p-ADIC PROPERTIES OF EIGENVALUES OF FROBENIUS

EHUD DE SHALIT

This is a set of notes for two talks at Kazhdan's Basic Notions seminar in 2018. Nothing, except for the mistakes, is due to me.

Part 1. Motivation and Examples

1. The problem: p-adic valuations of Weil numbers

Let X be a d-dimensional smooth projective variety over $\mathbb{F}_q$. One is interested in the behavior of

$$N_n = \#X(\mathbb{F}_{q^n})$$

when n varies. The Zeta function of X

$$Z(X;T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n T^n}{n}\right) = \prod_{x\in|X|}(1-T^{\deg(x)})^{-1}$$

is a formal power series in T with coefficients from $\mathbb{Z}$, encoding the numbers N_n. For example, it is an easy exercise to find that

$$Z(\mathbb{P}^d;T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^dT)}.$$

As another example, consider the elliptic curve $C \subset \mathbb{P}^2$ given by the equation

$$C:\ y^2z = x^3 + bxz^2 + cz^3 \tag{1.1}$$

with $b, c \in \mathbb{F}_q$ (saying that this is an *elliptic curve* implies that the cubic equation is non-singular). Then E. Artin conjectured, and shortly after Hasse proved that

$$Z(C;T) = \frac{1-a(C)T+qT^2}{(1-T)(1-qT)}$$

with $a(C)$ an integer satisfying $|a(C)| \le 2\sqrt{q}$. If we write

$$1-a(C)T+qT^2 = (1-\alpha T)(1-\alpha' T)$$

then $N_n = 1 + q^n - \alpha^n - \alpha'^n$ and what Hasse showed was actually that $|\alpha'| = |\alpha| = \sqrt{q}$ so $|N_n - 1 - q^n| \le 2\sqrt{q^n}$. More generally, we have the famous Weil conjectures.

Theorem 1. *(i) (Dwork) $Z(X;T)$ is a rational function of T.*

(ii) (Grothendieck) For $0 \le m \le 2d$ there are polynomials $P_m(T) \in \mathbb{Z}[T]$, $P_m(T) = \prod_{i=1}^{b_m}(1-\alpha_{m,i}T)$ such that

$$Z(X;T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)\cdots P_{2d}(T)}.$$

The Zeta function satisfies the functional equation

$$Z(X;\frac{1}{q^dT}) = \pm q^{d\chi/2}T^\chi Z(X;T)$$

where $\chi = \sum_{m=0}^{2d}(-1)^m b_m$ *is the Euler characteristic.*

(iii) (Deligne, RH for X) For every automorphism σ *of* $\overline{\mathbb{Q}}$, $|\sigma(\alpha_{m,i})| = \sqrt{q^m}$.

Remark. (i) Since every Galois conjugate of $\alpha_{m,i}$ is an $\alpha_{m,j}$ it is enough to verify that $|\alpha_{m,i}| = \sqrt{q^m}$.

(ii) Given any $l \neq p$, Grothendieck showed that there are vector spaces

$$H_l^m(X) = H_{et}^m(X_{\overline{\mathbb{F}}_q}, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

over $\mathbb{Q}_l$, $\dim H_l^m(X) = b_m$, equipped with a linear transformation Fr_q, called (geometric) Frobenius, such that

$$P_m(T) = \det(I - T \cdot Fr_q^{-1}|H_l^m(X))$$

and the $\alpha_{m,i}$ are therefore the "reciprocal eigenvalues of Frobenius". Note that $P_m(T)$ is independent of l and has coefficients in $\mathbb{Z}$, although it is in general impossible to find a vector space $H^m(X)$ over $\mathbb{Q}$ with a Fr_q from which all the $H_l^m(X)$ are obtained by extension of scalars.

(iii) For curves, i.e. $d = 1$, the theorem is due to Weil, and $b_1 = 2g$ where g is the genus. The RH for curves has the consequence that (and in fact is equivalent to)

$$|N_n - 1 - q^n| \leq 2g\sqrt{q^n}.$$

In this case

$$H_l^1(X) = \mathrm{Hom}(\varprojlim J[l^\nu], \mathbb{Z}_l)$$

is the dual of the l-adic Tate module of J, the Jacobian of X. Recall that as an abelian group

$$J = \mathrm{Div}^0(X(\overline{\mathbb{F}}_q))/\{\text{principal divisors}\}$$

and $J[l^\nu]$ is the subgroup of elements killed by l^ν. The inverse limit is w.r.t. multiplication by l.

(iv) One puts $\zeta_X(s) = Z(X, q^{-s})$. Then the RH says that the zeroes of $P_m(q^{-s})$ lie on the line $Re(s) = m/2$. This explains the relation to the classical Riemann Hypothesis.

Definition. Let q be a power of a prime number p. Then a complex number α is called a *q-Weil number* if α is an algebraic integer such that for every Galois automorphism σ we have $|\sigma(\alpha)| = \sqrt{q}$.

The $\alpha = \alpha_{m,i}$ are algebraic integers (since they are roots of monic polynomials over $\mathbb{Z}$) so the RH implies that they are q^m-Weil numbers. Let E be the Galois closure of $\mathbb{Q}(\alpha)$. Then E is a number field and since $\alpha\overline{\alpha} = q$, the decomposition of the principal ideal (α) into a product of prime ideals of $\mathcal{O}_E$ involves only primes dividing p. Thus α has non-trivial valuations only at the places above p and ∞. Knowing all these absolute values determines α up to a root of unity, and in many cases, if there are no roots of unity other than ± 1 in E, up to a sign. The archimedean valuations of the $\alpha_{m,i}$ teach us about the asymptotics of N_n. It is natural therefore to pose the following questions.

