Notes on Weil Conjectures

D. Zack Garza

January 20, 2020

Contents

Reference: Andre Weil, Numbers of Solutions of Equations in Finite Fields

1 External Background

Here we fix a prime p and a system of polynomials $S = \{f_i\}$ of degree n, take the variety $V(S)$ and let

- a_1 be its number of points of $\mathbb{F}_p$
- a_2 be its number of points of $\mathbb{F}_{p^2}$
- $\cdots a_n$ be its number of points of $\mathbb{F}_{p^n}$

Idea: assemble them into a generating function.

For unknown reasons, we put them in a zeta function instead: $\zeta(x) = \exp\left(\sum \frac{a_n x^n}{n}\right)$.

Conjectures:

1. $\zeta(x) = \frac{P(x)}{Q(x)}$ is a rational function.
2. There is an explicit formula $P(x) = \prod_{i \text{ odd}}^{2n-1} P_i(x)$ and $Q(x) = \prod i \text{ even} P_i(x)$ with each $P_i \in \mathbb{Z}[x]$.

- For every root r of every P_i, $\frac{1}{r}$ is algebraic
- (Riemann Hypothesis) Every root has modulus equal to $p^{-i/2}$ (???)

3. (Functional Equation) The function $z \mapsto \frac{1}{p^n z}$ interchanges roots of P_i with roots of P_{2n-i}.
4. (Under some conditions) $\deg P_i = \beta_i(V)$, the ith Betti number of i.

Relation to fixed points: In $\mathbb{F}_{p^m}$, every point is a fixed point of the Frobenius Φ_{p^m}. So for any field $F \supset \mathbb{F}_{p^m}$, the points in $\mathbb{F}_{p^m}$ are precisely the fixed points of $\Phi_{p^m} : F \to F$ (because enlarging the field can not add more solutions).

Claim: If $S \subset F^d$ is any subset defined by polynomial equations and $x = (x_1, x_2, \cdots, x_n) \in S$ is a point, then $\Phi_{p^m}(x) = (\Phi_{p^m}(x_1), \cdots) \in S$. Moreover, the fixed points of Φ_{p^m} restricted to S are precisely $S \bigcap \mathbb{F}_{p^m}^d$.

Compare 2b above: Riemann says roots are along critical strip $\Re(z) = \frac{1}{2}$; this says roots of P_i are on a circle of radius $p^{i/2}$ about the origin. (Note: there is a (conformal?) map that takes the circle to the line, so we can send the roots of P_i to the line $\Re(z) = \frac{1}{2}$. . . .but not for all i at once.)

Consequences: Riemann-Zeta: error estimates in the prime number theorem agree with probabilistic models Weil: error estimates in Ramanujan's τ is as small as hoped.

Proofs: Grothendieck: 1,3, and 4 with etale cohomology. Notably not Weil 2. Deligne: Weil 2, The Riemann Hypothesis

Cohomology of Complex Grassmannian: Schubert cells exhibit structure as a CW complex with only even-dimensional cells, and $H^{2d}(\mathrm{Gr}(k, \mathbb{C}^{n+k})) \cong \mathbb{Z}^\ell$ where ℓ is the number partitions of $[d]$, i.e. solutions to $\sum_{j=1}^k x_j = d$ with x_j weakly increasing, i.e. $x_1 \leq x_2 \leq \cdots x_k$. The ring structure is isomorphic to the ring of symmetric polynomials and is generated by Chern classes. I.e. $H^*(\mathrm{Gr}(k, \mathbb{C}^\infty)) \cong \mathbb{C}[a_1, \cdots, a_k]$ (with a_k Chern classes) which is invariant under the obvious action of the symmetric group S_k.

Example from end of paper: The number of rational points on $\mathrm{Gr}(m, r, \mathbb{P}_{\mathbb{F}_q})$

$$F(x) = \frac{\left(x^{m+1} - 1\right)\left(x^{m+1} - x\right) \cdots \left(x^{m+1} - x^r\right)}{\left(x^{r+1} - 1\right)\left(x^{r+1} - x\right) \cdots \left(x^{r+1} - x^r\right)}$$

and so the Poincare polynomial for $\mathrm{Gr}(m, r, \mathbb{P}_{\mathbb{C}})$ is $F(X^2)$.

2 Actual Paper

Considers equations of the form $\sum_{i=1}^r a_i x_i^{n_i} = b$.

Examples:

- $ax^3 - by^3 = 1$ in $\mathbb{F}_p$. ($p = 3n + 1$, Gauss, when studying "Gaussian sums"/ "cyclotomic periods")
- $ax^4 - by^4$ in $\mathbb{F}_p$ ($p = 4n + 1$, Gauss)

Can consider corresponding variety V over $\mathbb{C}$, want to relate numbers of solutions to topological properties of V.

Fix a finite field k with q elements, $a_i \in k \setminus 0$, $n_i \in \mathbb{Z}_{>0}$, and first discuss $b = 0$.

Definitions:

$$\begin{aligned} f : k[x_0, \cdots, x_r] &\to k \\ f(x_0, \cdots, x_r) &= a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r}. \end{aligned}$$

Only monomials appearing?

Example: Take $k = \mathbb{Z}_2$ and $g : k[x, y] \to k$ where $g(x, y) = x^2 + y^2$.

