1
Introduction

1.1 Alice and Bob

Suppose Alice wants to send a secret message s to Bob. If Eve intercepts the message, then she can read it and it will not be secret anymore. Thus, Alice and Bob should agree on a two ways protocol that will turn the secret message s into a public message p. This is called encryption. Reversing the operations will allow Bob to recover s from p. For example, Alice would shift the letters of the message in alphabetical order and Bob will simply do the same thing in the reverse order (Caesar cipher). The Advanced Encryption Standard (AES) protocol does the same thing in a more complicated way, but this is not the subject of this course.

If Eve knows the two ways protocol, then she can derive s from p as easily as Bob does and the message will not stay secret anymore. The solution is to use a protocol with a parameter, the *key*. Then, Alice and Bob can make their protocol public as long as they keep secret their key k. For example, the protocol could be "replacing each letter in the message with the letter that is k places further down the alphabet". Again, AES does the same thing in a more complicated way.

Still, Alice and Bob should agree on their common key k. If Alice chooses the key, it can be intercepted by Eve when Alice sends it to Bob. This problem can be fixed as was shown by Diffie, Hellman and Merkle: Alice and Bob can make public the choice of a finite order element g in a group G. Alice chooses a private key $a \in \mathbf{N}$ from which she derives her public key $A := g^a$. Bob does the same thing and obtains also a public key $B := g^b$. Then Alice chooses as common key $k := B^a$. She does not have to send it to Bob because he can derive the same key in the same way. More precisely, Bob knows his private key b, he knows the public key A of Alice and we have $k = A^b$.

At this point, I should mention that if Eve chooses a private key a' and publishes a fake public key $A' := g^{a'}$ for Alice, then Bob might use it to code his message. If Eve intercepts the message, she can then use her private key a' to read it. Thus, there is still a weakness in this system but we do not want to discuss this here. So we will assume that Alice and Bob can trust each other's public key.

Thus, Eve knows the group G and the generator g and she also knows the public keys A and B. But, in order to discover k, she needs to solve the *Diffie–Hellman problem*: recovering g^{ab} from g^a and g^b. Of course, it is sufficient to be able to derive x from $X := g^x$. This last question is called the *discrete logarithm* problem. Even if they cannot prove it, specialists think that, in fact, the Diffie–Hellman problem is as hard as the discrete logarithm problem. And, in practice, it takes way more time, given g, to recover x from X than to derive X from x. We will try to explain this below.

1.2 Complexity

How long does it take to make a computation and how much room do we need to store the data? This is called a *complexity* question. For example, what is the complexity of (discrete) exponentiation? If $|G| = n$, it takes at most $2\log_2 n$ elementary operations to get $X = g^x$ from x: this is derived from the 2-adic expansion of x. One says that the complexity of exponentiation is linear (in $\log_2 n$). On the other hand, since exhaustive search of x from X might need n elementary operations, and there is no clear alternative, it seems that the complexity of the discrete logarithm is exponential (in $\log_2 n$). Actually, there are many other methods that compute discrete logarithms which are more efficient than exhaustive search but their complexity is still exponential in general.

However, note that in the case $G := (\mathbf{Z}/n\mathbf{Z})^*$, there exists a sub-exponential algorithm, the so called *Index-Calculus method*. Roughly speaking, one first solves the discrete logarithm problem simultaneously for the small primes. In order to do that, one looks at primary decompositions of random powers g^r until we get enough linear relations. Then, it is sufficient to consider the primary decomposition of $g^s X$ for random s until only small prime factors appear. Although not polynomial, this is better than exponential. If G is no longer equal to $(\mathbf{Z}/n\mathbf{Z})^*$ but is the set of rational points of a more general algebraic group, there is no real equivalent to the Index-Calculus method, and there is no known sub-exponential method to compute discrete logarithms in G.

Actually, the best-known technique is the Pohlig–Hellman algorithm which is exponential but still quite fast when the order of the group has only small

prime factors. In order to discard such a group, it is necessary to compute its order. Thus, the crucial point becomes the determination of the number of rational points of an algebraic variety over a finite field (see [22] for a recent survey of the problem). As far as we stick to elliptic curves, the l-adic methods work perfectly. But already in the hyperelliptic case, the p-adic methods are way more effective for small primes p.

