

# Weil Conjectures

D. Zack Garza

Sunday 19<sup>th</sup> April, 2020

## Contents

<b>1</b>	<b>Notes from Daniel's Office Hours</b>	<b>1</b>
1.1	Definition of Zeta Function . . . . .	1
1.1.1	Simple but Useful Example: A Point . . . . .	3
1.1.2	Aside: Why call it a Zeta function? . . . . .	3
1.1.3	More Examples . . . . .	4
1.2	Statement of Weil Conjectures . . . . .	7
1.3	Hard Example: An Elliptic Curve . . . . .	8

## 1 Notes from Daniel's Office Hours

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

### References

- [http://www-personal.umich.edu/~mmustata/zeta\\_book.pdf](http://www-personal.umich.edu/~mmustata/zeta_book.pdf)
- <https://youtu.be/wEz7fCvK6sM?t=293>
- Explanation of exponential appearing

### 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

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

#### Definition 1.0.1.

Let

$$J = \langle f_1, \dots, f_N \rangle \trianglelefteq k[x_0, \dots, x_n]$$

be an ideal, then a *projective algebraic* variety  $X \hookrightarrow \mathbb{P}_{\mathbb{F}}^{\infty}$  can be given by

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

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

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

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  $\mathbb{P}^{\infty}$ ?

Examples:

- Dimension 1: Curves
- Dimension 2: Surfaces
- Codimension 1: Hypersurfaces

Example: Take  $f_1(x) = x \in \mathbb{F}[x]$ , consider  $V(\langle f_1 \rangle) \subset \mathbb{P}_{\mathbb{F}_n}^1$ . This is given by the single point  $x = \mathbf{0}$ .

Fix  $X/\mathbb{F}$  an  $N$ -dimensional projective algebraic variety. Note that it then has points in any finite extension  $L/K$ .

**Definition 1.0.2.**

Define the *local zeta function* (or *Hasse-Weil zeta function*) of  $X$  the following formal power series:

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

Note the following two properties:

$$\begin{aligned} \zeta_X(0) &= 1 \\ z \left( \frac{\partial}{\partial z} \right) \log \zeta_X(z) &= t \left( \frac{\zeta'_X(z)}{\zeta_X(z)} \right) = \sum_{n=1}^{\infty} \alpha_n z^n = \alpha_1 z + \alpha_2 z^2 + \cdots, \end{aligned}$$

which is an *ordinary generating function* for the sequence  $(\alpha_n)$ .

Thus if we define  $G(x)$  to be the OGF for  $(\alpha_n)$ , we have  $\zeta_X(t) = \exp$

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:

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

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

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

### 1.1.1 Simple but Useful Example: A Point

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

$$\begin{aligned} \#X(\mathbb{F}) &:= \alpha_1 = 1 \\ \#X(\mathbb{F}_2) &:= \alpha_2 = 1 \\ &\vdots \\ \#X(\mathbb{F}_n) &:= \alpha_n = 1 \\ &\vdots \end{aligned}$$

Recall that by integrating a geometric series we can derive

$$\begin{aligned} \log(1+t) &= \sum_{n=1}^{\infty} (-1)^{n-1} \frac{t^n}{n} \\ \implies \log(1-t) &= - \sum_{n=1}^{\infty} \frac{t^n}{n} \\ \implies -\log(1-t) &= \sum_{n=1}^{\infty} \frac{t^n}{n} \\ &= 1 \cdot t + 1 \cdot t^2 + 1 \cdot t^3 + \dots \end{aligned}$$

and so

$$\zeta_{\{\text{pt}\}}(t) = \exp(-\log(1-t)) = \frac{1}{1-t}.$$

### 1.1.2 Aside: Why call it a Zeta function?

Knowing the above calculation, we can now make a precise analogy.

Suppose

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

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

$$\mathbb{A}_{\mathbb{F}_p}^n \supseteq X_p := V(\langle f_1 \bmod p, \dots, f_d \bmod p \rangle) \quad \text{where} \quad f_i \bmod p \in \mathbb{F}_p[x_0, \dots, x_{n-1}]$$

Then define the “local at  $p$ ” zeta function:

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

Note: the index set for the product may require some minor adjustment over  $\mathbb{Q}$  in general. There are also potentially modifications needed to extend to schemes.

Taking  $X = \text{Spec } \mathbb{Q}$  and  $X_p = \text{Spec } \mathbb{F}_p$  (which is a single point since  $\mathbb{F}_p$  is a field) and noting that

$$\begin{aligned}\zeta_{X_p}(z) &= \exp\left(\sum_{n=1}^{\infty} \frac{1}{n} z^n\right) \\ &= \exp(-\log(1-z)) \\ &= \frac{1}{1-z},\end{aligned}$$

we find that

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

the classical Riemann Zeta function.

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

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

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.

Note for experts:  $\zeta_X(z)$  an honest generating function for the 0-cycles on  $X$  ( $F(X_{\text{cl}})$ ) where are effective (nonnegative coefficients).

### 1.1.3 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

$$\begin{aligned}X(\mathbb{F}) &= q \\ X(\mathbb{F}_2) &= q^2 \\ &\vdots \\ X(\mathbb{F}_n) &= q^n.\end{aligned}$$

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

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

Counting yields

$$\begin{aligned} X(\mathbb{F}) &= q^m \\ X(\mathbb{F}_2) &= (q^2)^m \\ &\vdots \\ X(\mathbb{F}_n) &= (q^n)^m. \end{aligned}$$

Thus

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

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

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

as the affine line with a point added at infinity.

