Weil Conjectures

D. Zack Garza

Monday 20th April, 2020

Contents

1 Notes from Daniel's Office Hours

0. Definition of Zeta functions
1. Statement of the conjectures
2. Easy examples: $\mathbb{P}^n_\daleth, \mathrm{Gr}_\daleth(k,n) = \mathrm{GL}(n,\daleth)/P$ the stabilizer of an $\daleth$-point in $\mathbb{C}^n, \mathbb{F}_{p^n}$.
3. Medium example: $E/\daleth$ 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

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

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

Definition 1.0.1.
Let

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

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

$$X = V(J) = \left\{ \mathbf{x} \in \mathbb{P}^\infty_{\mathbb{F}} \;\middle|\; f_1(\mathbf{x}) = \cdots = f_M(\mathbf{x}) = \mathbf{0} \right\}$$

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

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

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

Fix $X/\mathbb{F} \subset \mathbb{P}$ an N-dimensional projective algebraic variety, and say it's cut out by the equations $f_1, \cdots f_M \in \mathbb{F}[x_0, \cdots, x_n]$. 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:

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

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

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

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

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

Recall that by integrating a geometric series we can derive

$$\begin{aligned}
\frac{1}{1-z} &= \sum_{n=0}^{\infty} z^n && = 1 + z + z^2 + \cdots\\
\int \frac{1}{1-z} &= \int \sum_{n=0}^{\infty} z^n && = \sum_{n=0}^{\infty}\int z^n = \sum_{n=0}^{\infty}\frac{1}{n+1}z^{n+1} = z + \frac{1}{2}z^2 + \frac{1}{3}z^3 + \cdots\\
\implies \ln(1-z) &= \sum_{n=1}^{\infty}\frac{z^n}{n}.
\end{aligned}$$

and so

$$\begin{aligned}
\zeta_{\{\mathrm{pt}\}}(t) &= \exp\left(1\cdot t + 1\cdot\frac{t^2}{2} + 1\cdot\frac{t^3}{3} + \cdots\right)\\
&= \exp\left(-\log(1-t)\right)\\
&= \frac{1}{1-t}.
\end{aligned}$$

1.1.2 Aside: Why call it a Zeta function?

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

Suppose

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

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

$$\mathbb{A}^n_{\mathbb{F}_p} \supseteq X_p \coloneqq V(\langle f_1 \mod p, \cdots, f_d \mod p\rangle) \quad \text{where} \quad f_1 \mod p \in \mathbb{F}_p[x_0, \cdots, x_{n-1}]$$

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.

Then $X = \operatorname{Spec} \mathbb{Q}$ 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

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

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

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

which we can think of as attaching a "weight" to each closed point, $|x| \coloneqq p^{\deg(x)}$, 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).

1.2 Statement of Weil Conjectures

1. (Rationality) $\zeta_X(z)$ is a rational function:

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

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

2. (Functional Equation and Poincare Duality) Let E be the self-intersection number of the diagonal embedding $\Delta \hookrightarrow X \times X$; then

$$\zeta_X\left(\frac{1}{q^n z}\right) = \pm q^{\frac{nE}{2}} \cdot z^E \cdot \zeta_X(t).$$

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

Remarks:

- Resolved for varieties over $\mathbb{F}_q$
- 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 More Examples

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

$$\mathbb{A}^1(\mathbb{F}_n) = \left\{ \mathbf{x} = [x_1] \;\middle|\; x_1 \in \mathbb{F}_n \right\}$$

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

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

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

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

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:

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

Thus

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

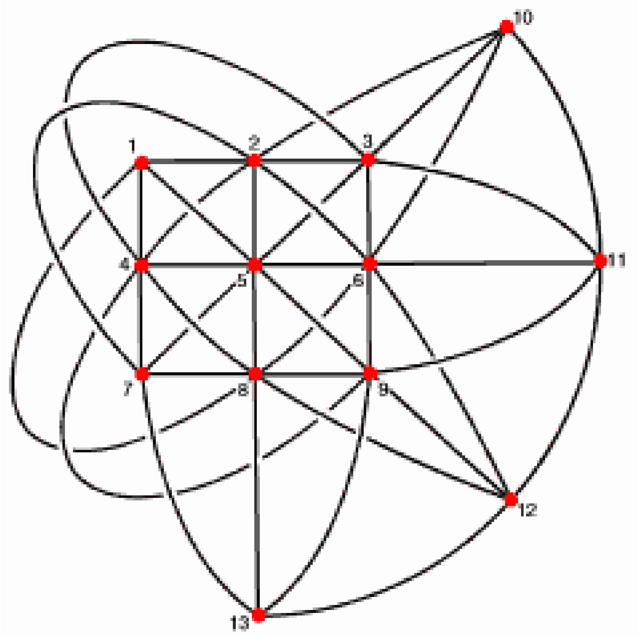
Thus

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

.

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

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



Note that we can identify $X = \mathrm{Gr}_{\mathbb{F}}(1, n)$ 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:

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

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 $\#\text{span}\{\mathbf{v}_1\} = \#\left\{\lambda \mathbf{v}_1 \;\middle|\; \lambda \in \mathbb{F}\right\} = \#\mathbb{F} = q$.
- Choose a nonzero vector $\mathbf{v}_2$ *not* in the span of $\mathbf{v}_1$ in

$$q^m - q$$

  ways.
  - Identify $\#\text{span}\{\mathbf{v}_1, \mathbf{v}_2\} = \#\left\{\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 \;\middle|\; \lambda_i \in \mathbb{F}\right\} = q \cdot q = q^2$.
- 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 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

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

■

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

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

Thus

$$\begin{aligned}
X(\mathbb{F}) &= \sum_{j=0}^{m-1} q^j \\
X(\mathbb{F}_2) &= \sum_{j=0}^{m-1} \left(q^2\right)^j \\
&\vdots \\
X(\mathbb{F}_n) &= \sum_{j=0}^{m-1} (q^n)^j.
\end{aligned}$$

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

$$\zeta_{X \coprod Y}(z) = \zeta_X(z) \cdot \zeta_Y(z)$$

and recalling that $\zeta_{\mathbb{A}^j}(z) = \dfrac{1}{1 - q^j z}$ 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 $X = \mathrm{Gr}_{\mathbb{F}}(k, n)$, then ????? so

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

1.3 Hard Example: An Elliptic Curve

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

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