(Pro)étale cohomology
Shane Kelly, UTokyo
Spring Semester 2024

Comments welcome!: shanekelly64[at]gmail[dot]com.

Lecture 1: Introduction

April 11th 2024

In this lecture we present some motivation for the course.

1 Counting points with Zeta functions

We begin with the following question:

Question 1. Let X is a smooth projective variety over $\mathbb{F}_q$, how many elements does the set $X(\mathbb{F}_{q^n}) = \hom_{\mathrm{Spec}(\mathbb{F}_q)}(\mathrm{Spec}(\mathbb{F}_{q^n}), X))$ of $\mathbb{F}_{q^n}$-points of X have for each n?

Or equivalently:

Question 2. If $f_1, \dots, f_c \in \mathbb{F}_q[t_0, \dots, t_d]$ are the homogeneous polynomials defining[1] X, how many solutions do $f_1, \dots, f_c$ have in $\mathbb{F}_{q^n}$ for each n?

$$\#X(\mathbb{F}_q) = \frac{\#\left\{(a_0, \dots, a_d) \in \mathbb{F}_{q^n}^{d+1} \setminus \{0\} \mid f_i(a) = 0, \forall i = 1, \dots c\right\}}{q^n - 1}$$

In order to work with all the sets $X(\mathbb{F}_{q^n})$ at once, we introduce the zeta function

$$Z(X,t) = \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})\frac{t^n}{n}\right) \overset{(*)}{=} \prod_{x \in X_{(0)}} \left(1 - t^{\deg(x)}\right)^{-1}.$$

Here, $\exp(T)$ is the power series $\sum_{i=0}^{\infty} \frac{1}{i!}T^i \in \mathbb{C}[[T]] = \lim_n \mathbb{C}[T]/T^n$. The product is over the set $X_{(0)}$ of closed points x of the scheme X and $\deg(x)$ means $[k(x) : \mathbb{F}_q]$ where $k(x)$ is the residue field at x.

Exercise 1. Using the power series $\log \frac{1}{1-T} = \sum_{i=1}^{\infty} \frac{1}{i}T^i$, prove the equality $(*)$.

Remark 3. Note $Z(X,t)$ is defined for any $\mathbb{F}_q$-variety, possibly not projective, not smooth.

[1] That is, $X = Proj\left(\frac{\mathbb{F}_q[t_0,\dots,t_d]}{\langle f_1,\dots,f_c\rangle}\right)$

Remark 4. For any sequence of closed subsets $Y_0 \subset Y_1 \subset \cdots \subset Y_n = X$, it follows from the definition that we have

$$Z(X,t) = \prod_i Z(Y_i \setminus Y_{i-1}, t).$$

Remark 5. There is a reason that the product form of $Z(X, p^{-s})$ looks similar to the Riemann zeta function $\zeta(X,s) = \prod_{p \text{ prime}}(1-p^{-s})^{-1}$. The Riemann zeta function and the above $Z(X,t)$ are both special cases of more general zeta functions defined for any scheme of finite type over $\mathbb{Z}$.

Now our question has become:

Question 6. Calculate $Z(X,t)$.

Example 7. First consider $Z(\mathbb{A}^d, t)$. We have $\#\mathbb{A}^d(\mathbb{F}_{q^n}) = q^{nd}$ so

$$Z(\mathbb{A}^d, t) = \exp \sum_{n=1}^{\infty} (q^d t)^n / n = \exp(-\log(1-q^d t)) = \frac{1}{(1-q^d t)}.$$

Example 8. Consider $X = \mathbb{P}^d$. Choosing coordinates gives a sequence $\mathbb{P}^0 \subset \mathbb{P}^1 \subset \cdots \subset \mathbb{P}^d$. Since $\mathbb{A}^i \cong \mathbb{P}^i \setminus \mathbb{P}^{i-1}$, we see that

$$Z(\mathbb{P}^d, t) = \frac{1}{(1-t)(1-qt)\dots(1-q^d t)}$$

Example 9. Let X be an elliptic curve. Using the action $T_\ell \phi : T_\ell X \to T_\ell X$ of the Frobenius $\phi : X \to X$ on the Tate module $T_\ell X = \varprojlim_n \ker(X \xrightarrow{\ell^n} X) \in \mathbb{Z}_\ell$-mod one can calculate

$$\#X(\mathbb{F}_{q^n}) = \deg(1-\phi^n) = \det(1 - T_\ell \phi^n) = 1 - \alpha^n - \beta^n + q^n.$$

where $\alpha, \beta \in \mathbb{C}$ are complex conjugates with absolute value $\sqrt{q}$. Then using the log argument as in the case of $\mathbb{A}^d$, we find that

$$Z(E,t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)}.$$

For more details see Silverman, "The Arithmetic of Elliptic Curves", Chapter 5. This method generalises to higher dimension abelian varieties.

