Weil Conjectures

D. Zack Garza

Tuesday 21st April, 2020

Contents

l	Not	otes from Daniel's Office Hours									1
	1.1	1 Definition of Zeta Function	 	 							1
		1.1.1 Simple but Useful Example: A Point	 	 							3
	1.2	2 Statement of Weil Conjectures	 	 							4
		1.2.1 Aside: Why call it a Zeta function?		 							5
		1.2.2 More Examples	 	 				 			6
	1.3	3 Hard Example: An Elliptic Curve	 	 							10

1 Notes from Daniel's Office Hours

- 0. Definition of Zeta functions
- 1. Statement of the conjectures
- 2. Easy examples: \mathbb{P}^n_{\exists} , $\operatorname{Gr}_{\exists}(k,n) = \operatorname{GL}(n,\exists)/P$ the stabilizer of an \exists -point in \mathbb{C}^n , \mathbb{F}_{p^n} .
- 3. Medium example: E/\mathbb{k} an elliptic curve.
- 4. Work out a harder example as in Weil

References

- http://www-personal.umich.edu/~mmustata/zeta_book.pdf
- https://youtu.be/wEz7fCvK6sM?t=293
- Explanation of exponential appearing
- https://arxiv.org/pdf/1807.10812.pdf
- http://www.math.canterbury.ac.nz/~j.booher/expos/weil_conjectures.pdf
- Weil's Paper

1.1 Definition of Zeta Function

Fix q a prime and $\mathbb{F} := \mathbb{F}_q$ the finite field with q elements, along with its unique degree n extensions

$$\mathbb{F}_n := \mathbb{F}_{q^n} = \left\{ x \in \overline{\mathbb{F}}_p \mid x^{q^n} - x = 0 \right\} \quad \forall \ n \in \mathbb{Z}^{\geq 2}$$

Definition 1.0.1.

Let

$$J = \langle f_1, \cdots, f_M \rangle \le k[x_0, \cdots, x_n]$$

be an ideal, then a projective~algebraic variety $X\subset \mathbb{P}^N_{\mathbb{F}}$ can be given by

$$X = V(J) = \left\{ \mathbf{x} \in \mathbb{P}_{\mathbb{F}}^{\infty} \mid f_1(\mathbf{x}) = \dots = f_M(\mathbf{x}) = \mathbf{0} \right\}$$

where an ideal generated by homogeneous polynomials in n+1 variables, i.e. there is some fixed $d \in \mathbb{Z}^{\geq 1}$ such that

$$f(\mathbf{x}) = \sum_{\substack{\mathbf{I} = (i_1, \dots, i_n) \\ \sum_i i_j = d}} \alpha_{\mathbf{I}} \cdot x_0^{i_1} \cdots x_n^{i_n} \quad \text{and} \quad f(\lambda \cdot \mathbf{x}) = \lambda^d f(\mathbf{x}).$$

For the experts: we can take a reduced (possibly reducible) scheme of finite type over a field \mathbb{F}_p . We will be thinking of K-valued points for K/\mathbb{F}_p algebraic extensions. From the audience: what condition do we need to put on such a scheme to guarantee an embedding into \mathbb{P}^{∞} ?

Examples:

• Dimension 1: Curves

• Dimension 2: Surfaces

• Codimension 1: Hypersurfaces

Fix $X/\mathbb{F} \subset \mathbb{P}$ an N-dimensional projective algebraic variety, and say it's cut out by the equations $f_1, \dots, f_M \in \mathbb{F}[x_0, \dots, x_n]$. Note that it then has points in any finite extension L/K.

Definition 1.0.2.