1.3 Weil conjectures

Concerning Weil conjectures, the case of diagonal hypersurfaces is completely worked out in André Weil's original article [85]. Also, if you want to go a little further into the p-adic point of view, you are encouraged to look at Paul Monsky's course [70]. For the l-adic approach, Milne's book [68] is the reference.

We want to compute the number of points of an algebraic variety X over a finite field $\mathbf{F}_q$ with $q := p^f$ elements, p a prime. For example, we are given

$$F_1, \dots, F_d \in \mathbf{Z}[T_1, \dots, T_n]$$

and we want to compute the number of solutions of

$$\begin{cases} F_1(a_1, \dots, a_n) = 0 \mod p \\ \vdots \\ F_d(a_1, \dots, a_n) = 0 \mod p \end{cases}$$

More generally, given an algebraic variety X over $\mathbf{F}_q$, we want to compute

$$N_r(X) := |X(\mathbf{F}_{q^r})|$$

for all r. The main result is the conjecture made by André Weil in 1949 ([85]) and proved in several steps, starting with *rationality* by Bernard Dwork in 1960 ([39]), using p-adic methods:

If X is an algebraic variety of dimension d over $\mathbf{F}_q$ there exists finitely many algebraic integers α_i and β_i such that for all r, we have

$$N_r(X) = \sum \beta_i^r - \alpha_i^r,$$

and ending with *purity* (also called *Riemann hypothesis*) by Pierre Deligne in 1974 ([36]), using l-adic methods (recall that a *Weil number of weight m* is an algebraic integer whose archimedean absolute values are of the form $q^{\frac{m}{2}}$):

The algebraic integers α_i and β_i are Weil numbers with weight in $[0, 2d]$, with many other results in between and, in particular, the *functional equation* by Grothendieck in 1965 ([49]):

If X is proper and smooth, the application $\gamma \mapsto q^d/\gamma$ induces a permutation of the α_i's and a permutation of the β_i's.

As an example, we can consider for $p \neq 2$, an affine hyperelliptic curve of equation $y^2 = F(x)$ with F separable of degree $2g+1$. Then,

$$N_r(X) = q^r - \sum_{i=1}^{2g} \alpha_i^r$$

where each α_i is a Weil number of weight 1 and $\alpha_i \alpha_{i+g} = q$.

1.4 Zeta functions

Weil conjectures are easier to deal with if we form the generating function

$$\zeta(X,t) := \exp(\sum_{r=1}^{\infty} N_r(X)\frac{t^r}{r}) = \prod_{x \in |X|} \frac{1}{1-t^{\deg x}},$$

which is called the *zeta function* of X. The above results are then better reformulated in the following way:

Rationality: the function $\zeta(X,t)$ is rational with coefficients in $\mathbf{Q}$.

Purity: its zeros and poles are Weil numbers with weights $\in [-2d, 0]$.

Functional equation: if X is proper and smooth, then

$$\zeta(X, \frac{1}{q^d t}) = \pm q^{dE/2} t^E \zeta(X,t)$$

with $E \in \mathbf{Z}$ (Euler characteristic).

Actually, this can be rewritten in the more precise form (recall that a *Weil Polynomial* is a monic polynomial with integer coefficients whose roots are all Weil numbers):

We have

$$\zeta(X,t) = \prod_{i=0}^{2d} P_i(t)^{(-1)^{i+1}}$$

where P_i is a Weil Polynomial with non-negative weights between $2(i-d)$ and i. Moreover, if X is proper and smooth, P_i is pure of weight i and

$$P_{2d-i}(t) = \pm C_i t^{B_i} P_i(\frac{1}{q^d t})$$

with $C_i \in \mathbf{Z}$ and $B_i \in \mathbf{N}$ (Betti numbers).

As an example, one can show that if X is an abelian variety, then $|X(\mathbf{F}_q)| = P_1(1)$. Actually, if X is a projective non singular curve and J is the jacobian of

X, we also have $|J(\mathbf{F}_q)| = P_1(1)$. In other words, if we can compute P_1 for a curve, then we can tell the number of rational points of its jacobian which is an algebraic group.

1.5 Arithmetic cohomology

If an algebraic variety X over $\mathbf{F}_q$ lifts to a compact manifold V over $\mathbf{C}$, then the numbers B_i that appear in the functional equation are the *Betti number* of V (and E is its *Euler characteristic*). In other words, B_i is the rank of $H^i(V, \mathbf{Z})$. Actually, as André Weil already knew, the whole story can be told using a suitable cohomology theory with a Fixed Point Lefschetz trace formula for Frobenius.