Example 10. If X is a curve, then the Zeta function can be rewritten in terms of divisors, and from there, in terms of linear systems of divisors of line bundles. Then using the Riemann-Roch theorem for curves, one can calculate

$$Z(X,t) = \frac{f(t)}{(1-t)(1-qt)}$$

where $f(t) \in \mathbb{Z}[t]$ has degree $2g$. For more details see, for example, Raskin, "The Weil conjectures for curves".

Example 11. Using characters $\chi : \mathbb{F}_{q^n}^* \to \mathbb{C}$, one can calculate explicitly the case X is a smooth hypersurface defined by an equation of the form $a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r}$.

$$Z(X,t) = \frac{1}{(1-t)(1-qt)\dots(1-q^{r-1}T)} \prod_{\alpha} (1 - C(\alpha) t^{\mu(\alpha)})^{\frac{(-1)^r}{\mu(\alpha)}}$$

where $\alpha \in (\mathbb{F}_q^*)^{r+1}$, $\mu(\alpha) \in \mathbb{N}$, $C(\alpha) \in \mathbb{C}$, $|C(\alpha)| = q^{\frac{(r-1)\mu(\alpha)}{2}}$, and we do not say what the product is over. For details see Weil, "Numbers of solutions of equations in finite fields".

Examples such as the above lead Weil to make the following conjectures:

Theorem 12 (Weil conjectures)**.** *Suppose X is a connected smooth projective variety of dimension n over $\mathbb{F}_q$. Then the Zeta function of X satisfies the following properties:*

1. *(Rationality) The Zeta function $Z(X,t)$ is a rational function of t.*
2. *(Functional equation) There is an integer e such that*
$$Z(X, q^{-n}t^{-1}) = \pm q^{en/2} t^e Z(X,t).$$
3. *(Riemann Hypothesis) The Zeta function can be written as an alternating product*
$$Z(X,t) = \frac{P_1(t)P_3(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)}$$
where each $P_i(t)$ is an integral polynomial all of whose roots have absolute value $q^{-i/2}$. Moreover, $P_0(t) = 1-t$ and $P_{2n}(t) = 1 - q^n t$.
4. *(Betti numbers) Suppose there is a number field $K/\mathbb{Q}$, and homogeneous polynomials $f_1, \dots, f_c \in \mathcal{O}_K[t_0, \dots, t_d]$ where $\mathcal{O}_K$ is the ring of integers of K, such that X is defined by the f_i mod $\mathfrak{p}$ for some prime $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_q$. Suppose furthermore that the complex projective variety $X(\mathbb{C})$ defined by the $f_i \in \mathcal{O}_K \subseteq K \subseteq \mathbb{C}$ is smooth (for some choice of embedding $K \subseteq \mathbb{C}$). Then*
$$\deg P_i(t) = \dim_{\mathbb{Q}} H^i(X(\mathbb{C}), \mathbb{Q})$$
where $X_{\mathbb{C}} \subseteq \mathbb{P}^d_{\mathbb{C}}$ is given the topology induced from $\mathbb{P}^d_{\mathbb{C}}$ considered as a complex analytic space.

Remark 13. The Riemann Hypothesis is so called because it places the zeroes and poles of $Z(X, q^{-s})$ on vertical lines in the complex plane.

Remark 14. In (Betti numbers) we are of course allowed to take $K = \mathbb{Q}$, in which case $\mathcal{O}_K = \mathbb{Z}$, and $\mathfrak{p}$ corresponds to a prime of $\mathbb{Z}$ so the base field is $\mathbb{F}_p$. When q is a larger power of p we need to use more general K.

