# Weil conjectures and Betti numbers of moduli spaces

Christopher Lazda

## 1 Lecture 1

Let's start with an object you'll hopefully all be reasonably familiar with.

$$\zeta(s) = \sum_{n\geq 1} n^{-s},\ s\in\mathbb{C},\ \mathrm{Re}(s)>1.$$

**Conjecture** (RH). *If* $\zeta(s)=0$ *and* $0<\mathrm{Re}(s)<1$, *then* $\mathrm{Re}(s)=\frac{1}{2}$.

This has an Euler product expansion

$$\zeta(s) = \prod_{p \text{ prime}} (1-p^{-s})^{-1}$$

and we note that

$$\{\text{prime numbers}\} \leftrightarrow \{\text{closed points of } \mathrm{Spec}(\mathbb{Z})\}$$

so we can write

$$\zeta(s) = \prod_{x\in|\mathrm{Spec}(\mathbb{Z})|} (1-\#k(x)^{-s})^{-1}$$

where $k(x)$ is the residue field at $x$.

**Definition.** For any scheme $X$ of finite type over $\mathbb{Z}$, (i.e. any "arithmetic scheme") we define

$$\zeta_X(s) = \prod_{x\in|X|} (1-\#k(x)^{-s})^{-1}$$

the product being taken over all closed points, and $k(x)$ denotes the residue field.

*Exercise.* Show that in this situation $k(x)$ is always a finite field, so the definition makes sense.

*Example.* Suppose that $K/\mathbb{Q}$ is finite, with ring of integers $\mathcal{O}_K$. Then taking $X=\mathrm{Spec}(\mathcal{O}_K)$ we get

$$\zeta_{\mathrm{Spec}(\mathcal{O}_K)}(s) = \prod_{\mathfrak{p}\subset\mathcal{O}_K} (1-N\mathfrak{p}^{-s})^{-1}$$

which is the usual Dedekind zeta function $\zeta_K(s)$ of $K$. There is also a Riemann hypothesis for $\zeta_K$, again stating that zeroes of $\zeta_K$ with $0<\mathrm{Re}(s)<1$ satisfy $\mathrm{Re}(s)=\frac{1}{2}$.

*Example.* $X=\mathbb{A}^1_{\mathbb{F}_p}=\mathrm{Spec}\left(\mathbb{F}_p[\![t]\!]\right)$.

$$\left\{\text{closed points of } \mathbb{A}^1_{\mathbb{F}_p}\right\} \leftrightarrow \left\{\text{irreducible polynomials over } \mathbb{F}_p\right\}$$

$$\Rightarrow \zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(s) = \prod_{d\geq 1}(1-p^{-ds})^{-N_d}$$

where $N_d$ = # irreducible polynomials of degree $d$. Let's try the following trick: set $u = p^{-s}$ and compute $uZ'(u)/Z(u)$ where $Z(u) = \prod_d (1-u^d)^{-N_d}$. We get

$$\begin{aligned} u\frac{d}{du}\log Z(u) &= \sum_{d\geq 1} \frac{dN_d u^d}{1-u^d} \\ &= \sum_{d,m\geq 1} dN_d u^{md} \\ &= \sum_{n\geq 1}\sum_{d|n} dN_d u^n \\ &= \sum_{n\geq 1} p^n u^n \end{aligned}$$

since (recall from Galois theory) $\sum_{d|n} dN_d = p^n$. Note that $p^n = \#\mathbb{A}^1_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ and that we also have

$$\begin{aligned} \frac{d}{du}\log Z(u) &= \frac{p}{1-pu} \\ \Rightarrow Z(u) &= \frac{1}{1-pu} \\ \Rightarrow \zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(s) &= \frac{1}{1-p^{1-s}}. \end{aligned}$$

This trivially satisfies the 'Riemann Hypothesis', since it has no zeroes.

**Lemma.** *Let $q$ be a prime power, and $X$ a scheme of finite type over $\mathbb{F}_q$ (therefore $X$ is a scheme of finite type over $\mathbb{Z}$ and has a zeta function). Write $B_n = \#X(\mathbb{F}_{q^n})$. Then we have*

$$\zeta_X(s) = \exp\left(\sum_{n\geq 1} \frac{B_n}{n} u^n\right)$$

*where $u = q^{-s}$*

*Proof.* Let $N_d$ be the number of closed points of $X$ of degree $d$ over $\mathbb{F}_q$, i.e. such that the residue field $k(x)$ is $\mathbb{F}_{q^d}$. Then we have the formula

$$\sum_{d|n} dN_d = B_n$$

since every closed point of degree $d$ gives rise to exactly $d$ points in $X(\mathbb{F}_{q^n})$ for $d \mid n$. Then exactly as in the calculation we've just done we can show

$$\zeta_X(s) = \prod_{d\geq 1} (1-u^d)^{-N_d}$$

where $u = q^{-s}$ and that if we let $Z(u) = \prod_{d\geq 1}(1-u^d)^{-N_d}$ then we have an identity of power series

$$u\frac{d}{du}\log Z(u) = \sum_{n\geq 1} B_n u^n$$

and the lemma follows. □

*Exercise.* By showing that when $X/\mathbb{F}_q$ has dimension $d$, $\#X(\mathbb{F}_{q^n}) = O(q^{nd})$ as $d \to \infty$, show that $\zeta_X(s)$ converges for $\mathrm{Re}(s) > \dim X$.

