

L -Functions and The Weil Conjectures

Nir Elber

8 August 2022

Abstract

In this talk, we introduce two major problems in modern number theory: understanding L -functions and counting points on varieties. The end goal is to motivate and state a subset of the Weil conjectures.

Contents

Contents	1
1 Introduction	1
2 L-Functions	1
2.1 The Riemann ζ -Function	1
2.2 Dedekind ζ -Functions	2
2.3 Dirichlet L -Functions	4
3 The Weil Conjectures	6
3.1 Affine Varieties	6

1 Introduction

This talk will be incredibly high-level. With this in mind, the goal will be to lay the groundwork for certain objects in number theory that seem to pervade the entire field. We will not prove anything here.

2 L -Functions

We will introduce L -functions by example. Roughly speaking, these are certain infinite series/products which seem to encode certain desired number-theoretic information.

2.1 The Riemann ζ -Function

The most famous example is the *Riemann ζ -function*, defined by the infinite series

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad (2.1)$$

for $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$. This function has the following magical properties.

1. By unique prime factorization, one can write

$$\zeta(s) = \prod_{p \text{ prime}} \left(\sum_{k=0}^{\infty} \frac{1}{p^{ks}} \right) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

for $\operatorname{Re} s > 1$. This infinite product is called an *Euler product*.

2. There is a unique way to define $\zeta(s)$ for all $s \in \mathbb{C}$ which agrees with (2.1) for $\operatorname{Re} s > 1$ while being differentiable everywhere. This is called the *analytic continuation*.
3. There is a functional equation, as follows: define

$$\xi(s) := \frac{1}{2} \pi^{-s/2} s(s-1) \Gamma(s/2) \zeta(s)$$

for all $s \in \mathbb{C}$, using the analytic continuation of ζ ; here Γ is the Gamma function. Yes, this is a very complicated definition, but do not worry about the details: the main point is that there is some function ξ defined in terms of some relatively understood functions (an exponential, polynomials, and Γ) and the function of interest ζ .

Then, magic happens: we have

$$\xi(s) = \xi(1-s)$$

for all $s \in \mathbb{C}$. This is called the *functional equation*.

4. It is conjectured that, if $\zeta(s) = 0$ for $0 < \operatorname{Re} s < 1$, then $\operatorname{Re} s = 1/2$. This is called the *Riemann hypothesis*.

It might not be immediately clear why one should care about a function like ζ . We will content ourselves with saying that, even though $\zeta(s) \rightarrow \infty$ as $s \rightarrow 1$, combining the Euler product with knowledge of how fast $\zeta(s) \rightarrow \infty$ as $s \rightarrow 1$ we are able to extract meaningful information about the distribution of primes.

Remark 1. To rigorize the above sentence, write

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

Expanding $-\log(1-x) \approx x$ for small x , we can write

$$\log \zeta(s) \approx \sum_{p \text{ prime}} \frac{1}{p^s}$$

as $s \rightarrow 1$. Thus, understanding how $\log \zeta(s)$ behaves as $s \rightarrow 1$ allows us to approximate primes.

Remark 2. As for why one should care about the Riemann hypothesis, the Riemann hypothesis is equivalent to the statement

$$\pi(x) = \int_2^x \frac{1}{\log t} dt + O(\sqrt{x} \log x),$$

where $\pi(x)$ is the number of primes below some $x \in \mathbb{R}$.

The moral of our story here is that we are going to encounter "lots" of functions like ζ which are at least conjectured to satisfy properties 1–4. Let's see two popular examples.

2.2 Dedekind ζ -Functions

Let K be a finite extension of \mathbb{Q} ; i.e., a number field.

Example 3. Throughout this example, one should let $K = \mathbb{Q}$ or $K = \mathbb{Q}(i)$ (where $i^2 = -1$) unless you are already familiar with these objects.

It turns out that there is an especially nice ring lying inside K , which we will name \mathcal{O}_K . Formally, \mathcal{O}_K is the ring of elements of K which are the root of some monic polynomial with integer coefficients.

Example 4. In the case of $K = \mathbb{Q}$, we have $\mathcal{O}_K = \mathbb{Z}$. In the case of $K = \mathbb{Q}(i)$, we have $\mathcal{O}_K = \mathbb{Z}[i]$.

