The Weil conjectures for dummies

Daniel Miller

September 23, 2013

Let's begin with some motivation. Let p be a prime, $q = p^r$ a power of p, and $\mathbb{F}_q$ be the finite field with q elements. For a variety X over $\mathbb{F}_q$, we define the *zeta function* of X as

$$Z(X,t) = \prod_{x \in |X|} \frac{1}{1 - t^{\deg(x)}}$$

Here $|X|$ is the set of closed points of X, and $\deg(x) = [\kappa(x) : \mathbb{F}_q]$. The function $Z(X, q^{-s})$ is quite similar to the Riemann-zeta function (or, more generally, Dedekind zeta functions) defined by

$$\zeta(k,s) = \sum_{\mathfrak{a} \subset \mathfrak{o}_k} \mathrm{N}(\mathfrak{a})^{-s} = \prod_{\mathfrak{p} \subset \mathfrak{o}_k} \frac{1}{1 - \mathrm{N}(p)^{-s}}$$

We are thinking of $Z(X,t)$ only as a formal power series, and our definition makes it clear that Z is in fact integral. However, our definition is not computationally useful. A better definition is

$$Z(X,t) = \exp\left(\int \sum_{n \geqslant 1} \#X\left(\mathbb{F}_{q^n}\right) t^n \, \frac{dt}{t} \right).$$

It is not at all obvious that these definitions agree. To see that they do, consider the map

$$D = t\frac{d}{dt}\log : 1 + \mathbb{Z}[\![t]\!] \to t\mathbb{Z}[\![t]\!]$$

To see that $Df \in t\mathbb{Z}[\![t]\!]$, note that $Df = \frac{tf'}{f}$, and $1/f \in 1 + t\mathbb{Z}[\![t]\!]$. One easily verifies that D is a continuous injection of topological groups with left inverse $f \mapsto \exp\left(\int f \, \frac{dt}{t}\right)$. To show that our definitions of $Z(X,t)$ agree, we will show that their images under D are equal. This is a straightforward computation:

$$\begin{aligned}
t\frac{d}{dt}\log\left(\prod_{x \in |X|} \frac{1}{1 - t^{-\deg(x)}} \right) &= \sum_{x \in |X|} \frac{\deg(x) t^{-\deg(x)}}{1 - t^{-\deg(x)}} \\
&= \sum_{x \in |X|} \deg(x) \sum_{n \geqslant 1} t^{n \cdot \deg(x)} \\
&= \sum_{n \geqslant 1} \left(\sum_{d \mid n} d \cdot \#\{x \in |X| : \deg(x) = d\} \right) t^n \\
&= \sum_{n \geqslant 1} \#X\left(\mathbb{F}_{q^n}\right) t^n
\end{aligned}$$

The final equality comes from the fact that $|X|$ is the set of closed points of X *as a scheme*, so an element of $|X|$ is a $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbit of $X(\overline{\mathbb{F}}_q)$ Weil conjectured that $Z(X,t)$ is a rational function of t satisfying a specified functional equation.

In some easy cases, $Z(X,t)$ is computable. For example:

$$\begin{aligned} Z(\mathbb{A}^d,t) &= \frac{1}{1-q^d t} \\ Z(\mathbb{P}^n,t) &= \frac{1}{(1-t)(1-qt)\cdots(1-q^d t)} \end{aligned}$$

To see this, we note that

$$\begin{aligned} Z(\mathbb{A}^d,t) &= \exp\left(\int \sum_{n\geqslant 1} (q^d t)^n \,\frac{dt}{t}\right) \\ &= \exp\left(\sum_{n\geqslant 1} \frac{q^{dn}t^n}{n}\right) \\ &= \exp\big(-\log(1-q^d t)\big) \\ &= \frac{1}{1-q^d t} \end{aligned}$$

To prove our formula for $Z(\mathbb{P}^n,t)$, one uses the decomposition $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$ along with induction and the fact (obvious from our second definition of Z) that

$$Z(X,t) = Z(V,t)Z(U,t)$$

whenever $V \subset X$ is a subvariety and $U = X \setminus V$. This fact lets us reinterpret $Z(X,t)$. Let $\mathbf{K}_{\mathbb{F}_p} = K(\mathsf{Var}_{\mathbb{F}_p})$ be the group generated by isomorphism classes of smooth projective varieties over $\mathbb{F}_p$, subject to the relation $[X] = [V] + [U]$ whenever $X = V \sqcup U$ is a decomposition as above. We see that

$$Z : \mathbf{K}_{\mathbb{F}_q} \to 1 + t\mathbb{Z}[\![t]\!]$$

is a group homomorphism. If we define $[X]\cdot[Y] = [X\times Y]$, then it is possible to give $\Lambda(\mathbb{Z}) = 1 + t\mathbb{Z}[\![t]\!]$ the structure of a commutative ring in such a way that $Z : \mathbf{K}_{\mathbb{F}_p} \to \Lambda(\mathbb{Z})$ is a ring homomorphism. It is obviously not surjective (quick: one ring is countable and the other is not).

