, we draw a proof without using them. The price to pay is that the concepts used are broader, from algebraic number theory to scheme theory. This is the reason we only sketch how the proof work. This proof comes from a seminar of Mihran Papikian and is recap in the article "Honda-Tate for elliptic curve". In this paper, he proves that the map $Hom_k(E, E') \otimes \mathbb{Z}_l l \longrightarrow Hom_G(T_l(E, E')$ is an isomorphism (where $Hom_k(E, E')$ are the morphism defined over the finite field $k = \mathbb{F}_q$ $(q = p^a)$, and $Hom_G(T_l(E, E')$ are the morphism that commute with the galois group G of the extension $\hat{k}/k$) . This statement is then a bit more general that the one we first made.
The idea here is to distinguish the case of supersingular elliptic curves and the singular one as they behave very differently when it comes to their torsion point and endomorphism ring.
Then we change a change the problem, as we know that the co-kernel of $Hom_k(E, E') \otimes \mathbb{Z}_l \longrightarrow Hom_G(T_l(E)T_l(E'))$ is free, it's enough to show that $Hom_k(E, E') \otimes \mathbb{Q}_l l \longrightarrow Hom_G(V_l(E), V_l(E'))$

where $V_l(E) = T_l(E) \otimes \mathbb{Q}_l$ is an isomorphism. We know can start the proof :

Démonstration. First we assume that E_1 and E_2 are isogenous over k meaning $Hom_k(E_1, E_2 \neq 0$. Then, we can see that the dimension of $End_k(E_1)$ and $Hom_k(E_1, E_2)$ as $\mathbb{Q}_l$ -vector space is the same. Then, as we already have the injectivity of the map,, we need to show that $dim_{\mathbb{Q}_l}(End_k(E) \otimes \mathbb{Q}_l) \geq dim_{\mathbb{Q}_l}(End_G(V_l(E)))$.
Now we look up the frobenius endomorphism of E that we denote π. We denote F the set $\mathbb{Q}(\pi)$ and $D = End_k(E) \otimes \mathbb{Q}$. The field F is actually in the center of the division algebra D, so that π is a semi-simple and so π_l is too this will be useful. Now we look at the two possibilities for the value of $[F : \mathbb{Q}]$that is to say 2 or 1 (as π satisfies the equation $\pi^2 - t\pi + q = 0$).
First consider the case $[F : \mathbb{Q}] = 2$. We know that G is generated by the frobenius, then, one can see that $End_G(V_l(E))$ is the centralizer of $\mathbb{Q}_l(\pi_l)$. But, $End(V_l(E))$ is isomorphic to $M_2(\mathbb{Q}_2)$ which is of dimension 4. then, the dimension of $\mathbb{Q}_l(\pi_l)$ must be 1, 2 or 4 as it divides 4. The last and first case are not possible as π_l is not a scalar, that implies that $dim(End(V_l(E)))$ is 2. Then, we got what we wanted here.
For the second case we have to suppose $F = \mathbb{Q}$ that is to say π is a scalar. As it is a scalar, we know that $\hat{\pi} = \pi$ which tells us it is not seperable and we even know that a must be an even number as $\pi^2 = [q] = [p^a]$. In the end, what matters is that every morphism defined over $\hat{k}$ is actually defined over k as the frobenius is in $\mathbb{Z}$. This shows E is supersingular and so $dim(D \otimes \mathbb{Q}_l) \geq 4 = dim(End(V_l(E))\ geqdim(End_G(V_l(E)))$, so once again we have the inquality wanted.
What remains to proove is that in the case where $Hom_G(V_l(E_1, E_2)$ is non-trivial then $Hom_k(E_1, E_2)$ is non-trivial. This is the part that use a lot more of tools. We give then a quick taste of how we can process (as we don't have all the tools for) but for the whole proof one can refer the reference [4]. We suppose $Hom_G(V_l(E_1, E_2)$ is non-trivial. It's long to show, but if so, that we can then assume either both of the elliptic curve are supersingular with their endomorphisms and isogenies between them defined over k or that they're ordinary. Here, we can be surprised of such a result, but as we found, isogeny is the great notion of some relaxed isomorphism of elliptic curve.
Then we have two cases to treat. The main object here is 12. Indeed, the idea is to left the elliptic curves from a finite field to $\mathbb{C}$. Because we get a much better understanding over $\mathbb{C}$ we are going to use it to solve the problem. More precisely the things that is easier in $\mathbb{C}$ is that to obtain an isogeny of. elliptic curves one can simply look for a morphsim between the lattices of those curves. It's here that the number theory is useful and so we are not going more far into the details and let the reader get a First we treat the case where E_1, E_2 are two supersingular curves. □

