CRAG

The Weil Conjectures

D. Zack Garza

April 2020

A Quick Note

- A big thanks to Daniel Litt for organizing this reading seminar, recommending papers, helping with questions!!
- Goals for this talk:
  - Understand the Weil conjectures,
  - Understand *why* the relevant objects should be interesting,
  - See elementary but concrete examples,
  - Count all of the things!

Generating Functions

Varieties

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

$$\mathbb{F}_{q^n} = \left\{ x \in \bar{\mathbb{F}}_q \;\middle|\; x^{q^n} - x = 0 \right\} \quad \forall\ n \in \mathbb{Z}^{\geq 1}$$

Definition (Projective Algebraic Varieties)

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 described as

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

where J is generated by *homogeneous* polynomials in $n+1$ variables, i.e. there is a fixed $d = \deg f_i \in \mathbb{Z}^{\geq 1}$ such that

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

Point Counts

- For a fixed variety X, we can consider its $\mathbb{F}_q$-points $X(\mathbb{F}_q)$.
  - Note that $\#X(\mathbb{F}_q) < \infty$ is an integer
- For any $L/\mathbb{F}_q$, we can also consider $X(L)$
  - For $[L : \mathbb{F}_q]$ finite, $\#X(L) < \infty$ and are integers for every such n.
  - In particular, we can consider the finite counts $\#X(\mathbb{F}_{q^n})$ for any $n \geq 2$.
- So we can consider the sequence

$$[N_1, N_2, \cdots, N_n, \cdots] := [\#X(\mathbb{F}_q),\ \#X(\mathbb{F}_{q^2}), \cdots,\ \#X(\mathbb{F}_{q^n}), \cdots].$$

- Idea: associate some generating function (a formal power series) encoding the sequence, e.g.

$$F(z) = \sum_{n=1}^{\infty} N_n z^n = N_1 z + N_2 z^2 + \cdots.$$

Why Generating Functions?

For *ordinary* generating functions, the coefficients are related to the real-analytic properties of F:

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

and also to the complex analytic properties:

$$[z^n] \cdot F(z) := \frac{1}{2\pi i} \oint_{\mathbb{S}^1} \frac{F(z)}{z^{n+1}} \, dz = \frac{1}{2\pi i} \oint_{\mathbb{S}^1} \frac{N_n}{z} \, dz = N_n.$$

Using the Residue theorem. The latter form is very amenable to computer calculation.

Why Generating Functions?

- An OGF is an infinite series, which we can interpret as an analytic function $\mathbb{C} \longrightarrow \mathbb{C}$
- In nice situations, we can hope for a closed-form representation.
- A useful example: by integrating a geometric series we can derive

$$
\begin{aligned}
\frac{1}{1-z} &= \sum_{n=0}^{\infty} z^n \qquad\qquad (= 1 + z + z^2 + \cdots) \\
\implies \int \frac{1}{1-z} &= \int \sum_{n=0}^{\infty} z^n \\
&= \sum_{n=0}^{\infty} \int z^n \quad for |z| < 1 \quad \text{by uniform convergence} \\
&= \sum_{n=0}^{\infty} \frac{1}{n+1} z^{n+1} \\
\implies -\log(1-z) &= \sum_{n=1}^{\infty} \frac{z^n}{n} \qquad\qquad \left(= z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots\right).
\end{aligned}
$$

Exponential

- For completeness, also recall that

$$\exp(z) := \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

- We can regard **exp**, **log** as elements in the ring of formal power series $\mathbb{Q}[[z]]$.
- In particular, for any $p(z) \in z \cdot \mathbb{Q}[[z]]$ we can consider $\exp(p(z)), \log(1 + p(z))$
- Since $\mathbb{Q} \hookrightarrow \mathbb{C}$, we can consider these as a complex-analytic functions, ask where they converge, etc.

Zeta Functions

Definition: Local Zeta Function

Problem: count points of a (smooth?) projective variety $X/\mathbb{F}$ in all (finite) degree n extensions of $\mathbb{F}$.

Definition (Local Zeta Function)

The *local zeta function* of an algebraic variety X is the following formal power series:

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

Note that

$$\begin{aligned} z\left(\frac{\partial}{\partial z}\right) \log Z_X(z) &= z \frac{\partial}{\partial z}\left(N_1 z + N_2 \frac{z^2}{2} + N_3 \frac{z^3}{3} + \cdots \right) \\ &= z\left(N_1 + N_2 z + N_3 z^2 + \cdots\right) \qquad \text{(unif. conv.)} \\ &= N_1 z + N_2 z^2 + \cdots = \sum_{n=1}^{\infty} N_n z^n, \end{aligned}$$

