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 $X$, how many solutions do $f_1, \dots, f_c$ have in $\mathbb{F}_{q^n}$ for each $n$?

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

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

**Exercise 1.** Applying log and using the identity $\log(1-T)^{-1} = \sum_{n=1}^{\infty} T^n/n$, prove the equality $(*)$.

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

**Remark 4.** For any sequence of closed subsets $Y_0 \subset Y_1 \subset \cdots \subset Y_n = X$, it follows from the sum description 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 $\zeta(X,s) = \prod_{p \text{ prime}} (1-p^{-s})^{-1}$ but we will not say much about this.

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 $\phi_\ell : T_\ell E \to T_\ell E$ of the Frobenius $\phi$ on the Tate module $T_\ell E = \varprojlim_n \ker(E \xrightarrow{\ell^n} E)$ one can calculate

$$|E(\mathbb{F}_{q^n})| = \deg(1 - \phi^n) = \det(1 - \phi_\ell^n) = 1 - \alpha^n - \beta^n + q^n$$

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".

After calculating many examples Weil made the following conjectures:

**Theorem 12** (Weil conjectures)**.** *Suppose $X$ is a 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 $\mathfrak{p}$, and the complex projective variety $X(\mathbb{C})$ defined by the $f_i$ is smooth. 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.

**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

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 $H^0(M, \mathbb{Q}), H^1(M, \mathbb{Q}), H^2(M, \mathbb{Q}), \dots$. The dimension of the $i$th 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 14.** If $M = S^m = \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_1^2 + \dots + x_n^2 = 1\}$ 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 15.** If $M$ is a sphere with $n$ handles, then

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

The case $n = 2$ is the surface of a doughnut. 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 16.** 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 $i > 2\dim_{\mathbb{C}} X(\mathbb{C})$.
2. (Functoriality) For any continuous map $\phi : M \to N$, there are induced maps $\phi_i : H^i(M, \mathbb{Q}) \to H^i(N, \mathbb{Q})$ compatible with composition.
3. (Poincaré Duality) There is a canonical isomorphism $H^{\dim M}(M, \mathbb{Q}) \cong \mathbb{Q}$, and a natural perfect pairing
$$H^i(M, \mathbb{Q}) \times H^{\dim M - i}(M, \mathbb{Q}) \to H^{\dim M}(M, \mathbb{Q}).$$
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
$$\#\{\text{ fixed points }\} = \sum_{i=0}^{n} (-1)^i \mathrm{tr}(\phi_i).$$

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

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

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

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

Combining this with

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

valid for any matrix $A$, we get

$$Z(X,t) = \prod_{i=0}^{2\dim X} \det(1-\phi_i \cdot t)^{(-1)^{i+1}}$$

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 $P_i(t) = \det(1-\phi_i \cdot t)$, and if so, then the second part is reformulated as: the eigenvalues of $\phi_i$ have absolute value $q^{-i/2}$.

# 3 Fundamental group

Notice that in the Zariski topology, every non-empty open subsets of a smooth connected variety is dense. Consequently, the sheaf cohomology groups $H^n(X, \mathbb{Q})$ are zero for all $n > 0$. So we need a more sophisticated cohomology.

Leaving cohomology alone for a moment, lets consider the fundamental group. Note that for smooth manifolds $M$, there is a canonical morphism

$$\pi_1(M) \to H_1(M)$$

and if $M$ is path connected then the Hurewicz Theorem says

$$\frac{\pi_1(M)}{[\pi_1(M), \pi_1(M)]} \xrightarrow{\sim} H_1(M),$$

and $H_1(M)$ is dual to $H^1(M)$ when $M$ is compact and oriented (e.g., if $M$ comes from a smooth projective variety). So if we can find a good algebraic version of the fundamental group, this might give some indication how to build cohomology groups.

Recall:

**Definition 17.** *The* fundamental group *of a smooth manifold $M$ is*

$$\pi_1(M,m) = \hom_{cont.}([0,1],(M,m))/\hom_{cont.}([0,1]^2,(M,m)).$$

That is, loops from $m$ to $m$, modulo homotopy.

$- - -$ picture of a loop and a contraction $- - -$

The first problem with this definition in the world of varieties is that $[0,1]$ is not algebraic. We could observe that extending $[0,1] \subseteq \mathbb{A}^1(\mathbb{C})$ gives the same groups, and try and use $\mathbb{A}^1$. But this is still no good. Topologically, for a complete elliptic curve $E$, we have $E(\mathbb{C}) \cong S^1 \times S^1$, but every algebraic map $\mathbb{A}^1 \to E$ is constant.

Lets use a different description of the fundamental group.

**Theorem 18.** *Let $M$ be a smooth (connected) manifold, and $\widetilde{M} \to M$ a smooth morphism of relative dimension zero such that $\widetilde{M}$ is contractible. Then*

$$\pi_1(M) \cong Aut(\widetilde{M}/M).$$

−−− picture of S1, universal cover, and a loop going to an automorphism −−−

Smooth morphisms can be defined algebraically, but contractibility cannot (yet). However, if we don't mind passing to the completion, we are ok.