One can show that $\# X(\mathbb{F}_{p^n}) = \#\operatorname{Sym}^n(X)(\mathbb{F}_p)$. This lets us reinterpret zeta functions once again. For κ any field, we can consider the ring $\mathbf{K}_\kappa = K(\mathsf{Var}_\kappa)$ defined exactly as before. For any variety X, let

$$Z(X) = \exp\left(\int \sum_{n\geqslant 1} [\operatorname{Sym}^n(X)] t^n \,\frac{dt}{t}\right)$$

In this context $Z : \mathbf{K}_\kappa \to \Lambda(\mathbf{K}_\kappa)$ is, I think, just the homomorphism $\lambda : A \to \Lambda(A)$ that exists for any λ-ring, where we have set $\lambda^k[X] = [\operatorname{Sym}^n(X)]$.

Let Var_κ be the category of smooth projective varieties over κ, and let $\mathsf{Var}_\kappa^{\circlearrowleft}$ be the category of objects of Var_κ with a specified endomorphism.

For a ring k, let grAlg_k be the category of graded (not necessarily commutative) k-algebras. We are going to construct a contravariant functor

$$A = A^\bullet : \mathsf{Var}_\kappa \to \mathsf{grAlg}_\mathbb{Z}$$

For a smooth projective variety X, let $Z^r(X)$ be the free abelian group generated by irreducible subvarieties of X of codimension r. Note that $Z^\bullet = \bigoplus_r Z^r$ is a (covariant) functor. For a subvariety $V \subset X$ and a map $f : X \to Y$, define

$$f_* V = \begin{cases} \deg\left(V \to f(V)\right)\cdot \overline{f(V)} & \text{if } \dim f(V) = \dim V \\ 0 & \text{otherwise} \end{cases}$$

Given any irreducible subvariety $V \subset V$, consider the normalization $\widetilde{V}$ of V together with its canonical map $m_V : \widetilde{V} \to V$. Let $w(V) \subset Z(X)$ be the subgroup generated by all elements of the form $m_{V*}(D)$, where D is a Weil divisor on $\widetilde{V}$ that is rationally equivalent to zero. We define

$$A(X) = A^\bullet(X) = Z(X)/\langle w(V) : V \subset X\rangle$$

For example, if X is a smooth curve, then $A(X) = \mathbb{Z} \oplus \operatorname{Pic}(X)$. If $X = \mathbb{P}^n$, then $A(X) = \mathbb{Z}[\varepsilon]/(\varepsilon^{n+1})$, where ε is the class of any hyperplane. There is a canonical group homomorphism $\deg : A^{2\dim(X)}(X) \to \mathbb{Z}$ that sends $\sum n_x \cdot [x]$ to $\sum n_x$.

It is possible to (functorially) give $A(X)$ the structure of a commutative ring in such a way that

1. A with f_* is a group-valued functor
2. if $f : X \to Y$ is proper, then $f_*(x \cdot f^*(y)) = f_*(x) \cdot y$
3. $x \cdot y = \Delta^*(x \times y)$ if x, y are cycles on X
4. if $Y, Z \subset X$ intersect properly, then $Y \cdot Z = \sum i(Z, Y; W_i) \cdot W_i$, where W_i runs over the irreducible components of $Y \cap Z$ and the $i(Y, Z; W_i)$ only depend on a neighborhood of the generic point of W_i
5. if Y and Z intersect properly and transversely, then $Y \cdot Z = Y \cap Z$.

One can prove that these requirements determine a unique ring structure on $A(X)$. There is actually a formula for the intersection multiplicities $i(Z, Y; W_i)$. One has

$$i(Z, Y; W) = \sum (-1)^i \operatorname{Length}_{\mathscr{O}_{X,z}} \operatorname{Tor}^i_{\mathscr{O}_{X,z}} \left(\mathscr{O}_{X,z}/I, \mathscr{O}_{X,z}/J\right),$$

where z is the generic point of W, I is the ideal defining Z, and J is the ideal defining Y. For $c \in A^{2\dim X}(X)$, one puts $(c) = \deg(c)$.

