DTU (Copenhagen) September 2005

AGM for elliptic curves

By
Christophe RITZENTHALER

Contents

Chapter 1

p-adic numbers

Our philosophy will be simple : take what is good about finite fields (i.e unicity of extensions of a given degree, Galois extensions with cyclic group structures) and leave the bad things (i.e analytic problems like $(x^p)' = 0$). Indeed, analysis in characteristic $p > 0$ (and also representation theory) are not very convenient and there is a common trick (projective limits) to pass to a characteristic 0 structure. In the case of finite fields, these new structures can be built in a lot of different ways and arrive then with rich (analytic and arithmetic) properties that we will try to sum up in this chapter.

References : Serre (Local fields) A.J. Baker (an introduction to p-adic numbers and p-adic analysis), on the web.

1.1 Projective limit, completion and discrete valuation ring

A first point of view is the (formal) algebraic construction that relies on projective limit. We give here an *ad-hoc* definition.

Definition 1.1.1. *Let $(A_i, p_{ij})_{i\in\mathbb{N}^*}$ a directed family of rings (i.e the p_{ij} are compatible homomorphisms from A_i to A_j for all $i \geq j$). Let $\Gamma = \prod A_i$ and consider the subset A of Γ of all elements (a_i) with $a_i \in A_i$ and for $i \geq j, p_{ij}(a_i) = a_j$. A is a subring of Γ denoted $\varprojlim A_i$ and called the* projective (or inverse) limit *of the $(A_i, p_{ij})_{i\in\mathbb{N}^*}$.*

Example 1. *Let p be a prime and for $i \geq j$ let $p_{ij} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ be the natural projections. This is a directed family.*

This inverse limit can also be characterized by an universal property :

Proposition 1.1.1. *A comes with a family of morphisms $p_i : A \to A_i$ such that : if B is a ring and $\phi_i : B \to A_i$ a family of compatible morphisms (i.e for $i \geq j$ the following diagram is commutative*

$$\begin{tikzcd}
B \arrow[r, "\phi_i"] \arrow[dr, "\phi_j"'] & A_i \arrow[d, "p_{ij}"] \\
 & A_j
\end{tikzcd}$$

) then there is a morphism $\phi : B \to A$ such that for all i the following diagram is commutative :

$$\begin{tikzcd}
B \arrow[r, "\phi"] \arrow[dr, "\phi_j"'] & A \arrow[d, "p_j"] \\
 & A_j
\end{tikzcd}$$

Remark 1. In the case of the example, the natural morphisms from $\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ shows that there is a morphism from $\mathbb{Z}$ to the projective limit. This morphism is injective so the projective limit is a ring of characteristic 0.

The second point of view is analytic. We want to say some words on completions. Let R be a domain (i.e an integral commutative ring with unity) and K its field of fractions.

Definition 1.1.2. *A surjective homomorphism $v : K^* \to (\mathbb{Z}, +)$ is called a* (discrete) valuation *if for all $x, y \in K^*$ one has*

$$v(x+y) \geq \inf(v(x), v(y)).$$

We make the convention that $v(0) = +\infty$.

Example 2. *In the case of $R = \mathbb{Z}$, one can define for each prime p a valuation $v = v_p$ called the p-*adic valuation *in the following way : for $0 \neq a \in \mathbb{Z}$, $v(a) = \max\{r : p^r | a\}$ and if $x = a/b \in \mathbb{Q}^*$ one defines $v(x) = v(a) - v(b)$. It is easy to check the different properties.*

Definition 1.1.3. *A map $N : R \to \mathbb{R}^+$ is called a* norm (or absolute value) *on R if*

- *$N(x) = 0$ iff $x = 0$.*
- *$N(xy) = N(x)N(y)$ for all $x, y \in R$.*
- *$N(x+y) \leq N(x) + N(y)$ for all $x, y \in R$.*

If moreover one can replace the last inequality by

$$N(x+y) \leq \max(N(x), N(y))$$

then the norm is called non-archimedian (or ultrametric).

Example 3. *On $\mathbb{Q}$ (or $\mathbb{R}, \mathbb{C}$) one has the usual norm which is archimedian. But on $\mathbb{Q}$ one can also create (infinitely many) non-archimedian norms in the following way : for each prime p, one defines for $x \neq 0$, $N(x) = |x|_p = p^{-v(x)}$. It is easy to check that this defines a non archimedian norm on $\mathbb{Q}$.*
Let us remark that a famous theorem (Ostrawski's theorem) claims that the norms presented here are the only (non-trivial) ones over $\mathbb{Q}$ up to equivalence (N_1, N_2 are equivalent if $N_1 = N_2^s$ for $s \in \mathbb{R}^{>0}$).

R is now given with a norm N.

Definition 1.1.4. *A sequence (a_n) of elements of R is said to be* Cauchy *(w.r.t N) if*

$$\forall \epsilon > 0 \, \exists M \in \mathbb{N} \text{ such that } \forall m, n > M \Rightarrow N(a_m - a_n) < \epsilon.$$

A ring R is said complete *(w.r.t. N) if every Cauchy sequence with coefficients in R converges in R.*

One remembers that not every Cauchy sequence with coefficients in $\mathbb{Q}$ (with its usual norm) is convergent in $\mathbb{Q}$ (for instance $\lfloor 10^n \sqrt{2} \rfloor / 10^n$) and that leads to the definition of $\mathbb{R}$ as limit of all Cauchy sequences. This construction works in general. Let us define $CS(R)$ the set of Cauchy sequences in R and $Null(R)$ the set of sequences with limit 0. One can then prove the following result.

Proposition 1.1.2. *The ring $\hat{R} = CS(R)/Null(R)$ with the norm $\hat{N}((a_n)) = \lim N(a_n)$ is complete. The norm $\hat{N}$ extends the norm N (for the canonical embedding of R in $\hat{R}$ as a constant sequence) and it is non archimedian iff N is.*

In the next section we will apply this result in the case $\mathbb{Q}$ (or $\mathbb{Z}$) and $|\cdot|_p$.
A last point of view will be the arithmetic one.

Proposition 1.1.3. *Let K be a field with a discrete valuation. Then the set R of $x \in K$ such that $v(x) \geq 0$ is a principal domain with a unique non-zero maximal ideal $\mathcal{M}$. Such a ring is called a* discrete valuation ring. *In particular R is a* local ring *(i.e with a unique non-zero prime ideal).*

Proof. Let π be an element such that $v(\pi) = 1$. Every $x \in R$ can be written in the form $x = \pi^n u$ with $n = v(x)$ and $v(u) = 0$. Now $v(u) = 0$ implies u invertible (because $v(1/u) = 0$ too). So every non-zero ideal of R is of the form $\pi^n R$ with $n \geq 0$ which shows that R is indeed a discrete valuation ring. □

Reciprocally if R is a discrete valuation ring with prime ideal (π), it is easy to see that every non zero element x of the field of fraction K^* can be written in $x = \pi^n u$ with u invertible and $n \in \mathbb{Z}$ unique. The map $x \mapsto n$ is a valuation on K. Note that the elements with valuation 0 are exactly the invertible elements of R. They are called the *units* of R.

Example 4. *If $K = \mathbb{Q}$ with the p-adic valuation, one finds $R = \mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ in p (i.e elements of $\mathbb{Q}$ of the form r/s with s not divisible by p). This ring has a unique maximal ideal, namely (p).*
Another kind of example is $k((T))$ the field of formal power series in one variable *over the field k. For every non zero formal series*

$$f(T) = \sum_{n \geq n_0} a_n T^n$$

one defines the order $v(f) = n_0$. The valuation ring is denoted $k[[T]]$.

A few more definitions. As $\mathcal{M}$ is maximal, $R/\mathcal{M}$ is a field called *the residue field* of R. In the first example it is $\mathbb{F}_p$, in the second it is k. The element π is called a *uniformizer.* If A has characteristic 0 and the residue field has characteristic $p > 0$, one can identify $\mathbb{Z}$ with a subring of R and p with an element of R. The integer $e = v(p)$ is called the *absolute ramification index* of R. R is *absolutely unramified* if $e = 1$, i.e if p is a uniformizer of R.

Theorem 1.1.1. *For every perfect field k of characteristic p, there exists a complete discrete valuation ring and only one (up to unique isomorphism) which is absolutely unramified and has k as its residue field. One denotes this ring $W(k)$ (*ring of Witt vectors*).*

1.2 $\mathbb{Z}_p, \mathbb{Q}_p$ and their (unramified) extensions

We have the following equivalent definitions, depending on the point of view (algebraic, analytic or arithmetic).

Theorem 1.2.1. *Let p be a prime. The following constructions yield the same ring denoted $\mathbb{Z}_p$.*

1. *The projective limit of the direct family $(\mathbb{Z}/p^i\mathbb{Z}, p_{ij})$ with $p_{ij} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ the natural projections.*

2. *The completion of $\mathbb{Z}$ with respect to $|\cdot|_p$.*

3. *$W(\mathbb{F}_p)$.*

In the same way $\mathbb{Q}_p$ can be seen as the field of fractions of $\mathbb{Z}_p$ or directly as the completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$.
This theorem shows us that $\mathbb{Z}_p$ is a complete discrete valuation ring of characteristic 0 with residue field $\mathbb{F}_p$ and field of fraction $\mathbb{Q}_p$. $\mathbb{Q}$ embeds in $\mathbb{Q}_p$ and is dense for the topology induced by $|\cdot|_p$.