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

Examples

Example: A Point

Take $X = \{\mathrm{pt}\} = V(\{f(x) = 0\})/\mathbb{F}$ a single point over $\mathbb{F}$, then

$$\begin{aligned}
\#X(\mathbb{F}_q) &\coloneqq N_1 = 1 \\
\#X(\mathbb{F}_{q^2}) &\coloneqq N_2 = 1 \\
&\vdots \\
\#X(\mathbb{F}_{q^n}) &\coloneqq N_n = 1 \\
&\ddots
\end{aligned}$$

and so

$$\begin{aligned}
Z_{\{\mathrm{pt}\}}(z) &= \exp\left(1 \cdot z + 1 \cdot \frac{z^2}{2} + 1 \cdot \frac{z^3}{3} + \cdots\right) \\
&= \exp\left(\sum_{n=1}^{\infty} \frac{z^n}{n}\right) \\
&= \exp\left(-\log\left(1 - z\right)\right) \\
&= \frac{1}{1 - z}.
\end{aligned}$$

Notice: Z admits a closed form **and** *is a rational function.*

Example: The Affine Line

Take $X = \mathbb{A}^1/\mathbb{F}$ the affine line over $\mathbb{F}$, then We can write

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

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

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

Then

$$\begin{aligned} Z_X(z) &= \exp\left(\sum_{n=1}^{\infty} q^n \frac{z^n}{n} \right) \\ &= \exp\left(\sum_{n=1}^{\infty} \frac{(qz)^n}{n} \right) \\ &= \exp(-\log(1 - qz)) \\ &= \frac{1}{1 - qz}. \end{aligned}$$

Example: Affine m-space

Take $X = \mathbb{A}^m/\mathbb{F}$ the affine line over $\mathbb{F}$, then We can write

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

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

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

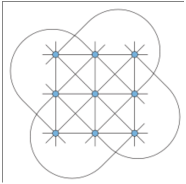


Figure: $\mathbb{A}^2/\mathbb{F}_3$ $(q = 3, m = 2, n = 1)$

Then

$$\begin{aligned} Z_X(z) &= \exp\left(\sum_{n=1}^{\infty} q^{nm} \frac{z^n}{n} \right) = \exp\left(\sum_{n=1}^{\infty} \frac{(q^m z)^n}{n} \right) \\ &= \exp(-\log(1 - q^m z)) \\ &= \frac{1}{1 - q^m z}. \end{aligned}$$

Example: Projective Line

Take $X = \mathbb{P}^1/\mathbb{F}$, we can still count by enumerating coordinates:

$$\mathbb{P}^1(\mathbb{F}_{q^n}) = \left\{ [x_1 : x_2] \;\middle|\; x_1, x_2 \neq 0 \in \mathbb{F}_{q^n} \right\} / \sim \quad = \left\{ [x_1 : 1] \;\middle|\; x_1 \in \mathbb{F}_{q^n} \right\} \coprod \{[1:0]\}.$$

Thus

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

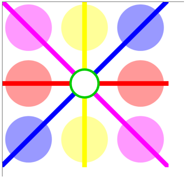


Figure: $\mathbb{P}^1/\mathbb{F}_3$ $(q = 3, n = 1)$

Thus

$$\begin{aligned} Z_X(z) &= \exp\left(\sum_{n=1}^\infty (q^n + 1) \frac{z^n}{n} \right) \\ &= \exp\left(\sum_{n=1}^\infty q^n \frac{z^n}{n} + \sum_{n=1}^\infty 1 \cdot \frac{z^n}{n} \right) \\ &= \frac{1}{(1 - qz)(1 - z)}. \end{aligned}$$

The Weil Conjectures

Weil 1

(Weil 1949)

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

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

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

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

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

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

where we've factored each P_i using its reciprocal roots a_{ij}.
In particular, this implies the existence of a meromorphic continuation of the associated function $\zeta_X(s)$, which a priori only converges for $\Re(s) \gg 0$. This also implies that for n large enough, N_n satisfies a linear recurrence relation.

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 $Z_X(z)$ satisfies the following *functional equation*:

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

Equivalently,

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

Note that when $N=1$, e.g. for a curve, this relates $\zeta_X(s)$ to $\zeta_X(1-s)$.

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

$$\begin{aligned} z &\iff \frac{q^N}{z} \\ \alpha_{j,k} &\iff \alpha_{2N-j,k} \end{aligned}$$

which sends interchanges the coefficients in p_j and p_{2N-j}.

Weil 3

CRAG

D. Zack Garza

Generating Functions

Zeta Functions

Examples

The Weil Conjectures

Weil for Curves

Weil for Projective m-space

Grassmannians

Weil's Proof

3. (Riemann Hypothesis)
   The reciprocal roots $\alpha_{j,k}$ are *algebraic* integers (roots of some monic $p \in \mathbb{Z}[x]$) which satisfy

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

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

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.