Problem. (1) What is the meaning of the p-adic valuations of the $\alpha_{m,i}$ at the primes of E? A natural guess would be that just as the archimedean absolute values taught us about the archimedean size of N_n, the p-adic absolute values should tell us something about the p-adic size of N_n, namely about congruences for N_n or related numbers modulo powers of p.

(2) Is there a natural cohomology theory $H_p^m(X)$ over $\mathbb{Q}_p$, or over a finite extension of $\mathbb{Q}_p$ perhaps, with an action of a "Frobenius", by means of which we will be able to study the p-adic absolute values of the $\alpha_{m,i}$?

(3) We have at hand nice cohomology theories over $\mathbb{F}_q$, namely algebraic de-Rham cohomology $H^m_{dR}(X/\mathbb{F}_q)$ and the Hodge cohomology groups $H^{r,s}(X) = H^s(X, \Omega^r)$. Are there relations between them and the reduction modulo p of suitable lattices in $H^m_p(X)$?

2. Example: ordinary and supersingular elliptic curves

As a first example consider the elliptic curve (1.1). Then C is called ordinary if $p \nmid a(C)$ and supersingular if $p|a(C)$. Note that if $q = p \geq 5$ and C is supersingular then from $|a(C)| \leq 2\sqrt{p}$ we must have $a(C) = 0$. If C is ordinary then

$$T^2 - a(C)T + q = 0$$

has the two roots α, α' in $\mathbb{Z}_p$, one of which, say α', is a unit. Then $|\alpha|_p = |q|_p$. In the supersingular case both α and α' are non-units. It follows that in the ordinary case for n sufficiently divisible, $p|N_n$, but in the supersingular case always $N_n \equiv 1 \mod p$. Thus C is supersingular if and only if $C(\overline{\mathbb{F}}_q)[p] = \{0\}$.

However, the congruence $N_n \equiv 1 \mod p$ says more about the finite abelian group $C(\mathbb{F}_{q^n})$ in the supersingular case. In fact, since $E = \mathbb{Q}(\alpha)$ is $\mathbb{Q}$ or a quadratic imaginary field in which p ramifies, then $N_n \to 1$ p-adically as $n \to \infty$. Somehow, the lack of p-torsion forces the non-p torsion to approach 1 p-adically, just as $\#\mathbb{G}_m(\mathbb{F}_{q^n}) \to -1$ p-adically.

3. Example: Stickelberger's theorem on Gauss sums

We write $\zeta_m = \exp(2\pi i/m)$. Let $q = p^f$ and let $\mathfrak{p}$ be a prime ideal of $E = \mathbb{Q}(\zeta_{q-1})$ dividing p. Note that

$$p\mathcal{O}_E = \mathfrak{p}_1 \dots \mathfrak{p}_g$$

where $gf = \phi(q-1)$ and the residue field of each $\mathfrak{p}_i$ is isomorphic to $\mathbb{F}_q$. We take $\mathfrak{p} = \mathfrak{p}_1$ and identify $\mathcal{O}_E/\mathfrak{p} = \mathbb{F}_q$. Let

$$\omega : \mathbb{F}_q^\times \to \langle \zeta_{q-1} \rangle$$

be the $\mathfrak{p}$-Teichmüller character, defined by $\omega(a) \mod \mathfrak{p} = a$. For any $1 \leq k \leq q-2$ let the Gauss sum of ω^k be defined by

$$g(\omega^k) = -\sum_{a \in \mathbb{F}_q^\times} \omega^k(a) \zeta_p^{Tr_{\mathbb{F}_q/\mathbb{F}_p}(a)}.$$

Then $g(\omega^k) \in E(\zeta_p)$ and if $\sigma \in Gal(E(\zeta_p)/E)$ satisfies $\sigma(\zeta_p) = \zeta_p^d$ $(d \in \mathbb{F}_p^\times)$ then

$$\sigma(g(\omega^k)) = -\sum_{a \in \mathbb{F}_q^\times} \omega^k(a) \zeta_p^{Tr_{\mathbb{F}_q/\mathbb{F}_p}(da)} = \omega^{-k}(d) g(\omega_k). \tag{3.1}$$

It follows that if $mk \equiv 0 \mod (p-1)$ then $g(\omega^k)^m \in E$. In any case

$$p\mathcal{O}_{E(\zeta_p)} = \mathfrak{P}_1 \dots \mathfrak{P}_g$$

where $\mathfrak{P}_i$ is the unique prime above $\mathfrak{p}_i$, and we let $\mathfrak{P} = \mathfrak{P}_1$. If $\tau \in Gal(E(\zeta_p)/\mathbb{Q}(\zeta_p))$ maps ζ_{q-1} to ζ_{q-1}^e then

$$\tau(g(\omega^k)) = g(\omega^{ke}). \tag{3.2}$$

It is also known that

$$g(\omega^k)\overline{g(\omega^k)} = q. \tag{3.3}$$

It follows from (3.1), (3.2) and (3.3) that $g(\omega^k)$ is a q-Weil number. The theorem of Stickelberger gives its decomposition in $E(\zeta_p)$.

Theorem 2. *(Stickelberger, 1890) Let* $k = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$ *where the digits* $a_i \in \{0, 1, \ldots, p-1\}$. *Let* $s(k) = \sum_{i=0}^{f-1} a_i$. *Then*

$$v_{\mathfrak{P}}(g(\omega^{-k})) = s(k).$$

Remark. Note that $s(kp) = s(k)$ because k is taken modulo $q-1$.

Example. Assume $f = 1$, so that $q = p$. Then $s(k) = k$. Let $g = g(\omega^{-m})$ $(1 \leq m \leq p-2)$, so that

$$g = -\sum_{a=1}^{p-1} \overline{\omega^m(a)}\zeta^a.$$

Then

$$g\mathcal{O}_{E(\zeta_p)} = \prod_{e \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times} \tau_e^{-1}(\mathfrak{P})^{\{me\}}$$

where $1 \leq \{me\} \leq p-1$ and $\{me\} \equiv me \mod (p-1)$. Let us prove this special case (the general case of the theorem is not much more difficult).