So zeta function of schemes over finite fields 'encode' the numbers of points over all finite extension fields, in that if you know one, you know the other. It's in practise often easier to work with the power series

$$Z(X,u) := \exp\left(\sum_{n\geq 1} \frac{\#X(\mathbb{F}_{q^n})}{n} u^n\right) \in \mathbb{Q}[\![u]\!].$$

Note that while the $\zeta$-function $\zeta_X(s)$ doesn't 'see' the base field $\mathbb{F}_q$, the $Z$-function $Z(X,u)$ does, since we have set $u = q^{-s}$.

### 1.1 Abelian Varieties

Now let's take $A/\mathbb{F}_q$ an abelian variety of dimension $g$, that is a smooth, projective, (geometrically) connected group variety over $\mathbb{F}_q$. We'll let $\overline{A} = A \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, and $F : \overline{A} \to \overline{A}$ be the $q$-power linear Frobenius morphism, that is if we have some projective embedding

$$\overline{A} \to \mathbb{P}^N_{\overline{\mathbb{F}}_q}$$

then in homogeneous co-ordinates we have $F(x_0 : \ldots : x_N) = (x_0^q : \ldots : x_N^q)$.

Therefore $A(\mathbb{F}_{q^n})$ is exactly the (closed) fixed points of $F^n$, or in other words, if we consider the isogeny

$$\Phi_n = \mathrm{id} - F^n : \overline{A} \to \overline{A}$$

then $A(\mathbb{F}_{q^n}) = \ker(\Phi_n)(\overline{\mathbb{F}}_q)$. Since $\mathrm{id} - F^n$ *separable*, we therefore have

$$\#A(\mathbb{F}_{q^n}) = \deg(\mathrm{id} - F^n).$$

To calculate this, we'll introduce the Tate module of $A$. Let $\ell \nmid q$ be a prime, so that $A[\ell^n]$ is an étale group scheme over $\mathbb{F}_q$ of order $\ell^{n2g}$, and

$$A[\ell^n](\overline{\mathbb{F}}_q) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$$

(non-canonically). The multiplication by $\ell$ induces transition maps

$$[\ell] : A[\ell^n](\overline{\mathbb{F}}_q) \to A[\ell^{n-1}](\overline{\mathbb{F}}_q)$$

so we can form the inverse limit

$$T_\ell(A) := \varprojlim_n A[\ell^n](\overline{\mathbb{F}}_q),$$

this is a free $\mathbb{Z}_\ell$-module of rank $2g$, and every endomorphism $\psi \in \mathrm{End}(\overline{A})$ of $\overline{A}$ induces an endomorphism $\psi_\ell$ of $T_\ell(A)$, and hence of $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

**Theorem** (See Mumford's "Abelian Varieties"). *For every endomorphism $\psi \in \mathrm{End}(\overline{A})$ there exists a unique polynomial $P_\psi(t) \in \mathbb{Z}[t]$ (the characteristic polynomial of $\psi$) such that for all integers $n$ we have*

$$P_\psi(n) = \deg([n] - \psi).$$

*Moreover for any $\ell \nmid q$ we have that*

$$P_\psi(t) = \det(t - \psi_\ell)$$

*is the characteristic polynomial of $\psi_\ell$ acting on $V_\ell(A)$.*

We're now going to take $\psi = F$, the Frobenius endomorphism, this tells us that if we let

$$P_F(t) = \prod_{i=1}^{2g}(t - \omega_j)$$

be the characteristic polynomial of $F$ acting on $V_\ell(A)$, and $n \geq 1$, then

$$P_{F^n}(t) = \prod_{i=1}^{2g}(t - \omega_j^n)$$

is the characteristic polynomial of $F^n$ acting on $V_\ell(A)$ and hence we can count the number of $\mathbb{F}_{q^n}$-rational points on $A$ as

$$\begin{aligned}\#A(\mathbb{F}_{q^n}) = \deg(\mathrm{id} - F^n) = P_{F^n}(1) &= \prod_{i=1}^{2g}(1 - \omega_j^n)\\ &= 1 - \sum_{j_1} \omega_{j_1}^n + \sum_{j_1, j_2} \omega_{j_1}^n \omega_{j_2}^n - \ldots + \omega_{j_1}^n \ldots \omega_{j_{2g}}^n.\end{aligned}$$

Actually, some simple linear algebra tells us that

$$\sum_{j_1,\ldots,j_k} \omega_{j_1}^n \ldots \omega_{j_k}^n$$

is exactly the trace of $F^n$ acting on $\Lambda^k V_\ell(A)$, so we can write

$$\#A(\mathbb{F}_{q^n}) = \sum_{k=0}^{2g} (-1)^k \mathrm{Tr}(F^n \mid \Lambda^k V_\ell(A)).$$

Substituting this in to the expression for $Z(A,u)$ gives us

$$Z(A,u) = \prod_{k=0}^{2g} \exp\left(-\sum_{n\geq 1} \mathrm{Tr}(F^n \mid \Lambda^k V_\ell(A) \frac{u^n}{n}\right)^{(-1)^{k+1}}$$

**Lemma.** *Let $V$ be a finite dimensional vector space over a field $K$, and $\varphi : V \to V$ and endomorphism. Then*

$$\det\left(\mathrm{id} - \varphi u\right) = \exp\left(-\sum_{n\geq 1} \mathrm{Tr}(\varphi^n) \frac{u^n}{n}\right).$$

*Proof.* Exercise (hint: express both sides in terms of the eigenvalues of $\varphi$). □

So we can therefore write the $Z$-function of $A$ as

$$\begin{aligned}Z(A,u) &= \prod_{k=0}^{2g} \det(\mathrm{id} - Fu \mid \Lambda^k V_\ell(A))^{(-1)^{k+1}}\\ &= \frac{P_1(t)\ldots P_{2g-1}(u)}{P_0(u)\ldots P_{2g}(u)}\end{aligned}$$

where

$$P_k(t) = \det(\mathrm{id} - Fu \mid \Lambda^k V_\ell(A)) \in \mathbb{Z}[u]$$

can be written as $\prod_i (1 - \alpha_{ik} u)$ with $\alpha_{ik}$ running over things of the form $\omega_{j_1} \dots \omega_{j_k}$.