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

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 to obtain $\widehat{\zeta}(s)$, there are three relevant properties

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

Suppose it holds for some X. Use the facts:

a. $|\exp(z)| = \exp(\Re(z))$ and
b. $a^z := \exp(z \operatorname{Log}(a))$,

and to replace the polynomials P_j with

$$L_j(s) := P_j(q^{-s}) = \prod_{k=1}^{\beta_j} \left(1 - \alpha_{j,k} q^{-s}\right).$$

Analogy to Riemann Hypothesis

Now consider the roots of $L_j(s)$: we have

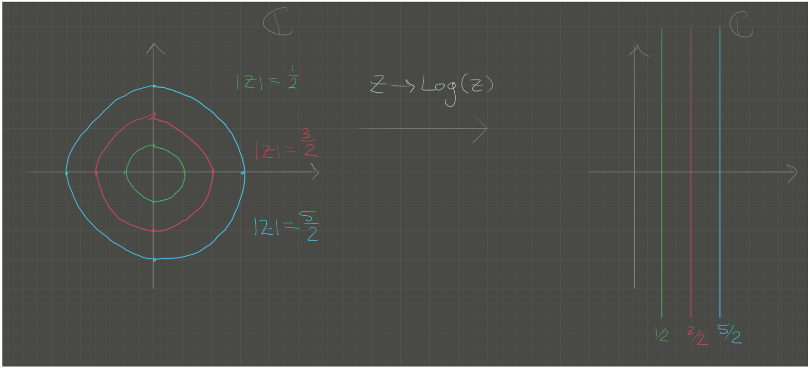
$$
\begin{aligned}
L_j(s_0) = 0 \iff (1 - \alpha_{j,k} q^{-s}) = 0 \quad \text{for some} \quad k \\
\iff q^{-s_0} = \frac{1}{\alpha_{j,k}} \\
\iff \left| q^{-s_0} \right| = \left| \frac{1}{\alpha_{j,k}} \right| \quad \overset{\text{by assumption}}{=} \quad q^{-\frac{j}{2}}
\end{aligned}
$$

$$
\begin{aligned}
\iff q^{-\frac{j}{2}} \overset{(a)}{=} \exp\left(-\frac{j}{2} \cdot \operatorname{Log}(q)\right) &= \left|\exp\left(-s_0 \cdot \operatorname{Log}(q)\right)\right| \\
&\overset{(b)}{=} \left|\exp\left(-(\Re(s_0) + i \cdot \Im(s_0)) \cdot \operatorname{Log}(q)\right)\right| \\
&\overset{(a)}{=} \exp\left(-(\Re(s_0)) \cdot \operatorname{Log}(q)\right)
\end{aligned}
$$

$$
\begin{aligned}
\iff -\frac{j}{2} \cdot \operatorname{Log}(q) = -\Re(s_0) \cdot \operatorname{Log}(q) \quad \text{by injectivity} \\
\iff \Re(s_0) = \frac{j}{2}.
\end{aligned}
$$

Analogy with Riemann Hypothesis

Roughly speaking, we can apply log (a conformal map) to send the $\alpha_{j,k}$ to zeros of the L_j, this says that the zeros all must lie on the "critical lines" $\frac{j}{2}$.



In particular, the zeros of L_1 have real part $\frac{1}{2}$ (analogy: classical Riemann hypothesis).

Precise Relation

- Difficult to find in the literature!
- Idea: make a similar definition for schemes, then take $X = \operatorname{Spec} \mathbb{Z}$.
- Define the "reductions mod p" X_p for closed points p.
- Define the *local* zeta functions $\zeta_{X_p}(s) = Z_{X_p}(p^{-s})$.
- (Potentially incorrect) Evaluate to find $Z_{X_p}(z) = \frac{1}{1-z}$.
- Take a product over all closed points to define

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

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

If anyone knows a reference for this, let me know!

Weil for Curves

Weil for Curves

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

1. (Rationality)

$$Z_X(z) = \frac{p_1(z)}{p_0(z)p_2(z)} = \frac{p_1(z)}{(1-z)(1-qz)}$$

2. (Functional Equation)

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

3. (Riemann Hypothesis)

$$p_1(z) = \prod_{i=1}^{\beta_1}(1-a_i z) \quad \text{where} \quad |a_i| = \sqrt{q}$$

4. (Betti Numbers) $\mathcal{P}_{\Sigma_g}(x) = 1 + 2g\cdot x + x^2 \implies \deg p_1 = \beta_1 = 2g$.

The Projective Line

Recall $Z_{\mathbb{P}^1/\mathbb{F}_q}(z) = \frac{1}{(1-z)(1-qz)}$.