The ring \mathcal{O}_K does not, in general, need to have unique prime factorization of elements as is the case with $\mathcal{O}_K = \mathbb{Z}$ or $\mathcal{O}_K = \mathbb{Z}[i]$. However, do not fear—we are not going to use elements to define our L -function! Instead, we will use ideals. We would like to write a series like

$$\sum_{\text{nonzero ideals } I \subseteq \mathcal{O}_K} \frac{1}{I^s}$$

for $\text{Re } s > 1$, but this doesn't make sense because we haven't defined what I^s should mean. To remedy this, we will take a hint from the case of $\mathcal{O}_K = \mathbb{Z}$: here, we would like to think about the ideal $4\mathbb{Z} \subseteq \mathbb{Z}$ is associated to the number 4. One naive way to see this is that 4 is the size of $\mathbb{Z}/4\mathbb{Z}$. As such, we will define the *Dedekind ζ -function*

$$\zeta_K(s) := \sum_{\text{nonzero ideal } I \subseteq \mathcal{O}_K} \frac{1}{|\mathcal{O}_K/I|^s}. \quad (2.2)$$

As before, ζ_K has the following magical properties.

1. By unique prime factorization of ideals (which we won't elaborate on here), one can write

$$\zeta_K(s) = \prod_{\text{maximal ideal } \mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - |\mathcal{O}_K/\mathfrak{p}|^{-s}}.$$

This is called the *Euler product* for $\zeta_K(s)$.

2. There is a unique way to define $\zeta(s)$ for all $s \in \mathbb{C}$ which agrees with (2.2) for $\text{Re } s > 1$ while being differentiable everywhere. This is called the *analytic continuation*.
3. There is a functional equation. This is somewhat difficult to state precisely, but we will first just say that there is some ξ_K defined using various known constants and Γ functions as well as the desired function ζ_K , which satisfies

$$\xi_K(s) = \xi_K(1-s).$$

This is called the *functional equation* for $\zeta_K(s)$.

To be exact, there exists integers $\text{disc } \mathcal{O}_K$, r_1 , and r_2 such that we may set

$$\xi_K(s) = |\text{disc } \mathcal{O}_K| \cdot \left(\pi^{-s/2} \Gamma(s) \right)^{r_1} \cdot \left(2(2\pi)^{-s} \Gamma(s) \right)^{r_2/2} \cdot \zeta_K(s).$$

For experts, $\text{disc } \mathcal{O}_K$ is the discriminant of \mathcal{O}_K , r_1 is the number of field embeddings $K \hookrightarrow \mathbb{R}$, and r_2 is the number of field embeddings $K \hookrightarrow \mathbb{C}$ which have image not contained in \mathbb{R} .

4. It is conjectured that, if $\zeta_K(s) = 0$ for $0 < \text{Re } s < 1$, then $\text{Re } s = 1/2$. This is called the (*extended*) *Riemann hypothesis* for $\zeta_K(s)$.

The reasons why one should care about ζ_K are essentially the same for ζ . Namely, questions about the distribution of primes in \mathbb{Z} often have natural analogues in \mathcal{O}_K ; for example, one can show that

$$\pi_K(x) := \#\{\mathfrak{p} \subseteq \mathcal{O}_K : |\mathcal{O}_K/\mathfrak{p}| \leq x\}$$

satisfies

$$\pi_K(x) \sim \frac{x}{\log x},$$

and $\zeta_K(s)$ is once again the main object of the argument.

Exercise 5. Let $K = \mathbb{Q}(i)$ so that $\mathcal{O}_K = \mathbb{Z}[i]$. Using the classification of primes in $\mathbb{Z}[i]$, write out the Euler product for $\zeta_K(s)$ in terms of primes in \mathbb{Z} .

2.3 Dirichlet L -Functions

We begin with the following definition.

Definition 6 (Character). Let G be a group. Then a *character* is a group homomorphism $\chi: G \rightarrow S^1$. Here,

$$S^1 = \{e^{i\theta} : \theta \in \mathbb{R}\} \subseteq \mathbb{C}^\times.$$

More specifically, we will speak of Dirichlet characters, which are group homomorphisms $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow S^1$ extended to a multiplicative function $\mathbb{Z} \rightarrow \mathbb{C}$ by setting $\chi(k) = 0$ whenever $\gcd(k, m) \neq 1$. Here are some examples.