Actually, if l is any prime (even $l = p$), there exists a finite extension K of $\mathbf{Q}_l$ such that the following holds (an operator ϕ on a finite-dimensional vector space will be called a *Weil operator* if its characteristic polynomial is a Weil polynomial):

We have (rationality)

$$\zeta(X, t) = \prod_{i=0}^{2d} \det(1 - t\varphi_i)^{(-1)^{i+1}}$$

where φ_i is a Weil operator (purity) with non-negative weights inside $[2(i - d), i]$ on a finite-dimensional K-vector space $H^i_c(X)$. Moreover, If X is proper and smooth (in which case we write $H^i := H^i_c$), then φ_i is pure of weight i and there is a perfect pairing (functional equation or Poincaré duality*)*

$$H^i(X) \times H^{2d-i}(X) \to K(-d)$$

compatible with the operators (with multiplication by q^d on the right).

In the case $l \neq p$, l-adic cohomology with compact support has all these properties. As already mentioned, a good introduction to l-adic cohomology is Milne's book [68].

We will now stick to the case $l = p$. There is a good theory for proper and smooth algebraic varieties that was developed by Pierre Berthelot in the late 1960s. It is called *crystalline cohomology* (see for example [20]). For smooth affine varieties, *Monsky–Washnitzer cohomology* was also available at that time (see for example [83], but also [72], [69] and [71]) although finite dimensionality was not known. *Rigid cohomology* is a theory that generalizes both crystalline and Monsky–Washnitzer theories and was developed by Pierre Berthelot in the 1980s (see [11]).

1.6 Bloch–Ogus cohomology

Rigid cohomology is a Bloch–Ogus cohomology ([74]). We explain below what it means. We fix a complete ultrametric field K of characteristic zero with valuation ring $\mathcal{V}$ and residue field k. Although it does not seem necessary, according to a yet unpublished result of Vladimir Berkovich based on an idea of Offer Gabber, we prefer assuming that the valuation is discrete.

There exists a contravariant functor

$$(Y \hookrightarrow X) \mapsto H^i_{Y,\mathrm{rig}}(X)$$

from the category of closed embeddings of algebraic varieties over k (with cartesian diagrams as morphisms) to the category of finite dimensional vector spaces over K. This cohomology only depends on a neighborhood of Y in X. If we are given a sequence of closed immersions

$$Z \hookrightarrow Y \hookrightarrow X,$$

there is a functorial long exact sequence

$$\cdots \to H^i_{Z,\mathrm{rig}}(X) \to H^i_{Y,\mathrm{rig}}(X) \to H^i_{Y\setminus Z,\mathrm{rig}}(X \setminus Z) \to \cdots$$

There is another "functor"

$$X \mapsto H^i_{\mathrm{rig},c}(X)$$

from the category of algebraic varieties over k to the category of finite-dimensional vector spaces over K. Actually, this is only covariant with respect to open immersions and contravariant with respect to proper maps (and these two functorialities are compatible). If we are given a closed immersion $Y \hookrightarrow X$, there is a functorial long exact sequence

$$\cdots \to H^i_{\mathrm{rig},c}(X \setminus Y) \to H^i_{\mathrm{rig},c}(X) \to H^i_{\mathrm{rig},c}(Y) \to \cdots$$

For $Y \hookrightarrow X$ a closed immersion, there is a cup-product

$$H^i_{\mathrm{rig},c}(Y) \times H^j_{Y,\mathrm{rig}}(X) \to H^{i+j}_{\mathrm{rig},c}(X)$$

which is functorial with respect to proper morphisms. For X irreducible of dimension d, there exists a trace map

$$\mathrm{tr} : H^{2d}_{\mathrm{rig},c}(X) \to K$$

which is functorial with respect to open immersions. In the case X is smooth, the *Poincaré pairing*

$$H^i_{\mathrm{rig},c}(Y) \times H^{2d-i}_{Y,\mathrm{rig}}(X) \to H^{2d}_{\mathrm{rig},c}(X) \to K$$

is perfect and compatible with the long exact sequences (*Poincaré duality*).