Proposition 1.2.1. *Let R be a complete discrete valuation ring with field of fractions K and residue field k. Let S be a system of representatives of k in R and π an uniformizer. Every element $a \in R$ can be written uniquely as a convergent series*

$$a = \sum_{n=0}^{\infty} s_n \pi^n \text{ with } s_n \in S.$$

Every element $x \in K$ can be written as

$$x = \sum_{n \gg -\infty}^{\infty} s_n \pi^n \text{ with } s_n \in S.$$

Proof. The second assertion results from the first by multiplying by a suitable negative power of π. By definition of S, there exists $s_0 \in S$ such that $a - s_0 \equiv 0 \pmod{\pi}$. If ones writes $a = s_0 + \pi a_1$ and apply the same procedure to a_1 one obtains an $s_1 \in S$ such that

$$a = s_0 + s_1 \pi + a_2 \pi^2,$$

and so on. The series $\sum s_n \pi^n$ converges to a and one sees that it is unique. Conversely every series of this form is convergent since its general term converges to zero and R is complete. □

In the case of $\mathbb{Z}_p$ we can take $\pi = p$ and $S = \{0, \ldots, p-1\} \subset \mathbb{N}$.
The first and second interpretations give also convenient ways to represent an element : in the first case it is the sequence $(\sum_{n=0}^{i-1} s_n p^n \pmod{p^i})$ and the sequence $(\sum_{n=0}^{i-1} s_n p^n)$ in the second case.

Example 5. *The integer* 13 *is represented by* $(1, 4, 13, 13, \ldots)$, $(13, 13, \ldots) = (1, 4, 13, \ldots)$ *or* $1 + 1 \cdot 3 + 1 \cdot 3^2$ *in* $\mathbb{Z}_3$.

Th. 1.1.1 shows us also that we can define complete discrete valuation rings with residue field $\mathbb{F}_q$ for every $q = p^m$ in a unique way. One denotes such rings $\mathbb{Z}_q$ and their field of fractions $\mathbb{Q}_q$. Applying Prop. 1.2.1 one can represent elements of these fields by series

$$\sum_{n \gg -\infty}^{\infty} s_n p^n \text{ with } s_n \in S$$

for some representative set S of $\mathbb{F}_q$. A convenient way to proceed is then the following : let $\tilde{P} \in \mathbb{F}_p[T]$ be a defining polynomial of the extension $\mathbb{F}_q/\mathbb{F}_p$ and $P \in \mathbb{Z}[T]$ a lift of this polynomial as a monic polynomial of degree m. Then the elements of $\mathbb{Q}_q$ can be represented by

$$\sum_{n \gg -\infty}^{\infty} P_n(\alpha) p^n$$

where P_n is a polynomial of degree less than m with coefficient in $\{0, \ldots, p-1\}$ and α is a root of P.

Of course $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) embeds naturally in $\mathbb{Z}_q$ (resp. $\mathbb{Q}_q$) and so we have an extension of fields $\mathbb{Q}_q/\mathbb{Q}_p$. As our fields copy the case of finite fields, one obtains the following pleasant result.

Proposition 1.2.2. *The extension $\mathbb{Q}_q/\mathbb{Q}_p$ is Galois with Galois group $\mathbb{Z}/m\mathbb{Z} \simeq Gal(\mathbb{F}_q/\mathbb{F}_p)$. It is generated by an element σ called* the Frobenius substitution *characterized by the property : for all $x \in \mathbb{Z}_q$, $x^\sigma \pmod{p} = x^p \pmod{p}$.*

Remark 2. More generally, every finite extension K of $\mathbb{Q}_p$ is a *local field* (i.e a complete field with discrete valuation and a finite residue field). But K/Q_p may be ramified and p not an uniformizer in K.
Note also that the appellation 'local field' has a counterpart, the *global fields* (i.e number fields or function fields in one variable over finite fields). In a sense, global fields may be studied locally and then by gluing the various local information together. This leads to the theory of adèles.

1.3 Exercises

1.3.1 p-adics

Write $50, 137$ as a power series in $\mathbb{Z}_{13}$. Compute $137 + 50$ in $\mathbb{Z}_{13}$.
We would like to do that with the software MAGMA. If you have never used MAGMA before, start with the next section.

1. Create the structure.
2. Change the output shape.
3. Compute $137 + 50$ in $\mathbb{Z}_{13}$.
4. Compare.

Now we can do other operations : take the inverse of 137 for instance, or its square. Does 137 admit a square root in $\mathbb{Q}_{13}$?
We want to deal now with extensions :

1. Create the structure.
2. What is the defining polynomial of L.
3. Does 137 admits a square root in this extension ?
4. Give the residue field of L.
5. Give the Frobenius substitution.
6. Apply it to $\sqrt{137}$ and check the reduction property.

1.3.2 For beginners

To start : type magma (and return).

The most important thing is the help. There exist two sorts : the html files are the most convenient. They contain, besides the description of each command, examples and even mathematical background. You can access commands by topic (finite groups, commutative algebra, algebraic geometry) or through the index.
The second help is online : when you want information about a command, let's say `RandomPrime`, you type `RandomPrime;`.

A last tip before we start : there is a automatic completion with 'tab'. This is useful when you do not remember exactly the name : MAGMA follows very closely the exact definition.

We will start with some examples that look really similar to MAPLE. To Evaluate an expression you need to end it with `;`. To define an object you write `f:=`.... As you may see it does not display the result. To see it you have to write `f;`.

1. Compute $\frac{123}{10} + \frac{33}{127}$.
2. Compute $2 + \sqrt{3}$.
3. Compute 200! and factorize this number.
4. Is $2^{1233} + 321$ prime ?

Some examples how to handle sets, sequences, lists :

1. Define the sets $I = \{1, 4, 10\}$, $J = \{2, 4, 8\}$. Do the following operations : $I \cup J$ and $I \cap J$.
2. Create a random list of 10 integers. Extract the 8th.

Unlike MATHEMATICA/MAPLE, MAGMA require to define properly where you are working. You cannot open a MAGMA section and write : $f = x^3 + 3$;. MAGMA does not know yet what is x. It is sometimes a bit tedious when you want to work with polynomials in a lot of variables but the counterpart is that it allows much more objects than the two others softwares : polynomials over extensions of finite fields or p-adic fields, matrices with coefficients in function fields .... And it is much more accurate, mathematically speaking !

Very important fields for us are finite fields :

1. Create the field $F = \mathbb{F}_{23}$.
2. Add 20 and 5 in this field. This leads to the notion of coercion.
3. Create the field $K = \mathbb{F}_{23^4}$. What is a defining polynomial for this field ? Compute the square root of 10 in this field.

One would like also to create extensions by choosing a defining polynomial.

1. Create the polynomial ring R with variable x over $\mathbb{F}_5$.

2. Create the polynomial $f = x^6 + 3x + 3$. Evaluate f at 2. Is f irreducible ? What is its splitting field ? Call it $F < w >$.

3. Create an extension of F of degree 3 by a polynomial of your choice.

Chapter 2

Elliptic curves over $\mathbb{C}$

Curves have not always been curves, before they were ...surfaces ! Indeed it is a deep and nice result that irreducible algebraic smooth curves over $\mathbb{C}$ and compact Riemann surfaces are actually the same notion seen under two different spotlights. Hence curves over $\mathbb{C}$ inherit a bunch of analytic properties. Moreover in the case of elliptic curves over $\mathbb{C}$, the structure is even richer : the curves are (connex, compact) Lie groups and can be represented by quotients of $\mathbb{C}$ by a lattice (i.e tori) as we will see.
Reference : Silverman (the arithmetic of elliptic curves, Chap.VI)

2.1 Torus and elliptic curves

Let $\Lambda \subset \mathbb{C}$ be a lattice, that is Λ is a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis of $\mathbb{C}$. There exists two elements $\omega_i \in \mathbb{C}$ (linearly independent over $\mathbb{R}$) such that $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.
Let us consider the topological variety $X = \mathbb{C}/\Lambda$. X is called a *torus*. Indeed, topologically, X is a square where the 2 pairs of opposite borders have been identified. In particular X is of genus 1 (it is a 'donuts' with 1 hole). One shows that X is in fact an compact analytic variety. Moreover it is easy to describe the functions on it

Definition 2.1.1. *An* elliptic function *is a meromorphic function $f(z)$ on $\mathbb{C}$ which satisfies*

$$f(z+\omega) = f(z) \textit{ for all } \omega \in \Lambda, z \in C.$$

Elliptic functions with no poles are constant as the surface is compact. Can we construct non constant elliptic functions ?

Definition 2.1.2. *The* Weierstrass $\mathcal{P}$-function *is defined by the series*

$$\mathcal{P}(z,\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right).$$

The function $\mathcal{P}' = d\mathcal{P}(z,\Lambda)/dz$ is also an elliptic function. One can prove that all elliptic function is a polynomial in $\mathcal{P}$ and $\mathcal{P}'$.
Let us define also the *Eisenstein series* G_n of weight n by

$$G_n = \sum_{\omega \in \in \Lambda \setminus \{0\}} \omega^{-n}.$$

The fundamental result is

Theorem 2.1.1. *The elliptic functions $\mathcal{P}$ and $\mathcal{P}'$ satisfy the equation*

$$\mathcal{P}'^2 = 4\mathcal{P}^3 - 60G_4\mathcal{P} - 140G_6.$$

This is the affine equation for an elliptic curve E. The map

$$\begin{array}{llll} u: & \mathbb{C}/\Lambda & \rightarrow & E(\mathbb{C}) & \\ & [z] & \mapsto & (x = \mathcal{P}(z) : y = \mathcal{P}'(z) : 1) & z \notin \Lambda \\ & [z] & \mapsto & (0 : 1 : 0) & z \in \Lambda \end{array}$$

is a complex analytic isomorphism of Riemann surfaces and a group homomorphism (for the natural additive structure on $\mathbb{C}/\Lambda$.
Reciprocally if $E/\mathbb{C}$ is an elliptic curve, there exists a lattice Λ such that $\mathbb{C}/\Lambda$ is isomorphic to $E(\mathbb{C})$ (uniformization theorem).