Let X be a proper variety over κ with an endomorphism f. We define the *zeta function of X relative to f* to be

$$Z(X, f, t) = \exp\left(\int \sum_{n \geqslant 1} (\Gamma_{f^n} \cdot \Delta_X)\, t^n \frac{dt}{t}\right)$$

The *baby Weil conjectures* state that for X a smooth projective variety over $\mathbb{F}_q$, one has

1. $Z(X, t) \in \mathbb{Q}(t)$
2. $Z(X, 1/q^d t) = \pm q^{d\chi/2} t^\chi Z(X, t)$, where $\chi = (\Delta^2)$ is the *Euler characteristic* of X

We will prove the baby Weil conjectures by assuming the existence of a *baby Weil cohomology theory*. Since such cohomology theories exist, this is actually a proof. We define a baby Weil cohomology theory to be a contravariant functor $\mathrm{H} : \mathsf{Var}_\kappa \to \mathsf{grAlg}_k$, where k is a field of characteristic zero, such that

1. $\mathrm{H}(X)$ is finite-dimensional and $\mathrm{H}^i(X) = 0$ for $i > 2d$
2. there is a natural transformation $\mathrm{cl} : A^\bullet \to \mathrm{H}^{2\bullet}$
3. there is a k-linear trace map $\operatorname{tr} : \mathrm{H}^{2d}(X) \to k$ that is compatible with the degree map.
4. if $f : X \to X$, then $\deg(\Gamma_f \cdot \Delta) = \operatorname{tr}(f^*, \mathrm{H}(X))$
5. the pairing $\mathrm{H}^i(X) \otimes \mathrm{H}^{2d-i}(X) \to \mathrm{H}^{2d}(X) \xrightarrow{\operatorname{tr}} k$ is nondegenerate

Axiom 4 is often called the *Lefschetz fixed-point theorem*, and axiom 5 is called *Poincaré duality.* Note that this is not the standard way of defining a Weil cohomology theory (these axioms are a bit weaker than usual).

There are plenty examples of baby Weil cohomology theories. If $\kappa \subset \mathbb{C}$, then $\mathrm{H}^i(X) = \mathrm{H}^i_{\mathrm{dR}}(X(\mathbb{C}), \mathbb{C})$ and $\mathrm{H}^i(X) = \mathrm{H}^i_{\mathrm{sing}}(X(\mathbb{C}), \mathbb{Q})$ work. On the other hand, if $\kappa = \mathbb{F}_p$, we can set $\mathrm{H}^i(X) = \mathrm{H}^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ for $\ell \neq p$, or $\mathrm{H}^i(X) = \mathrm{H}^i_{\mathrm{crys}}(X/\mathbb{Q}_p)$. A more computationally tractable theory is rigid cohomology, which also takes values in $\mathbb{Q}_p$-vector spaces. One can show that there are no Weil cohomology theories on $\mathsf{Var}_{\mathbb{F}_p}$ with values in $\mathbb{Q}$-vector spaces. For, there exist elliptic curves with endomorphism ring a four-dimensional division algebra over $\mathbb{Q}$. This would have to act on $\mathrm{H}^1(E)$, which is two-dimensional, a contradiction.

We need to define $\mathrm{tr}(f^*, \mathrm{H}(X))$. Let k be a field, and let grVect_k be the category of finite-dimensional $\mathbb{Z}$-graded k-vector spaces. Let $\mathsf{grVect}_k^{\circlearrowleft}$ be the category of "graded vector spaces with endomorphisms." We define $\mathrm{tr}, \det : \mathsf{grVect}_k^{\circlearrowleft} \to k$ by

$$\mathrm{tr}(f, V) = \sum (-1)^i \, \mathrm{tr}(f^i, V^i)$$
$$\det(f, V) = \prod \det(f^i, V^i)^{(-1)^i}$$

A key fact is that tr and det factor through $K(\mathsf{grVect}_k^{\circlearrowleft})$. An even more crucial fact is that we have an equality of formal power series:

$$t \frac{d}{dt} \log \frac{1}{\det(1 - ft, V)} = \sum_{n \geqslant 1} \mathrm{tr}(f^n, V^n) t^n$$

This is proved by noting that we can assume k is algebraically closed. Since $K(\mathsf{grVect}_k^{\circlearrowleft})$ is generated by one-dimensional spaces in that case, it suffices to show that for $f : k \to k$ being multiplication by λ, the identity holds. But this is trivial.