We can say a little more about rigid cohomology. First of all, by definition, we have

$$H^i_{\mathrm{rig}}(X) := H^i_{X,\mathrm{rig}}(X)$$

and there is a canonical morphism

$$H^i_{\mathrm{rig},c}(X) \to H^i_{\mathrm{rig}}(X)$$

which is an isomorphism for X proper. Note that $H^i_{\mathrm{rig},c}(X)$ and $H^i_{\mathrm{rig}}(X)$ are both 0 unless $0 \leq i \leq 2d$. Also, there are *Künneth formulas*

$$H^i_{\mathrm{rig},c}(X) \otimes H^i_{\mathrm{rig},c}(X') \simeq H^i_{\mathrm{rig},c}(X \times X')$$

in general and

$$H^i_{\mathrm{rig}}(X) \otimes H^i_{\mathrm{rig}}(X') \simeq H^i_{\mathrm{rig}}(X \times X')$$

when X and X' are both smooth. And finally, rigid cohomology and rigid cohomology with compact support both commute to isometric extensions of K.

1.7 Frobenius on rigid cohomology

Before introducing the Frobenius map, I want to recall that the *Chow group* of an algebraic variety X is defined as the quotient $A(X)$ of the cycle group $Z(X)$ modulo rational equivalence. More precisely, a *cycle* T on X is a closed integral subvariety and the *cycle group* is the free abelian group on cycles. A cycle is *rationally equivalent to* 0 if it is of the form $f_*(D)$ where D is a principal Cartier divisor and

$$f : X' \to X$$

a proper map. In [74], Denis Pétrequin shows that in the situation of the previous paragraph, there is a canonical pairing

$$\begin{aligned} A_i(X) \times H^{2i}_{\mathrm{rig},c}(X) &\longrightarrow K \\ (T, \omega) &\longmapsto \textstyle\int_T \omega := tr(\omega_{|T}). \end{aligned}$$

From this, one can derive a *Lefschetz trace formula*. More precisely, if $\varphi : X \to X$ is an endomorphism with a finite number of fixed points N (counting multiplicities), then

$$N = \sum_{i=0}^{2d} (-1)^{i+1} \mathrm{tr} \varphi^*_{|H^i_{\mathrm{rig},c}(X)}.$$

When k is a field of characteristic p, then the Frobenius map $x \mapsto x^q$ with $q = p^f$ acts by functoriality on $H^i_{Y,\mathrm{rig}}(X)$ and $H^i_{\mathrm{rig},c}(X)$. Actually, we need to choose a continuous lifting σ of Frobenius to K and we get semi-linear maps. Anyway, it can be shown that the above Bloch–Ogus formalism is compatible with the Frobenius actions up to a twist by q^d in the trace map.

When $k = \mathbf{F}_q$, we can derive from the Lefschetz trace formula the following equalities:

$$\zeta(X,t) = \prod_{i=0}^{2d} \det(1 - tF^*_{|H^i_{\mathrm{rig},c}(X)})^{(-1)^{i+1}}$$

and, for $Y \subset X$ smooth,

$$\zeta(Y,t) = \prod_{i=0}^{2d} \det(1 - tq^d(F^*)^{-1}_{|H^i_{Y,\mathrm{rig}}(X)})^{(-1)^{i+1}}$$

One can show (see for example [23]) that the Frobenius is a Weil operator on $H^i_{\mathrm{rig},c}(X)$ with positive weights between $2(i-d)$ and i. By duality again, we see that when X is smooth, Frobenius is also a Weil operator on $H^i_{Y,\mathrm{rig}}(X)$ with weights between i and $2i$ but less than $2d$.

1.8 Slopes of Frobenius

Up to this point, l-adic cohomology does as well as, and in general better than, rigid cohomology. However, the latter becomes essential when it comes to the computation of slopes. So, let us assume that the valuation is discrete and that σ fixes a uniformizer π. Then, Dieudonné–Manin theorem tells us that, up to a finite extension of k, any σ-linear operator has a basis $\{e_{ij}\}$ with

$$e_{i1} \mapsto e_{i2} \mapsto \cdots \mapsto e_{is} \mapsto \pi^r e_{i1}$$

in which case

$$\lambda := \frac{1}{[K : \mathbf{Q}_p]} \frac{r}{s}$$

is called a *slope*. It is shown in [23] that any slope λ of $H^i_{\mathrm{rig},c}(X)$ satisfies $0 \leq \lambda \leq d$ and $0 \leq i - \lambda \leq d$. By duality again, the same is true for $H^i_{Y,\mathrm{rig}}(X)$ when X is smooth.