**Theorem** (Riemann Hypothesis)**.** *Each $\omega_j$ has norm $q^{1/2}$.*

*Exercise.* What does this tell us about the zeroes of $\zeta_A(s) = Z(A, q^{-s})$?

*Exercise.* We expect a functional equation

$$Z(A, (q^g u)^{-1}) = Z(A, u)$$

can you interpret this in terms of a statement about the $\omega_j$?

## 2 Lectures 2 & 3

James told you about the Weil conjectures, and said that a 'good' cohomology theory for varieties over $\overline{\mathbb{F}}_q$ would imply them more or less formally. Let's look at that in a bit more detail.

### Weil cohomology theories

**Definition.** Fix an algebraically closed field $k$ and let $\mathcal{V}_k$ be the category of smooth, projective, connected varieties over $k$, that is non-singular, connected varieties cut out by homogenous equations in some $\mathbb{P}^N(k)$. Let $K$ be a field of characteristic 0. A $K$-valued Weil cohomology theory is a contravariant functor

$$\begin{aligned} H^*(-) : \mathcal{V}_k &\to \{\text{graded vector spaces over } K\} \\ X &\mapsto H^*(X) \\ f : X \to Y &\mapsto f^* : H^*(Y) \to H^*(X) \end{aligned}$$

together with a graded commutative product

$$\cup : H^i(X) \otimes_K H^j(X) \to H^{i+j}(X)$$

a trace morphism

$$\mathrm{Tr} : H^{2\dim X}(X) \to K$$

and a cycle class map

$$\mathrm{cl} : C^r(X) \to H^{2r}(X)$$

such that:

i) $H^i(X)$ is finite dimensional, and zero outside the range $[0, 2\dim X]$.

ii) (Künneth formula) if we let $p_1, p_2 : X \times Y \to X, Y$ denote the two projections, then the natural map

$$\begin{aligned} H^*(X) \otimes_K H^*(Y) &\to H^*(X \times Y) \\ \alpha \otimes \beta &\mapsto \alpha \boxtimes \beta := p_1^*(\alpha) \cup p_2^*(\beta) : \end{aligned}$$

is an isomorphism.

iii) (Poincaré duality) For $X$ of dimension $n$, cup product follows by the trace map induces a perfect pairing

$$H^i(X) \otimes_K H^{2n-i}(X) \to H^{2n}(X) \cong K$$

iv) For $X$, $Y$ of dimension $n, m$ respectively, and $\alpha \in H^{2n}(X)$, $\beta \in H^{2m}(Y)$ we have

$$\mathrm{Tr}_{X \times Y}(\alpha \boxtimes \beta) = \mathrm{Tr}_X(\alpha)\mathrm{Tr}_Y(\beta)$$

v) Suppose that $Z \subset X$ and $W \subset Y$ are irreducible closed subvarieties. Then

$$\mathrm{cl}(Z \times W) = \mathrm{cl}(Z) \boxtimes \mathrm{cl}(W)$$

vi) Let $f : X \to Y$ be a morphism in $\mathcal{V}_k$, and $Z \subset X$ irreducible. Let $m = \deg(Z/f(Z))$. Then for all $\alpha \in H^{2\dim Z}(Y)$ we have

$$\mathrm{Tr}_X(\mathrm{cl}(Z) \cup f^*(\alpha)) = m\mathrm{Tr}_Y(\mathrm{cl}(f(Z)) \cup \alpha)$$

vii) $f : X \to Y$ and $Z \subset X$ as above. Then under suitable conditions on $f, Z$ we have

$$f^* \mathrm{cl}(Z) = \mathrm{cl}(f^{-1}(Z))$$

viii) If $X = x$ is a point, then $\mathrm{Tr}_x(\mathrm{cl}(x)) = 1$.

*Remark.* Actually one can show from the axioms that the cycle class map induces a ring homomorphism

$$A^*(X) \to H^*(X)$$

where $A^*(X)$ is cycles module rational equivalence.

*Example.* i) The prototypical example is for $k = \mathbb{C}$, $K = \mathbb{Q}$ and $H^i(X)$ is just the usual singular cohomology of algebraic varieties over $\mathbb{C}$ (with the topology induced by the natural topology on $\mathbb{A}^n(\mathbb{C}) \cong \mathbb{C}^n$).

ii) For abelian varieties and $k$ arbitrary, then $V_\ell(A)$ is a way to construct a $\mathbb{Q}_\ell$-valued version of $H_1(A)$, for $\ell \neq \mathrm{char}(k)$, we therefore take $H^1(A) := V_\ell(A)^\vee$. Any abelian variety over $\mathbb{C}$ is $\cong \mathbb{C}^g/L$ for some lattice $L \cong \mathbb{Z}^{2g}$ and topologically we have $H^i(A) \cong \Lambda^i H^1(A)$. For general $A/k$ we therefore set $H^i(A) = \Lambda^i V_\ell(A)^\vee$. Then our expression for the zeta function of $A$ defined over $\mathbb{F}_q$ last week looked like

$$Z(A, u) = \prod_{k=0}^{2g} \det(1 - Fu \mid H_k(A))^{(-1)^{k+1}}$$

and 'Poincaré duality' allows us to write this as

$$Z(A, u) = \prod_{k=0}^{2g} \det(1 - Fu \mid H^k(A))^{(-1)^{k+1}}.$$

Actually, $A \mapsto H^i(A)$ can be extended to a Weil cohomology theory with values in $\mathbb{Q}_\ell$ for any algebraically closed field of characteristic $\neq \ell$. This involves a huge amount of hard work!