We can then count by enumerating coordinates:

$$\begin{aligned} \mathbb{P}^1(\mathbb{F}_n) &= \left\{ [x_1, x_2] \mid x_1, x_2 \neq 0 \in \mathbb{F}_n \right\} / \sim \\ &= \left\{ [x_1, 1] \mid x_1 \in \mathbb{F}_n \right\} \amalg \{[1, 0]\}. \end{aligned}$$

Thus

$$\begin{aligned} X(\mathbb{F}) &= q + 1 \\ X(\mathbb{F}_2) &= q^2 + 1 \\ &\vdots \\ X(\mathbb{F}_n) &= q^n + 1 \end{aligned}$$

Thus

$$\zeta_X(t) = \frac{1}{(1 - q^{-t})(1 - q^{1-t})}$$

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

Identifying  $\mathbb{P}_{\mathbb{F}}^n = \text{Gr}_{\mathbb{F}}(1, n)$  So  $\alpha_n = 1 + q^m + (q^m)^2 + \dots + (q^m)^n$ . Note that we can identify  $X = \text{Gr}_{\mathbb{F}}(1, n)$  as the space of lines in  $\mathbb{A}_{\mathbb{F}}^n$ .

**Proposition 1.1.**

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

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

*Proof.*

To choose a  $k$ -dimensional subspace,

- Choose a nonzero vector  $\mathbf{v}_1 \in \mathbb{A}_{\mathbb{F}}^m$  in

$$q^m - 1$$

ways.

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

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

$$q^m - q$$

ways.

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

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

$$q^m - q^2$$

ways.

- $\cdots$  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 linearly independent vectors in  $V_k$
- By the same argument, this is given by

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

■

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

$$\begin{bmatrix} m \\ 1 \end{bmatrix}_q = \frac{q^m - 1}{q - 1} = q^{m-1} + q^{m-2} + \cdots + q + 1.$$

Thus

`\begin{align*}`

`\# \text{subspaces}`

`&= \frac{(q^{m-1})(q^{m-2}) \cdots (q^{m-k+1})}{(q^{k-1})(q^{k-2}) \cdots (q^1)}`

$$\zeta_X(t) = \frac{(q^m - 1)}{(q^k - 1)} \cdots \frac{(q^{m-1} - 1)}{(q^{k-1} - 1)} \cdots$$

$$\zeta_X(t) = \left( \frac{1}{1 - q^{-t}} \right) \left( \frac{1}{1 - q^{1-t}} \right) \left( \frac{1}{1 - q^{2-t}} \right) \cdots \left( \frac{1}{1 - q^{n-t}} \right)$$

or equivalently, take your favorite curve  $\gamma \in \mathbb{C}$  homotopic to  $\mathbb{S}^1$ .

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.

Todo: how to manually count points in  $\mathbb{P}^n$ !

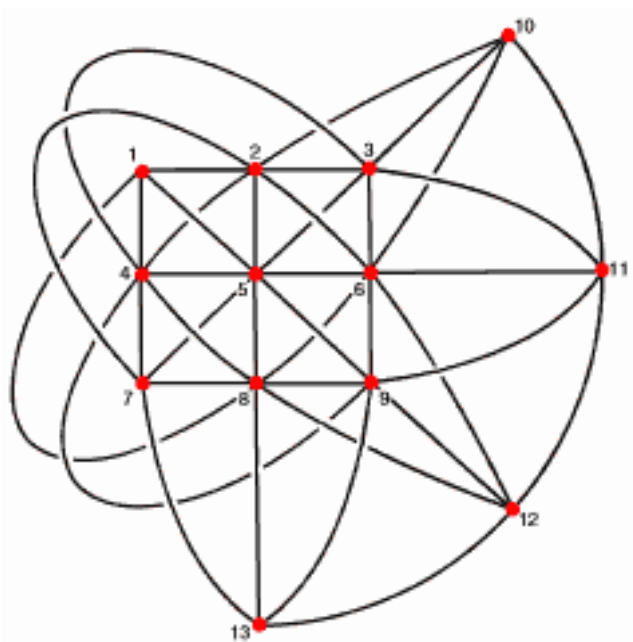


Image of  $\mathbb{P}_{\mathbb{GF}(3)}^2$

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

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

Questions about properties

- $\zeta_X \prod_Y(t) = ? \zeta_X(t) \zeta_Y(t)$ ?
- $\zeta_{X \times Y} = ?$

## 1.2 Statement of Weil Conjectures

1. (Rationality)

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

$$\begin{aligned} P_0(t) &= 1 - t \\ P_{2n}(t) &= 1 - q^n t \\ P_i(t) &= \prod_j (1 - a_{ij}t), \quad a_{ij} \in \mathbb{C}. \end{aligned}$$

2. (Functional Equation and Poincare Duality)

$$\zeta_X(n-t) = \pm q^{\frac{1}{2}(nE)-Et} \zeta(x, t).$$

- 3. (Riemann Hypothesis)
- 4. (Betti Numbers)

### 1.3 Hard Example: An Elliptic Curve

Take  $X = E/\mathbb{F}$ , then  $\alpha_n = q^n - (a^n + \bar{a}^n - 1)$  where  $|a|_{\mathbb{C}} = |\bar{a}|_{\mathbb{C}} = \sqrt{q}$ . Then

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