1. Rationality: Clear!
2. Functional Equation: $g = 0 \implies 2g - 2 = 2$

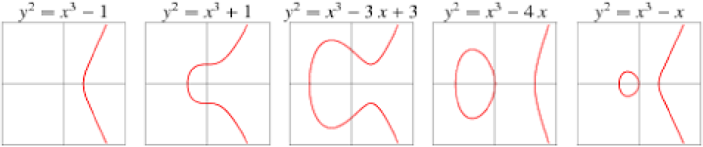
$$Z_{\mathbb{P}^1}\left(\frac{1}{qz}\right) = \frac{1}{(1-\frac{1}{qz})(1-\frac{q}{qz})} = \frac{qz^2}{(1-z)(1-qz)} = \frac{(\sqrt{q}z)^2}{(1-z)(1-qz)}.$$

3. Riemann Hypothesis: Nothing to check (no $p_1(z)$)
4. Betti numbers: Use the fact that $\mathcal{P}_{\mathbb{CP}^1} = 1 + 0 \cdot x + x^2$, and indeed $\deg p_0 = \deg p_2 = 1, \;\; \deg p_1 = 0$.

   Note that even Betti numbers show up as degrees in the denominator, odd in the numerator. Allows us to immediately guess the zeta function for $\mathbb{P}^n/\mathbb{F}_q$ by knowing $H^*\mathbb{CP}^\infty$!

Elliptic Curves

Figure: Some Elliptic Curves



Consider $E/\mathbb{F}_q$.

- (Nontrivial!) The number of points is given by

$$N_n := E(\mathbb{F}_{q^n}) = (q^n + 1) - (\alpha^n + \overline{\alpha}^n) \quad \text{where} \quad |\alpha| = |\overline{\alpha}| = \sqrt{q}$$

  - Proof: Involves trace (or eigenvalues?) of Frobenius, (could use references)
- $\dim_{\mathbb{C}} E/\mathbb{C} = N = 1$ and $g = 1$.

The Weil Conjectures say we should be able to write

$$Z_E(z) = \frac{p_1(z)}{p_0(z)p_2(z)} = \frac{p_1(z)}{(1-z)(1-qz)} = \frac{(1-a_1 z)(1-a_2 z)}{(1-z)(1-qz)}.$$

Elliptic Curves: Weil 1

1. Rationality: using the point count, we can compute

$$\begin{aligned}
Z_E(z) &= \exp \sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{z^n}{n} \\
&= \exp \sum_{n=1}^{\infty} (q^n + 1 - (\alpha^n + \bar{\alpha}^n)) \frac{z^n}{n} \\
&= \exp \left(\sum_{n=1}^{\infty} q^n \cdot \frac{z^n}{n} \right) \exp \left(\sum_{n=1}^{\infty} 1 \cdot \frac{z^n}{n} \right) \\
&\qquad \exp \left(\sum_{n=1}^{\infty} -\alpha^n \cdot \frac{z^n}{n} \right) \exp \left(\sum_{n=1}^{\infty} -\bar{\alpha}^n \cdot \frac{z^n}{n} \right) \\
&= \exp\left(-\log\left(1 - qz\right)\right) \cdot \exp\left(-\log\left(1 - z\right)\right) \\
&\qquad \exp\left(\log\left(1 - \alpha z\right)\right) \cdot \exp\left(\log\left(1 - \bar{\alpha} z\right)\right) \\
&= \frac{(1 - \alpha z)(1 - \bar{\alpha} z)}{(1 - z)(1 - qz)} \in \mathbb{Q}(z),
\end{aligned}$$

which is a rational function of the expected form (Weil 1).

2. Functional Equation: we use the equivalent formulation of "Poincare duality":

$$\frac{(1-\alpha z)(1-\bar{\alpha} z)}{(1-z)(1-qz)} = \frac{p_1(z)}{p_0(z)p_2(z)} \implies \begin{cases} z & \iff \frac{q}{z} \\ \alpha_{j,k} & \iff \alpha_{2-j,k} \end{cases}$$

This amounts to checking that the coefficients of p_0, p_2 are interchanged, and that the two coefficients of p_1 are interchanged:

$$\mathrm{Coefs}(p_0) = \{1\} \xrightarrow{z \longrightarrow \frac{q}{z}} \left\{ \frac{1}{q} \right\} = \mathrm{Coefs}(p_2)$$

$$\mathrm{Coefs}(p_1) = \{\alpha, \bar{\alpha}\} \xrightarrow{z \longrightarrow \frac{q}{z}} \left\{ \frac{q}{\alpha}, \frac{q}{\bar{\alpha}} \right\} = \{\bar{\alpha}, \alpha\} \quad \text{using} \quad \alpha\bar{\alpha} = q.$$

3. RH: Assumed as part of the point count ($|\alpha| = q^{\frac{1}{2}}$)
4. Betti Numbers: $\mathcal{P}_{\Sigma_1}(x) = 1 + 2x + x^2$, and indeed $\deg p_0 = \deg p_2 = 1, \ \deg p_1 = 2$.