The basic approach is to completely redefine what constitutes a topology - the idea is that for the purposes of sheaf theory it is the 'category' of open sets of a topological space that matter more than the actual space itself. The main object of study in this approach is then the 'étale topology for schemes' where an 'open set' of some variety $X$ is a morphism $U \to X$ which locally looks like an unramified cover. We can do sheaf theory for this topology, and hence define the 'étale cohomology $H^i_{\text{ét}}(X, A)$ of varieties' which for finite coefficients like $\mathbb{Z}/n\mathbb{Z}$ behaves very much like the singular cohomology of complex manifolds. Actually for complex varieties, it gives exactly the same answer as singular cohomology.

To get well behaved groups over $\mathbb{Q}_\ell$, we take

$$H^i_{\text{ét}}(X, \mathbb{Z}_\ell) = \varprojlim_n H^i_{\text{ét}}(X, \mathbb{Z}/\ell^n)$$
$$H^i_{\text{ét}}(X, \mathbb{Q}_\ell) = H^i_{\text{ét}}(X, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

giving a characteristic zero theory.

iii) Suppose that $k$ has characteristic zero, and let $X$ be a smooth *affine* variety over $k$, so that $X$ is the zero set inside $\mathbb{A}^n(k)$ of some polynomials $f_1, \ldots, f_r$. Let $A = \mathcal{O}(X)$ be the ring of functions on $X$, that is $k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$.

Define the module of differentials

$$\Omega^1_A = \frac{Adx_1 \oplus \ldots \oplus Adx_n}{(df_1, \ldots, df_r)}$$

where for $f$ some polynomial we set $df = \sum_i \frac{df}{dx_i} dx_i$. This is an 'algebraic' construction of differential forms on $X$, and is a finitely generated $A$-module by construction. There is a natural map $d : A \to \Omega^1_A$ given again by $df = \sum_i \frac{df}{dx_i} dx_i$. Let $\Omega^p_A = \Lambda^p Omega^1_A$ be the $p$th exterior power, then the Leibniz rule

$$d(f\omega_1 \wedge \ldots \wedge \omega_p) = df \wedge \omega_1 \wedge \ldots \wedge \omega_p,\ f \in A, \omega_i \in \Omega^1_A$$

gives a map

$$\Omega^p_A \to \Omega^{p+1}_A$$

and we get a complex

$$0 \to A \to \Omega^1_A \to \ldots.$$

We define the de Rham cohomology

$$H^i_{\text{dR}}(X) = H^i(\Omega^*_A).$$

*Example.* Let $X = \mathbb{A}^1(k)$, so that $A = k[x]$. Then $\Omega^1_A = k[x]dx$ and $\Omega^i_A = 0$ for $i > 0$. Then the cohomology of the complex

$$0 \to k[x] \overset{f \mapsto \frac{df}{dx} dx}{\to} k[x]dx \to 0$$

is just $k$ in degree 0, so that

$$H^0_{\text{dR}}(\mathbb{A}^1(k)) = k,\ H^i_{\text{dR}}(\mathbb{A}^1(k)) = 0 \text{ for } i > 0$$

*Example.* Now suppose that $X = V(xy-1) \subset \mathbb{A}^2(k) \cong \mathbb{A}^1(k) \setminus \{0\}$, so that $A = k[x,x^{-1}]$. Then we have $\Omega^1_A = k[x,x^{-1}]dx$ and the de Rham cohomology of $X$ is the cohomology of

$$0 \to k[x,x^{-1}] \to k[x,x^{-1}]dx \to 0.$$

Again we have $H^0_{\mathrm{dR}}(X) = k$, but we can't integrate $x^{-1}$ algebraically, so $H^1_{\mathrm{dR}}(X)$ is non-zero. In fact, you can check that $H^1_{\mathrm{dR}}(X)$ is one dimensional, generated by the class of $x^{-1}$.

To extend this to projective varieties, we need to glue. I'll show you how to do this for $\mathbb{P}^1$. First of all we write $\mathbb{P}^1(k) = U_0 \cup U_1$, where $U_i$ is a copy of $\mathbb{A}^1(k)$ with co-ordinate $x_i$, say. Let $A_i = \mathcal{O}(U_i)$ and $B = \mathcal{O}(U_0 \cap U_1)$, so that there are 'restriction maps'

$$\Omega^*_{A_i} \to \Omega^*_B.$$

Then the general formula for calculating the de Rham cohomology of $\mathbb{P}^1(k)$ is as the cohomology of the total complex

$$\Omega^*_{A_0} \oplus \Omega^*_{A_1} \to \Omega^*_B$$

So the de Rham cohomology of $\mathbb{P}^1(k)$ is the cohomology of

$$0 \to k[x_0] \oplus k[x_1] \to k[x_0]dx_0 \oplus k[x_1]dx_1 \oplus k[x_0,x_0^{-1}] \to k[x_0,x_0^{-1}]dx_0 \to 0,$$

recall that on $U_0 \cap U_1$ we have $x_1 = x_0^{-1}$ so the map $k[x_1]dx_1 \to k[x_0,x_0^{-1}]dx_0$ sends $x_1$ to $x_0^{-1}$ and $dx_1$ to $-x_0^{-2}dx_0$. So we can calculate this as

$$H^0_{\mathrm{dR}}(\mathbb{P}^1(k)) = k,\ H^1_{\mathrm{dR}}(\mathbb{P}^1(k)) = 0,\ H^2(\mathbb{P}^1(k)) = k.$$

iv) Now suppose that $k = \overline{\mathbb{F}}_q$. Then the approach we're going to try to take to give a Weil cohomology theory for varieties over $k$ is to 'lift' them to characteristic 0 and then use de Rham cohomology. Actually, we're going to work with finitely generated algebras $A \cong k[x_1,\dots,x_n]/(f_1,\dots,f_r)$ over $\mathbb{F}_q$ such that the associated affine variety over $\overline{\mathbb{F}}_q$ is non-singular to get a theory for smooth affine varieties defined over $\mathbb{F}_q$, we can then 'glue' to get a theory for projective varieties.