2.15 The Weil-Conjecture

The last thing we will treat here are the Weil's conjecture. These conjecture applies to a larger class of curve that the elliptic curve and have been an interest as soon as they've been stated. Numerous famous figure of mathematics started to work on it, as Deligne and Grothendieck. To state those conjectures, Weil took example on Artin. Indeed, Artin stated these conjectures only for algebraic curves, but Weil had the idea of generalizing them to any projective variety. We set some definitions before giving them. To give some context, we consider a projective variety V defined over a finite field $\mathbb{F}_q$, and with homogenous equations $f_1(x_0, ..., x_N) = ... = f_m(x_0, ..., x_N) = 0$. Naturally, the set $V(\mathbb{F}_{q^n})$ (the point of V in $\mathbb{F}_{q^n}$). We define the zeta function of V :

Definition 15 (zeta function)**.** *The zeta function of $V/\mathbb{F}_q$ is the power series :*

$$Z(V/\mathbb{F}_q; T) = exp(\sum_{n\geq 1}(card(V(\mathbb{F}_{q^n})\frac{T^n}{n})$$

Now we present the Weil Conjectures :

Theorem 14. *Let $V/\mathbb{F}_q$ be a smooth projective variety of dimension N.*
(a) There is an integrer ϵ, called the Euler characterisric of V such that : $Z(V/\mathbb{F}_q; 1/q^N T) = +/- Q^{N\epsilon/2} Z(V/\mathbb{F}_q; T)$
(b) Riemann Hypothesis : The zeta functions factors as $\frac{P_1(T)...P_{2N-1}(T)}{P_0(T)P_2(T)...P_{2N}(T)}$ with $P_i(T) \in \mathbb{Z}[X]$, $P_0(T) = 1 - T$ and $P_{2N}(T) = 1 - q^N T$. Also, the polynomial $P_i(T)$ factors over $\mathbb{C}$ as $\prod_{1 \leq i \leq b_i}(1 - \alpha_{ij})T$ with $|\alpha_{ij}| = q^{1/2}$, and b_i being the degree of P_i also named the i^{th} Betti number of V

This state is out of our context and we are going to proove it only for the elliptic curve. We will see that, in this case, the conjecture is pretty simple to prove. This is the next theorem, which is the update version for elliptic curve :

Theorem 15. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then there's an $a \in \mathbb{Z}$ such that :*
$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$ and $Z(E/\mathbb{F}_q; 1/qT) = Z(E/\mathbb{F}_q; T)$. In addition to that, $1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$ with $|\alpha| = |\beta| = \sqrt{q}$

Démonstration. We first compute

$$\begin{aligned} log(Z(E/\mathbb{F}_q; T)) &= \sum_{n \geq 1} (card(V(\mathbb{F}_{q^n})) \frac{T^n}{n} \\ &= \sum_{n \geq 1} (\frac{(1 - \alpha^n - \beta^n + q^n T^n}{n}) \\ &= -log(1 - T) + log(1 - \alpha T) + log(1 - \beta T) - log(1 - qT) \end{aligned}$$

The second equality comes from what we have said about the Frobenius before. Then, by taking the exponential of this expression, we have the expression we were looking for. Also, the complex root of our polynomials are of absolute value $\sqrt{q}$ as expected. □

One can be surprised that we call our function, the zeta function of the elliptic curve. We show how is motivated such a name. We make a change of variable, and set $T = q^{-s}$ and we look now at the zeta function as a series that depends of the variable s, which gives :
$\zeta(s) = Z(E/\mathbb{F}_q; q^{-s}) = \frac{1 - aq^s + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$. It verifies the fundamental relation of the zeta function of Riemann i.e : $\zeta(s) = \zeta(1 - s)$. Then, the Weil conjecture says that the zero of the zeta function are of absolute value $\sqrt{q}$ which means $Re(s) = \frac{1}{2}$.

2.16 Conclusion

To conclude this document, I would like to put an emphasis on a strategy that is important in math : write/enounce question in a new way. Honda-tate theorem is a wonderful representation of this, cause it allows to translate into the world of linear algebra a problem that at first might not be linear. In particular in finite field, where elliptic curves are not defined by lattices, the Tate-Module essentially try to mimic this role of going into the linear world. Also, we see how mathematician can be inspired by work from other field as in the Weil conjecture that mimic the Riemann hypothesis. We hope that the reader can now see how interesting elliptic curves are.

Bibliographie

[1] Joseph H.Silvermann (2009) *The Arithmetic of Elliptic Curve*, Springer New York, NY, GTM 106, 2nd ed.

[2] Joseph H.Silvermann (1994) *Advanced topics in the aritmetic of elliptic curves*, Springer New York, NY,GTM 151.

[3] S. Lang (1987) *Elliptic functions*, GTM 112.

[4] Mihran Papikan (2012) *Honda-Tate for elliptic curves.*