History

- 1801, Gauss: Point count and RH showed for specific elliptic curves
- 1924, Artin: Conjectured for algebraic curves ,
- 1934, Hasse: proved for elliptic curves.
- 1949, Weil: Proved for smooth projective curves over finite fields, proposed generalization to projective varieties
- 1960, Dwork: Rationality via p-adic analysis
- 1965, Grothendieck et al.: Rationality, functional equation, Betti numbers using étale cohomology
  - Trace of Frobenius on ℓ-adic cohomology)
  - Expected proof via *the standard conjectures*.
- 1974, Deligne: Riemann Hypothesis using étale cohomology, circumvented the standard conjectures
- Recent: Hasse-Weil conjecture for arbitrary algebraic varieties over number fields
  - Similar requirements on L-functions: functional equation, meromorphic continuation
  - 2001: Full modularity theorem proved, extending Wiles, implies HW for elliptic curves
  - Inroad in Langlands: show every L function coming from an algebraic variety also comes from an automorphic representation.

Weil for Projective m-space

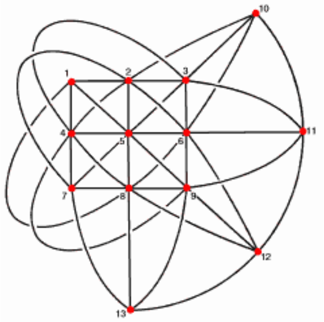
Setup

Take $X = \mathbb{P}^m/\mathbb{F}$ We can write

$$\mathbb{P}^m(\mathbb{F}_{q^n}) = \mathbb{A}^{m+1}(\mathbb{F}_{q^n}) \setminus \{\mathbf{0}\} / \sim \quad = \left\{ \mathbf{x} = [x_0, \cdots, x_m] \;\middle|\; x_i \in \mathbb{F}_{q^n} \right\} / \sim$$

But how many points are actually in this space?

Figure: Points and Lines in $\mathbb{P}^2/\mathbb{F}_3$



A nontrivial combinatorial problem!

To illustrate, this can be done combinatorially: identify $\mathbb{P}^m_{\mathbb{F}} = \mathrm{Gr}_{\mathbb{F}}(1, m+1)$ as the space of lines in $\mathbb{A}^{m+1}_{\mathbb{F}}$.

Theorem

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

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

Remark: Note $\lim_{q \longrightarrow 1} \begin{bmatrix} N \\ k \end{bmatrix}_q = \binom{N}{k}$*, the usual binomial coefficient.*

Proof: To choose a k-dimensional subspace,

- Choose a nonzero vector $\mathbf{v}_1 \in \mathbb{A}^n_{\mathbb{F}}$ in $q^N - 1$ ways.
  - For next step, note that $\#\mathrm{span}\{v_1\} = \#\left\{\lambda v_1 \;\middle|\; \lambda \in \mathbb{F}_q\right\} = \#\mathbb{F}_q = q$.
- Choose a nonzero vector $\mathbf{v}_2$ *not* in the span of $\mathbf{v}_1$ in $q^N - q$ ways.
  - Now note $\#\mathrm{span}\{v_1, v_2\} = \#\left\{\lambda_1 v_1 + \lambda_2 v_2 \;\middle|\; \lambda_i \in \mathbb{F}\right\} = q \cdot q = q^2$.

Proof continued

- Choose a nonzero vector $\mathbf{v}_3$ *not* in the span of $\mathbf{v}_1, \mathbf{v}_2$ in $q^N - q^2$ ways.
- $\cdots$ until $\mathbf{v}_k$ is chosen in

$$(q^N - 1)(q^N - q)\cdots(q^N - q^{k-1}) \quad \text{ways}$$

.

  - 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 ways to 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

$$\#\text{subspaces} = \frac{(q^N-1)(q^N-q)(q^N-q^2)\cdots(q^N-q^{k-1})}{(q^k-1)(q^k-q)(q^k-q^2)\cdots(q^k-q^{k-1})}$$

$$= \frac{q^N-1}{q^k-1}\cdot\left(\frac{q}{q}\right)\frac{q^{N-1}-1}{q^{k-1}-1}\cdot\left(\frac{q^2}{q^2}\right)\frac{q^{N-2}-1}{q^{k-2}-1}\cdots\left(\frac{q^{k-1}}{q^{k-1}}\right)\frac{q^{N-(k-1)}-1}{q^{k-(k-1)-1}}$$

$$= \frac{(q^N-1)(q^{N-1}-1)\cdots(q^{N-(k-1)}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Note that we've actually computed the number of points in any Grassmannian.

Identify $\mathbb{P}^m_{\mathbb{F}} = \mathrm{Gr}_{\mathbb{F}}(1, m+1)$ as the space of lines in $\mathbb{A}^{m+1}_{\mathbb{F}}$.