### Weil cohomologies ⇒ Weil conjectures

**Theorem.** *Suppose that a Weil cohomology theory exists for $k = \overline{\mathbb{F}}_q$. Then the rationality and functional equation part of the Weil conjectures are true.*

The difficult part of this is in proving the following version of the Lefschetz trace formula.

**Proposition.** *Let $H^*(-)$ be a Weil cohomology theory over some algebraically closed field $k$, and $f : X \to X$ an endomorphism of some $X \in \mathcal{V}_k$. Let $\Delta, \Gamma_f \subset X \times X$ be the diagonal and the graph of $f$ respectively. Then*

$$\Delta \cdot \Gamma_f = \sum_i (-1)^i \mathrm{Tr}(f \mid H^i(X)),$$

*and if $\Gamma_f$ and $\Delta$ intersect properly ('$f$ has isolated fixed points') then the LHS is just the number of fixed points of $f$.*

*Remark.* This is why we need $K$ of characteristic 0 - if $K$ had characteristic $p$, we would only be able to count fixed points mod $p$.

*Proof.* Let $n = \dim X$ and fix a basis $e^i_j$ of $H^i(X)$, with dual basis $f^{2n-i}_j$ of $H^{2n-i}(X)$, that is

$$\mathrm{Tr}_X(e^i_j \cup f^{2n-i}_k) = \delta_{jk}.$$

The class of $\Gamma_f$ lies in $H^{2n}(X \times X) = \bigoplus_{i=0}^{2n} H^i(X) \otimes_K H^{2n-i}(X)$ and it can be shown that we can calculate this class as

$$\mathrm{cl}(\Gamma_f) = \sum_{i=0}^{2n} \sum_j f^*(e^i_j) \boxtimes f^{2n-i}_j.$$

We can therefore similarly (using graded commutativity) write

$$\mathrm{cl}(\Delta) = \sum_{i=0}^{2n} (-1)^i \sum_j f^{2n-i}_j \boxtimes e^i_j.$$

Now, for any point $x \in X$ we have $\mathrm{Tr}_X(\mathrm{cl}(x)) = \mathrm{Tr}_x(\mathrm{cl}(x)) = 1$ from the axioms for a Weil cohomology theory, and hence the fact that $A^*(X) \to H^*(X)$ is a ring homomorphism implies that for any two subvarieties $Z, W \subset X$ of complementary codimension that

$$Z \cdot W = \mathrm{Tr}_X(\mathrm{cl}(Z) \cup \mathrm{cl}(W))$$

and hence applying this to $\Delta, \Gamma_f \subset X \times X$ we get

$$\begin{aligned}\Delta \cdot \Gamma_f &= \sum_{i=0}^{2n} (-1)^i \mathrm{Tr}_{X \times X} \left( \sum_{j,k} (f^*(e^i_j) \cup f^{2n-i}_k) \boxtimes (f^{2n-i}_j \cup e^i_k) \right) \\ &= \sum_{i=0}^{2n} (-1)^i \sum_{j,k} \mathrm{Tr}_X(f^*(e^i_j) \cup f^{2n-i}_k) \delta_{jk} \\ &= \sum_{i=0}^{2n} (-1)^i \sum_j \mathrm{Tr}_X(f^*(e^i_j) \cup f^{2n-i}_j) \\ &= \sum_{i=0}^{2n} (-1)^i \mathrm{Tr}(f \mid H^i(X))\end{aligned}$$

where the last equality follows from a simple statement in linear algebra. □

So (modulo showing that Frobenius 'has isolated fixed points') this proposition implies that

$$X(\mathbb{F}_{q^n}) = \sum_i (-1)^i \mathrm{Tr}(F^n \mid H^i(X))$$

and *exactly* the same manipulation that we did last time then shows that

$$Z(X, u) = \prod_i \det(1 - Fu \mid H^i(X))^{(-1)^{i+1}}.$$

Before we prove the functional equation, we need a linear algebra lemma.

**Lemma.** *Let $V \times W \to K$ be a perfect pairing of $K$-vector spaces of dimension $r$, and $\psi, \phi, \lambda$ endomorphisms of $V, W, K$ respectively compatible with the pairing (note that $\lambda \in K$). Then*

$$\det(1 - \psi u | W) = \frac{(-\lambda u)^r}{\det(\phi | V)} \det(1 - \phi(\lambda u)^{-1} | V)$$

*and*

$$\det(\psi \mid W) = \lambda^r \det(\phi | V)^{-1}.$$

*Proof.* Exercise. □

**Corollary.** *Suppose that a Weil cohomology theory exists over $\overline{\mathbb{F}}_q$. Then the $Z$-function of any smooth and projective variety $X$ defined over $\mathbb{F}_q$ satisfies a functional equation.*

*Proof.* This more or less follows immediately from Poincaré duality. Let $X$ be of dimension $n$. Since Frobenius is a finite morphism of degree $q^n$, it follows from the axioms that it acts as multiplication by $q^n$ on $H^{2n}(X) \cong K$. Now the previous lemma applied to the perfect pairing