Proof. Because of the relation (3.2) it is enough to prove that $v_{\mathfrak{P}}(g(\omega^{-m})) = m$. Let $\pi = \zeta_p - 1$ so that $v_{\mathfrak{P}}(\pi) = 1$ and recall that $v_{\mathfrak{P}}(p) = p-1$. We have

$$g(\omega^{-m}) \equiv -\sum_{a=1}^{p-1} a^{-m}(1+\pi)^a \mod p$$

and

$$(1+\pi)^a = \sum_{k=0}^{p-1} \binom{a}{k}\pi^k.$$

Now, if $0 \leq i < m$ we have $\sum_{a=1}^{p-1} a^{i-m} \equiv 0 \mod p$. This implies that $\sum_{a=1}^{p-1} a^{-m}\binom{a}{k} \equiv 0 \mod p$ if $k < m$. On the other hand, if $k = m$ we get a unit (precisely $-1/m!$ modulo p) so when we collect terms according to powers of π we see that the lowest term where the coefficient of π^k is not 0 mod p is when $k = m$. This proves the theorem in the case of the example. □

4. The Fermat curve

Consider the curve $C_d : X^d + Y^d = Z^d$ where $d \geq 3$ is odd, and let $(p, d) = 1$. Let $q = p^f$ be any power of p which is 1 modulo d. We consider C_d over $\mathbb{F}_q$. The advantage of using $\mathbb{F}_q$ and not $\mathbb{F}_p$ is that over this field the curve has many automorphisms obtained by multiplying the coordinates by d-power roots of unity. The genus of C_d is

$$g = (d-1)(d-2)/2.$$

Use notation as before. Let $\chi = \omega^k$ be the unique power of ω which is of order d (possible since $d|q-1$ so a cyclic group of order $q-1$ has a unique quotient of order d). If a, b are between 1 and $d-1$ but $a + b \neq d$ then χ^a, χ^b and χ^{a+b} are non-trivial characters of $\mathbb{F}_q^\times$. The Jacobi sum

$$J_q(\chi^a, \chi^b) = -\sum_{u \in \mathbb{F}_q, u \neq 0,1} \chi^a(u)\chi^b(1-u) = \frac{g(\chi^a)g(\chi^b)}{g(\chi^{a+b})}.$$

There are $(d-1)(d-2) = 2g$ pairs (a, b) as above.

Theorem 3. *(Weil) The reciprocal eigenvalues of Frobenius Fr_q on $H^1_l(C_d)$ are the numbers $J_q(\chi^a, \chi^b)$. Thus*

$$N_n(C_d) - 1 - q^n = \sum_{1\le a,b\le d-1,\, a+b\neq d} J_q(\chi^a, \chi^b)^n.$$

Remark. (i) Weil in fact computed the LHS by the RHS directly, and from this *deduced* that the Jacobi sums are the eigenvalues of Frobenius.

(ii) One may wonder what happens if we replace q by q^n. One gets a similar equation with $J_{q^n}(\chi^a \circ N, \chi^b \circ N)$ instead of $J_q(\chi^a, \chi^b)^n$ in the RHS. Here N is the norm from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. The relation

$$J_{q^n}(\chi^a \circ N, \chi^b \circ N) = J_q(\chi^a, \chi^b)^n$$

was in fact *needed* to prove the theorem for all n. Fortunately, it was available to Weil. It is the Hasse-Davenport relation.

(iii) The estimate $|J_q(\chi^a, \chi^b)| = \sqrt{q}$ gives the archimedean estimate

$$|N_n(C_d) - 1 - q^n| \le (d-1)(d-2)\sqrt{q^n}.$$

This example was computed, historically, by Weil, before he proved the RH for curves, and was an important motivation for the general case.

(iii) Stickelberger's theorem can now be viewed as telling us something about N_n as a p-adic number. If we fix the prime $\mathfrak{p}$ of $E = \mathbb{Q}(\zeta_d)$ above p (note that all the Jacobi sums take values in E) it turns out that some of the Jacobi sums are divisible by $\mathfrak{p}$ and some are not - which exactly is determined by the "combinatorics of CM types" in E.

(iv) Assume for simplicity that $p \equiv 1 \mod d$ and $q = p$. Note $J_p(\chi^a, \chi^b) \in \mathbb{Q}(\zeta_d)$. If we denote by $P = \mathfrak{p} \cap \mathbb{Q}(\zeta_d)$ then for $e \in (\mathbb{Z}/d\mathbb{Z})^\times$ we get

$$v_{\tau_e^{-1}(P)}(J_p(\chi^a, \chi^b)) = \left\{\frac{-ae}{d}\right\} + \left\{\frac{-be}{d}\right\} - \left\{\frac{-(a+b)e}{d}\right\},$$

where by $\{x\}$ we denote the fractional part of x. This number is 1 for half of the $2g$ pairs of (a, b) and 0 for the other half. As we shall see soon, this implies that the Newton polygon of $Jac(C_d)[p^\infty]$ mod P equals to its Hodge polygon, or that this p-divisible group is *ordinary at P.*

In this case, if we let n be divisible by $(p-1)p^r$ where $r \to \infty$, then $N_n(C_d)$ tends to $1 + (d-1)(d-2)/2$ p-adically.

