These notes on the Weil conjectures are a blend of the exposition in Poonen [5, Chap. 7], Milne [3, Chap. II] and Mustaţă [4].

34.1 Riemann and Dedekind zeta functions

Our main object of interest will be the Hasse-Weil zeta function associated to a variety over a finite field, but we begin with a brief discussion of the Riemann zeta function for comparison and motivation.

For a complex number s with $\mathrm{Re}(s) > 1$, we define

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{1}$$

Though there are interesting features to investigate in the right "half" of the plane (for example, $\zeta_{2m}/\pi^{2m} \in \mathbb{Q}$ for $m \in \mathbb{Z}$), the main interest in the zeta function lies in its extension to the *critical strip* $\{z \in \mathbb{C} : 0 \le \mathrm{Re}(z) \le 1\}$. This extension relies on a theorem in complex analysis: if $U \subset V$ are nonempty connected open subsets of $\mathbb{C}$ and $f(z)$ and $g(z)$ are holomorphic functions on V that agree on U then $f(z) = g(z)$ for all $z \in V$.[1] We may thus speak of the analytic continuation of a holomorphic function to a larger open subset of $\mathbb{C}$ (or the meromorphic continuation if we allow poles); such a continuation is unique by the argument above, but may or may not exist for a given subset. The function defined by (1) in fact has a meromorphic continuation to the whole complex plane, with one simple pole at $s = 1$. The resulting function is known as the Riemann zeta function.

The proof of analytic continuation[2] is closely connected to the functional equation for $\zeta(s)$. Recall that the Γ function is a complex meromorphic function function extending the factorial function; it is defined for $\mathrm{Re}(s) > 0$ by the integral equation

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} dx.$$

Meromorphic continuation to $\mathbb{C}$ is much easier for Γ than for ζ since Γ satisfies[3] $\Gamma(s+1) = s\Gamma(s)$ using integration by parts:

$$\Gamma(s+1) = \int_0^\infty x^s e^{-x} dx = \left[-x^s e^{-x}\right]_0^\infty + \int_0^\infty s x^{s-1} e^{-x} dx = s\Gamma(s).$$

We can use the functional equation to iteratively extend Γ into the half planes $\{s \in \mathbb{C} : \mathrm{Re}(s) > -m\}$ for $m = 1, 2, \ldots$ using $\Gamma(s) = 1/s\Gamma(s+1)$. This process yields no zeros, and simple poles at non-positive integers. The functional equation also confirms that Γ extends the factorial function: we have $\Gamma(n) = (n-1)!$ for $n \in \mathbb{Z}_{>0}$.

[1] This follows from the fact that Taylor series for holomorphic functions converge in a disc and thus a nonzero holomorphic function cannot vanish completely on a disc. Note the contrast with real C^∞ functions: $f(x) = e^{-1/x^2}$ for $x > 0$ and $f(x) = 0$ for $x \le 0$ is C^∞.

[2] The proof would take us too far afield into analytic number theory, but is readily available, e.g. [1, Ch. 5 §4.2-4.4] or [2]

[3] This functional equation is enough to characterize the Γ function if one additionally requires $\log(\Gamma(s))$ is convex on the positive real axis

Now define an auxiliary function[4] $\xi(s)$ by

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

One proves that the function $s(s-1)\xi(s)$ is analytic on all of $\mathbb{C}$ and gives the functional equation for $\zeta(s)$:

$$\xi(s) = \xi(1-s). \tag{2}$$

The main connection of $\zeta(s)$ to number theory comes from its expression as an Euler product.

Proposition 34.1. *If* $\mathrm{Re}(s) > 1$ *then*

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

Proof. We have

$$\begin{aligned}\prod_p \frac{1}{1-p^{-s}} &= \prod_p \sum_{m=0}^{\infty} (p^m)^{-s} \\ &= \sum_{n=1}^{\infty} n^{-s}\end{aligned}$$

using unique factorization and the fact that $\sum_{m=0}^{\infty} p^{-ms}$ is absolutely convergent when $\mathrm{Re}(s) > 0$. □

The Euler product allows us to get an initial handle on where the zeros of $\zeta(s)$ lie.