Define the local zeta function of X the following formal power series:

$$\zeta_X(z) = \exp\left(\sum_{n=1}^{\infty} \alpha_n \frac{z^n}{n}\right) \in \mathbb{Q}[[z]] \text{ where } \alpha_n := \#X(\mathbb{F}_n).$$

Concretely, for $X \subset \mathbb{P}^M$ a variety cut out by $\{f_i\} \subset \mathbb{F}[x_0, \cdots, x_M]$ we are measuring the sizes of the sets

$$\alpha_n \coloneqq \# \left\{ \mathbf{x} \in \mathbb{P}^M_{\mathbb{F}_{q^n}} \mid f_i(\mathbf{x}) = \mathbf{0} \ \forall i \right\}.$$

Note the following two properties:

$$\zeta_X(0) = 1$$

$$z\left(\frac{\partial}{\partial z}\right)\log\zeta_X(z) = t\left(\frac{\zeta_X'(z)}{\zeta_X(z)}\right) = \sum_{n=1}^{\infty} \alpha_n z^n = \alpha_1 z + \alpha_2 z^2 + \cdots,$$

which is an ordinary generating function for the sequence (α_n) .

Todo: why not an OGF.

Remark: Note that for an OGF $F(x) = \sum_{n=0}^{\infty} f_n x^n$, we can extract coefficients in the following way:

$$f_n := [x^n]F(x) = [x^n]T_{F,0}(x) = \frac{1}{n!} \left(\frac{\partial}{\partial x}\right)^n F(x) \Big|_{x=0}.$$

Using the Residue theorem, we can also extract in the following way:

$$[x^n]F(x) = \frac{1}{2\pi i} \oint_{\mathbb{S}^1} \frac{F(z)}{z^{n+1}}.$$

Note: this is extremely amenable to numerical approximation if you have a closed form for F or even just a black-box numerical version of F! I.e. easy to throw at a computer.

1.1.1 Simple but Useful Example: A Point

Take $X = \{x = 0\} / \mathbb{F}$ a single point over \mathbb{F} , then

$$\#X(\mathbb{F}) \coloneqq \alpha_1 = 1$$

 $\#X(\mathbb{F}_2) \coloneqq \alpha_2 = 1$
 \vdots
 $\#X(\mathbb{F}_n) \coloneqq \alpha_n = 1$
 \vdots

Recall that by integrating a geometric series we can derive

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n = 1 + z + z^2 + \cdots$$

$$\int \frac{1}{1-z} = \int \sum_{n=0}^{\infty} z^n = \sum_{n=0}^{\infty} \int z^n = \sum_{n=0}^{\infty} \frac{1}{n+1} z^{n+1} = z + \frac{1}{2} z^2 + \frac{1}{3} z^3 + \cdots$$

$$\implies -\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}.$$

and so

$$\zeta_{\{\text{pt}\}}(z) = \exp\left(1 \cdot z + 1 \cdot \frac{z^2}{2} + 1 \cdot \frac{z^3}{3} + \cdots\right)$$

$$= \exp\left(-\log(1 - z)\right)$$

$$= \frac{1}{1 - z}.$$

1.2 Statement of Weil Conjectures

(Weil 1949)

Let X be a smooth projective variety of dimension N over \mathbb{F}_q for q a prime and let $\zeta_X(z)$ be its zeta function.

1. (Rationality)

 $\zeta_X(z)$ is a rational function:

$$\zeta_X(z) = \frac{p_1(z) \cdot p_3(z) \cdots p_{2N-1}(z)}{p_0(z) \cdot p_2(z) \cdots p_{2N}(z)} \in \mathbb{Q}(z), \quad \text{i.e.} \quad p_i(z) \in \mathbb{Z}[z]$$

$$P_0(z) = 1 - z$$

$$P_{2N}(z) = 1 - q^N z$$

$$P_j(z) = \prod_{j=1}^{\beta_i} (1 - a_{j,k}z) \quad \text{for some reciprocal roots} \quad a_{j,k} \in \mathbb{C}$$

where we've factored each P_i using its reciprocal roots a_{ij} .