(v) At the other extreme, suppose that $(\mathbb{Z}/d\mathbb{Z})^\times$ is cyclic (e.g. d is a power of an odd prime) and p is a primitive root modulo d. Then there is only one inert prime P above p in $\mathbb{Q}(\zeta_d)$ and every $J_q(\chi^a, \chi^b)$ has $v_P = \phi(d)/2$ (note that $q = p^{\phi(d)}$ in this case). In this case the Newton polygon of $Jac(C_d)[p^\infty]$ mod P has constant slope $1/2$ and is therefore *supersingular* (The difference between $\phi(d)/2$ and $1/2$ is the difference between Fr_q and the absolute Frobenius Fr_p used to compute the Newton polygon, because $J_q(\chi^a, \chi^b)$ are the eigenvalues of Fr_q but C_d is defined over $\mathbb{F}_p$.)

In this case, as $n \to \infty$, $N_n(C_d)$ tends to 1 p-adically.

For more on this example, see [Ka2].

5. Crystalline cohomology

Let k be a perfect field of char. p, $W = W(k)$ the ring of Witt vectors, K its field of fractions, and X a proper and smooth scheme over W. We write X_0 for its special fiber, and remark that in general it is not true that a proper and smooth X_0/k can be lifted to a proper and smooth

X/W, although this is known in some cases, e.g. curves, or abelian varieties admitting a principal polarization.

Crystalline cohomology $H^m_{cris}(X_0/W)$ is a finitely-generated W-module functorially associated to smooth and proper X_0/k (Berthelot). Its construction has been improved and generalized over the years, and nowadays is often replaced by Berthelot's rigid cohomology. In particular, the restriction that X_0 must be smooth and proper has been removed, but for simplicity we keep it. The key points to know are the following.

- Although $H^m_{cris}(X_0/W)$ is a W-module, it does not depend on the lifting (if such a lifting exists at all), but only on X_0.
- Assume that a proper smooth lifting X exists. Then there is a canonical isomorphism
$$H^m_{cris}(X_0/W) \simeq H^m_{dR}(X/W) := \mathbb{H}^m(X, \Omega^{\cdot}_{X/W}).$$
In particular, (a) $\dim_K H^m_{cris}(X_0/W)_K = b_m$ is the mth Betti number and (b) $H^m_{dR}(X/W)$ and $H^m_{dR}(X'/W)$ are canonically isomorphic, for any two smooth and proper liftings X and X'.
- The absolute Frobenius $Frob : X_0 \to X_0^{(p)}$ induces, by functoriality, a map
$$F : H^m_{cris}(X_0/W)^{(p)} \to H^m_{cris}(X_0/W),$$
or, equivalently, a σ-semi-linear endomorphism F of $H^m_{cris}(X_0/W)$, where σ is the absolute Frobenius automorphism of W.
- Assume that k is a finite field of $q = p^a$ elements. Then F^a is a K-linear endomorphism of $H^m_{cris}(X_0/W)_K$ and (Katz-Messing) its eigenvalues are the $\alpha_{m,i}$ obtained from l-adic etale cohomology.

Part 2. Rigid (crystalline) cohomology and Katz's Conjecture

6. Rigid cohomology

6.1. **p-adic cohomologies - history. Scholie**: to understand the p-adic absolute values of the eigenvalues of Frobenius, we want to have at our disposal a cohomology theory with p-adic coefficients, and make sure that the eigenvalues of Frobenius on it are the same as the eigenvalues of Frobenius on l-adic étale cohomology.

Set-up: k a perfect field of characteristic p, $W = W(k)$ its ring of Witt vectors, $K = Fr(W)$. Examples: $\mathbb{F}_q$ and $\mathbb{Z}_q$ ($q = p^a$), or $\overline{\mathbb{F}}_p$ and the completion of the ring of integers in $\mathbb{Q}_p^{nr}$. Let X be a smooth variety over k. Say that X *lifts to characteristic 0* in the strong sense if there exists a scheme $\mathcal{X}$ smooth over W with $\mathcal{X} \times_{Spec(W)} Spec(k) \simeq X$. Note $\mathcal{X}$ need not exist. In dimension ≥ 2, there is an example of Serre where X does not lift even weakly, i.e. does not lift to *any* local noetherian domain with residue field k, even if we allow ramification. Using moduli spaces it is easy to construct examples of abelian varieties that lift in the weak sense, but not to W. For example, certain abelian varieties with a polarization of degree p. When $\mathcal{X}_{/W}$ exists, it is clearly not unique.

There are situations where X does lift in the strong sense: e.g. X is a curve, or a principally polarized abelian variety (X can then be lifted even with the polarization), or a smooth affine variety. Both for curves and for affine varieties the liftability follows from the fact that one can always lift *locally Zariski*, and the obstruction for global lifting lives in a coherernt H^2, which vanishes if either X is 1-dimensional or affine.

Failure of étale cohomology with p-adic coefficients

Why is it not a good candidate?

- May be too small. E.g. if X is a proper smooth curve of genus g, $H^1_{et}(X_{\overline{k}}, \mathbb{Q}_p)$ has dimension less than $2g$ and may even vanish.
- If X lifts to $\mathcal{X}$,$H^*_{et}(\mathcal{X}_{\overline{K}}, \mathbb{Q}_p)$ has the right size but depends on $\mathcal{X}$, and the Galois action on it is in general ramified, so we do not get an action of Frobenius.
- Base change in étale cohomology does not hold with p-adic coefficients, so we cannot compare $H^*_{et}(\mathcal{X}_{\overline{K}}, \mathbb{Q}_p)$ with $H^*_{et}(X_{\overline{k}}, \mathbb{Q}_p)$.
- Eventually, there will be a comparison theorem between $H^*_{et}(\mathcal{X}_{\overline{K}}, \mathbb{Q}_p)$ and $H^*_{cris}(X/W) \otimes_W K$ but it requires the introduction of a very large field B_{dR} and is quite difficult (Fontaine-Messing, Faltings).