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

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

Thus

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

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

$$\vdots$$

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

Computing the Zeta Function

So

$$
\begin{aligned}
Z_X(z) &= \exp\left(\sum_{n=1}^{\infty}\sum_{j=0}^{m}(q^n)^j \frac{z^n}{n}\right) \\
&= \exp\left(\sum_{n=1}^{\infty}\sum_{j=0}^{m}\frac{\left(q^j z\right)^n}{n}\right) \\
&= \exp\left(\sum_{j=0}^{m}\sum_{n=1}^{\infty}\frac{\left(q^j z\right)^n}{n}\right) \\
&= \exp\left(\sum_{j=0}^{m-1} -\log(1-q^j z)\right) \\
&= \prod_{j=0}^{m}\left(1-q^j z\right)^{-1} \\
&= \left(\frac{1}{1-z}\right)\left(\frac{1}{1-qz}\right)\left(\frac{1}{1-q^2 z}\right)\cdots\left(\frac{1}{1-q^m z}\right),
\end{aligned}
$$

Miraculously, still a rational function!

$$Z_X(z) = \prod_{j=0}^{m} \left(\frac{1}{1-q^j z} \right).$$

1. Rationality: Clear!
2. Functional Equation: Less clear, but true:

$$\begin{aligned}
Z_X\left(\frac{1}{q^m z}\right) &= \frac{1}{(1-1/q^m t)\,(1-q/q^m t)\cdots(1-q^m/q^m z)} \\
&= \frac{q^m z \cdot q^{m-1} z \ldots qz \cdot z}{(1-z)(1-qz)\ldots(1-q^m z)} \\
&= q^{\frac{m(m+1)}{2}} z^{m+1} \cdot Z_X(z) \\
&= \left(q^{\frac{m}{2}} z\right)^{\chi(X)} \cdot Z_X(z)
\end{aligned}$$

.

Checking

$$Z_X(z) = \prod_{j=0}^{m} \left(\frac{1}{1 - q^j z} \right).$$

3. Riemann Hypothesis: Reduces to the statement $\{\alpha_i\} = \left\{ \frac{q^m}{\alpha_j} \right\}$.
4. Betti Numbers: Use the fact that $\mathcal{P}_{\mathbb{CP}^m}(x) = 1 + x^2 + x^4 + \cdots + x^{2m}$.

An Easier Proof: "Paving"

Quick recap:

$$Z_{\{\mathrm{pt}\}} = \frac{1}{1-z} \qquad Z_{\mathbb{P}^1}(z) = \frac{1}{1-qz} \qquad Z_{\mathbb{A}^1}(z) = \frac{1}{(1-z)(1-qz)}.$$

Note that $\mathbb{P}^1 = \mathbb{A}^1 \coprod \{\infty\}$ and correspondingly $Z_{\mathbb{P}^1}(z) = Z_{\mathbb{A}^1}(z) \cdot Z_{\{\mathrm{pt}\}}(z)$.
This works in general:

Lemma (Excision)

If $Y/\mathbb{F}_q \subset X/\mathbb{F}_q$ is a closed subvariety, for $U = X \setminus Y$,
$Z_X(z) = Z_Y(z) \cdot Z_U(z)$.

Proof: Let $N_n = \#Y(\mathbb{F}_{q^n})$ and $M_n = \#U(\mathbb{F}_{q^n})$, then

$$\begin{aligned}
\zeta_X(z) &= \exp\left(\sum_{n=1}^{\infty} (N_n + M_n)\frac{z^n}{n}\right) \\
&= \exp\left(\sum_{n=1}^{\infty} N_n \cdot \frac{z^n}{n} + \sum_{n=1}^{\infty} M_n \cdot \frac{z^n}{n}\right) \\
&= \exp\left(\sum_{n=1}^{\infty} N_n \cdot \frac{z^n}{n}\right) \cdot \exp\left(\sum_{n=1}^{\infty} M_n \cdot \frac{z^n}{n}\right) = \zeta_Y(z) \cdot \zeta_U(z).
\end{aligned}$$

An Easier Proof: "Paving"

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

$$\mathbb{P}^m = \coprod_{j=0}^{m} \mathbb{A}^j = \mathbb{A}^0 \coprod \mathbb{A}^1 \coprod \cdots \coprod \mathbb{A}^m,$$

and recalling that

$$Z_{X \coprod Y}(z) = Z_X(z) \cdot Z_Y(z)$$

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

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

Grassmannians

Motivation

Consider now $X = \mathrm{Gr}(k,m)/\mathbb{F}$ – by the previous computation, we know

$$X(\mathbb{F}_{q^n}) = \begin{bmatrix} m \\ k \end{bmatrix}_{q^n} := \frac{(q^{nm}-1)(q^{nm-1}-1)\cdots(q^{nm-n(k-1)}-1)}{(q^{nk}-1)(q^{n(k-1)}-1)\cdots(q^n-1)}$$

but the corresponding Zeta function is much more complicated than the previous examples:

$$Z_X(z) = \exp\left(\sum_{n=1}^\infty \begin{bmatrix} m \\ k \end{bmatrix}_{q^n} \frac{z^n}{n}\right) = \cdots ?.$$

Since $\dim_{\mathbb{C}} \mathrm{Gr}_{\mathbb{C}}(k,m) = 2k(m-k)$, by Weil we should expect

$$Z_X(z) = \prod_{j=0}^{2k(m-k)} \frac{p_{2(j+1)}(z)}{p_{2j}(z)}$$

with $\deg p_j = \beta_j$.