Remark 3. Note that $u^*(dx/y) = d(\mathcal{P}(z))/\mathcal{P}'(z) = dz$.

A natural question is then the following : starting from $\mathbb{C}$ how can we compute a lattice Λ ?

Proposition 2.1.1. *Let $E/\mathbb{C}$ be an elliptic curve with Weierstrass coordinate functions x, y. Let α, β be paths on $E(\mathbb{C})$ giving a basis for $H_1(E, \mathbb{Z})$. Then if*

$$\omega_1 = \int_\alpha dx/y \text{ and } \omega_2 = \int_\beta dx/y$$

and if Λ is the lattice generated by the ω_i one has complex analytic isomorphism

$$F : E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda, \quad F(P) = \int_O^P dx/y \pmod{\Lambda}.$$

This map is inverse of u.

2.2 Isogeny

Let Λ_1, Λ_2 be lattices in $\mathbb{C}$. If $\alpha \in \mathbb{C}$ has the property that $\alpha\Lambda_1 \subset \Lambda_2$, then

$$\phi : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2, \ \phi(z) = \alpha z \pmod{\Lambda_2}$$

is clearly a holomorphic homomorphism. They are more or less the only ones and more important for us, they give all the isogenies on the associated elliptic curve.

Proposition 2.2.1. *The association*

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \to \{\textit{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \textit{ with } \phi(0) = 0\}$$

is a bijection.
The natural inclusion

$$\{\textit{isogenies } E_1 \to E_2\} \to \{\textit{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \textit{ with } \phi(0) = 0\}$$

is a bijection.

Remark 4. Knowing the isogeny f, one can easily get α by the relation $f^*(dx/y) = \alpha \cdot dx/y$. In particular $[m] \mapsto m$.

This theorem is very convenient to prove without troubles some results about isogenies that require much more work in a pure algebraic setting. Recall the following definition, valid for any field K.

Definition 2.2.1. *Let E/K be an elliptic curve and $m \geq 2$ be an integer. The isogeny $[m] : E \to E$ is of degree m^2 and we can look at the kernel of this map, which we denote $E[m]$ and which is called the m-*torsion subgroup *of E. It is a group (scheme) of order m^2.*

Over $\mathbb{C}$ (and by Lefschetz's principle, for any algebraically closed field of characteristic 0), one gets easily

Corollary 2.2.1. *As abstract group*

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Proof. Let Λ be a lattice such that $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda$. Then

$$E[m] \simeq (\mathbb{C}/\Lambda)[m] \simeq \frac{1}{m}\Lambda/\Lambda \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

□

Theorem 2.2.1. *Let $E/\mathbb{C}$ be an elliptic curve and ω_i generators for the lattice Λ associated to E. Then either*

1. *End$(E) = \mathbb{Z}$ or*

2. *$\mathbb{Q}(\omega_1/\omega_2)$ is a quadratic imaginary extension of $\mathbb{Q}$ and End(E) is an order in $\mathbb{Q}(\omega_2/\omega_1)$.*

Recall that an order R in a number field K is a subring of K which is finitely generated as a $\mathbb{Z}$-module and satisfies $R \otimes \mathbb{Q} = K$.

Proof. Let $\tau = \omega_2/\omega_1$. Since Λ is homothetic to $\mathbb{Z} + \tau\mathbb{Z}$ we may replace Λ by $\mathbb{Z} + \tau\mathbb{Z}$. Let

$$R = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\},$$

so $R \simeq \mathrm{End}(E)$. Then for any $\alpha \in R$ there exists integers a, b, c, d such that

$$\alpha = a + b\tau \text{ and } \alpha\tau = c + d\tau.$$

Eliminating τ yields

$$\alpha^2 - (a + d)\alpha + ad - bc = 0.$$

So R is integral over $\mathbb{Z}$.
If $R \neq \mathbb{Z}$ let choose $\alpha \in R \setminus \mathbb{Z}$. Then with the notations as above $b \neq 0$ so eliminating α gives a non trivial equation

$$b\tau^2 - (a - d)\tau - c = 0.$$

Therefore $\mathbb{Q}(\tau)$ is a quadratic imaginary extension of $\mathbb{Q}$. As $R \subset \mathbb{Q}(\tau)$ and R is integral over $\mathbb{Z}$ it follows that R is an order in $\mathbb{Q}(\tau)$. □

Remark 5. Elliptic curves over $\mathbb{C}$ (or in characteristic 0) which have a strictly bigger endomorphism group than $\mathbb{Z}$ are rare and are called *CM*-elliptic curves (CM for Complex Multiplication). They play a deep and important role in both theoretical and computational arithmetic as we will see in Sec. 3.2.2.

Chapter 3

Elliptic curves over finite fields

This is the main object of this course. Indeed if we consider the rational points of an elliptic curve over a finite field, they form a finite group which is used as cryptosystem for the Diffie-Helman protocol. An important thing about this group is to be able to compute its order quickly in order to check that it is a prime number (or almost a prime number). Methods to do this exist as we will see at the end of the week (Chap. 4) but they are based on heavy mathematical notions.
Note that these properties are not particular to elliptic curves but can be adapted to curves in general. However, we will restrict here to the genus 1 case.
In the following k is the finite field $\mathbb{F}_q$ with $q = p^m$ and K denotes any (perfect) field.

3.1 Zeta function of elliptic curves

In 1949, André Weil made a series of very general conjectures concerning the number of points on varieties defined over finite fields. We restrict here to the case of curves.
Let $k = \mathbb{F}_q$ and for all $n \geq 1$, let k_n be the extension of degree n of k. Let C/k be a (projective smooth) curve of genus g over k.

Definition 3.1.1. *The* Zeta function *of C over k is the power series*

$$Z(C/k;T) = \exp\left(\sum_{n=1}^{\infty} |C(k_n)| \frac{T^n}{n}\right).$$

Theorem 3.1.1 (Weil conjectures). *With the above notations, we have the following properties.*

1. *Rationality :*

$$Z(C/k;T) \in \mathbb{Q}(T).$$

2. *Functional equation :*

$$Z(C/k;1/(qT)) = (qT^2)^{1-g} Z(C/k;T).$$

3. *Riemann hypothesis :*
   there exists a polynomial $f \in \mathbb{Z}[T]$ of degree $2g$ such that

$$f(T) = \prod_{i=1}^{2g}(1 - T\alpha_i)$$

   with $|\alpha_i| = \sqrt{q}$ for all i and such that

$$Z(C/k;T) = \frac{f(T)}{(1-T)(1-qT)}.$$

Corollary 3.1.1. *We have $|C(\mathbb{F}_{q^n})| = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n$.*

Proof. We have

$$\begin{aligned} \log(Z(C/k;T) = \sum |C(k_n)|T^n/n &= \log(f(T)) - \log(1-T) - log(1-qT) \\ &= \sum \log(1 - \alpha_i T) + \sum T^n/n + \sum q^n T^n/n \\ &= \sum_n \left(-\sum_i (\alpha_i^n) + 1 + q^n \right) T^n/n \end{aligned}$$

□

If we particularize to the case of elliptic curves ($g = 1$).

Theorem 3.1.2. *Let k be a field with q elements and E/k be an elliptic curve. Then there is an $a \in \mathbb{Z}$ (called* the trace *of E/k) such that*

$$Z(E/k;T) = \frac{1 - aT + qT}{(1-T)(1-qT)}$$

Further $Z(E:k;1/qT) = Z(E/k;T)$ and

$$1 - aT + qT^2 = (1-\alpha T)(1-\beta T) \textit{ with } |\alpha| = |\beta| = \sqrt{q}.$$

Corollary 3.1.2. *With the notations above, there exists a polynomial (called the* Frobenius polynomial *of E/k)*

$$\chi := T^2 - aT + q = (T-\alpha)(T-\beta)$$

such that $|E(k)| = \chi(1)$ and for every extension k_n of k of degree n, $|E(k_n)| = (1 - \alpha^n)(1-\beta^n)$.
Moreover (Hasse-Weil bound)

$$||E(k)| - q - 1| \leq 2\sqrt{q}.$$

Example 6. *Consider the elliptic curve :* $E/\mathbb{F}_7 : y^2 = x^3 + 2$*. It has* 9 *rational points, namely* $(0:1:0), (0:3:1), (0:4:1), (3:1:1), (3:6:1), (5:1:1), (5:6:1), (6:1:1), (6:6:1)$*. So we must have*

$$Z(E/\mathbb{F}_7; T) = \frac{7T^2 + T + 1}{(1-T)(1-7T)}.$$

In particular the number of points of $E/\mathbb{F}_{49}$ *is* $1 + 49 - (1^2 - 2 \cdot 7) = 63$ *(which can be checked with a computer).*

These conjectures were solved by Weil (in the case of curves and abelian varieties). The general case was solved by Deligne in 1973.
The first case $g = 0$ can be done by hand : indeed $|\mathbb{P}^1(k_n)| = q^n + 1$ so

$$Z(\mathbb{P}^1/k; T) = \exp(-\log(1-T) - \log(1-qT)) = \frac{1}{(1-T)(1-qT)}.$$

Now a genus 0 curve C/k is always k-isomorphic to a non degenerate plane conic. Chevalley's theorem shows then that this conic has always a rational point so in fact C is also k-isomorphic to $\mathbb{P}^1$.
The next case, $g = 1$, is the case of elliptic curves.