History

- (protohistory: 1960) Dwork's proof of the rationality of the Zeta function $Z(X;T)$.
- (1968) *Monsky-Washnitzer cohomology.* A good theory when X is *smooth and affine* over k.
- (1974) Berthelot: *crystalline cohomology*, following a blue-print by Grothendieck (1966). Idea: replace Zariski open sets by nilpotent thickening of Zariski open sets with a divided power structure on the ideal defining the thickening. Then go to a limit over the thickenings. Crystalline cohomology satisfied the axioms of a Weil cohomology, but gave a good theory only when X was *smooth and proper.* It produces a W-module, possibly with torsion, which can be a head-ache. Advantages: works in the relative setting $X \to S$, and works also "with coefficients" (crystals) as coefficients. Developed further by Berthelot, Messing, Ogus, Illusie and Mazur. Key feature: has a natural comparison to the de Rham cohomology of a lifting.
- (1986) Berthelot: *rigid cohomology.* Works well for any X a scheme of finite type over k, and produces K-vector spaces of finite dimension. When X is smooth and affine it agrees with Monsky-Washnitzer, when X is smooth and proper it agrees with (rational) crystalline cohomology. Uses de Rham cohomology of certain rigid analytic "pieces" of a lift to characteristic 0 to define it, so comparison with de Rham cohomology is more or less automatic.

6.2. **An example.**

6.2.1. *The example.* I will follow a nice set of slides by Bernard Le Stum (2012) [L-S] that can be found on the web.

$k = \mathbb{F}_q$, $q = p^a$, $p > 3$, $q = 1 \mod 4$ (otherwise elliptic curve is supersingular, and counting points becomes trivial in this example). Note that we allow $p = 3 \mod 4$ and a even. Note that $\pm i \in k$.

$X = Spec(A)$, $A = k[x, y, y^{-1}]/(y^2 - x^3 - x)$, $\overline{X} = Proj\left(k[x, y, z]/(y^2 z - x^3 z - xz^2)\right)$ an elliptic curve.

Thus $X = \overline{X} \setminus \overline{X}[2]$ and it projects via x to $\mathbb{P}^1 \setminus \{0, i, -i, \infty\}$.

Take $\mathcal{X} = Spec(\mathcal{A})$, $\mathcal{A} = W[x, y, y^{-1}]/(y^2 - x^3 - x)$ and similarly $\overline{\mathcal{X}}$.

Quite generally, assume X is smooth over k, $\mathcal{X}$ a smooth lifting over W, and assume that there exists $\overline{\mathcal{X}}$ smooth and proper over W containing $\mathcal{X}$ so that $\overline{\mathcal{X}} \setminus \mathcal{X}$ is a divisor with normal crossings, all of whose irreducible components are smooth over W. This is the "best of all worlds", but it very often holds, e.g. in our example.

Then define

$$H^*_{rig}(X) = H^*_{dR}(\mathcal{X}_K/K) = \mathbb{H}^*(\mathcal{X}_K, \Omega^{\cdot}_{\mathcal{X}_K/K}).$$

If $\mathcal{X}$ is affine then

$$H^*_{rig}(X) = h^{\cdot}(\Omega^{\cdot}(\mathcal{X}_K/K), d).$$

In our example $\mathcal{A} = \mathcal{B} \oplus \mathcal{B}y$ where $\mathcal{B} = K[x, 1/(x^3+x)]$ and

$$dy = \frac{3x^2+1}{2(x^3+x)} ydx \in \mathcal{B}ydx.$$

Thus

$$H^1_{rig}(X) = h^1(\mathcal{A} \to \mathcal{A}dx) = h^1(\mathcal{B} \to \mathcal{B}dx) \oplus h^1(\mathcal{B}y \to \mathcal{B}ydx)$$

where

$$h^1(\mathcal{B} \to \mathcal{B}dx) = K\left[\frac{dx}{y^2}\right] \oplus K\left[\frac{xdx}{y^2}\right] \oplus K\left[\frac{x^2dx}{y^2}\right]$$

$$h^1(\mathcal{B}y \to \mathcal{B}ydx) = K\left[\frac{dx}{y}\right] \oplus K\left[\frac{xdx}{y}\right].$$

These two pieces can be interpreted as the ± parts w.r.t. the automorphism $(x,y) \mapsto (x,-y)$, or alternatively as the pull backs of the cohomologies of $\mathbb{P}^1 \setminus \{0, i, -i, \infty\}$ and of $\overline{X}$ respectively.

6.2.2. *Lifting Frobenius.* Quite generally let $Fr : X \to X^{(p)}$ be "raising the coordinates to power p". If $k = \mathbb{F}_q$ then $Fr_q = Fr^a : X \to X$ is an endomorphism of the variety.

In general, even in the "best of all worlds" situation, $k = \mathbb{F}_q$, there need not be a lifting of Fr_q to an endomorphism of $\mathcal{X}$. In our example, by the theory of complex multiplication, Fr_q lifts to an endomorphism of $\mathcal{X}$, but this is an accident, and if we took $\mathcal{X}$ to be the curve $y^2 = x^3 + x - p$ for example, such a lifting would not exist. So let's try to do something that would work for all liftings $\mathcal{X}$.

Idea: replace $\mathcal{X}$ by its p-adic completion $\widehat{\mathcal{X}} = \{\mathcal{X} \mod p^{n+1}\}_{n=0}^{\infty}$, strictly speaking a *formal scheme* (affine if X is affine).