Proposition 34.2. *If* $\zeta(s) = 0$ *then either* $s/2 \in \mathbb{Z}_{\leq 0}$ *or* $0 \leq \mathrm{Re}(s) \leq 1$*.*

Proof. We first show that $\zeta(s)$ has no zeros with $\mathrm{Re}(s) > 1$. By Prop. 34.1,

$$\begin{aligned}\zeta(s) &= \prod_p \frac{1}{1-p^{-s}} \\ &= \prod_p \left(1 + \frac{1}{p^s - 1}\right)\end{aligned}$$

Since $\sum_p \frac{1}{p^s-1}$ converges absolutely, this product converges and is thus nonzero.

The result now follows from the functional equation (2) together with the fact that Γ only has poles at non-positive integers. □

Why do we care about the zeros of $\zeta(s)$? The first spectacular application was to proving the following theorem on the distribution of prime numbers. Let $\pi(x)$ be the number of primes less than or equal to x.

Theorem 34.3 (Prime number theorem)**.** *The probability that a random integer with k base-e digits is prime is asymptotic to $1/k$. More precisely, $\pi(x) \sim x/\log(x)$.*

[4] Sometimes $\xi(s)$ is scaled by $s(s-1)$ in order to cancel the poles and make it entire

Proof. Let $\vartheta(x) = \sum_{p \le x} \log(p)$. The proof has the following structure. First, show that there are no zeros of $\zeta(s)$ with $\mathrm{Re}(s) = 1$. Second, use this zero-free line together with analytic results to show that $\vartheta(x) \sim x$. Finally, note that

$$\begin{aligned}
\vartheta(x) &= \sum_{p \le x} \log(p) \le \sum_{p \le x} \log(x) = \pi(x)\log(x) \\
\vartheta(x) &\ge \sum_{x^{1-\epsilon} \le p \le x} \log(p) \ge (1-\epsilon) \sum_{x^{1-\epsilon} \le p \le x} \log(x) \\
&= (1-\epsilon)\log(x)(\pi(x) + O(x^{1-\epsilon})).
\end{aligned}$$

For more details, see Zagier's short article [6]. □

So the nontrivial zeros of $\zeta(s)$ are known to lie in the open critical strip with $0 < \mathrm{Re}(s) < 1$, but more is believed to be true:

Conjecture 34.4 (Riemann hypothesis)**.** *All nontrivial zeros of* $\zeta(s)$ *have* $\mathrm{Re}(s) = 1/2$.

The conjecture is known to hold for the first 10 trillion zeros and for at least 41% of all nontrivial zeros. A proof is worth one million dollars from the Clay Math Institute, and it is one of the most common assumptions for conditional results in the mathematical literature.[5]

The broad class of generalizations of $\zeta(s)$ are known as *L-functions*, but we will focus on the subset of zeta functions among them. Suppose K is a number field. The *Dedekind zeta function* of K is the meromorphic continuation of

$$\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{\mathrm{Nm}_{K/\mathbb{Q}}(I)^s} = \prod_{P \text{ prime ideal}} \frac{1}{1 - \mathrm{Nm}_{K/\mathbb{Q}}(P)^{-s}}. \tag{3}$$

34.2 Hasse-Weil zeta functions

Suppose now that X is a variety over a finite field $k = \mathbb{F}_q$. Since $\mathbb{F}_q$ is finite, we may count the number of points, not just over $\mathbb{F}_q$ but also for any extension $\mathbb{F}_{q^m}/\mathbb{F}_q$. Let $N_m = \#X(\mathbb{F}_{q^m})$, and let X_{cl}. We then define the Hasse-Weil zeta function of X to be the power series

$$Z_X(T) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} T^m\right) \in \mathbb{Q}[[T]].$$

The use of the term "zeta function" is justified by the following proposition.