3.1.1 Reviews on elliptic curves

Tate module

We have seen in Chap.2 that for an elliptic curve over $\mathbb{C}$ the structure of the m-torsion is very easy to carry out. In characteristic $p > 0$, the uniformization theorem is not true anymore and nasty things happen when $[m]$ is not separable.

Proposition 3.1.1. *If* m *is prime to the characteristic then*

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},$$

and if Char$(K) = p > 0$ *then either*

$$E[p^e] \simeq \{0\} \text{ or}$$

$$E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$$

for all $e \geq 1$*.*

One assumes now that m is prime to the characteristic. The group $E[m]$ comes equipped with more structure. Namely, each element of the Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$. We thus obtain a representation

$$\mathrm{Gal}(\overline{K}/K) \rightarrow \mathrm{Aut}(E[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z}).$$

This representation is not completely satisfactory because it is generally easier to deal with representations whose matrices have coefficients in a ring of characteristic 0. What we will do is to fit them together thanks to the projective limit we introduced in Chap. 1 :

Definition 3.1.2. *Let E be an elliptic curve and $l \in \mathbb{Z}$ a prime. The (l-adic) Tate module of E is the group*

$$T_l(E) = \varprojlim_{n} E[l^n],$$

the inverse limit being taken with respect to the natural maps

$$[l] : E[l^{n+1}] \to E[l^n].$$

Since each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a $\mathbb{Z}_l$-module.

Proposition 3.1.2. *As a $\mathbb{Z}_l$-module $T_l(E) \simeq \mathbb{Z}_l \times \mathbb{Z}_l$.*

Now the action of $\mathrm{Gal}(\overline{K}/K)$ on each $E[l^n]$ commutes with the multiplication by $[l]$ maps used to form the inverse limit, so $\mathrm{Gal}(\overline{K}/K)$ also acts on $T_l(E)$.
The Tate module is also a useful tool for studying isogenies. If

$$\phi : E_1 \to E_2$$

is an isogeny then it induces a map

$$\phi_l : T_l(E_1) \to T_l(E_2).$$

We thus obtain a homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_l(E_1), T_l(E_2)).$$

It is not hard to show that the above homomorphism is injective : indeed if $\phi : E_1 \to E_2$ is a non-zero isogeny of degree d then its kernel has at most d^2 points. If it is 0 on $T_l(E_1)$ it is 0 on $E[l^n]$ for an n such that $l^n > d$ and so the kernel should contain $|E[l^n]| = l^{2n} > d^2$ points.

Weil pairing

We want to add structure on the Tate module. This is achieved by the Weil pairing. We will not recall the construction but it is a map

$$\overline{e}_m : E[m] \times E[m] \to \mu_m$$

satisfying the following properties :

Proposition 3.1.3 ([Sil92, III.8.1])**.** *The Weil pairing is :*

1. *bilinear : $\overline{e}_m(S_1+S_2, T) = \overline{e}_m(S_1, T)\overline{e}_m(S_2, T)$ and $\overline{e}_m(S, T_1+T_2) = \overline{e}_m(S, T_1)\overline{e}_m(S, T_2)$.*

2. *alternating : $\overline{e}_m(S, T) = \overline{e}_m(T, S)^{-1}$.*

3. *non-degenerate : if $\overline{e}_m(S, T) = 1$ for all $S \in E[m]$, then $T = 0$.*

4. *Galois-invariant : for all $\sigma \in Gal(\overline{K}/K)$,*
$$\overline{e}_m(S,T)^\sigma = \overline{e}_m(S^\sigma, T^\sigma).$$

5. *compatible : if $S \in E[mm']$ and $T \in E[m]$ then*
$$\overline{e}_{mm'}(S,T) = \overline{e}_m([m']S,T).$$

6. *adjoint : let $S \in E_1[m], T \in E_2[m]$ and $\phi : E_1 \to E_2$ be an isogeny. Then*
$$\overline{e}_m(S,\hat{\phi}(T)) = \overline{e}_m(\phi(S),T).$$

Corollary 3.1.3. *If $E[m] \subset E(K)$ then $\mu_m \subset K^*$.*

Proof. The image of $\overline{e}_m(S,T)$ as S,T range over $E[m]$ is a subgroup of μ_m, say equal to μ_d. It follows that for all $S,T \in E[m]$,
$$1 = \overline{e}_m(S,T)^d = \overline{e}_m([d]S,T).$$
The non-degeneracy of $\overline{e}_m$ implies that $[d]S = O$, ans since S is arbitrary, we must have $d = m$. Finally if $E[m] \subset E(K)$ then from the Galois invariance of the $\overline{e}_m$ pairing we see that $\overline{e}_m(S,T) \in K^*$ for all S,T. Therefore $\mu_m \subset K^*$. □

Let l be a prime different from the characteristic of K. We would like to fit together the pairings
$$\overline{e}_{l^n} : E[l^n] \times E[l^n] \to \mu_{l^n}$$
for all n to give an l-adic Weil pairing on the Tate module
$$e_l : T_l(E) \times T_l(E) \to T_l(\mu)$$
where
$$T_l(\mu) = \varprojlim_{n} \mu_{l^n} \simeq \mathbb{Z}_l.$$

We need only to check the compatibility
$$\overline{e}_{l^{n+1}}(S,T)^l = \overline{e}_{l^n}([l]S,[l]T)$$
which follows from Prop.3.1.3 (1) and (5).

Proposition 3.1.4. *There exists a bilinear, alternating, non-degenerate, Galois invariant pairing*
$$e_l : T_l(E) \times T_l(E) \to T_l(\mu)$$
such that if $\phi : E_1 \to E_2$ is an isogeny, ϕ and $\hat{\phi}$ are adjoints for the pairing.

3.1.2 Weil conjectures : the proof for $g = 1$

For the proof we will need the following lemma.

Lemma 3.1.1. *Let $\psi \in End(E)$. Then*

$$\det(\psi_l) = \deg(\psi) \textit{ and } tr(\psi_l) = 1 + \deg(\psi) - \deg(1 - \psi).$$

Proof. Let v_1, v_2 be a $\mathbb{Z}_l$-basis for $T_l(E)$ and write the matrix of ψ_l for this basis as

$$\psi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We compute

$$\begin{aligned} e_l(v_1, v_2)^{\deg(\psi)} &= e_l([\deg(\psi)]v_1, v_2) \\ &= e_l(\hat{\psi}\psi v_1, v_2) \\ &= e_l(\psi v_1, \psi v_2) \\ &= e_l(av_1 + cv_2, bv_1 + dv_2) \\ &= e_l(v_1, v_2)^{ad-bc} \\ &= e_l(v_1, v_2)^{\det(\psi_l)} \end{aligned}$$

Since e_l is non-degenerate, we conclude that $\deg(\psi) = \det(\psi_l)$. The second part is classical. □

Proof. Let $\pi : E \to E$ be the q-th power of Frobenius endomorphism. Since $1 - \pi$ is separable (because the map $(1 - \pi)^*$ is the identity on the regular differential and so is not 0), we have

$$|E(k)| = \deg(1 - \pi).$$

Similarly for every $n \geq 1$ and for every extension k_n of degree n, $|E(k_n)| = \deg(1 - \pi^n)$. From the previous lemma, the characteristic polynomial of π_l has coefficients in $\mathbb{Z}$, so we can factor it over $\mathbb{C}$:

$$\det(T - \pi_l) = T^2 - \mathrm{tr}(\pi_l)T + \det(\pi_l) = (T - \alpha)(T - \beta).$$

Further, since for every rational number m/n,

$$\det((m/n) - \pi_l) = \det(m - n\pi_l)/n^2 = \deg(m - n\pi)/n^2 \geq 0,$$

it follows that the quadratic polynomial $\det(T - \pi_l)$ has complex conjugate roots. Thus $|\alpha| = |\beta|$ and

$$\alpha\beta = \det(\pi_l) = \deg(\pi) = q,$$

we conclude that $|\alpha| = |\beta| = \sqrt{q}$.
Finally we note that the characteristic polynomial of π_l^n is given by $(T - \alpha^n)(T - \beta^n)$,

so

$$\begin{aligned}\log Z(E/k;T) &= \sum_{n=1}^{\infty}(|E(k_n)|T^n/n)\\ &= \sum_{n=1}^{\infty}(1-\alpha^n-\beta^n+q^n)T^n/n\\ &= -\log(1-T)+\log(1-\alpha T)+\log(1-\beta T)-\log(1-qT)\end{aligned}$$

which concludes the proof. □

Remark 6. If we let $T = q^{-s}$ then we have

$$\zeta_{E/k}(s) := Z(E/k, q^{-s})$$

and the functional equation reads

$$\zeta_{E/k}(1-s) = \zeta_{E/k}(s),$$

which is an analog for elliptic curve of the Riemman Zeta function for $\mathbb{Q}$. Further if $\zeta_{E/k}(s) = 0$ then $|q^s| = \sqrt{q}$, so $\Re(s) = 1/2$.

Remark 7. The general case follows more or less the same pattern. The main difference is that the elliptic curve is its own Jacobian. Another is that the real analogue of an elliptic curve is not only an abelian variety but an abelian variety plus a polarization.

3.2 Ordinary and supersingular elliptic curves

3.2.1 Characterization

Theorem 3.2.1. *Let E/k be an elliptic curve. Let $Fr : E \to E^{(p)}$ be the Frobenius morphism. The following are equivalent :*

1. *$E[p^r] = 0$ for one (all) $r \geq 1$.*
2. *$\hat{Fr}$ is purely inseparable.*
3. *The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.*
4. *$End(E)$ is an order in a quaternion algebra.*
5. *$\chi_E(T) = T^2 + aT + q$ with $p|a$.*

In this case the curve E is said supersingular *(or of* Hasse-Witt invariant 0*). Otherwise E is said* ordinary *(or of Hasse-Witt invariant 1). In the later case one has $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$ and $End(E)$ is an order in an imaginary quadratic field.*

Remark 8. We know that $E_1 \sim E_2 \iff |E_1(k)| = |E_2(k)|$. So the Hasse-Witt invariant is invariant under isogeny.