The above p-adic cohomological formula for the Zeta function shows that the slopes of rigid cohomology of X determine the p-adic absolute values of

the algebraic integers α_i and β_i such that

$$|X(\mathbf{F}_q^r)| = \sum_i \alpha_i^r - \beta_i^r .$$

1.9 The coefficients question

In his marvellous article [85], Weil proves his conjecture for diagonal hypersurfaces $\sum x_i^r = 0$. The method consists in projecting to the diagonal hyperplane $\sum x_i = 0$. In other words, if $f : Y \to X$ is the projection $x \mapsto x^r$, we have

$$N_r(Y) = \sum_{x \in X(\mathbf{F}_{q^r})} N_r(Y_x)$$

with $Y_x := f^{-1}(x)$ and therefore, we are led to compute more complicated sums (than just counting points) on simpler algebraic varieties.

In order to generalize this, we must define in a functorial way, for each algebraic variety X, a category of coefficients E on X. Moreover, we need to associate to E, at each closed point $x \in X$, some $S(X, E, x)$. Then, we will define

$$S_r(X, E) = \sum_{x \in X(\mathbf{F}_{q^r})} S(X, E, x)$$

and

$$L(X, E, t) := \exp\Big(\sum_{r=1}^{\infty} S_r(X, E)\frac{t^r}{r}\Big).$$

Of course, the cohomology theory should take into account these coefficients and provide a cohomological formula for computing L-functions.

Ideally, one looks for a "constructible" theory of coefficients satisfying Grothendieck six operations formalism. The p-adic candidate is the theory of arithmetic $\mathcal{D}$-modules of Berthelot ([14], [18] and [19]) and its study is beyond the scope of this course. We will consider here the "lisse" p-adic theory and introduce the category or *overconvergent F-isocrystals*.

1.10 F-isocrystals

For an algebraic variety X over k, we will define the category

$$F\text{-isoc}^{\dagger}(X/K)$$

of overconvergent F-isocrystals over X/K. This is an abelian category with $\otimes$, internal Hom and rank. If $f : Y \to X$ is any morphism, there is an inverse image functor

$$f^* : F-\mathrm{isoc}^\dagger(X/K) \to F-\mathrm{isoc}^\dagger(Y/K).$$

If f is proper and smooth, there should be a direct image functor

$$f_* : F-\mathrm{isoc}^\dagger(Y/K) \to F-\mathrm{isoc}^\dagger(X/K).$$

This is the case when f is finite or if it has a "nice" lifting.

Let us concentrate for a while on the case of a closed point. First of all, $F-\mathrm{isoc}^\dagger(\mathrm{Spec}k/K)$ is identical to the category $F-\mathrm{isoc}(K)$ of strong finite dimensional *F-isocrystals* over K: an F-isocrystal over K is a vector space E with a σ-linear endomorphism φ. It is said to be *strong* when the Frobenius endomorphism is actually bijective. More generally, let k' be a finite extension of k. If K' is an unramified extension of K with residue field k' and σ' a frobenius on K' compatible with σ, then $F-\mathrm{isoc}^\dagger(\mathrm{Spec}k'/K)$ is equivalent to $F-\mathrm{isoc}(K')$.

Assume that $k = \mathbf{F}_q$ and let $d := [k' : k]$. If (E, ϕ) is an F-isocrystal on K', then ϕ^d is linear and one sets

$$S(k', E) := Tr\phi^d.$$

Now, if X is any algebraic variety over $\mathbf{F}_q$ and E is an overconvergent F-isocrystal over X/K, then for each closed point $x \in X$, the inverse image E_x of E on x is an overconvergent F-isocrystal on $k(x)$ and one sets

$$S(X, E, x) = S(k(x), E_x).$$

Using the formulas of Section 1.9, we can define $S_r(X, E)$ and $L(X, E, t)$. Note that, as before, if $K(x)$ denotes an unramified extension of K having $k(x)$ as residue field, we have

$$L(X, E, t) = \prod_{x \in |X|} \frac{1}{\det_{K(x)}(1 - t^{\deg x}\phi_x^{\deg x})}.$$

One can define the rigid cohomology of overconvergent F-isocrystals. These vector spaces come with a Frobenius automorphism and one can prove cohomological formulas

$$L(X, E, t) = \prod_{i=0}^{2d} \det(1 - tF^*_{|H^i_{\mathrm{rig},c}(X,E)})^{(-1)^{i+1}}$$