Grassmannian

It turns out that (proof omitted) one can show

$$\begin{bmatrix} m \\ k \end{bmatrix}_q = \sum_{j=0}^{k(m-k)} \lambda_{m,k}(j) q^j \implies Z_X(z) = \prod_{j=0}^{k(m-k)} \left(\frac{1}{1 - q^j x} \right)^{\lambda_{m,k}(j)}$$

where $\lambda_{m,k}$ is the number of integer partitions of of $[i]$ into at most $m-k$ parts, each of size at most k.

- One proof idea: use combinatorial identities to write q-analog $\begin{bmatrix} m \\ k \end{bmatrix}_q$ as a *sum*
- Second proof idea: "pave by affines".

This lets us conclude that the Poincare polynomial of the complex Grassmannian is given by

$$\mathcal{P}_{\mathrm{Gr}_{\mathbb{C}}(m,k)}(x) = \sum_{n=1}^{k(m-k)} \lambda_{m,k}(n) x^{2n},$$

In particular, the cohomology vanishes in odd degree.

Weil's Proof

Proof of rationality of $Z_X(T)$ for X a diagonal hypersurface.

- Set q to be a prime power and consider $X/\mathbb{F}_q$ defined by

$$X = V(a_0 x_0^n + \cdots + a_r x_r^n) \subset \mathbb{F}_q^{r+1}.$$

- We want to compute $N = \# X$.
- Set $d_i = \gcd(n_i, q-1)$.
- Define the character

$$\begin{aligned} \psi_q : \mathbb{F}_q &\longrightarrow \mathbb{C}^\times \\ a &\mapsto \exp\left(\frac{2\pi i \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}{p} \right). \end{aligned}$$

  - By Artin's theorem for linear independence of characters, $\psi_q \not\equiv 1$ and every additive character of $\mathbb{F}_q$ is of the form $a \mapsto \psi_q(ca)$ for some $c \in \mathbb{F}_q$.
- Shorthand notation: say $a \sim 0 \iff a \equiv 0 \mod 1$.

A Diagonal Hypersurface

- Fix an injective multiplicative map

$$\phi : \bar{\mathbb{F}}_q^\times \longrightarrow \mathbb{C}^\times.$$

- Define

$$\begin{aligned}\chi_{\alpha,n} : \mathbb{F}_{q^n}^\times &\longrightarrow \mathbb{C}^\times \\ x &\mapsto \phi(x)^{\alpha(q^n-1)}\end{aligned}$$

$$\text{for} \quad \alpha \in \mathbb{Q}/\mathbb{Z}, n \in \mathbb{Z}, \quad \alpha(q^n - 1) \equiv 0 \mod 1.$$

  - Extend this to $\mathbb{F}_{q^n}$ by

$$\begin{cases} 1 & \alpha \equiv 0 \mod 1 \\ 0 & \text{else} \end{cases}.$$

  - Set $\chi_\alpha = \chi_{\alpha,1}$.

- Proposition:

$$\alpha(q-1) \equiv 0 \mod 1 \implies \chi_{\alpha,n}(x) = \chi_\alpha(\mathrm{Nm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$$

- Proposition:

$$d := \gcd(n, q-1), u \in \mathbb{F}_q \implies \#\left\{x \in \mathbb{F}_q \;\middle|\; x^n = u\right\} = \sum_{d\alpha \sim 0} \chi_\alpha(u)$$

A Diagonal Hypersurface

- This implies

$$N = \sum_{\substack{\alpha=[\alpha_0,\cdots,\alpha_r] \\ d_i\alpha_i\sim 0}} \sum_{\substack{u=[u_0,\cdots,u_r] \\ \sum a_i u_i = 0}} \prod_{j=0}^{r} \chi_{\alpha_j}(u_j)$$

$$= q^r + \sum_{\substack{\alpha,\ \alpha_i\in(0,1) \\ d_i\alpha_i\sim 0}} \left(\prod_{j=0}^{r} \chi_{\alpha_j}(a_j^{-1}) \sum_{\sum u_i = 0} \prod_{j=0}^{r} \chi_{\alpha_j}(u_j) \right).$$

since the inner sum is zero if some *but not all* of the $\alpha_i \sim 0$.