We want to give an easy way to see when a curve is or not ordinary.

Theorem 3.2.2 ([Sil92, V.4.1]). *Let $E : y^2 = f(x)$ be defined over the finite field $k = \mathbb{F}_q$ of characteristic $p > 2$.*

1. *E is supersingular iff the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.*
2. *Let $m = (p-1)/2$ and define the polynomial*
$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i.$$
Let $f(x) = x(x-1)(x-\lambda)$. E is supersingular iff λ is a root of H_p.
3. *The polynomial $H_p(\lambda)$ has distinct roots in $\overline{k}$.*

Proof. We are going to prove the first point.
Let $x \in k$. Then the number of points in $E(k)$ with abscissas x is $0, 1$ or 2 and is equal to $f(x)^{(q-1)/2} + 1$ (seen as an integer). So we have the formula

$$|E(k)| = 1 + q + \sum_{x \in k} f(x)^{(q-1)/2},$$

which gives modulo p (or seen in k)

$$|E(k)| = 1 + \sum_{x \in k} f(x)^{(q-1)/2}.$$

We have now easily that

$$\sum_{x \in k} x^i = \begin{cases} -1 \text{ if } q-1|i \\ 0 \text{ otherwise.} \end{cases}$$

Since f has degree 3, if we multiply out $f(x)^{(q-1)/2}$ and sum over $x \in k$, the only non-zero term comes from x^{q-1}. Hence if we let

$$A_q = \text{coefficient of } x^{q-1} \text{ in } f(x)^{(q-1)/2}$$

then

$$|E(k)| = 1 + A_q = 1 - \operatorname{tr}(\pi)$$

where $\pi : E \to E$ is the Frobenius endomorphism. Now $A_q = 0 \iff \operatorname{tr}(\pi) \equiv 0 \pmod{p}$. But $\hat{\pi} = [\operatorname{tr}(\pi)] - \pi$, so

$$A_q = 0 \iff \hat{\pi} \text{ is inseparable} \iff E \text{ is supersingular.}$$

It remains to show that $A_q = 0$ iff $A_p = 0$. Writing

$$f(x)^{(p^{r+1}-1)/2} = f(x)^{(p^r-1)/2}(f(x)^{(p-1)/2})^{p^r}$$

and equating coefficients (remember f is a cubic) yields

$$A_{p^{r+1}} = A_{p^r} A_p^{p^r}$$

and we have the desired result by induction on r. □

Remark 9. Note that (3) shows that there is roughly $(p-1)/12$ classes of supersingular elliptic curves up to $\overline{\mathbb{F}_p}$-isomorphism.

Supersingular elliptic curves seem to be convenient for cryptography. Indeed it is very easy to compute their number of points : if E is a supersingular elliptic curve, its j-invariant is in $\mathbb{F}_{p^2}$. Let E' be a curve defined over $\mathbb{F}_{p^2}$ with this invariant. E' is supersingular, so if a is the trace of the Frobenius over $\mathbb{F}_{p^2}$ $p|a$ and moreover $|a| \leq 2p$. There is then only 5 possibilities for a and it is easy to decide which one is the good one. Now E'/k and E/k are twists so one can easily compute the order knowing a.
Unfortunately these curves have been proved weak for the discrete logarithm and so people work rather with ordinary curves. There is no easy way to decide the trace for an ordinary elliptic curve as it can range over almost the complete interval $[-2\sqrt{q}, 2\sqrt{q}]$. However people have developed fast algorithms to compute this number. In small characteristics, the fastest algorithms are based on p-adic computations via the so-called *canonical lift* of the curve.

3.2.2 Lift, canonical lift

Let E be an elliptic curve over $k = \mathbb{F}_q$. Let $\mathbb{Z}_q = W(\mathbb{F}_q)$ be the ring constructed in Chap.1 and $\mathbb{Q}_q$ its field of fractions. Let also σ be the Frobenius substitution. As E is defined by an equation with coefficients in k, we can lift the non-zero coefficients of this equation over $\mathbb{Z}_q$ and then obtain the equation of an elliptic curve $\mathcal{E}$ over $\mathbb{Q}_q$. The curve $\mathcal{E}$ is called *a lift* of E.
As we have seen in the proof of the Weil conjectures, the Frobenius endomorphism π is strongly connected to the number of points of the curve and we would like to find on $\mathcal{E}$ an isogeny that lifts π. We restrict to the case of ordinary curves. In this case, we know that $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}(\pi)$ so we actually ask that our curve $\mathcal{E}$ has a quadratic field for its endomorphism ring. This situation is quite rare in characteristic 0 as we have seen in Chap. 2 and we cannot expect this to happen for an arbitrary lift. On this other hand, such a lift always exists :

Theorem 3.2.3 ([Mes72, V, Th.3.3, Cor. 3.4])**.** *Let E/k be an ordinary elliptic curve. There exists an unique –up to isomorphism– elliptic curve $E^{\uparrow}$ over $\mathbb{Z}_q$ such that $E^{\uparrow} \otimes k \simeq E$ and*

$$End_{\mathbb{Q}_q}(E^{\uparrow}) \simeq End_k(E).$$

We call $E^{\uparrow}$ the canonical lift *of E.*

If $f \in \mathrm{End}_k(E)$, we denote $f^{\uparrow} \in \mathrm{End}_{\mathbb{Q}_q}(E^{\uparrow})$ its canonical lift.

Remark 10. This theorem was proved in the case of elliptic curves by Deuring [Deu41] then generalized by Lubin, Serre and Tate [LST64].

Corollary 3.2.1 ([Mes72, Appendix, Cor 1.2])**.** *$E^{\uparrow}$ is the canonical lift of E iff there exists $Fr^{\uparrow} : E^{\uparrow} \to {}^{\sigma}(A^{\uparrow})$ lifting Fr.*

Remark 11. It is not always possible to lift a supersingular elliptic curve with its ring of endomorphism as this one may be an order in a quaternion algebra (Caution : it may also be $\mathbb{Z}$ if all the endomorphisms are not rational).

As an isomorphism class of elliptic curve is given by its j-invariant, we can characterized this curve by an unique element $J \in \mathbb{Z}_q$. Another useful characterization is the following.

Theorem 3.2.4 ([VPV01, §. 2])**.** *Let $x \in \mathbb{Z}_q$ such that $x \equiv J \pmod{2^i}$ with $i \in \mathbb{N}$. Then there exists a unique $y \in \mathbb{Z}_q$ such that $y \equiv x^2 \pmod 2$ and $\Phi_2(x, y) = 0$. Moreover $y \equiv j((\tilde{E}^{(2)})^{\uparrow}) = J^{\sigma} \pmod{2^{i+1}}$.*

Recall that Φ_p is the modular polynomial of order p.

Remark 12. It is an important result in CM theory that J is in fact an algebraic integer and the curve $E^{\uparrow}$ exists actually over $\overline{Q}$. The degree of the extension $\mathbb{Q}(J)/\mathbb{Q}$ is given by the class number of $\mathrm{End}(E) \otimes \mathbb{Q}$. As the discriminant of this extension is heuristically in $\sqrt{q}$, the degree of this extension may quickly becomes too big for explicit computations.

As we explained earlier, the general philosophy is to obtain curves in characteristic 0 in order to apply analytic results. Indeed, one has then the outstanding result linking the geometry and the arithmetic of the Frobenius.

Proposition 3.2.1 (Satoh)**.** *Let E be an elliptic curve over k with trace of Frobenius a. Let ω be a regular differential on $E^{\uparrow}$ and let $c \in \mathbb{Q}_q$ the element defined by $(\pi^{\uparrow})^*(\omega) = c{\cdot}\omega$. Then $a = c + q/c$.*

Chapter 4

Fast computations of Zeta functions

4.1 Introduction

Cryptography is playing a more and more important role in our society : smart-card, INTERNET payment, online banking. . . . All these applications needs to protect information. There exists two main strategies. The first one, historically, is called *symmetric key cryptography.* Roughly speaking, it is based on combinatoric tricks and only the owners of the secret key can cipher and decipher. In 1976, Diffie and Hellman introduced the new concept of *public key cryptography.* This protocol solves in particular the important problem (for INTERNET) of a creation of secret key over a non-secure channel (which was not possible with symmetric cryptography). Here is the principle :

1. Goal : Alice and Bob wants to share a secret key (to cipher and decipher after with a traditional symmetric protocol for instance).
2. let G be a group that we can assume to be isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Let $g \in G$ be a generator.
3. Alice chooses $a \in \mathbb{Z}$ and sends g^a to Bob.
4. Bob chooses $b \in \mathbb{Z}$ and sends g^b to Alice.
5. Secret shared : g^{ab}.

One sees that the difficulty to break the code is based on the difficulty to compute $a = \log_g(g^a)$ (in fact to compute g^{ab} knowing g^a, g^b but these two problems are believed equivalent). This type of problem is called *discrete logarithm problem.* Does it exist groups for which this problem is difficult (whereas the computation of g^a remains easy of course) ? A problem is said difficult if one cannot solve it in a reasonable time with a good computer. More specifically that means that the number of operations would be greater than 2^{60}.

For a general group G, there is always an attack in $\sqrt{|G|}$, so $|G|$ must have at least 120 bits.
The first concrete example was given in 1978 and is known as RSA (Rivest, Shamir, Adleman). It is based on the group $\mathbb{F}_q^*$. In order to obtain a difficult problem, one has to take q with at least 1024 bits because there exist subexponential attacks.