On the level of functions, in our example,

$$\widehat{\mathcal{A}} = W\left\{x, y, y^{-1}\right\}/(y^2 - x^3 - x) = \Gamma(\widehat{\mathcal{X}}, \mathcal{O})$$

and we tensor with K to get

$$\widehat{\mathcal{A}}_K = K\left\{x, y, y^{-1}\right\}/(y^2 - x^3 - x)$$

where $K\left\{x, y, y^{-1}\right\}$ is the *Tate algebra* of all the power series $\sum_{i\in\mathbb{N}, j\in\mathbb{Z}} a_{ij}x^iy^j$ converging on $|x| \leq 1$, $|y| = 1$. A lifting of Frobenius then may be defined as

$$F : (x,y) \mapsto (x^q, y^q\sqrt{\frac{x^{3q}+x^q}{(x^3+x)^q}})$$

(note that the RHS indeed belongs to $\widehat{\mathcal{X}}$). The expression under the square root is congruent to 1 modulo p, so a square root of it exists in $\widehat{\mathcal{A}}$.

This fact is general.

Proposition 4. *Let $k = \mathbb{F}_q$ and assume $\widehat{\mathcal{X}}_K = Spm(\widehat{\mathcal{A}}_K)$ is an affinoid over K with good reduction, i.e. the affine scheme X obtained upon its reduction is smooth over k. Then Fr_q lifts (in a non-unique way) to an endomorphism F of $\widehat{\mathcal{X}}_K$.*

Alas, we solved one problem and created another !

6.2.3. *Overconvergence.* **Problem**: Unless $\mathcal{X}$ is proper, $H^*_{dR}(\mathcal{X}_K/K) \neq H^*_{dR}(\widehat{\mathcal{X}}_K/K)$. Example: Take $X = Spec(k[x])$, $\mathcal{X} = Spec(K[x])$, $\widehat{\mathcal{X}}_K = Spm(K\{x\})$. The cohomology of X or $\mathcal{X}$ vanishes, but the cohomology of $\widehat{\mathcal{X}}_K$ is infinite dimensional, because a general power series differential

$$\sum_{n=0}^{\infty} a_n x^n dx$$

with $a_n \to 0$ is not integrable to a function in $K\{x\}$.

Solution: Introduce the ring

$$\mathcal{A} \subset \mathcal{A}^\dagger \subset \widehat{\mathcal{A}}_K$$

of all "overconvergent functions", i.e. functions that converge on *some* "wide open neighborhood" of the affinoid $\widehat{\mathcal{X}}_K$ (not specifying the neighborhood). In our example

$$\mathcal{A}^\dagger = K[x, y, 1/y]^\dagger/(y^2 - x^3 - x)$$

where $K[x, y, 1/y]^\dagger$ is the ring of formal power series that converge in $|x| < 1 + \varepsilon$, $1 - \varepsilon < |y| < 1 + \varepsilon$ for some $\varepsilon > 0$.

Facts (in the smooth affine case)

(1) Any lifting F of Fr_q to $\widehat{\mathcal{A}}_K$ is overconvergent, i.e. preserves $\mathcal{A}^\dagger$.
(2) Any two liftings induce the same endomorphism on $H^*_{dR}(\mathcal{X}^\dagger) = h^*(\Omega^{\cdot}(\mathcal{A}^\dagger/K), d)$. Think of the two liftings as being homotopic to each other.
(3) The de Rham cohomology $H^*_{dR}(\mathcal{X}^\dagger)$ is "good" - gives what is expected - and agrees with $H^*_{dR}(\mathcal{X}/K)$ in the "best of all worlds" situation. Notice that to define $H^*_{dR}(\mathcal{X}^\dagger)$ we do not need $\mathcal{X}$. Only the formal weak (dagger) completion counts.

These three facts are basically due to Monsky-Washnitzer. Thus we get a well-defined action of F on $H^*_{rig}(X) = H^*_{dR}(\mathcal{X}^\dagger/K)$.

6.3. **Rigid cohomology.**

6.3.1. *Tubes.* Start with any perfect field k and *any* k-variety X. Take a closed embedding $X \hookrightarrow P$ where P is a *smooth formal scheme* over W (should really say *over* $Spf(W)$). Take this to mean that we have closed embeddings

$$\begin{tikzcd}
 & P_{n+1} \\
X \arrow[ur] \arrow[r, hook, "i_n"] & P_n \arrow[u]
\end{tikzcd}$$

where P_n is a smooth scheme over $W_n = W/p^{n+1}W$ and the vertical map identifies $P_{n+1} \times_{Spec(W_{n+1})} Spec(W_n)$ with P_n. It is important to allow P to be large. In applications, it is sometimes taken as projective space, but to develop the theory and prove independence of the embedding we can not restrict to projective space.

If X is *smooth* and *liftable* we can take P to be a smooth formal scheme having $X = P_0$ as the special fiber, but again this choice is too narrow for the general theory.

Any formal scheme P over W has a "generic fiber" P_K which is a (rigid/ Berkovich) analytic space. Its reduction is the scheme $P_0 = P_k$ and it has a specialization map

$$\mathrm{sp} : P_K \to P_k \supset X.$$

If, locally, $P_n = Spec(W_n[T_1, \dots, T_m]/\mathfrak{a}_n)$ where $\mathfrak{a}_{n+1} \mod p^n = \mathfrak{a}_n$, then

$$P_K = Spm(K\{T_1, \dots, T_m\}/\widehat{\mathfrak{a}})$$

and sp takes the coordinates $(t_1, \dots, t_m) \in D(0,1)^m$ ("closed" unit ball) of a point on P_K and reduces them modulo p. Define the *tube* $]X[_P$ *of* X *in* P to be the analytic space

$$]X[_P = \{x \in P_K \,|\, \mathrm{sp}(x) \in X\}\,.$$

Example. P is $\widehat{\mathbb{A}}^m$, $f_1, \dots, f_r, g$ are primitive polynomials in $W[T_1, \dots, T_m]$ and

$$X = Spec\left(k[T_1, \dots, T_m]/(\overline{f_i})\right)[\overline{g}^{-1}].$$

Then

$$]X[_P = \{x \in D(0,1)^m |\ |f_i(x)| < 1,\ |g(x)| = 1\}\,.$$

For example, if X is a point (say, the origin) then $]X[_P = D(0,1^-)^m$ ("open" ball). At the other extreme, if X is open in P_k then $X = \widehat{\mathcal{X}}_k$ for an open formal subscheme $\widehat{\mathcal{X}} \subset P$ over W, and $]X[_P = \widehat{\mathcal{X}}_K$ is its generic fiber.