Example 7. The function $\chi(n) = 0$ for all $n \in \mathbb{Z}$ is a Dirichlet character, with $m = 1$.

Example 8. The function

$$\chi(n) := \begin{cases} 1 & n \text{ is odd,} \\ 0 & n \text{ is even,} \end{cases}$$

is a Dirichlet character, with $m = 2$.

Example 9. The function

$$\chi(n) := \begin{cases} 1 & n \equiv 1 \pmod{4}, \\ -1 & n \equiv 3 \pmod{4}, \\ 0 & n \equiv 0 \pmod{2} \end{cases}$$

is a Dirichlet character, with $m = 4$.

Now, given a Dirichlet character $\chi: \mathbb{Z} \rightarrow \mathbb{C}$, we define the *Dirichlet L -function* by the infinite series

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad (2.3)$$

for $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$. As usual, this function has the following magical properties.

1. By unique prime factorization and the multiplicativity of χ , we have

$$L(s, \chi) = \prod_{p \text{ prime}} \left(\sum_{k=0}^{\infty} \frac{\chi(p)^k}{p^{ks}} \right) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}}$$

for $\operatorname{Re} s > 1$. This is called the *Euler product* for $L(s, \chi)$.

2. There is a unique way to define $L(s, \chi)$ for all $s \in \mathbb{C}$ which agrees with (2.3) while being differentiable everywhere. This is called the *analytic continuation* for $L(s, \chi)$.
3. There is a functional equation. As usual, this is incredibly annoying to state precisely, but we will give a taste for it: pick up a character $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow S^1$ where m is as small as possible, and extend χ to a Dirichlet character $\chi: \mathbb{Z} \rightarrow \mathbb{C}$. Then one can compute an integer $a \in \mathbb{Z}$ (depending on χ) and define

$$\xi(s, \chi) := \left(\frac{q}{\pi}\right)^{(s+a)/2} \Gamma\left(\frac{s+a}{2}\right) L(s, \chi).$$

Then we have

$$\xi(s, \chi) = \varepsilon(\chi) \xi(1-s, \bar{\chi})$$

for some complex number $\varepsilon(\chi) \in \mathbb{C}$ depending on χ . Note that χ became $\bar{\chi}$ in the functional equation! Anyway, this is called the *functional equation* for $L(s, \chi)$.

4. It is conjectured that, if $L(s, \chi) = 0$ for $0 < \operatorname{Re} s < 1$, then $\operatorname{Re} s = 1/2$. This is called the (generalized) Riemann hypothesis for $L(s, \chi)$.

Let's spend a moment to discuss why one might care about these L -functions. For one, the generalization from ζ has taught us something about how the functional equation behaves: when looking at L -functions in general, we should no longer expect to be looking at the same L -function on both sides!

For another reason, the difficult step in the following theorem is showing that $L(1, \chi) \neq 0$ for all Dirichlet characters χ .

Theorem 10. Let a and m be integers with $\gcd(a, m) = 1$. Then there are infinitely primes p such that $p \equiv a \pmod{m}$.

It will help us a little later to have a notion of how $L(1, \chi)$ enters the picture. We will want the following result.

Lemma 11. Let m be an integer and $a, b \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then

$$\frac{1}{\varphi(m)} \sum_{\chi} \chi(a) \chi(b)^{-1} = \begin{cases} 1 & a = b, \\ 0 & a \neq b, \end{cases}$$

where the sum is over all characters $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow S^1$.

Correct proofs of this statement would take us too far afield to give here, so we won't prove this. However, we will assign the following exercise.

Exercise 12. Let G be a cyclic group. Then, for $g, h \in G$,

$$\frac{1}{\#G} \sum_{\chi} \chi(g) \chi(h)^{-1} = \begin{cases} 1 & g = h, \\ 0 & g \neq h, \end{cases}$$

where the sum is over all characters $\chi: G \rightarrow S^1$.