Exercise 2. Show that if s is a zero or pole of $Z(X, q^{-s})$ then $\Re s = j/2$ for some $j \in \mathbb{Z}$.

2 Counting points with cohomology

References for this section could include:

[Hatcher, "Algebraic topology"§2.1, §2.2]

[Bott, Tu, "Differential forms in algebraic topology", III§15]

[Weibel, "An introduction to homological algebra"]

Now we show why one might expect cohomology to be useful. Suppose M is an n-dimensional compact real manifold. Its *cohomology groups* (with $\mathbb{Q}$-coefficients) are a sequence of $\mathbb{Q}$-vector spaces

$$H^0(M,\mathbb{Q}), H^1(M,\mathbb{Q}), H^2(M,\mathbb{Q}), \ldots.$$

The dimension of the ith space is roughly how many "i-dimensional holes" M has in some sense.

The definition is not so important here. We are more interested in the properties listed below.

Before we get to them though, let us give some examples.

Example 15. If $M = S^m = \{(x_0, \ldots, x_m) \in \mathbb{R}^{m+1} : x_0^2 + \cdots + x_m^2 = 1\}$ is the m-dimensional sphere, then

$$H^n(S^m,\mathbb{Q}) = \begin{cases} \mathbb{Q} & n = 0, m \\ 0 & \text{otherwise} \end{cases}$$

So S^m has one zero dimension hole (i.e., one connected component), and one m-dimensional hole. As cohomology groups are homotopy invariant, and there is a continuous retraction of $\mathbb{C}^m \setminus \{0\} \cong \mathbb{R}^{2m} \setminus \{0\}$ to S^{2m-1}, we get

$$H^n(\mathbb{C}^m \setminus \{0\},\mathbb{Q}) = \begin{cases} \mathbb{Q} & n = 0, 2m-1 \\ 0 & \text{otherwise} \end{cases}$$

Example 16. If M is a sphere with g handles, then

$$H^n(M,\mathbb{Q}) = \begin{cases} \mathbb{Q} & n = 0 \\ \mathbb{Q}^{2g} & n = 1 \\ \mathbb{Q} & n = 2 \\ 0 & \text{otherwise} \end{cases}$$

The case $g = 1$ is the surface of a doughnut. A model is the topological space $\mathbb{C}/\mathbb{Z} + \mathbb{Z}i$. The two dimensions of H^1 correspond to the fact that there are two distinct ways of going "around" the doughnut (horizontally or vertically).

Example 17. If $M = \mathbb{P}^m(\mathbb{C})$ is projective space of dimension m (considered as a real manifold) then

$$H^n(\mathbb{P}^m(\mathbb{C}),\mathbb{Q}) = \begin{cases} \mathbb{Q} & n = 0, 2, 4, \ldots, 2m \\ 0 & \text{otherwise} \end{cases}$$

In general, the cohomology groups of a connected compact real manifold have the following properties.

1. (Finiteness) $\dim_{\mathbb{Q}} H^i(M, \mathbb{Q}) < \infty$ for all i. Moreover, if $M = X(\mathbb{C})$ comes from a complex algebraic variety X, then $H^i(M, \mathbb{Q}) = 0$ for $i > 2\dim_{\mathbb{C}} X$.

2. (Functoriality) For any continuous map $\phi : M \to N$, there are induced maps $H^i(\phi) : H^i(N, \mathbb{Q}) \to H^i(M, \mathbb{Q})$ compatible with composition. That is, $H^i(\psi \circ \phi) = H^i(\phi) \circ H^i(\psi)$ for any two composable morphisms $M \xrightarrow{\phi} N \xrightarrow{\psi} N'$.

3. (Poincaré Duality) There is a canonical isomorphism $H^{\dim M}(M, \mathbb{Q}) \cong \mathbb{Q}$, and a natural perfect pairing

$$H^i(M, \mathbb{Q}) \times H^{\dim M - i}(M, \mathbb{Q}) \to H^{\dim M}(M, \mathbb{Q}).$$

   In other words, there is a canonical identification of $H^{\dim M - i}(M, \mathbb{Q})$ with the dual vector space $H^i(M, \mathbb{Q})^* = \hom_{\mathbb{Q}}(H^i(M, \mathbb{Q}), \mathbb{Q})$.