6.3.2. *Rigid cohomology in the proper case.* Assume first that X is *proper*. Let $X \hookrightarrow P$ be a closed embedding in a smooth formal scheme over W as before. Define

$$H^*_{rig}(X) = H^*_{dR}(]X[_P)$$

(hypercohomology). If X happens to be also smooth and liftable and we put $P = \widehat{\mathcal{X}}$ as before then we recover $H^*_{rig}(X) = H^*_{dR}(\mathcal{X}_K/K)$.

To prove (a) independence of the embedding in P and (b) functoriality in X, Berthelot uses two key results:

(1) **Local Poincaré Lemma**: If V is an affinoid variety and $D = D(0,1^-)$ is the open unit disk with parameter t then the sequence

$$0 \to \Gamma(V, \mathcal{O}) \to \Gamma(V \times D, \mathcal{O}) \overset{\partial/\partial t}{\to} \Gamma(V \times D, \mathcal{O}) \to 1$$

is exact.

(2) **Weak fibration theorem**: Let

$$\begin{tikzcd} & P' \arrow[d, "\pi"] \\ X \arrow[ur] \arrow[r, hook, "i"] & P \end{tikzcd}$$

be a diagram of closed embeddings of X in smooth formal schemes P, P' over W with π a smooth map. Then, locally on $]X[_P$ (in the analytic topology)

$$]X[_{P'} \simeq]X[_P \times D^r$$

with D as above.

Functoriality yields of course that $Fr : X \to X^{(p)}$ induces a K-linear map

$$F : H^*_{rig}(X)^{(p)} \to H^*_{rig}(X),$$

which is the same as a σ-semilinear endomorphism of $H^*_{rig}(X)$ (σ being the Frobenius automorphism of K).

6.3.3. *Rigid cohomology in general.* If X is not proper anymore, we encounter the same problem that we encountered in the example, in that de Rham cohomology of affinoids / Tate algebras is not well-behaved, and we must opt for overconvergent cohomology. One still embeds X as a *locally closed embedding* (open in closed) in a *smooth and proper* P (even if X is not proper, e.g. projective space) and defines then

$$H^*_{rig}(X) = H^*_{dR}(]X[^\dagger_P).$$

We skip the precise definitions and details.

7. Katz' conjecture

7.1. **Newton and Hodge polygons.** From now on let $q = p^a$, $k = \mathbb{F}_q$ and X *proper and smooth* over k. In this case

$$H^m_{rig}(X) = H^m_{cris}(X/W) \otimes_W K.$$

The following assumption was made by Mazur in his proof of the conjecture of Katz that we are about to discuss. It was later removed by Ogus, who gave a new proof of the conjecture, but the formulation had to be also changed somewhat, so we stick to it for the exposition.

(Ass) X is liftable to a proper and smooth $\mathcal{X}/W$ and the Hodge groups $H^j(\mathcal{X}, \Omega^i)$ are W-torsion free.

In this case we have the following theorem.

Theorem 5. *(Katz-Messing) The characteristic polynomial of F^a on $H^m_{rig}(X)$ is the same as the characteristic polynomial of the arithmetic Frobenius Fr_q^{-1} on $H^m_{et}(X_{\overline{k}}, \mathbb{Q}_l)$.*

Etesse and Le Stum proved the same result when X is only assumed to be smooth, but not necessarily proper.

Write the characteristic polynomial as

$$f_m(t) = det(1 - t(F^a)^* | H^m_{rig}(X)) = 1 + a_1 t + a_2 t^2 + \cdots + a_\beta t^\beta = \prod_{i=1}^{\beta}(1 - \alpha_{i,m} t)$$

where the $\alpha_{i,m}$ are the eigenvalues of F^a. They are q^m-Weil numbers and make up a complete set of Galois conjugates. Let ord_q be the valuation on $\overline{\mathbb{Q}}_p$ normalized by $ord_q(q) = 1$.

To record the absolute value of the $\alpha_{i,m}$ we introduce the Newton polygon of f_m, which is

$$NP(f_m) = \text{conv}\left\{(0,\infty), (i, ord_q(a_i)), (\beta, \infty)\right\}_{0 \leq i \leq \beta}.$$

Sometimes we shall denote by $NP(f_m)$ also the lower boundary of this polygon. Since $a_\beta = q^{\beta m/2}$, it connects $(0,0)$ to $(\beta, \beta m/2)$. We have the following elementary lemma.

Lemma 6. *If the slopes of the segments making up $NP(f_m)$ are $0 \leq r_1/s_1 < r_2/s_2 < \cdots < r_k/s_k$ with horizontal lengths s_i then there are precisely s_i eigenvalues α with $ord_q(\alpha) = r_i/s_i$.*

On the other hand we have the Hodge polygon $Hdg(H^m)$. Let

$$h^{i,m-i} = \dim H^{m-i}(X, \Omega^i)$$

and let Hdg be the polygon connecting the points $(\sum_{j=0}^{i} h^{j,m-j}, \sum_{j=0}^{i} jh^{j,m-j})$ for $-1 \leq i \leq m$. The degeneration of the Hodge spectral sequence is equivalent to the equality

$$\sum_{j=0}^{i} h^{j,m-j} = \beta$$

and the Hodge symmetries $h^{i,j} = h^{j,i}$ imply that the last point is $(\beta, \beta m/2)$. Thus $Hdg(H^m)$ has the same end points as $NP(H^m)$.