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

says that

$$\det(1 - Fu \mid H^{2n-i}(X)) = \frac{(-q^n u)^{b_i}}{\det(F \mid H^i(X))} \det(1 - F(q^n u)^{-1} | H^i(X))$$

and

$$\det(F \mid H^{2n-i}(X)) = \frac{q^{nb_i}}{\det(F \mid H^i(X))}$$

where $b_i = \dim_K H^i(X)$. Now set $\epsilon = \sum_i (-1)^i b_i$, then substituting into the expression

$$Z(X, u) = \prod_i \det(1 - Fu \mid H^i(X))^{(-1)^{i+1}}$$

for the $Z$-function gives

$$\begin{aligned} Z(X, (q^n u)^{-1}) &= \prod_i \det(1 - Fu \mid H^{2n-i}(X))^{(-1)^{i+1}} \frac{(-q^n u)^{(-1)^i b_i}}{\det(F^* \mid H^i(X))^{(-1)^i}} \\ &= \frac{Z(X, u)(-q^n u)^{\epsilon}}{\prod_i \det(F \mid H^i(X))^{(-1)^i}} \end{aligned}$$

and since $\det(F \mid H^i(X)) \det(F \mid H^{2n-i}(X)) = q^{nb_i}$ we have

$$\prod_i \det(F \mid H^i(X))^{(-1)^i} = \pm q^{n\epsilon/2}$$

and hence

$$Z(X, (q^n u)^{-1}) = \pm q^{n\epsilon/2} u^{\epsilon} Z(X, u)$$

as required. □

In this course we're not actually going to prove that a Weil cohomology exists. Instead we're going to construct something that behaves very much like a Weil cohomology theory and prove the Leftschetz trace formula directly. In fact, our starting point is actually going to be a theory for smooth *affine* varieties over $\mathbb{F}_q$, i.e. closed subsets of $\mathbb{A}^n(\overline{\mathbb{F}}_q)$ defined by polynomials with coefficients in $\mathbb{F}_q$, rather than smooth *projective* varieties over $\overline{\mathbb{F}}_q$.

The main theme of the number theory part of the course is that the Weil conjectures give a way of passing back and forth between topological and arithmetic information. For example, knowledge of the topological behaviour of Riemann surfaces tells us the following estimate for the number of points on a curve of genus $g$ over a finite field.

**Proposition.** *Let $C/\mathbb{F}_q$ be a curve of genus $g$ defined over a finite field $\mathbb{F}_q$. Then we have*

$$\left|\#C(\mathbb{F}_{q^n}) - q^n - 1\right| \leq 2gq^{n/2}.$$

*Proof.* We can write the $Z$-function of $C$ as

$$Z(C,u) = \frac{P(u)}{(1-u)(1-qu)}$$

where $P(u)$ is a polynomial of degree $2g$, and $P(u) = \prod_{i=1}^{2g}(1-\omega_i u)$ with $|\omega_i| = q^{1/2}$. Therefore we have

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_i \omega_i^n$$

and since $|\omega_i| \leq q^{1/2}$ we have $\left|\sum_i \omega_i^n\right| \leq 2gq^{n/2}$ by the triangle inequality. □

We'll be concerned with going in the other direction - by counting the number of vector bundles on a curve over a finite field, we can calculate the Betti numbers of the moduli space of stable bundles.

### "Standard Conjectures"

Actually, we can add in some extra axioms for Weil cohomology theories that would (amongst other things) imply the Riemann hypothesis. These are known as the standard conjectures. To explain them, we note that the Künneth formula together with Poincaré duality give an isomorphism

$$H^*(X \times Y) \cong \mathrm{Hom}(H^*(X), H^*(Y))$$

of graded $K$-algebras. We can therefore talk of a morphism $H^*(X) \to H^*(Y)$ being *algebraic*, that is induced by an algebraic cycle on $X \times Y$

- (Lefschetz) Let $W$ be a hyperplane section in $X$, for some projective embedding $X \hookrightarrow \mathbb{P}^N$, and let $L : H^i(X) \to H^{i+2}(X)$ denote cup product with $\mathrm{cl}(W) \in H^2(X)$. Then

  $$L^{n-i} : H^i(X) \xrightarrow{\sim} H^{2n-i}(X).$$

  is an isomorphism. Moreover, if we define operators $\Lambda : H^i(X) \to H^{i-2}(X)$ as the 'transport' of $L$ via these isomorphisms, then $\Lambda : H^*(X) \to H^*(X)$ is algebraic.

- (Künneth) Projection followed by inclusion

$$H^*(X) \to H^i(X) \to H^*(X)$$

is induced by some algebraic cycle $\pi_i$ on $X \times X$.

- (Hom vs. Num) A cycle $Z \in A^*(X)$ is numerically equivalent to zero iff $\mathrm{cl}(Z) = 0$.
- Another one that's too complicated to explain.

These are not known for any Weil cohomology theory! The known proofs of the Riemann Hypothesis come via the 'yoga of weights'.

**Outline for the rest of the course**

- 27/11 Thursday 9-11, South Wing Garwood LT. James Newton will talk about Monsky-Washnitzer cohomology, which will be the Weil cohomology theory we'll try to construct over $\mathbb{F}_q$ by lifting to characteristic zero.
- 1/12 Monday 10-11 (usual place) and 4/12 Thursday 9:30-10:30 (Imperial seminar Room). Luis Garcia will talk about proving the Lefschetz trace formula for MW cohomology.
- 8/12 Monday 10-12 (usual place) Olivier Taïbi will talk about Tamagawa numbers for algebraic groups, and Siegel's formula for counting vector bundles over finite fields.
- 11/12 Thursday 9:30-10:30 (Imperial seminar room) Try to put things together to compute some Betti number of the moduli space of bundles.