**Theorem 19.** *Let $M$ be a smooth (connected) manifold, and consider the category of all finite, smooth, relative dimension zero morphisms $N \to M$.*

$$\pi_1(M)^\vee \cong \varprojlim_{N \to M} Aut(N/M).$$

−−− picture of S1, universal cover, and a loop going to an automorphism −−−

This leads to a useful notion of fundamental group.

**Definition 20.** *Let $X$ be a smooth variety and consider the category of finite, smooth, relative dimension zero morphisms $Y \to X$. Define*

$$\pi_1^{et}(X) = \varprojlim_{Y \to X} Aut(Y/X).$$

A consequence of the Riemann Existence Theorem is the following.

**Theorem 21.** *Let $X$ be a smooth $\mathbb{C}$-variety. Then*

$$\pi_1^{et}(X) \cong \pi_1(X(\mathbb{C}))^\vee$$

Moreover, this étale fundamental group contains arithmetic information.

**Proposition 22.** *Let $k$ be a field with algebraic closure $\overline{k}$. Then*

$$\pi_1^{et}(k) \cong Gal(\overline{k}/k)$$

# 4 Cohomology via local homeomorphisms

**Remark 23** (This remark may not appear in the lecture)**.** What does the Hurewicz Theorem look like now? A finite smooth morphism $N \to M$ is called *Galois* if $|Aut(N/M)| = \deg N$. In this case there is a canonical[1] isomorphism $N \times_M N \cong \amalg_{Aut} N$. Let $\Lambda$ be any abelian group. When $N$ is connected, set morphisms $N \times_M N \to \Lambda$ are in bijection with global sections of the constant sheaf $\Gamma(N \times_M N, \Lambda)$. One can check that a function $N \times_M N \to \Lambda$ corresponds to a group homomorphism $\phi : Aut(N) \to \Lambda$ if and only if the corresponding section $\sigma_\phi \in \Gamma(N \times_M N, \Lambda)$ is a cocycle. Moreover, the morphism $\phi$ is trivial if and only if the section $\sigma_\phi$ comes from $\Gamma(N, \Lambda)$. So we see that $\hom(Aut(N), \mathbb{Z}/n) \cong \check{H}^1(N/M, \Lambda)$, where $\check{H}^\bullet(N/M, \Lambda)$ is the cohomology of the complex associated to

$$\substack{\to\\\to\\\to\\\to} N \times_M N \times_M N \substack{\to\\\to\\\to} N \times_M N \rightrightarrows N.$$

Note how similar this looks to Čech cohomology, which for a covering $\{U_i \to M\}_{i \in I}$ is the complex associated to $\substack{\to\\\to\\\to\\\to} U \times_M U \times_M U \substack{\to\\\to\\\to} U \times_M U \rightrightarrows U$ where $U = \amalg U_i$.

All of this suggests that we should be working with smooth relative dimension zero morphisms.

**Definition 24.** *A smooth relative dimension zero morphism $f : Y \to X$ is called* étale*.*

To give more support for this idea, notice that the inverse function theorem now holds:

**Proposition 25.** *Let $f : Y \to X$ be a smooth morphism of varieties. Then for every $y \in Y$, there exists an étale morphism $j : U \to X$, a point $u \in U$ with $j(u) = f(y)$, and a factorisation*

$$\begin{tikzcd} & Y \arrow[d] \\ U \arrow[r] \arrow[ur, dashed] & X \end{tikzcd}$$

**Exercise 3.** Prove the above proposition when $Y \to X$ is of relative dimension zero.

Moreover, just as locally every manifold looks like $\mathbb{R}^n$, étale locally every smooth variety looks like $\mathbb{A}^n$:

**Proposition 26.** *If $X$ is a smooth variety of dimension $n$, then for every $x \in X$, there exists an open subset $U \ni x$, and an étale morphism $U \to \mathbb{A}^n$.*

**Exercise 4** (Advanced)**.** Prove the above proposition when $X$ is of dimension one. Hint: use the fact that each $\mathcal{O}_{X,x}$ is a discrete valuation ring.

[1]The diagonal $N \to N \times_M N$ is a canonical choice of connected component, and then $Aut$ acting on the right of $N \times_M N$ permutes the components.

The above suggest that we should consider étale morphisms as “unwrapped” open subsets.

Now notice that the definition of a sheaf only the structure of the poset of open sets, and nothing to do with the fact that they are subsets:

**Definition 27.** *A functor $F : Open(M)^{op} \to Ab$ is a sheaf, if for every open subset $V \subseteq M$ and every open cover $\{U_i \to V\}_{i\in I}$ the sequence*

$$0 \to F(V) \to \prod_{i\in I} F(U_i) \to \prod_{i,j\in I} F(U_i \times_V U_j)$$

*is exact.*

Finally, we arrive at the definition of an étale sheaf.

**Definition 28.** *Let $X$ be a scheme, and $Et(X)$ the category of étale morphisms $V \to X$. A functor $F : Et(X)^{op} \to Ab$ is an étale sheaf, if for every $V \in Et(X)$, and every jointly surjective family $\{U_i \to V\}_{i\in I}$ in $Et(X)$, the sequence*

$$0 \to F(V) \to \prod_{i\in I} F(U_i) \to \prod_{i,j\in I} F(U_i \times_V U_j)$$

*is exact.*