- Evaluate the innermost sum by restricting to $u_0 \neq 0$ and setting $u_i = u_0 v_i$ and $v_0 := 1$:

$$\sum_{\sum u_i=0} \prod_{j=0}^{r} \chi_{\alpha_j}(u_j) = \sum_{u_0\neq 0} \chi_{\sum \alpha_i}(u_0) \sum_{\sum v_i = 0} \prod_{j=0}^{r} \chi_{\alpha_j}(v_j)$$

$$= \begin{cases} (q-1) \sum_{\sum v_i=0} \prod_{j=0}^{r} \chi_{\alpha_j}(v_j) & \text{if} \quad \sum \alpha_i \sim 0 \\ 0 & \text{else} \end{cases}.$$

A Diagonal Hypersurface

- Define the *Jacobi sum* for α where $\sum \alpha_i \sim 0$:

$$J(\alpha) := \left(\frac{1}{q-1}\right) \sum_{\Sigma\ u_i = 0} \prod_{j=0}^{r} \chi_{\alpha_j}(u_j) = \sum_{\Sigma\ v_i = 0} \prod_{j=1}^{r} \chi_{\alpha_j}(v_j)$$

- Express N in terms of Jacobi sums as

$$N = q^r + (q-1) \sum_{\substack{\Sigma \alpha_i \sim 0 \\ d_i \alpha_i \sim 0 \\ \alpha \in (0,1)}} \prod_{j=0}^{r} \chi_{\alpha_j}(a_j^{-1}) J(\alpha).$$

- Evaluate $J(\alpha)$ using Gauss sums: for $\chi : \mathbb{F}_q \longrightarrow \mathbb{C}$ a multiplicative character, define

$$G(\chi) := \sum_{x \in \mathbb{F}_q} \chi(x) \psi_q(x).$$

- Proposition: for any $\chi \neq \chi_0$,
  - $|G(\chi)| = q^{\frac{1}{2}}$
  - $G(\chi)G(\bar{\chi}) = q\chi(-1)$
  - $G(\chi_0) = 0$

$$\chi(t) = \frac{G(\chi)}{q} \sum_{x \in \mathbb{F}_q} \bar{\chi}(x) \psi_q(tx).$$

A Diagonal Hypersurface

- Proposition: if

$$\sum \alpha_i \sim 0 \implies J(\alpha) = \frac{1}{q} \prod_{k=1}^{r} G(\chi_{\alpha_k}) \quad \text{and} \quad |J(\alpha)| = q^{\frac{r-1}{2}}.$$

- We thus obtain

$$N = q^r + \left(\frac{q-1}{q}\right) \sum_{\substack{\Sigma\alpha_i \sim 0 \\ d_i\alpha_i \sim 0 \\ \alpha \in (0,1)}} \prod_{j=0}^{r} \chi_{\alpha_j}(a_j^{-1}) G(\chi_{\alpha_j}).$$

- We now ask for number of points in $\mathbb{F}_{q^\nu}$ and consider a point count

$$\overline{N}_\nu = \#\left\{ [x_0 : \cdots : x_r] \in \mathbb{P}^r_{\mathbb{F}_q^\nu} \;\middle|\; \sum_{i=0}^{r} a_i x_i^n = 0 \right\}.$$

- Theorem (Davenport, Hasse)

$$(q-1)\alpha \sim 0 \implies -G(\chi_{\alpha,\nu}) = (-G(\chi_\alpha))^\nu.$$

A Diagonal Hypersurface

- We have a relation $(q^\nu - 1)\overline{N}_\nu = N_\nu$.
- This lets us write

$$\overline{N}_\nu = \sum_{j=0}^{r-1} q^{j\nu} + \sum_{\substack{\sum \alpha_i \sim 0 \\ \gcd(n, q^\nu - 1)\alpha_i \sim 0 \\ \alpha_i \in (0,1)}} \prod_{j=0}^{r} \overline{\chi}_{\alpha_{j,\nu}}(a_i) J_\nu(\alpha).$$

- Set

$$\mu(\alpha) = \min\left\{ \mu \;\middle|\; (q^\mu - 1)\alpha \sim 0 \right\}$$

$$C(\alpha) = (-1)^{r+1} \prod_{j=1}^{r} \overline{\chi}_{\alpha_0, \mu(\alpha)}(a_j) \cdot J_{\mu(\alpha)}(\alpha).$$

- Plugging into the zeta function Z yields

$$\exp\left(\sum_{\nu=1}^{\infty} \overline{N}_\nu \frac{T^\nu}{\nu} \right) = \prod_{j=0}^{r-1} \left(\frac{1}{1 - q^j T} \right) \prod_{\substack{\sum \alpha_i \sim 0 \\ \gcd(n, q^\nu - 1)\alpha_i \sim 0 \\ \alpha_i \in (0,1)}} \left(1 - C(\alpha) T^{\mu(\alpha)} \right)^{\frac{(-1)^r}{\mu(\alpha)}},$$

which is evidently a rational function.