We thus have a simplified expression:

$$\zeta_X(z) = \left(\frac{1}{1-z}\right) \cdot \frac{(1-\alpha_{1,1}z)(1-\alpha_{1,2}z)\cdots(1-\alpha_{1,\beta_1}z)}{(1-\alpha_{2,1}z)(1-\alpha_{2,2}z)\cdots(1-\alpha_{2,\beta_2}z)} \cdots \\
\cdot \frac{(1-\alpha_{2N-1,1}z)(1-\alpha_{2N-1,2}z)\cdots(1-\alpha_{2N-1,\beta_{2N-1}}z)}{(1-\alpha_{2N-2,1}z)(1-\alpha_{2N-2,2}z)\cdots(1-\alpha_{2N-2,\beta_{2N-2}}z)} \left(\frac{1}{1-q^Nz}\right).$$

2. (Functional Equation and Poincare Duality)

Let $\chi(X)$ be the Euler characteristic of X, i.e. the self-intersection number of the diagonal embedding $\Delta \hookrightarrow X \times X$; then $\zeta_X(z)$ satisfies the following functional equation:

$$\zeta_X\left(\frac{1}{q^N z}\right) = \pm \left(q^{\frac{N}{2}} z\right)^{\chi(X)} \zeta_X(z).$$

Equivalently,

$$\zeta_X(N-z) = \pm q^{\chi(X)\cdot \left(\frac{n}{2}-2\right)} \zeta_X(z).$$

Equivalently, there is an involutive map on the (reciprocal) roots

$$z \iff \frac{q^N}{z}$$

$$\alpha_{j,k} \iff \alpha_{2N-j,k}$$

which sends roots of p_j to roots of p_{2N-k} .

3. (Riemann Hypothesis)

The reciprocal roots $a_{j,k}$ are algebraic integers (roots of some monic $p \in \mathbb{Z}[x]$) which satisfy

$$|a_{i,k}|_{\mathbb{C}} = q^{\frac{j}{2}} \qquad \forall 1 \le j \le 2N - 1, \ \forall k.$$

4. (Betti Numbers) If X is a "good reduction mod q" of a nonsingular projective variety \tilde{X} in characteristic zero, then the $\beta_i = \deg p_i(z)$ are the Betti numbers of the topological space $\tilde{X}(\mathbb{C})$.

Why is (3) called the "Riemann Hypothesis"?

We can use the fact that $|e^z| = e^{\Re(z)}$ and $c^z := e^{z \operatorname{Log}(c)}$, and we'll consider a new function

$$L(s) := \zeta_X(q^{-s}) = .$$

Moral: the Diophantine properties of a variety's zeta function are governed by its (algebraic) topology. Conversely, the analytic properties of encode a lot of geometric/topological/algebraic information.

Historical note

• Desire for a "cohomology theory of varieties" drove 25 years of progress in AG

Remarks:

- Resolved for varieties over \mathbb{F}_q
- \bullet On L_X :
 - Conjectured for smooth varieties over \mathbb{Q} (rationality \sim analytically continues to a meromorphic function, some functional equation), little is known.
 - Resolved for elliptic curves (Taylor-Wiles c/o the Taniyama-Shimura conjecture), implies L_X is an L function coming from a modular form.

1.2.1 Aside: Why call it a Zeta function?

Knowing the zeta function of a point, we can now make a precise analogy.

Suppose we have an algebraic variety cut out by equations:

$$\mathbb{A}^n_{\mathbb{Z}} \supseteq X = V(\langle f_1, \cdots, f_d \rangle)$$
 where $f_i \in \mathbb{Z}[x_0, \cdots, x_{n-1}].$

Then for every prime q, we can reduce the equations mod p and consider

$$\mathbb{A}_{\mathbb{F}_q}^n \supseteq X_q \coloneqq V(\langle f_1 \mod q, \cdots, f_d \mod q \rangle) \quad \text{where} \quad f_1 \mod q \in \mathbb{F}_q[x_0, \cdots, x_{n-1}]$$

Then define the *Hasse-Weil* zeta function:

$$L_X(s) = \prod_{p \text{ prime}} \zeta_{X_p}(p^{-s}).$$

Take $X = \operatorname{Spec} \mathbb{Q}$ and $X_p = \operatorname{Spec} \mathbb{F}_p$, which is a single point since \mathbb{F}_p is a field. The previous example shows that

$$\zeta_{X_p}(z) = \frac{1}{1-z},$$

We then find that

$$L_X(s) = \prod_{p \text{ prime}} \zeta_{X_p}(p^{-s})$$
$$= \prod_{p \text{ prime}} \left(\frac{1}{1 - p^{-s}}\right)$$
$$= \zeta(s),$$

which is the Euler product expansion of the classical Riemann Zeta function.