Remark 13. The complexity of the attack –or of construction, computations– (exponential, subexponential, polynomial) is measured in term of $\log_2 |G|$.

One is of course interested in groups for which the order is small (and then the protocol fast) in other words groups with no subexponential attacks. People have tried with ideal class groups of number fields, but here again there exists a subexponential attack.
Cryptographers are now very interested in the group of rational points of a Jacobian over a finite fields, at least when the dimension g is less than 4. Indeed with this restriction no subexponential attack is known in general. We have to consider curves over $k = \mathbb{F}_{2^N}$ with $N \approx 120/g$ (because the order of the group of rational points on the Jacobian is approximately $|k|^g$).
Note however that nobody has proved that a better attack does not exist and this is of course a big fear of all banks and governments as cryptosystems based on Jacobian (at least elliptic curves) are wide used nowadays.

Remark 14. One has proved that a secure group (where no sub-exponential attack occurs) exists. But nobody is able to construct it.

One important practical aspect is the choice of the curve : indeed we need that the order of the group of rational points of its Jacobian is almost a prime (i.e contains a large prime factor). Otherwise it is easy to break the code by working on each factor and using the Chinese Remainder Theorem. One cannot compute this number by brute force (counting points on g extensions). Indeed this method is clearly of exponential complexity and cannot be used with $\mathbb{F}_q$ of cryptographic sizes. Fortunately, two ways exist to obtain this curve :

- One takes random curves of genus g over $\mathbb{F}_q$ and one has a fast way to compute the number of points. These algorithms belongs to four categories :

    1. l-adics methods : for $g = 1$ (Schoof); works in large characteristics.
    2. Cohomological methods : the most used today is Kedlaya's algorithm. It works well when the characteristic is small.
    3. p-adic methods based on the canonical lift : they were introduced by Satoh for elliptic curves in 2000.
    4. Deformation theory : this (for the moment theoretical) method was introduced by Lauder in 2002.

- On construct a curve over a number field whose Jacobian endomorphism ring has a good structure (CM). Then one reduces the curve modulo suitable large prime for which it is easy to compute the order from the structure. These CM methods have been developed for $g = 1, 2$ (and certain $g = 3$) curves.

On can sum up the state of arts in point counting (i.e methods of the first strategy) in the following charts.

⊠ Polynomial time algorithm, possible to deal with crypto sizes
⧅ Polynomial time algorithm, impossible to reach crypto sizes
⬚ Theoretical polynomial time algorithm, not implemented

l-adic methods

	$g=1$	$g=2$	$g=3$		
			hyper	C_{34}	general
$p=2$	⊠	⬚	⬚	⬚	⬚
p small	⊠	⧅ ↑?	⬚	⬚	⬚
p large	⊠	⧅	⬚	⬚	⬚

Names: Schoof, Elkies, Atkin, Couveignes, Lercier, Morain, Müller, Dewaghe, Vercauteren, Pila, Cantor, Kampkötter, Huang, Ierardi, Adleman, Harley, Gaudry.

Cohomological methods

	$g=1$	$g=2$	$g=3$		
			hyper	C_{34}	general
$p=2$	⊠	⊠	⊠	⊠	⬚
p small	⊠	⊠	⊠	⊠	⬚
p large					

Names: Kedlaya, Gürel, Gaudry, Vercauteren.

p-adic methods (canonical lift)

	$g=1$	$g=2$	$g=3$		
			hyper	C_{34}	general
$p=2$	⊠	⊠	⊠	⊠	⊠
p small	⬚	↓?	↓?	↓?	↓?
p large					

Names: Satoh, Skjernaa, Fouquet, Harley, G., Vercauteren, Mestre, Taguchi, Ritzenthaler, Carls.

Deformation

	$g=1$	$g=2$	$g=3$		
			hyper	C_{34}	general
$p=2$	░	░	░	░	░
p small	░	░	░	░	░
p large					

Names: Lauder.

All together

	$g=1$	$g=2$	$g=3$		
			hyper	super	general
$p=2$	▩	▩	▩	▩	▩
p small	▩	▩	▩	▩	░
p large	▩	▧	░	░	░

One sees that even if this domain is only 30 years old, a lot of techniques have been developed. We will focus on a 2-adic method which is a elegant variant of Satoh's algorithm : the AGM-method for genus 1 curve. This method developed in 2000 by Mestre and implemented by Lercier-Lubicz is nowadays the fastest one in characteristic 2 : a record over $\mathbb{F}_{2^{100002}}$ was obtained. Note that this method was then generalized to hyperelliptic curves [Mes02] and to non hyperelliptic curves of genus 3 [Rit03]. This method is based on formulas coming from the analytic theory and theta functions. We will begin by recalling these classical aspects.

4.2 The complex theory

4.2.1 Computation of periods

It was historically the first case handled : Lagrange [Lag67, t.II,p.253-312] and Gauss [Gau70, t.III,p.352-353,261-403] introduced the *Arithmetic geometric mean* to compute elliptic integrals.

Theorem 4.2.1. *Let a, b be two reals such that $0 < b < a$. We have*

$$\int_0^{\pi/2} \frac{dt}{\sqrt{a^2\cos^2 t + b^2\sin^2 t}} = \frac{\pi}{2\mathrm{M}(a,b)},$$

where $\mathrm{M}(a,b)$ *(*arithmetic geometric mean *of a and b) is the common limit of*

$$\begin{cases} a_0 = a & a_{n+1} = \frac{a_n+b_n}{2} \\ b_0 = b & b_{n+1} = \sqrt{a_n b_n} \end{cases}$$

Since

$$|a_{n+1} - b_{n+1}| = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2} = \frac{(a_n - b_n)^2}{2(\sqrt{a_n} + \sqrt{b_n})^2} \leq \frac{(a_n - b_n)^2}{8b_1}$$

these two sequences are adjacent and the convergence is quadratic. This method is then better than traditional numeric integrations.

The proof is based on a tricky change of variables which transforms the parameters a, b in the integral into a_1, b_1. Taking the limit one has then the theorem.

To understand this change of variables we are going to algebraize our problem. Put $x = e_3 + (e_2 - e_3)\sin^2 t$ with

$$\begin{cases} a_0^2 & = e_1 - e_3 \\ b_0^2 & = e_1 - e_2 \\ 0 & = e_1 + e_2 + e_3 \end{cases}$$

We can reformulate the theorem as :

Theorem 4.2.2.

$$\int_{e_3}^{e_2} \frac{dx}{\sqrt{P(x)}} = \frac{\pi}{2\mathrm{M}(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})}$$

with $P(x) = 4(x - e_1)(x - e_2)(x - e_3)$, $e_3 < e_2 < e_1$.

One recognizes the integral of a regular differential form on the elliptic curve $E : y^2 = P(x)$. More precisely, if one denotes by $\mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ (ω_1 real ω_2 purely imaginary) the complex torus $E(\mathbb{C})$, one has the isomorphism

$$\begin{array}{llll} u: & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) & \\ & [z] & \mapsto & (x = \mathcal{P}(z) : y = \mathcal{P}'(z) : 1) & z \notin \Lambda \\ & [z] & \mapsto & (0 : 1 : 0) & z \in \Lambda \end{array}$$

and (see figure 4.1)

$$\omega_1 = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} dz = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} \frac{d\mathcal{P}(z)}{\mathcal{P}'(z)} = 2\int_{e_3}^{e_2} \frac{dx}{y} = 2\int_{e_3}^{e_2} \frac{dt}{\sqrt{P(t)}}$$

The problem is now the computation of a period of a differential of the 1st kind on a Riemann surface.

Let $\tau = \omega_2/\omega_1$. In the theory of abelian varieties over $\mathbb{C}$, it is classical to introduce *theta functions*. They can be seen as holomorphic sections of sheaves but we want to give here a more straightforward definition for elliptic curves (see [Ros86] for the general theory).

Definition 4.2.1. *Let* $\tau \in \mathbb{H}$, $\epsilon, \epsilon' \in \{0,1\}$. *One defines the* theta function with characteristic (ϵ, ϵ') *by*

$$\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](z,\tau) = \sum_{n\in\mathbb{Z}} \exp(i\pi(n+\epsilon/2)^2\tau + 2i\pi(n+\epsilon/2)(z+\epsilon'/2))$$

It is an analytic function of the variable z. If $z = 0$, one denotes also $\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](0,\tau) = \vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)$. When $(\epsilon,\epsilon') \neq (1,1)$, $\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau) \neq 0$ and is called a *theta constant.*
These values have the following properties.

Proposition 4.2.1. *1. Limit :*

$$\lim_{\text{Im }\tau\to+\infty} \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau) = \lim_{\text{Im }\tau\to+\infty} \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau) = 1.$$

2. Thomae's formula :

$$\begin{cases} \omega_1\sqrt{e_1-e_3} = & \pi \cdot \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 \\ \omega_1\sqrt{e_1-e_2} = & \pi \cdot \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2 \end{cases}$$

3. Duplication formula :

$$\begin{cases} \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](2\tau)^2 = & \frac{\vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 + \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2}{2} \\ \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](2\tau)^2 = & \sqrt{\vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2} \end{cases}$$

Remark 15. As the theta constants are positive reals (because τ is purely imaginary), the sign of the square roots is always the positive one. When it is no more the case, the choice is a bit more subtle (see [Cox84]).