## 3 Lecture 10

References:

- Attiyah-Bott, Yang-Mills equations over Riemann surfaces
- Harder-Narasimhan, On the cohomology groups of moduli spaces.....
- Desale-Ramanan, Poincaré polynomials of the variety of stable bundles

Let's start with a quick calculation. Suppose $X/\mathbb{F}_q$ is smooth and projective, of dimension $n$. Then by the Weil conjectures we can write

$$Z(X,u) = \frac{P_1(u)\dots P_{2n-1}(u)}{P_0(u)\dots P_{2n}(u)}$$

where $P_i(u) = \prod_{j=1}^{b_i}(1-\alpha_{ij}u)$, $b_i$ is the $i$th Betti number of $X$, and each $\alpha_{ij}$ has 'weight' $i$. This is equivalent to being able to write

$$\#X(\mathbb{F}_{q^m}) = \sum_i (-1)^i \sum_j \alpha_{ij}^m$$

for all $m \geq 1$. Now, note that if we consider this as a formal expression in the $\alpha_{ij}$, and substitute in $t^i$ for $(-1)^i \alpha_{ij}$ in the formula for $\#X(\mathbb{F}_q)$ we get

$$\sum_i b_i t^i$$

that is the Poincaré polynomial for $X$.

*Example.* $X = \mathbb{P}^n$. Then $\#X(\mathbb{F}_q) = 1 + q + \ldots + q^n$ and $q^i$ has weight $2i$, so we substitute in $q^i = t^{2i}$ to get $1 + t^2 + \ldots + t^{2n}$, the Poincaré polynomial for $\mathbb{P}^n$.

We want to do this for the moduli space of stable bundles - count the number of points, and then make a substitution to get the Poincaré polynomial.

So let $Y/\mathbb{F}_q$ be a smooth, projective curve of genus $g$, and fix a line bundle $L$ on $Y$ of degree (Chern class) $k$. Then for $n \geq 1$ coprime to both $q$ and $k$ we have the moduli space

$$N_0(n, L)$$

of stable, rank $n$ vector bundles on $Y$ with determinant $L$. This is the 'reduction mod $p$' of the moduli space you saw in the geometry part of the course, so its Betti numbers are the same as the Betti numbers of the object over $\mathbb{C}$. After enlarging $\mathbb{F}_q$, we may assume that $N_0(n, L)$ is actually defined over $\mathbb{F}_q$, and we want to count points, that is calculate

$$\#N_0(n, L)(\mathbb{F}_q) = \#\{\deg n \text{ stable bundles on } Y \text{ w/ det } L\}/\cong.$$

The main ingredient we're going to use to do this is the following.

**Theorem** (Siegel's formula)**.**

$$\sum_E \frac{1}{\#\mathrm{Aut}(E)} = \frac{q^{(n^2-1)(g-1)}}{q-1} \zeta_Y(2) \ldots \zeta_Y(n)$$

*where the sum is over all isomorphism classes of rank n bundles on Y with determinant L (not necessarily stable). We also do not assume that n is coprime to the degree of L.*

To use this formula, define for any $n', L'$

$$\beta(n', L') = \sum_{E \text{ semi-stable}} \frac{1}{\#\mathrm{Aut}(E)}.$$

the sum being over semi-stable $E$ of rank $n'$ and determinant $L'$. Since $(n, k) = 1$, a vector bundle of rank $n$ and determinant $L$ is stable iff it is semi-stable, and stable vector bundles have $\#\mathrm{Aut}(E) = q - 1$, we get

$$\#N_0(n, L)(\mathbb{F}_q) = \beta(n, L)(q-1)$$

so to compute the former it suffices to compute $\beta(n, L)$. To do this, we use the Harder-Narasimhan filtration, and the *type* of the vector bundle.

**Recap on HN-filtrations and the inductive formula for $\beta(n,L)$**

Recall that every vector bundle $E$ on $Y$ has a canonical filtration

$$0 = F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_r = E$$

such that each $D_i := F_i/F_{i-1}$ is semi-stable and we have

$$\mu(D_1) > \mu(D_2) > \ldots > \mu(D_r)$$

(when $E$ is semi-stable we have $r = 1$). We let $n_i$ be the rank of each $D_i$, $L_i$ its determinant, and $k_i$ the degree of $L_i$. We refer to the collection of pairs $(n_i, k_i)$ as the *type* of $E$, note that if $E$ has rank $n$ and determinant $L$ of degree $k$ then we have $\sum_i k_i = k$ and $\sum_i n_i = n$. We then group the terms in Siegel's formula according to their type:

$$\sum_E \frac{1}{\#\mathrm{Aut}(E)} = \sum_{\{(n_i,k_i)\}_i} \sum_{\text{type } E=\{(n_i,k_i)\}_i} \frac{1}{\#\mathrm{Aut}(E)}$$

the terms of type $\{(n,k)\}$ are exactly the semi-stable bundles which contribute $\beta(n,L)$ to this sum. The point is that now we can express the terms corresponding to the type $\{(n_i,k_i)\}_i$ in terms of $\beta(n_i,L_i)$, as follows.