Moreover, it is a theorem (difficult, not proved here!) that for any variety X/\mathbb{F}_p , we have

$$\zeta_X(t) = \prod_{x \in X_{\operatorname{cl}}} \left(\frac{1}{1 - t^{\operatorname{deg}(x)}} \right) \quad \overset{t = p^{-s}}{\Longrightarrow} \quad \zeta_X(s) = \prod_{x \in X_{\operatorname{cl}}} \left(\frac{1}{1 - \left(p^{\operatorname{deg}(x)} \right)^{-s}} \right),$$

which we can think of as attaching a "weight" to each closed point, $|x| := p^{\deg(x)}$, and the usual Riemann Zeta corresponds to assigning a weight of 1 to each point.

Note that this immediately implies that $\zeta_X(t) \in \mathbb{Z}[[t]]$ is a rational function.

Recall the Riemann zeta function is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

After modifying ζ to make it symmetric about $\Re(s) = \frac{1}{2}$ and eliminate the trivial zeros at $-2\mathbb{Z}$ to obtain $\widehat{\zeta}(s)$, there are three relevant properties

- "Rationality": $\widehat{\zeta}(s)$ has a meromorphic continuation to $\mathbb C$ with simple poles at s=0,1.
- "Functional equation": $\widehat{\zeta}(1-s) = \widehat{\widehat{\zeta}}(s)$
- "Riemann Hypothesis": The only zeros of $\hat{\zeta}$ have $\Re(s) = \frac{1}{2}$.

1.2.2 More Examples

Example (Affine Line): $X = \mathbb{A}^1/\mathbb{F}$ the affine line over \mathbb{F} , then Note that we can write

$$\mathbb{A}^{1}(\mathbb{F}_{n}) = \left\{ \mathbf{x} = [x_{1}] \mid x_{1} \in \mathbb{F}_{n} \right\}$$

as the set of one-component vectors with entries in \mathbb{F}_n , so

$$X(\mathbb{F}) = q$$

$$X(\mathbb{F}_2) = q^2$$

$$\vdots$$

$$X(\mathbb{F}_n) = q^n.$$

Thus

$$\zeta_X(z) = \exp\left(\sum_{n=1}^{\infty} \frac{q^n}{n} z^n\right) = \frac{1}{1 - qz}.$$

Example (Affine Space): Set $X = \mathbb{A}^m/\mathbb{F}$, affine m-space over \mathbb{F} , so we can just repeat with now m coordinates

$$\mathbb{A}^1(\mathbb{F}_n) = \left\{ \mathbf{x} = [x_1, \cdots, x_m] \mid x_i \in \mathbb{F}_n \right\}$$

Counting yields

$$X(\mathbb{F}) = q^m$$

$$X(\mathbb{F}_2) = (q^2)^m$$

$$\vdots$$

$$X(\mathbb{F}_n) = (q^n)^m.$$

Thus

$$\zeta_X(z) = \exp\left(\sum_{n=1}^{\infty} \frac{q^{nm}}{n} z^n\right) = \frac{1}{1 - q^m z}.$$

Example (Projective Line): $X = \mathbb{P}^1/\mathbb{F}$ the projective line over \mathbb{F} , then we can write use some geometry to write

$$\mathbb{P}^1_{\mathbb{F}}=\mathbb{A}^1_{\mathbb{F}}\coprod\{\infty\}$$

as the affine line with a point added at infinity.

We can then count by enumerating coordinates:

$$\mathbb{P}^{1}(\mathbb{F}_{n}) = \left\{ [x_{1}, x_{2}] \mid x_{1}, x_{2} \neq 0 \in \mathbb{F}_{n} \right\} / \sim$$
$$= \left\{ [x_{1}, 1] \mid x_{1} \in \mathbb{F}_{n} \right\} \coprod \left\{ [1, 0] \right\}.$$