Remark. Without the liftability of X, neither the degeneration of the Hodge spectral sequence, nor the Hodge symmetries must hold. Serre gave an example of a surface with $h^{0,1} = 1$ but $h^{1,0} = 0$. In the non-liftable case substitute for $h^{i,j}$ the *reduced Hodge numbers* made from the E_∞ page of the Hodge spectral sequence.

Theorem 7. *(Mazur, Katz' conjecture) The Newton polygon lies on or above the Hodge polygon. Viewing these polygons as graphs of functions*

$$Hdg(H^m)(t) \leq NP(f_m)(t).$$

For example, if X is a curve of genus g and $m = 1$ then Hdg has two segments of horizontal lengths g and slopes 0 and 1. The NP must have, by Poincaré duality, slopes λ and $1 - \lambda$ with equal multiplicities (horizontal lengths). This in itself, together with coincidence of end points, implies the theorem. The same is true for abelian varieties and any m. But in general, the theorem says that the Hodge numbers impose further severe restrictions on the Newton polygon, hence on the p-adic absolute values of the eigenvalues of Frobenius. For example, it has the following immediate corollary.

Corollary 8. *Suppose that $h^{j,m-j} = 0$ for $j < i$. Then all the eigenvalues α have $ord_q(\alpha) \geq i$.*

7.2. **Spans and the abstract Hodge polygon.** Mazur's approach to Katz' conjecture is based on the following idea. First, generalize and assume that k is any perfect field, and consider the absolute Frobenius, rather than its ath power. Let H be $H^m_{dR}(\mathcal{X}/W)$ and $M = H^{(p)}$. Both are free W-modules of rank β. By the theory of elementary divisors there are bases of these two modules over W w.r.t. which the matrix of F is $diag.(1, 1, \ldots, 1, p, \ldots, p, p^2, \ldots, \ldots, p^m, \ldots, p^m)$. This is because $F(M) \supset p^m H$. The number h^i of times p^i appears is called the abstract ith Hodge number. The abstract Hodge polygon $\widetilde{Hdg}(H^m)$ of H^m is the polygon having slope i with multiplicity h^i.

On the other hand, using the Manin-Dieudonné classification of F-isocrystals one can associate to H^m a Newton polygon $NP(H^m)$ even if k is not a finite field and the eigenvalues of F^a do not make sense for any a. If $k = \mathbb{F}_q$ it is the same $NP(f_m)$ that was defined before.

The proof of the Theorem is based on the following two results.

Theorem 9. $NP(H^m) \geq \widetilde{Hdg}(H^m)$.

This theorem is easy. It involves only simple semi-linear algebra.

Theorem 10. $\widetilde{Hdg}(H^m) = Hdg(H^m)$.

The proof of this theorem, given in Mazur's Annals paper, is complicated. It is amazing and not at all clear why the Hodge numbers are determined by the elementary divisors of $F : M \to H$. For lack of time and expertese we shall not go into any more details.

7.3. **Families.** We shall only make a few remarks about what happens when we vary X in a family. Suppose now that $X \to S$ is a proper smooth family over a smooth base S over an algebraically closed field k. A typical example would be the universal abelian scheme over the moduli space $\mathcal{A}_{g,n}$ of principally polarized abelian varieties of genus g and full level n structure, $n \geq 3$.

Let m be any degree for cohomology. The Betti number $\beta = \dim H^m_{rig}(X_s)$ is independent of $s \in S$. Fix a Newton polygon Π connecting $(0,0)$ to $(\beta, \beta m/2)$.

Theorem 11. *(Grothendieck) The set* $\{s \in S | \, NP(H^m(X_s)) \geq \Pi\}$ *is Zariski closed.*

This theorem is often phrased as saying that the "Newton polygon rises under specialization". Maybe Grothendieck only proved it for families of abelian varieties and $m = 1$ because he was dealing with Dieudonné modules, but the general theorem should also be true, see e.g. [Ka1], Theorem 2.3.1.

The theorem implies, for example, that $\mathcal{A}_{g,n}$ is *stratified* by the Newton polygon of the abelian varieties uniformized by it. These Newton polygons are *symmetric* (because of the polarization), i.e. the slopes λ and $1 - \lambda$ appear with the same multiplicity.

Theorem 12. *(i) (Manin's conjecture) Any symmetric Newton polygon connecting* $(0,0)$ *to* $(g, g/2)$ *is realized by a principally polarized abelian variety of genus g.*

(ii) (Grothendieck's conjecture) If $s \in \mathcal{A}_{g,n}$ is such that the universal abelian variety A_s has NP β which lies above a symmetric Newton polygon γ then s belongs to the Zariski closure of $\mathcal{A}_{g,n}[\gamma]$.

The first assertion is a consequence of Honda-Tate theory, but for the second one needs deformation theory. It was proved by Oort.

We end with an open problem.

Problem 13. Is every symmetric Newton polygon connecting $(0,0)$ to $(g, g/2)$ realized by a Jacobian of a curve?

A lot of work has been done on this question by Oort, van der Geer, and others.

References

[Wan] D. Wan: Lectures on Zeta functions over finite fields (Göttingen).,

[Maz] B. Mazur: Frobenius and the Hodge filtration, Bull. Amer. Math. Soc., **78** (1972), 653-667.

[Ka1] N. Katz: Slope filtration of F-crystals, Astérisque **63** (1979), 113-164.

[Ka2] N. Katz: Crystalline Cohomology, Dieudonné Modules, and Jacobi Sums, in: *Automorphic Forms, Representation Theory and Arithmetic*, Springer, 165-246.

[L-S] B. Le Stum: An intoduction to rigid coohmology, Strasbourg 2012, a course of 140 slides on the web.