4. (Lefschetz Trace Formula) Suppose $\phi : M \to M$ is a continuous map with only simple isolated fixed points (e.g., the graph is transverse to the diagonal). Then

$$\#\{\text{ fixed points }\} = \sum_{i=0}^{n} (-1)^i \mathrm{tr}(H^i(\phi))$$

   where tr is the trace of the vector space automorphism $H^i(\phi) : H^i(M, \mathbb{Q}) \to H^i(M, \mathbb{Q})$.

Now suppose we had cohomology groups defined for algebraic varieties over finite fields, satisfying versions of the above properties. Since

$$X(\mathbb{F}_{q^m}) = \text{ fixed points of } Frob^m : X(\overline{\mathbb{F}_q}) \to X(\overline{\mathbb{F}_q})$$

we could hope that a version of (Lefschetz Trace Formula) would give

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim X} (-1)^i \mathrm{tr}(H^i(\phi^m))$$

with $\phi = Frob$. Inserting this to the sum description of $Z(X, t)$ we get

$$\begin{aligned} Z(X,t) &= \exp \sum_{n=1}^{\infty} \left(\sum_{i=0}^{2\dim X} (-1)^i \mathrm{tr}(H^i(\phi^n)) \right) \frac{t^n}{n} \\ &= \prod_{i=1}^{2\dim X} \left(\exp \sum_{n=1}^{\infty} \mathrm{tr}(H^i(\phi^n)) \frac{t^n}{n} \right)^{(-1)^i} \end{aligned}$$

Combining this with

$$\det(1 - A)^{-1} = \exp \sum_{n=1}^{\infty} \mathrm{tr} A^n / n$$

valid for any matrix A, we get

$$Z(X, t) = \prod_{i=0}^{2 \dim X} \det\Big(\mathrm{id} - t \cdot H^i(\phi) \Big)^{(-1)^{i+1}}$$

and we would get (Rationality). Moreover, an appropriate version of (Poincaré Duality) would give (Functional equation), and if our new cohomology groups are compatible with usual cohomology groups in an appropriate way, then we would get (Betti numbers). Finally, this description suggests that the polynomials in (Riemann Hypothesis) are $P_i(t) = \det(\mathrm{id} - t \cdot H^i(\phi))$, and if so, then the second part is reformulated as: the eigenvalues of $H^i(\phi)$ have absolute value $q^{-i/2}$.

3 Coefficients

It was observed very early that there could be no cohomology for $\mathbb{F}_p$-varieties with $\mathbb{Q}$-coefficients. However, essentially due to the fact that polynomials have finitely many solutions, using $\mathbb{Z}/\ell^n$-coefficients (for $\ell \neq p$) works well. Then defining

$$H^r_{et}(X, \mathbb{Q}_\ell) := \left(\lim_n H^r_{et}(X, \mathbb{Z}/\ell^n) \right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

one obtains vector spaces over a field, $\mathbb{Q}_\ell$, of characteristic zero. This is technically awkward, especially when one tries to have a six functor formalism.

Namely, the cohomology groups $H^r_{et}(X, \mathbb{Z}/\ell^n)$ are representable in a triangulated category $D(X, \mathbb{Z}/\ell^n)$ in the sense that

$$H^r_{et}(X, \mathbb{Z}/\ell^n) = \hom_{D(X, \mathbb{Z}/\ell^n)}(\mathbb{Z}/\ell^n, \mathbb{Z}/\ell^n[r]).$$

Given a morphism $f : Y \to X$ one has an adjunction

$$f^* : D(X, \mathbb{Z}/\ell^n) \rightleftarrows D(Y, \mathbb{Z}/\ell^n) : f_*,$$

for nice f an adjunction

$$f_! : D(Y, \mathbb{Z}/\ell^n) \rightleftarrows D(X, \mathbb{Z}/\ell^n) : f^!,$$

and for nice X and $\mathcal{E} \in D(X, \mathbb{Z}/\ell^n)$ an adjunction

$$- \otimes \mathcal{E} : D(X, \mathbb{Z}/\ell^n) \rightleftarrows D(Y, \mathbb{Z}/\ell^n) : \mathcal{H}om(\mathcal{E}, -),$$

and these six functors interact with each other in nice ways (proper base change, smooth base change, projection formula, duality, ...). If one wants to promote these six functors to something with $\mathbb{Q}_\ell$-coefficients, one would first try to work with uncomfortable[2] objects such as $\lim_n D(X, \mathbb{Z}/\ell^n)$. In practice, this is not exactly what was used, but it was still technically awkard.