Proposition 34.5. *For any variety* X *over* $\mathbb{F}_q$,

$$Z_X(T) = \prod_{x \in X_{\mathrm{cl}}} \frac{1}{1 - T^{\deg(x)}}.$$

[5] See https://mathoverflow.net/questions/17209/consequences-of-the-riemann-hypothesis for a list of major consequences of the Riemann hypothesis and the generalized Riemann hypothesis, which also considers zeros of Dirichlet L-functions

Proof. For $r \geq 1$, let $a_r = \#\{x \in X_{\mathrm{cl}} : [k(x) : k] = r\}$. Note that $N_m = \sum_{r|m} r \cdot a_r$. We have

$$\log(Z_X(T)) = \sum_{m\geq 1} \frac{N_m}{m} T^m = \sum_{m\geq 1}\sum_{r|m} \frac{r \cdot a_r}{m} T^m = \sum_{r\geq 1} a_r \sum_{\ell\geq 1} \frac{T^{\ell r}}{\ell}$$
$$= \sum_{r\geq 1} (-a_r)\log(1-T^r) = \sum_{r\geq 1} \log(1-T^r)^{-a_r} = \log\left(\prod_{r\geq 1}(1-T^r)^{-a_r}\right).$$

Applying log to both sides we get the result. □

If we substitute $T = q^{-s}$ we get a function that looks very similar to the Dedekind zeta function in (3). Also note that Prop. 34.5 implies that $Z_X(T) \in \mathbb{Z}[[T]]$.

Example 34.6. Let $X = \mathbb{A}^n$. Then $N_m = q^{mn}$ so

$$Z_X(T) = \exp\left(\sum_{m\geq 1} \frac{q^{mn}}{m} T^m\right) = \exp(-\log(1-q^n)) = \frac{1}{1-q^n T}.$$

Proposition 34.7. *Suppose that Y is a closed subvariety of X, and set $U = X \backslash Y$. Then*

$$Z_X(T) = Z_Y(T) \cdot Z_U(T).$$

Proof. This follows from properties of the exp and the fact that $\#X(\mathbb{F}_{q^m}) = \#Y(\mathbb{F}_{q^m}) + \#U(\mathbb{F}_{q^m})$. □

Example 34.8. Let $X_n = \mathbb{P}^n$. As a base case, we have $X_0 \cong \mathbb{A}^0$ is a point and thus $Z_{X_0}(T) = \frac{1}{1-T}$. In general, we may take $Y = \mathbb{P}^{n-1}$ and $U = \mathbb{A}^n$. Thus $Z_{X_n}(T) = \frac{Z_{X_{n-1}}(T)}{1-q^n T}$, so by induction we get

$$Z_{X_n}(T) = \frac{1}{(1-T)(1-qT)\ldots(1-q^n T)}.$$

34.3 The Weil Conjectures

We are now ready to state the Weil conjectures. Despite the name, they are now a theorem: after being conjectured by Weil in 1949 the rationality of $Z_X(T)$ was shown by Dwork in 1960, the functional equation by Grothendieck in 1965, and the Riemann hypothesis by Deligne in 1974.

Theorem 34.9. *Suppose that X is a smooth, geometrically irreducible, projective variety of dimension n defined over $\mathbb{F}_q$.*

1. *(Rationality) The zeta function of X is rational, ie $Z_X(T) \in \mathbb{Q}(T)$.*
2. *(Functional equation) There is an integer χ so that*

$$Z_X\left(\frac{1}{q^n T}\right) = \pm q^{n\chi/2} T^{\chi} Z_X(T).$$

3. *(Riemann hypothesis) There is a decomposition*

$$Z_X(T) = \frac{P_1(T)\dots P_{2n-1}(T)}{P_0(T)\dots P_{2n}(T)},$$

where each $P_i(T) \in \mathbb{Z}[T]$ can be factored over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i}(1-\alpha_{i,j}T)$$

with $|\alpha_{i,j}| = q^{i/2}$. We also have $P_0(T) = 1-T$ and $P_{2n}(T) = 1-q^nT^{2n}$.