Non-example: $h(x, y) = x^2 + y^2 + xy$.

Let $N := \left| x \in k \,\middle|\, f(x) = 0 \right|$ the number of solutions over k.

Note: shouldn't this be the number of solutions in k^{r+1}, since a "solution" is an $(r + 1)$-tuple?

Example: For g above, $(x, y) = (0, 0),\ (1, 1)$ are the only two solutions, so here $N = 2$

Define $d_i := \gcd(n_i, q - 1)$

Example: For $\mathbb{Z}_2$, $q = 1$ so $d_1 = \gcd(2, 1) = 1$ and $d_2 = \gcd(2, 1)$.

For an arbitrary $u \in k$, define

$$N_i(u) = \left| \left\{ x \in k \,\middle|\, x^{n_i} = u \right\} \right|,$$

i.e. the number of solutions to $x^{n_i} = u$ in k, i.e. the number of d_ith roots of u.

This is equal to:

- 1 if $u = 0$,
- d_i if $u \neq 0$ is a d_ith power in k
- 0 otherwise

Not entirely clear why case 2 holds. Try for an example in the case $n_i = 2$ to compare to quadratic residues?

Define

$$\begin{aligned} L &: k^{r+1} \to k \\ L(u) &= L(u_0, \cdots, u_r) = \sum_{i=0}^{r} a_i u_i. \end{aligned}$$

We'll consider the variety $V(L)$ defined by L.

This yields a decomposition

$$\begin{aligned} N &= \sum_{u \in k^{r+1} \,\middle|\, L(u)=0} N_0(u_0) \cdots N_r(u_r) \\ &= \sum_{u \in V(L)} \prod_{i=0}^{r} N_i(u_i), \end{aligned}$$

i.e. any solutions to $f = 0$ over k^{r+1} can be found by first choosing a point $u = (u_0, \cdots, u_r)$ in the variety cut out by L, so $L(u) = \sum a_i u_i = 0$, then picking an $n_i$the root $s_i \in k$ of each u_i to obtain some $s = (s_0, \cdots, s_r) \in k^{r+1}$. Then $u_i = s_i^{n_i}$ implies that $0 = \sum a_i u_i = \sum a_i s_i^{n_i}$, so s is a solution to f.

Definition: Let G be a group and V a vector space over a field F, then a representation is morphism of groups $\rho : G \to \mathrm{GL}(V)$. For V finite-dimensional, a character of ρ is the function $\chi_\rho : G \to F$ where $g \mapsto \mathrm{Tr}(\rho(g))$. (Recall that the trace can be defined by choosing a basis for V and taking the trace of the image of g, and is basis-independent.) A character is irreducible iff ?

Lemma: Let $G = \mathbb{Z}/n\mathbb{Z}$ and define $\lambda : G \to \mathbb{C}^\times$ where $1 \mapsto \zeta_n$ a primitive nth root of unity, then $\left\{ \lambda^i \;\middle|\; 0 \le i \le n-1 \right\}$ is a complete set of irreducible characters.

Aside, maybe not useful: The irreducible characters span the space of class functions $\mathcal{C}(G)$, so we can define a surjective map

$$\begin{aligned} \Phi : \mathbb{C}[x] &\to \mathcal{C}(G) \\ f &\mapsto f(\lambda) \end{aligned}$$

and since $\lambda^n = \mathrm{id}_\mathbb{C}$, we have $\ker \Phi = (x^n - 1)$, so $\mathcal{C}(G) \cong \mathbb{C}[x]/(x^n - 1)$ is a polynomial algebra.

Let $G = k^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$, and let $\chi : G \to \mathbb{C}$ be any character.

> Note: are the representations actually taking values in $\mathbb{C}$ here?

Since G is cyclic, let ω by any generator; then χ is fully determined by $\chi(\omega)$.

For $\alpha \in \mathbb{Q}$ any rational such that $(q-1)\alpha \in \mathbb{Z}$, define a character

$$\begin{aligned} \chi_\alpha : k^\times &\to \mathbb{C} \\ \omega &\mapsto e^{2\pi i \alpha}. \end{aligned}$$

We extend this to a character on k by setting $\chi_\alpha(0) = 1 \iff \alpha \in \mathbb{Z}$ and 0 otherwise.

Let $S_i = \left\{ \alpha \in \mathbb{Q} \bigcap [0,1) \;\middle|\; d_i \alpha \in \mathbb{Z} \right\}$. We can then write

$$N_i(u) = \sum_{\alpha \in S_i} \chi_\alpha(u).$$

> Note: no clue why!

A priori, this is a countable infinite sum. The claim is that it can in fact be reduced to a finite sum. (?)

We can then let $\zeta = \chi_{\frac{1}{d_i}}(u)$, which is d_ith root of unity. Then $\zeta = 1 \iff u$ is a d_ith power in $k^\times$.

Since both sides equal 1 if $u = 0$, we can rewrite this as

$$N_i(u) = \sum_{j=1}^{d_i - 1} \zeta^j,$$

and thus

$$N = \sum_{u \in V(L)} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \quad \text{where } \alpha_i \in [0,1),\ d_i \alpha_i \in ZZ.$$

Definitely countable due to the previous equation, hence the i index. But where did the ζs go?