It now follows trivially from axiom 4 of a baby Weil cohomology theory that

$$Z(X, f, t) = \frac{1}{\det\left(1 - f^* t, \mathrm{H}(X)\right)}$$

We need to show that each $P_i(X, t) = \det(1 - f^* t, \mathrm{H}^i(X))$ is actually in $\mathbb{Z}[t]$. For that, we need a little bit about Hankel determinants.

Let $f \in k[\![t]\!]$; we are interested in a criterion for f to be rational. Suppose we have $f = g/h$ with $g, \in k[t]$. Then $hf = g$, and writing $h = \sum h_i t^i$, we get that

$$\sum_{n \geqslant 0} \left(\sum_{i=0}^{\deg(h)} h_i f_{n-i} \right) t^n = g$$

In other words, the sums $\sum h_i f_{n-i}$ are zero for $n \gg 0$. We have essentially proved that for a power series f to be rational, it is necessary and sufficient for there to exist a sequence $(h_0, \ldots, h_d)$ such that for n sufficiently large, we have $\sum_{i=0}^d h_i f_{n-i} = 0$. But this condition holds for a field if and only it holds for some subfield. In other words, $Z(X, f, t) \in \mathbb{Q}[\![t]\!] \cap k(t)$ implies $Z(X, f, t) \in \mathbb{Q}(t)$.

All that remains it to prove the functional equation. Our hypothesis on the trace map implies that for $x \in X$, we have $\mathrm{tr}(\mathrm{cl}) = \deg(x) = 1$, so $\mathrm{cl}(x) \neq 0$. Since $\mathrm{H}^{2d}(X)$ is one-dimensional, it is generated by $\mathrm{cl}(x)$ for any $x \in X$. Now, if $f : X \to X$ is finite, then there is some $x \in X$ such that $f^{-1}(x)$ has size $\deg(f)$. One then computes

$$\mathrm{tr}(f^* \, \mathrm{cl}(x)) = \mathrm{tr}(\mathrm{cl}(f^* x)) = \deg(f^* x) = \deg(f)$$

It follows that $f^* : \mathrm{H}^{2d}(X) \to \mathrm{H}^{2d}(X)$ is multiplication by $\deg(f)$. We now use a lemma from linear algebra:

Lemma Let U, V be vector spaces of dimension r with endomorphisms f, g. If there is a perfect pairing $\langle \cdot, \rangle$ between U and V so that $\langle fu, gv \rangle = \lambda \langle u, v \rangle$ for all u, v, then

$$\det(1 - ft, U) = \frac{(-\lambda t)^r}{\det(g, V)} \det\left(1 - \frac{g}{t\lambda}, V\right)$$

and

$$\det(f, U) \det(g, V) = \lambda^r$$

One proves the lemma by assuming the field is algebraically closed, and conjugating f so that it is upper triangular.

We now compute

$$\begin{aligned}
\det(1 - f^* t, \mathrm{H}(X)) &= \prod_{i=0}^{2d} \det(1 - f^* t, \mathrm{H}^i(X))^{(-1)^i} \\
&= \prod_{i=0}^{2d} \left(\frac{(-\deg(f)t)^{h^i(X)}}{\det(f^*, \mathrm{H}^i(X))} \right)^{(-1)^i} \det\left(1 - \frac{f^*}{t\deg(f)}, \mathrm{H}^{2d-i}(X)\right)^{(-1)^{2d-i}} \\
&= (-\deg(f)t)^{\sum (-1)^i h^i(X)} \det\left(1 - \frac{f^*}{\deg(f)t}, \mathrm{H}(X)\right) \prod_{i=0}^{d} \left(\det(f^*, \mathrm{H}^i) \det(f^*, \mathrm{H}^{2d-i})\right)^{(-1)^i} \\
&= (-\deg(f)t)^{\mathrm{tr}(1, \mathrm{H}(X))} \det\left(1 - \frac{f^*}{\deg(f)t}, \mathrm{H}(X)\right) \prod_{i=0}^{d-1} (\deg f)^{-(-1)^i h^i(X)} \cdot (\deg f)^{-(-1)^d h^d(X)/2}
\end{aligned}$$

By the Lefschetz fixed point theorem, $\mathrm{tr}(1, \mathrm{H}(X)) = (\Delta^2) = \chi$, so this reduces to

$$Z\left(X, f, \frac{1}{t \cdot \deg f}\right) = \pm t^{\chi} (\deg f)^{\chi/2} Z(X, f, t)$$