The integer χ is the Euler characteristic of X, and can be expressed either as the alternating sum $\sum_{i=0}^{2n}(-1)^i b_i$ or as the intersection multiplicity of the diagonal Δ with itself in $X \times X$. Moreover, if R is a finitely generated subalgebra of $\mathbb{C}$, $\tilde{X}$ is a smooth projective variety over R, P a prime ideal of R with $R/P \cong \mathbb{F}_q$ and X is the reduction of $\tilde{X}$ modulo P then the integers b_i are the dimensions of the singular cohomology groups

$$b_i = \dim_{\mathbb{Q}} H^i((\tilde{X}_{\mathbb{C}})^{an}, \mathbb{Q}).$$

Setting $\zeta_X(s) = Z_X(q^{-s})$ and $\xi_X(s) = q^{-\chi s/2}\zeta_X(s)$ makes the connection with the Riemann zeta function more clear. The functional equation becomes

$$\xi_X(n-s) = \pm\xi_X(s).$$

In the case of a smooth projective curve, the zeros of $Z_X(T)$ are precisely the zeros of the numerator $P_1(T)$, which all have absolute value $\sqrt{q}$ by the Riemann hypothesis. Translating to $\zeta_X(s)$ we see that the zeros of $\zeta_X(s)$ have $\mathrm{Re}(s) = 1/2$, justifying the use of the term "Riemann hypothesis."

The constraints that all roots of P_i have absolute value q^i is a serious one. For a fixed q, i and degree b_i there are only finitely many polynomials $P_i(T)$ satisfying this condition. One can list all such polynomials in Sage as follows:

```
from sage.rings.polynomial.weil.weil_polynomials import WeilPolynomials
for f in WeilPolynomials(n, q):
    print(f)
```

For example, there are 35 possible $P_1(T)$ of degree 4 when $q = 2$. For small values of n and q, these are also listed online at `lmfdb.org/Variety/Abelian/Fq/`.[6]

We may also translate the statements about $Z_X(T)$ into more direct statements about the number of points N_m of X over $\mathbb{F}_{q^m}$. Namely, if X is a smooth projective variety of dimension n then there are algebraic integers $\alpha_{i,j}$ so that

$$\#X(\mathbb{F}_{q^m}) = \sum_{j=1}^{b_0}\alpha_{0,j}^m - \sum_{j=1}^{b_1}\alpha_{1,j}^m + \dots - \sum_{j=1}^{b_{2n-1}}\alpha_{2n-1,j}^m + \sum_{j=1}^{b_{2n}}\alpha_{2n,j}^m$$

with

- $b_i = b_{2n-i}$,
- $\alpha_{i,j} = q^n/\alpha_{2n-i,j}$ for $i \neq n$ and $\alpha_{n,j} = q^n/\alpha_{n,b_n+1-j}$,
- $|\alpha_{i,j}| = q^{i/2}$ for all i, j,
- if X is geometrically irreducible then $b_0 = b_{2n} = 1$ and $\alpha_{0,1} = 1$, $\alpha_{2n,1} = q^n$.

[6] Actually, only a certain subset are shown in the LMFDB, subject to the conditions of the Honda-Tate theorem that describes isogeny classes of abelian varieties over finite fields in terms of Weil polynomials

References

[1] Lars Ahlfors. *Complex analysis: an introduction to the theory of analytic functions of one complex variable.* 3rd ed., McGraw-Hill Book Co., New York, 1978.

[2] Noam Elkies. *Math 259: the Riemann zeta function and its functional equation.* http://people.math.harvard.edu/~elkies/M259.02/zeta1.pdf

[3] James Milne. *Lectures on étale cohomology.* https://www.jmilne.org/math/CourseNotes/LEC.pdf

[4] Mircea Mustaţă. *Zeta functions in algebraic geometry.* http://www-personal.umich.edu/~mmustata/zeta_book.pdf

[5] Bjorn Poonen. *Rational points on varieties.* Graduate Studies in Mathematics 186. Amer. Math. Soc., Providence, 2017. https://math.mit.edu/~poonen/papers/Qpoints.pdf

[6] Don Zagier. *Newman's short proof of the prime number theorem.* Amer. Math. Monthly **104** (8), 1997. pp. 705-708.