As we mentioned above, the obstacle to using $\mathbb{Z}_\ell$-coefficients was that polynomials only have finitely many solutions. However, if we allow our polynomials to have rational exponents (e.g., $t^3 + 5t^{1/2} - 2t^{3/7}$), then instead of finitely many solutions, we can obtain profinitely many.

Exercise 3.

1. Consider the ring homomorphism $\phi : \mathbb{C}[t, t^{-1}] \to \mathbb{C}[t, t^{-1}]$; $t \mapsto t^n$ (or equivalently, the inclusion $\mathbb{C}[t, t^{-1}] \subseteq \mathbb{C}[t^{1/n}, t^{-1/n}]$). Show that for each $a \in \mathbb{C}^*$, there are exactly n prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ such that $\phi^{-1}\mathfrak{p}_i = \langle t - a\rangle$. Hint.[3]

   In other words, there are $n = \#\mathbb{Z}/n$ points in the fibre of $\mathrm{Spec}(\phi) : \mathrm{Spec}(\mathbb{C}[t, t^{-1}]) \to \mathrm{Spec}(\mathbb{C}[t, t^{-1}])$ at $t = a$.

2. (Harder) Now consider the inclusion $\phi : \mathbb{C}[t, t^{-1}] \subseteq \mathbb{C}[t^{\mathbb{Q}}]$ where

$$\mathbb{C}[t^{\mathbb{Q}}] := \{\sum_{i \in \mathbb{Q}} a_i t^i \mid a_i \in \mathbb{C} \text{ and all but finitely many } a_i \text{ are zero}\}.$$

   Show that primes $\mathfrak{p}$ such that $\phi^{-1}\mathfrak{p} = \langle t - a\rangle$ are in bijection with $\widehat{\mathbb{Z}} = \lim_n \mathbb{Z}/n$. Hint.[4]

   In other words, there are $\#\widehat{\mathbb{Z}}$ points in the fibre of $\mathrm{Spec}(\phi) : \mathrm{Spec}(\mathbb{C}[t^{\mathbb{Q}}]) \to \mathrm{Spec}(\mathbb{C}[t, t^{-1}])$ at $t = a$.

The idea behind proetale cohomology is to take the lim in $H^r_{et}(X, \mathbb{Q}_\ell) := \left(\lim_n H^r_{et}(X, \mathbb{Z}/\ell^n)\right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and move it into the category of schemes (notice that $\mathrm{Spec}(\mathbb{C}[t^{\mathbb{Q}}]) = \lim_n \mathrm{Spec}(\mathbb{C}[t^{1/n}, t^{-1/n}])$). So the lim is then dealt with geometrically, instead of homologically. Then one can recover $H^r_{et}(X, \mathbb{Q}_\ell)$ directly as $H^r_{proet}(X, \mathbb{Q}_\ell)$; which is not built articificially from a limit of sheaf cohomology groups, but is directly a sheaf cohomology group itself.

---

[2] These are awkward because one works with categories defined up to equivalence, not isomorphism. So the universal property of the limit has to take into account isomorphisms in each of the factors $D(X, \mathbb{Z}/\ell^n)$.

[3] For an nth root of unity ζ consider the ring homomorphism $\mathbb{C}[t, t^{-1}] \to \mathbb{C}$; $t \mapsto \zeta a$.

[4] Consider the abelian group $\mathbb{Z}/n$ as the multiplicative group of nth roots of unity in $\mathbb{C}$. So an element of $\widehat{\mathbb{Z}}$ is a system $(\zeta_n)_{n \in \mathbb{N}}$ of $\zeta_n \in \mathbb{C}$ such that $\zeta_1 = 1$ and $\zeta_{rm}^r = \zeta_m$ for all $r, m \in \mathbb{N}$. Given such a system, show that there is a well-defined ring homomorphism $\mathbb{C}[t^{\mathbb{Q}}] \to \mathbb{C}$ sending $t^{1/n}$ to $\zeta_n a$.