4.2.2 Proofs

We want to give two proofs of Th.4.2.2. The first one is straightforward. As the duplication formula is exactly the AGM recursion, we can write

$$\begin{cases} a_0 = \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 & a_n = \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](2^n\tau)^2 \\ b_0 = \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2 & b_n = \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](2^n\tau)^2 \end{cases}$$

By the limit property, one has

$$\mathrm{M}\left(\vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2, \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2\right) = 1.$$

The AGM recursion being homogeneous, one obtains the theorem thanks to Thomae formula :

$$M(a_0,b_0) = M(\frac{\omega_1\sqrt{e_1-e_3}}{\pi}, \frac{\omega_1\sqrt{e_1-e_2}}{\pi}) = \frac{\omega_1}{\pi}M(\sqrt{e_1-e_3}, \sqrt{e_1-e_2}) = 1.$$

The second proof will reveal the true geometry behind the result. Consider again the elliptic curve $E : y^2 = P(x)$. This curve is isomorphic to the curve $E_\tau = E_{a_0,b_0}$ defined by

$$\begin{aligned} E_\tau : y_0^2 &= x_0(x_0-(e_1-e_3))(x_0-(e_1-e_2)) && (4.1)\\ &= x_0\left(x_0-\frac{\pi^2}{\omega_1^2}\cdot\vartheta\begin{bmatrix}0\\0\end{bmatrix}(\tau)^4\right)\left(x_0-\frac{\pi^2}{\omega_1^2}\cdot\vartheta\begin{bmatrix}0\\1\end{bmatrix}(\tau)^4\right) && (4.2)\\ &= x_0(x_0-a_0^2)(x_0-b_0^2), && (4.3)\end{aligned}$$

One can then construct the following diagram.

$$\begin{tikzcd} \mathbb{C}/\mathbb{Z}\omega_1+\mathbb{Z}2\omega_2 \arrow[r, "G:z\mapsto z"] \arrow[d, "u_{2\tau}"', "\simeq"] & \mathbb{C}/\mathbb{Z}\omega_1+\mathbb{Z}\omega_2 \arrow[d, "u_\tau", "\simeq"'] \\ E_{2\tau}(\mathbb{C}) \arrow[r, shift left, "g"] & E_\tau(\mathbb{C}) \arrow[l, shift left, "f"] \end{tikzcd}$$

where $E_{2\tau} = E_{a_1,b_1}$ and f, g are 2-isogenies given by (see for instance [BM89]):

$$\begin{aligned} g : (x_1, y_1) &\mapsto \left(x_1\left(1+\frac{a_1^2-b_1^2}{x_1-a_1^2}\right), \frac{y_1(x_1^2-2x_1a_1^2+a_1^2b_1^2)}{(x_1-a_1^2)^2}\right) && (4.4)\\ f : (x_0, y_0) &\mapsto \left(\frac{y_0^2}{4x_0^2}+\left(\frac{a+b}{2}\right)^2, -\frac{y_0(a^2b^2-x_0^2)}{8x_0^2}\right) && (4.5)\end{aligned}$$

In particular the kernel of f is $< (0,0) >$.
We can now finish the proof : since $G^*(dz) = dz$ we have $g^*(dx_0/y_0) = dx_1/y_1$. Now

$$\omega_1 = 2\int_{e_1}^{\infty}\frac{dx}{y} = 2\int_0^{-\infty}\frac{-i}{2}\frac{dx_0}{y_0} = \int_0^{-\infty}-i\frac{dx_1}{y_1} = \ldots = \int_0^{-\infty}-i\frac{dx_n}{y_n}.$$

By iteration :

$$E_\tau \to E_{2\tau} \to \ldots \to E_{2^n\tau} \to \ldots \to E_\infty : y^2 = x(x-M(a_0,b_0)^2)^2.$$

But E_∞ is a genus 0 curve which means that there exists a parametrization which gives

$$\omega_1 = \int_0^{-\infty} -i\frac{dx}{\sqrt{x(x-M(a_0,b_0)^2)^2}} = \left[-2\frac{\mathrm{Arctan}\left(\frac{\sqrt{\mathrm{x}}}{\mathrm{M}(\mathrm{a}_0,\mathrm{b}_0)}\right)}{\mathrm{M}(\mathrm{a}_0,\mathrm{b}_0)}\right]_0^{-\infty} = \frac{\pi}{\mathrm{M}(a_0,b_0)}.$$

4.3 2-adic method

Let $q = 2^N, k = \mathbb{F}_q$ and $\mathbb{Q}_q$ be the unramified extension of degree N of $\mathbb{Q}_2$, $\mathbb{Z}_q$ its ring of integers, ν its valuation and σ the Frobenius substitution (i.e the unique Galois automorphism of $\mathbb{Q}_q$ such that $\sigma x \equiv x^2 \pmod 2$, see Chap. 1). The aim of this section is to give an algorithm which we can present as

$$\tilde{E}/\mathbb{F}_q \text{ ordinary e.c.} \overset{\text{lift}}{\longrightarrow} E/\mathbb{Z}_q \underset{\text{cv}}{\overset{\text{AGM}}{\longrightarrow}} \mathcal{E}/\mathbb{Z}_q \text{ canonical lift} \overset{\text{AGM}}{\longrightarrow} \text{Frobenius trace}.$$

Let us detail now the different parts.

4.3.1 Lift

In characteristic 0 we want to use the form $E_{a,b} : y^2 = x(x-a^2)(x-b^2)$. Of course we cannot use this model in characteristic 2. We propose two different solutions to solve this problem.

First solution

Lemma 4.3.1 ([Ver03]). *Let $a, b \in 1 + 4\mathbb{Z}_q$ with $b/a \in 1 + 8\mathbb{Z}_q$. Then*

$$\begin{array}{rcl} E_{a,b} & \overset{\sim}{\to} & E : y^2 + xy = x^3 + rx^2 + sx + t \\ (x,y) & \to & \left(\dfrac{x-ab}{4}, \dfrac{y-x+ab}{8}\right) \end{array}$$

for some $r, s, t \in \mathbb{Z}_q$ such that

$$\tilde{E} : y^2 + xy = x^3 + \left(\frac{a-b}{8}\right).$$

We then consider $\tilde{E}$ as $y^2 + xy = x^3 + c$, let $r \in \mathbb{Z}_q$ such that $r \equiv \sqrt{c} \pmod 2$ and take

$$\begin{cases} a_0 = 1 + 4r \\ b_0 = 1 - 4r \end{cases}$$

The advantage of this model is that there is a rational 4 torsion point $(c^{1/4}, c^{1/2})$. This point enables to find the sign of $\pm\mathrm{tr}(\pi)$ that occurs at the end of the algorithm because $\mathrm{tr}(\pi) \equiv 1 \pmod 4$. The drawback is that this model does not represent all cases. Moreover it gives no clue about a possible generalization to hyperelliptic cases.

Second solution

Starting with a general ordinary elliptic curve $\tilde{E} : y^2 + xy = x^3 + a_2x^2 + a_4x + a_6$, we can always get rid of the a_6 coefficient. We lift then $\tilde{E}$ naturally and make the transformation

$$Y^2 = (y + \frac{x}{2})^2 = x(x^2 + \frac{4a_2+1}{4}x + 1).$$

We can factorize the left member over $\mathbb{Q}_q$ in $x(x-\alpha)(x-\beta)$ with $\nu(\alpha) = -2$ and $\nu(\beta) = 2$. Let $X = x - \alpha$ we have then a model

$$Y^2 = X(X+\alpha)(X+\alpha-\beta).$$

As $\nu(\frac{\alpha-\beta}{\alpha} - 1) = \nu(\frac{\alpha}{\beta}) = 4$, we can take

$$\begin{cases} a_0 = 1 \\ b_0 = \sqrt{\frac{\alpha-\beta}{\alpha}} \in \mathbb{Z}_q \end{cases}$$

and consider the curve

$$Y^2 = X(X-1)(X-b_0^2).$$

Note that this curve is not isomorphic over $\mathbb{Q}_q$ to the original one but is a quadratic twist. However, as we will obtain the trace of the Frobenius only up to a sign, this is not an issue.

Remark 16. We have to get rid of the a_6 coefficient, otherwise we might have to factorize the left member in a ramified extension of $\mathbb{Q}_2$ (it is the case for instance with $y^2 + xy = x^3 + 1$).

4.3.2 Convergence

Let start with a model $E_0 = E_{a_0,b_0}$ over $\mathbb{Z}_q$ lifting $\tilde{E}$. Let denote $E_i = E_{a_i,b_i}$ the elliptic curves obtained by AGM iterations. Let denote also $\tilde{E}^{\uparrow}$ the canonical lift of $\tilde{E}$ which is completely characterized by its j-invariant J. We want to prove that the AGM sequence converges to the Galois cycle associated to the canonical lift. We give two proofs.

First proof

We are going to use Th. 3.2.4. If E and E' are two elliptic curves that are p-isogenous then $\Phi_p(j(E), j(E')) = 0$.
We have of course $\Phi_2(E_i, E_{i+1}) = 0$ by the complex computations of 4.2. An easy computation shows also the following congruence.

Lemma 4.3.2. *$j(E_{i+1}) \equiv j(E_i)^2 \pmod 2$.*

By iteration of the AGM we then obtain

$$j(E_n) \equiv j((\tilde{E}^{(2^n)})^{\uparrow}) \pmod{2^{n+1}}.$$

Second proof

The second proof uses a result of Carls. It avoids explicit invariants and is then useful for generalization.