Thus

$$X(\mathbb{F}) = q + 1$$

$$X(\mathbb{F}_2) = q^2 + 1$$

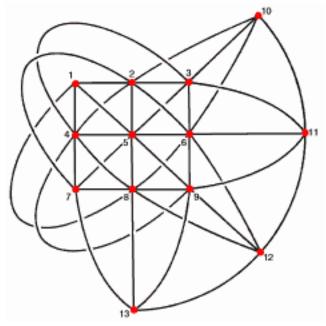
$$\vdots$$

$$X(\mathbb{F}_n) = q^n + 1$$

Thus

$$\zeta_X(z) = \frac{1}{(1-z)(1-qz)}$$

Example (Projective Space): Take $X = \mathbb{P}_{\mathbb{F}}^n$,



Example image of $\mathbb{P}^2_{\mathbb{GF}(3)}$:

Note that we can identify $X = Gr_{\mathbb{F}}(1, n)$ as the space of lines in $\mathbb{A}^n_{\mathbb{F}}$.

Proposition 1.1.

The number of k-dimensional subspaces of $\mathbb{A}^m_{\mathbb{F}}$ is the q-binomial coefficient:

$$\begin{bmatrix} m \\ k \end{bmatrix}_q \coloneqq \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-(k-1)}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Proof.

To choose a k-dimensional subspace,

• Choose a nonzero vector $\mathbf{v}_1 \in \mathbb{A}^n_{\mathbb{F}}$ in

$$q^{m} - 1$$

ways.

- Identify #span
$$\{\mathbf{v}_1\} = \#\{\lambda \mathbf{v}_1 \mid \lambda \in \mathbb{F}\} = \#\mathbb{F} = q.$$

• Choose a nonzero vector \mathbf{v}_2 not in the span of \mathbf{v}_1 in

$$q^m - q$$

ways.

- Identify #span
$$\{\mathbf{v}_1, \mathbf{v}_2\} = \# \{\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 \mid \lambda_i \in \mathbb{F} \} = q \cdot q = q^2.$$

• Choose a nonzero vector \mathbf{v}_3 not in the span of \mathbf{v}_1 , \mathbf{v}_2 in

$$q^m - q^2$$

ways.

• · · · until \mathbf{v}_k is chosen in

$$(q^m - 1)(q^m - q) \cdots (q^m - q^{k-1})$$

ways.

- This yields a k-tuple of linearly independent vectors spanning a k-dimensional subspace V_k
- This overcounts because many linearly independent sets span V_k , we need to divide out by the number of choose a basis inside of V_k .
- By the same argument, this is given by

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$$

Thus

#subspaces =
$$\frac{(q^m - 1)(q^m - q)(q^m - q^2)\cdots(q^m - q^{k-1})}{(q^k - 1)(q^k - q)(q^k - q^2)\cdots(q^k - q^{k-1})}$$
=
$$\frac{q^m - 1}{q^k - 1}\cdot\left(\frac{q}{q}\right)\frac{q^{m-1} - 1}{q^{k-1} - 1}\cdot\left(\frac{q^2}{q^2}\right)\frac{q^{m-2} - 1}{q^{k-2} - 1}\cdots\left(\frac{q^{k-1}}{q^{k-1}}\right)\frac{q^{m-(k-1)} - 1}{q^{k-(k-1)-1}}.$$

We obtain a nice simplification for the number of lines corresponding to setting k = 1:

$$\begin{bmatrix} m \\ 1 \end{bmatrix}_q = \frac{q^m - 1}{q - 1} = q^{m-1} + q^{m-2} + \dots + q + 1 = \sum_{j=0}^{m-1} q^j.$$

Thus

$$X(\mathbb{F}) = \sum_{j=0}^{m-1} q^j$$

$$X(\mathbb{F}_2) = \sum_{j=0}^{m-1} (q^2)^j$$

$$\vdots$$

$$X(\mathbb{F}_n) = \sum_{j=0}^{m-1} (q^n)^j.$$

So

$$\zeta_X(z) = \left(\frac{1}{1-z}\right) \left(\frac{1}{1-qz}\right) \left(\frac{1}{1-q^2z}\right) \cdots \left(\frac{1}{1-q^mz}\right)$$