Why do we care? Well, fix integers a and m with $\gcd(a, m) = 1$. The main goal is to show that the sum

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s}$$

diverges, where \sum_p is a sum over primes. This divergence forces there to be infinitely many primes p with $p \equiv a \pmod{m}$. For this, define $\delta_a: \mathbb{Z} \rightarrow \mathbb{Z}$ by $\delta_a(n) = 1$ if $n \equiv a \pmod{m}$ and 0 otherwise. Now, we can write

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = \sum_p \frac{\delta_a(p)}{p^s} = \sum_p \left(\frac{1}{\varphi(m)} \sum_{\chi} \chi(a)^{-1} \chi(p) \right) \frac{1}{p^s},$$

where \sum_{χ} is over all Dirichlet characters χ extended from $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow S^1$. Continuing, this rearranges into

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_{\chi} \left(\chi(a)^{-1} \sum_p \frac{\chi(p)}{p^s} \right).$$

It might look like we've just made things more complicated, but they are about to simplify because we have infinite series involving characters χ , which are better-behaved than the indicator function δ_a . Indeed, we argue as in [Remark 1](#) and use the Euler product for $L(s, \chi)$ to write

$$\log L(s, \chi) = - \sum_p \log(1 - \chi(p)p^{-s}) \approx \sum_p \frac{\chi(p)}{p^s},$$

so

$$\sum_{\substack{p \equiv a \\ (\text{mod } m)}} \frac{1}{p^s} \approx \frac{1}{\varphi(m)} \sum_{\chi} \chi(a)^{-1} \log L(s, \chi).$$

Now, the proof of [Theorem 10](#) proceeds by showing that $L(1, \chi)$ is a nonzero complex number for all but one character $\chi = \chi_0$ and that $L(1, \chi_0) = \infty$ there. (Make no mistake—showing the previous sentence is the hard part of the proof!) As such, the sum on the right has a divergent term, so the sum on the left diverges as well.

Remark 13. One can also attach characters to Dirichlet ζ -functions. This produces Hecke L -functions, but we will not discuss them here.

3 The Weil Conjectures

We will state the Weil conjectures, focusing on affine varieties. We will not state the Betti numbers conjecture because we won't want to have to define what a Betti number is.

3.1 Affine Varieties

In [section 2](#), we focused on number theory, but we will now turn our attention to geometry. We will let K be a field in this section; for concreteness one should take $K = \mathbb{R}$ or $K = \mathbb{C}$ throughout.

Definition 14 (Affine space). Let K be a field and n a positive integer. Then we define *affine n -space* over K , denoted \mathbb{A}_K^n , to be the set of n -tuples $(a_1, \dots, a_n) \in K^n$.

It might seem silly to introduce entirely new notation for just writing K^n , but this has an important psychological effect: we want to think about \mathbb{A}_K^n as a purely geometric object, while K^n we might be tempted to think about as having some extra structure (for example, as a vector space).

Now, here is our central definition.

Definition 15 (Affine variety). Let K be a field and n a positive integer. Then, given a subset of polynomials $S \subseteq K[x_1, \dots, x_n]$, we define the vanishing set

$$V(S) := \{(a_1, \dots, a_n) \in \mathbb{A}_K^n : f(a_1, \dots, a_n) = 0 \text{ for all } f \in S\}.$$

Now, an *affine variety* is any subset $V \subseteq \mathbb{A}_K^n$ for which there exists an $S \subseteq K[x_1, \dots, x_n]$ with $V = V(S)$.

Remark 16. Some authors also require some extra geometric conditions to be a variety (e.g., irreducibility). We will not discuss these here.

We've defined some geometric objects, so the next demand is to see some pictures. Throughout, we will let $K = \mathbb{R}$.

Example 17. Set $K = \mathbb{R}$ and $n = 1$, with $S = \{0\}$. Then $V(S) = \mathbb{A}_{\mathbb{R}}^1$ is the red set, as follows.



Observe that $V(\emptyset) = \mathbb{A}_{\mathbb{R}}^1$ as well.

Example 18. Set $K = \mathbb{R}$ and $n = 1$, with $S = \{(x - 1)(x - 2)\}$. Then $V(S)$ is the red set.