Theorem 4.3.1 ([Car02, Th.3])**.** *Let A be an abelian variety over $\mathbb{F}_q$, $\mathcal{A}/\mathbb{Z}_q$ be an ordinary abelian scheme with special fiber A. One defines a sequence*

$$\mathcal{A} = \mathcal{A}_0 \to \mathcal{A}_1 \to \dots$$

where the kernel of the isogenies are the components $\mathcal{A}_i[2]^{loc}$ (i.e the 2-torsion points in the kernel of the reduction). We have

$$\lim_{n\to\infty} \mathcal{A}_{nN} = A^{\uparrow}$$

i.e for all n, $(\mathcal{A}_{Nn})/\mathbb{Z}_q^{(Nn+1)} \simeq (A^{\uparrow}_{Nn})/\mathbb{Z}_q^{(Nn+1)}$ where $\mathbb{Z}_q^{(i)} = \mathbb{Z}_q/2^i\mathbb{Z}_q \simeq \mathbb{Z}/2^i\mathbb{Z}$. In particular the convergence is linear.

Using 4.2 we see that if we still denote by $f : E_i \to E_{i+1}$ the 2-isogeny induced by the AGM-iteration, then $\ker f =< (0,0) >$ and $(0,0)$ reduces on $\tilde{O}$ (because the kernel corresponds to the point $(\alpha, 0)$ in the reduction, which is of negative valuation). We can then apply the previous theorem.

4.3.3 Trace of the Frobenius

To compute the Frobenius polynomial we only need the trace of the Frobenius on $V_l(\tilde{E})$ for $l \neq p$. But this trace can be already read on regular differentials as we have seen in Prop. 3.2.1. With the notations of the proposition, we have $\chi(X) = X^2 - (c + q/c) \cdot X + q$. We need also the following elementary lemma.

Lemma 4.3.3. *Let $E_{a,b} : y^2 = x(x-a^2)(x-b^2)$ et $E_{a',b'} : y'^2 = x'(x'-a'^2)(x'-b'^2)$ with $\frac{a^2}{b^2} \equiv \frac{a'^2}{b'^2} \equiv 1 \pmod 2$. If E and E' are isomorphic then $x = u^2 x'$ and $y = u^3 y'$ with $u^2 = \frac{a^2+b^2}{a'^2+b'^2}$. Furthermore $\frac{a^2}{b^2} = \frac{a'^2}{b'^2}$ or $\frac{a^2}{b^2} = \frac{b'^2}{a'^2}$.*

Proof. The two curves being isomorphic, there exists $(u, r) \in (\mathbb{Z}_q^* \times Q_q)$ such that $x = u^2 x' + r$ and $y = u^3 y'$. It is enough to show that $r = 0$. With the usual notations of [Sil92, chap.III,1.2], one has

$$\begin{aligned} -4u^2(a'^2 + b'^2) = b'_2 &= b_2 + 12r = -4(a^2+b^2) + 12r \\ 0 = u^6 b'_6 &= 4r(r-a^2)(r-b^2) \end{aligned}$$

The first equality shows that $r \equiv 0 \pmod 2$ and the second that $r = 0$ since neither a^2 or b^2 are congruent to 0. The first equality gives also the value of u^2. □

Let $\mathcal{E}_{a_0,b_0}$ be the canonical lift. We can then construct the following diagram

$$\begin{tikzcd}
\mathcal{E}_{a_0^\sigma,b_0^\sigma} \arrow[d, "\phi"'] \arrow[dr, bend left, "\mathrm{Ve}^\uparrow"] & \\
\mathcal{E}_{a_1,b_1} \arrow[r, shift left, "g"] \arrow[d] & \mathcal{E}_{a_0,b_0} \arrow[l, shift left, "f"] \arrow[ul, "\mathrm{Fr}^\uparrow"'] \arrow[d] \\
\tilde{E}^{(2)} & \tilde{E} \arrow[l, "\mathrm{Fr}"]
\end{tikzcd}$$

where ϕ is an isomorphism because the two maps have the same kernel $< (0,0) >$. Let $\omega = dx/y$, we then get

$$(\mathrm{Ve}^\uparrow)^*(\omega) = (g \circ \phi)^*(\omega) = \phi^*(\omega) = \frac{\omega}{u}$$

with $u^2 = \frac{a_1^2 + b_1^2}{(a_0^2)^\sigma + (b_0^2)^\sigma}$ because g acts by identity as we can see on the explicit formula or with the complex interpretation of g as $z \mapsto z$.

We want to simplify a bit the expression of u^2. we have

$$u^2 = \left(\frac{a_1}{a_0^\sigma}\right)^2 \frac{1 + \left(\frac{b_1}{a_1}\right)^2}{1 + \left(\frac{b_0^\sigma}{a_0^\sigma}\right)^2}.$$

Let $\lambda_1 = b_1/a_1$ and $\lambda_0 = b_0/a_0$. By Lem.4.3.3, $\lambda_1^2 = (\lambda_0^2)^\sigma$ or $\lambda_1^2 = \frac{1}{(\lambda_0^2)^\sigma}$. Let us prove that it is the first case which occurs. We can write $\lambda_i = 1 + 8c_i$ with $c_i \in \mathbb{Z}_q$ so the first case occurs iff

$$c_1 \equiv c_0^\sigma \pmod 4.$$

By the AGM iteration, we have

$$1 + 8c_1 = \frac{1 + 4c_0}{\sqrt{1 + 8c_0}} \Rightarrow c_1 \equiv c_0^2 \pmod 4.$$

As after the first iteration c_0 is itself a square α_0^2 modulo 4, we have

$$c_0^\sigma \equiv (\alpha_0^2)^\sigma \equiv \alpha_0^4 \equiv c_0^2 \pmod 4.$$

So we get $c_1 \equiv c_0^\sigma \pmod 4$ which proves

$$u = \pm \frac{a_1}{a_0^\sigma}.$$

The trace of the Frobenius endomorphism is the same as the trace of the Verschiebung. One has

$$\mathrm{tr}(\pi) = \mathrm{tr}(V) = \mathrm{tr}(\mathrm{Ve}^{\sigma^{N-1}} \circ \cdots \circ \mathrm{Ve}) = \pm \left(\frac{1}{N(u)} + 2^N N(u) \right)$$

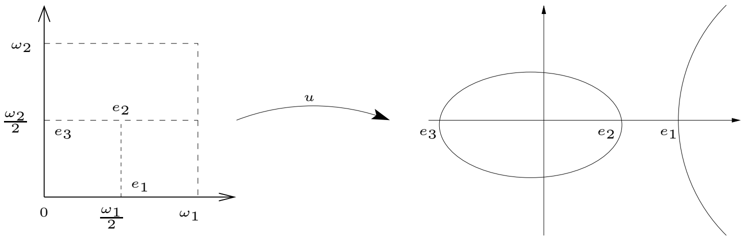
with $N(u) = \mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}(a_1/a_0)$.

4.3.4 Complexity and Conclusion

Since by the Hasse-Weil theorem $\mathrm{tr}(\pi) \leq 2\sqrt{q}$ it is enough to compute the previous norm with $\lceil N/2 \rceil + 2$ bits. Several implementations of this method have been achieved : see [Ver03] for a nice overview and running times. The best complexity obtained is quasi-quadratic in time and quadratic in space.

One of the attractive aspect of the AGM method is the simplicity of the formulas involved. Another one is the natural generalizations one can obtain for hyperelliptic curves and non hyperelliptic curves of genus 3. On the contrary it seems that generalization to other characteristics would be less efficient and less elegant due to the complexity of the new AGM formulas.

Figure 4.1: The map u



Bibliography

[BM89] J.-B. Bost & J.-F. Mestre, Moyenne Arithmético-géométrique et Périodes des courbes de genre 1 et 2, Gaz. Math., S.M.F. **38** (1989) , 36-64.

[Car02] R. Carls, Approximation of canonical lifts, in preparation, (2002) available on `http://www.math.leidenuniv.nl/~carls/`.

[Cox84] D. Cox, The arithmetic-geometric mean of Gauss, Enseign. Math. **30** (1984), 275-330.

[Deu41] M. Deuring, Die Typen der Multiplikatoringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ Hamburg **14** (1941), 197-272.

[Gau70] C.F. Gauss, *Werke*, Vol. **12**, Göttingen, (1870-1927).

[Lag67] J.L. Lagrange, *Oeuvres*, Vol. **14**, Gauthiers-Villars, Paris (1867-1892).

[LST64] J. Lubin & J.-P. Serre & J. Tate, *Elliptic Curves and formal groups*, notes disponibles sur `http://ma.utexas.edu/users/voloch/lst.html`, (1964).

[Mes72] W. Messing, *The crystals Associated to Barsotti-Tate Groups : with Applications to Abelian Schemes*, Lect. Notes in Math., **264**, Berin-Heidelberg-New-York, Springer (1972).

[Mes02] J.-F. Mestre, Algorithmes pour compter des points en petite caractéristique en genre 1 et 2, available at `www.maths.univ-rennes1.fr/crypto/2001-02/mestre.ps` (2002).

[Sil92] J.H Silverman, *The Arithmetic of Elliptic Curves*, **106**, Springer, (1992).

[Rit03] C. Ritzenthaler : *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*, PhD thesis, Université Paris 7 - Denis Diderot, June 2003 available on `http://www.math.jussieu.fr/~ritzenth`.

[Ros86] M. Rosen, Abelian varieties over $\mathbb{C}$, in *Arithmetic Geometry*, Cornell & Silverman, Springer-Verlag, (1986).

[VPV01] F. Vercauteren, B. Preneel & J. Vandewalle , A memory efficient version of Satoh's algorithm, Adv. in Cryptology, Eurocrypt (2001) (Innsbruck, Austria, Mai

2001), Lect. Notes in Comput. Sci. **2045**, 1-13, ed. Pfitzmann, Berlin, Heidelberg: Springer-Verlag (2001).

[Ver03] F. Vercauteren *computing Zeta functions of curves over finite fields*, PhD thesis, Katholicke Universiteit Leuven, 2003.