Note that geometry can help us here: we have a "cell decomposition" $\mathbb{P}^n = \mathbb{P}^{n-1} \coprod \mathbb{A}^n$, and so inductively

$$\mathbb{P}^n = \mathbb{A}^0 \coprod \mathbb{A}^1 \coprod \cdots \coprod \mathbb{A}^n,$$

and it's straightforward to prove that

$$\zeta_{XIIY}(z) = \zeta_X(z) \cdot \zeta_Y(z)$$

and recalling that $\zeta_{\mathbb{A}^j}(z) = \frac{1}{1 - q^j z}$ we have

$$\zeta_{\mathbb{P}^m}(z) = \prod_{j=0}^m \zeta_{\mathbb{A}^j}(z) = \prod_{j=0}^n \frac{1}{1-q^j z}.$$

Example: Take $X = Gr_{\mathbb{F}}(k, n)$, then ????? so

$$\zeta_X(t) = ?.$$

1.3 Hard Example: An Elliptic Curve

The Weyl conjectures take on a particularly nice form for curves. Let X/\mathbb{F} be a smooth projective curve of genus g, then

1. (Rationality)

$$\zeta_X(z) = \frac{p(z)}{(1-z)(1-qz)}$$

2. (Functional Equation)

$$\zeta_X\left(\frac{1}{qz}\right) = q^{1-g}z^{2-2g}\zeta_X(z)$$

3. (Riemann Hypothesis)

$$p(t) = \prod_{i=1}^{2g} (q - a_i z)$$
 where $|a_i| = \frac{1}{\sqrt{q}}$

Take $X = E/\mathbb{F}$.

Consider the curve E defined by the following equation:

$$E: y^2 + y = x^3 - x^2$$

This is a cubic, whose graph is presented in Figure 1.

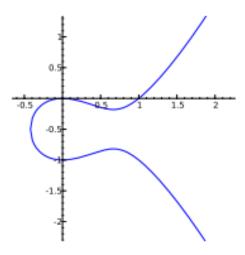


Figure 1: Implicit plot of E

Then

$$\zeta_X(t) = \frac{(1 - aq^{-t})(1 - \bar{a}q^{-t})}{(1 - q^{-t})(1 - q^{1-s})}.$$

The betti numbers are $[1, 2, 1, 0, \cdots]$.

The number of points are

$$X(\mathbb{F}_n) = (q^n + 1) - (\alpha^n + \overline{\alpha}^n)$$
 where $|\alpha| = |\overline{\alpha}| = \sqrt{q}$

Rough outline of proof:

• ??

The (complex?) dimension of X is N = 1, The WC say we should be able to write this as

$$\frac{p_1(z)}{p_0(z)p_2(z)} = \frac{p_1(z)}{(1-z)(1-qz)} = \frac{(1-\alpha_{1,1}z)(1-\alpha_{1,2}z)}{(1-z)(1-qz)}.$$

Since we know the number of points, we can compute

$$\zeta_X(z) = \exp \sum_{n=1}^{\infty} \#X(\mathbb{F}_n) \frac{z^n}{n}$$

$$= \exp \sum_{n=1}^{\infty} (q^n + 1 - (\alpha^n + \bar{\alpha}^n)) \frac{z^n}{n}$$

$$= \exp \left(\sum_{n=1}^{\infty} q^n \cdot \frac{z^n}{n}\right) \exp \left(\sum_{n=1}^{\infty} 1 \cdot \frac{z^n}{n}\right) \exp \left(\sum_{n=1}^{\infty} -\alpha^n \cdot \frac{z^n}{n}\right) \exp \left(\sum_{n=1}^{\infty} -\bar{\alpha}^n \cdot \frac{z^n}{n}\right)$$

$$= \exp \left(-\log (1 - qz)\right) \exp \left(-\log (1 - z)\right) \exp \left(\log (1 - \alpha z)\right) \exp \left(\log (1 - \bar{\alpha}z)\right)$$

$$= \frac{(1 - \alpha z)(1 - \bar{\alpha}z)}{(1 - z)(1 - qz)} \in \mathbb{Q}(z),$$

which is indeed a rational function.

Originally conjectured for curves by Artin Proved by Weil in 1949, proposed generalization to projective varieties Proof had work contributed by Dwork (rationality using p-adic analysis), Artin, Grothendieck (etale cohomology), with completion by Deligne in 1970s (RH)