**Theorem** (Desale-Ramanan)**.** *The numbers $\beta(n,L)$ only depend on the degree $k$ of $L$, we therefore write $\beta(n,k)$. Moreover, we have*

$$\sum_{\text{type } E=\{(n_i,k_i)\}_i} \frac{1}{\#\mathrm{Aut}(E)} = \frac{\#J^{r-1}(\mathbb{F}_q)}{q^\chi} \prod_{i=1}^{r} \beta(n_i,k_i)$$

*where $J$ is the Jacobian of $Y$, and $\chi$ is an integer depending only on the type $\{(n_i,k_i)\}_i$.*

Now looking at Siegel's formula

$$\sum_{\{(n_i,k_i)\}_i} \sum_{\text{type } E=\{(n_i,k_i)\}_i} \frac{1}{\#\mathrm{Aut}(E)} = \frac{q^{(n^2-1)(g-1)}}{q-1}\zeta_Y(2)\ldots\zeta_Y(n)$$

we can split off one 'grouping' corresponding to $\beta(n,k)$, the term we are interested in, and the other terms all have $n_i < n$, so this leads to an inductive formula for the $\beta(n,k)$ in terms of the $\beta(n_i,k_i)$ for $n_i < n$.

**Detailed case $n = 2$, $k = 1$**

Let's look in detail at the case $n = 2$, $k = 1$ to see what's actually going on, we'll also keep the assumption that $(2,q) = 1$. Then we have

$$\beta(2,1) + \sum_{E \text{ unstable}} \frac{1}{\#\mathrm{Aut}(E)} = \frac{q^{3(g-1)}}{q-1}\zeta_Y(2)$$

If $E$ is unstable, then we get a canonical filtration

$$0 \to L_1 \to E \to L_2 \to 0$$

with $L_i$ line bundles such that $L_1 \otimes L_2 = L$ has degree 1, therefore there exists some unique integer $r \geq 0$ such that $\deg(L_1) = r+1$, $\deg(L_2) = -r$, since we have $\mu(L_1) > \mu(L_2)$. Such extensions correspond to cohomology classes in

$$H^1(Y, L_2^\vee \otimes L_1)$$

and proportional (over $\mathbb{F}_q$) classes give the same *bundle*, we therefore get

$$\sum_{E \text{ unstable}} \frac{1}{\#\mathrm{Aut}(E)} = \sum_{r=0}^{\infty} \sum_{\deg L_1 = r+1} \sum_{c \in H^1(Y, L_2^\vee \otimes L_1)/\mathbb{F}_q^*} \frac{1}{\#\mathrm{Aut}(E_c)}$$

where $E_c$ is the extension corresponding to a cohomology class, and $L_2 = L_1^\vee \otimes L$. Now, to calculate $\#\mathrm{Aut}(E_c)$, we consider trivial and non-trivial extensions separately. In the trivial case, $E \cong L_1 \oplus L_2$, any automorphism has to preserve $L_1$, and hence has the form

$$\begin{pmatrix} \alpha & \psi \\ 0 & \beta \end{pmatrix}$$

for $\alpha, \beta \in \mathbb{F}_q^*$ and $\psi \in \mathrm{Hom}(L_2, L_1) = H^0(Y, L_2^\vee \otimes L_1)$. Hence we get exactly $(q-1)^2 h_0$ automorphisms, where $h_0 = \# H^0(Y, L_2^\vee \otimes L_1)$.

When the extension is non-trivial, a slightly more tricky (but still elementary) calculation gives $\#\mathrm{Aut}(E_c) = (q-1)h_0$ where $h_0 = \# H^0(Y, L_2^\vee \otimes L_1)$. Plugging this into the above expression gives

$$\sum_{E \text{ unstable}} \frac{1}{\#\mathrm{Aut}(E)} = \sum_{r=0}^{\infty} \sum_{\deg L_1 = r} \frac{h_1}{(q-1)^2 h_0}$$

where $h_1 = \# H^1(Y, L_2^\vee \otimes L_1)$. Now Riemann-Roch gives $h_0/h_1 = q^{2r+2-g}$ so we can write this as

$$\begin{aligned} \sum_{E \text{ unstable}} \frac{1}{\#\mathrm{Aut}(E)} &= \sum_{r=0}^{\infty} \frac{1}{(q-1)q^{2r+2-g}} \sum_{\deg L_1 = r+1} \frac{1}{q-1} \\ &= \sum_{r=0}^{\infty} \frac{1}{(q-1)q^{2r+2-g}} \beta(1,r) \end{aligned}$$

so we can see the inductive part coming in. But $\beta(1,r)$ is just the number of $\mathbb{F}_q$-rational points on the Jacobian $J$ of $Y$ divided by $(q-1)$, so this sum is equal to

$$\sum_{r=0}^{\infty} \frac{1}{(q-1)^2 q^{2r+2-g}} \# J(\mathbb{F}_q).$$

If we write the $Z$-function of $Y$ as

$$\frac{\prod_{j=1}^{2g}(1-\omega_j u)}{(1-u)(1-qu)}$$

then we have

$$\# J(\mathbb{F}_q) = \prod_{i=1}^{2g}(1-\omega_j)$$

and hence Siegel's formula gives

$$\# N_0(n,L) + \frac{\prod_{i=1}^{2g}(1-\omega_j)q^{g-2}}{(q-1)} \sum_{r=0}^{\infty} \frac{1}{q^{2r}} = q^{3(g-1)} \frac{\prod_{j=1}^{2g}(1-\omega_j q^{-2})}{(1-q^{-2})(1-q^{-1})}.$$

Now summing the infinite series, and substituting in $q = t^2$ and $-\omega_j = t$ will give an expression for the Poincaré polynomial of $N_0(n,L)$.

### Similarities with topological approach

| number theoretic | topological |
|---|---|
| count *all* bundles using Siegel's formula | look at the space of all complex structures on a given bundle |
| split this sum by the type of the bundle | stratify this space according to the type of the bundle |
| inductive formula for $\beta(n,L)$ | inductive formula for the Poincaré polynomial |