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

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-funtions 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

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

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
$$\xi(s) \coloneqq \frac{1}{2} \pi^{-s/2} s(s-1) \Gamma(s/2) \zeta(s)$$
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 $\zeta(s) \to \infty$ as $s \to 1$, combining the Euler product with knowledge of how fast $\zeta(s) \to \infty$ as $s \to 1$ we are able to extract meaningful information about the distribution of primes.

Remark 1. To rigorize the above sentence, write
$$\log \zeta(s) = - \sum_{p \text{ prime}} \log \left(1 - p^{-s}\right).$$
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 $s \to 1$. Thus, understanding how $\log \zeta(s)$ behaves as $s \to 1$ 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
$$\pi(x) = \int_2^x \frac{1}{\log t} \, dt + O\left(\sqrt{x} \log x\right),$$
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 $\operatorname{Re} s > 1$, 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*

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

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 $\operatorname{Re} s > 1$ 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 $\operatorname{disc} \mathcal{O}_K$, r_1, and r_2 such that we may set

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

   For experts, $\operatorname{disc} \mathcal{O}_K$ 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 $0 < \operatorname{Re} s < 1$, then $\operatorname{Re} s = 1/2$. 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

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

satisfies

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

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

Remark 5. These ζ-functions do not exist in isolation. For example, if $K/\mathbb{Q}$ is a finite field extension and L/K is finite Galois extension, then it is conjectured that $\zeta_L(s)/\zeta_K(s)$ is defined everywhere.

Exercise 6. 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 $\mathbb{Z}$. Use this Euler product to compute an Euler product for $\zeta_{\mathbb{Q}(i)}(s)/\zeta_{\mathbb{Q}}(s)$.

Remark 7. In the discussion that follows, we will want to generalize this example a little more. Observe that the Euler product for ζ allows us to write

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \prod_{\text{maximal } \mathfrak{m} \subseteq \mathbb{Z}} \frac{1}{1-|\mathbb{Z}/\mathfrak{m}|^{-s}}.$$

More generally, given any ring R, we have the *arithmetic ζ-function*

$$\zeta_R(s) \coloneqq \prod_{\substack{\text{maximal } \mathfrak{m} \subseteq R \\ |R/\mathfrak{m}|<\infty}} \frac{1}{1-|R/\mathfrak{m}|^{-s}}.$$

For example, for number fields K, we have $\zeta_{\mathcal{O}_K}(s) = \zeta_K(s)$. We will not discuss convergence issues or precisely state the functional equation or Riemann hypothesis for these ζ functions because there are some technical hypotheses on R which we are going to actively avoid.

2.3 Dirichlet L-Functions

We begin with the following definition.

Definition 8 (Character)**.** Let G be a group. Then a *character* is a group homomorphism $\chi\colon R \to S^1$. Here,

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

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

Example 9. The function $\chi(n) = 0$ for all $n \in \mathbb{Z}$ is a Dirichlet character, with $m = 1$.

Example 10. The function

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

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

Example 11. The function

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

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

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

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

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 $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to S^1$ where m is as small as possible, and extend χ to a Dirichlet character $\chi\colon \mathbb{Z} \to \mathbb{C}$. Then one can compute an integer $a \in \mathbb{Z}$ (depending on χ) and define
$$\xi(s,\chi) \coloneqq \left(\frac{q}{\pi}\right)^{(s+a)/2} \Gamma\left(\frac{s+a}{2}\right) L(s,\chi).$$
Then we have
$$\xi(s,\chi) = \varepsilon(\chi)\xi(1-s,\overline{\chi})$$
for some complex number $\varepsilon(\chi) \in \mathbb{C}$ depending on χ. Note that χ became $\overline{\chi}$ 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 12. 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 13. Let G be a finite group. Then

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

where the sum is over all characters $\chi\colon G \to S^1$.

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 14. 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 $\chi \colon G \to S^1$.

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 $\delta_a \colon \mathbb{Z} \to \mathbb{Z}$ by $\delta_a(n) = 1$ if $n \equiv a \pmod{m}$ and 0 otherwise. Now, we can use Lemma 13 to 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 $\sum_\chi$ is over all Dirichlet characters χ extended from $\chi \colon (\mathbb{Z}/m\mathbb{Z})^\times \to S^1$. Continuing, this rearranges into

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

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

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

so

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

Now, the proof of Theorem 12 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 15. One can also attach characters to Dedekind ζ-functions. This produces Hecke L-functions, but we will not discuss them here.

Remark 16. Again, these L-functions do not live in isolation: given a positive integer m, let $\zeta_m = e^{2\pi i/m}$ denote a primitive mth root of unity. Then one can show that

$$\zeta_K(s) = \prod_{\chi \pmod{m}} L(s, \chi),$$

where the product is over all Dirichlet characters χ lifted from a character $\chi \colon (\mathbb{Z}/m\mathbb{Z})^\times \to S^1$.

Exercise 17. Verify Remark 16 for $K = \mathbb{Q}(i)$, where here $i = \zeta_4$. Exercise 6 may be helpful.

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. And despite great gnashing of teeth, we will only state the functional equation and Riemann hypothesis at the very end of the discussion, in order to avoid having to talk in detail about projective varieties and other such geometric things.

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

It might seem silly to introduce entirely new notation for just writing K^d, but this has an important psychological effect: we want to think about $\mathbb{A}_K^d$ as a purely geometric object, while K^d 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 19 (Affine variety)**.** Let K be a field and d a positive integer. Then, given a subset of polynomials $S \subseteq K[x_1, \ldots, x_d]$, we define the vanishing set

$$V(S) \coloneqq \left\{(a_1, \ldots, a_d) \in \mathbb{A}_K^d : f(a_1, \ldots, a_d) \text{ for all } f \in S\right\}.$$

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

Remark 20. Some authors also require some extra geometric conditions to be a variety (e.g., irreducibility). We will not discuss these here.

Remark 21. Observe that we have a point $p \in V(S)$ if and only if p vanishes on all the polynomials in S. However, p vanishing on the polynomials in S means that p will also vanish on any linear combination of polynomials in S. As such, $p \in V(S)$ if and only if $p \in V((S))$, where $(S) \subseteq K[x_1, \ldots, x_d]$ is the ideal generated by the elements of S.

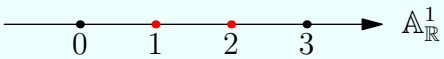
We've defined some geometric objects, so the next demand is to see some pictures. Throughout, we will let $K = \mathbb{R}$.

Example 22. Set $K = \mathbb{R}$ and $d = 1$, with $S = \{1\}$. Then $V(S) = \varnothing$.

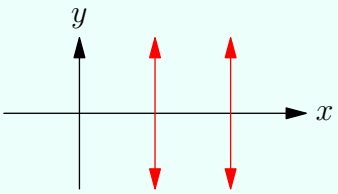
Example 23. Set $K = \mathbb{R}$ and $d = 1$, with $S = \{0\}$. Then $V(S) = \mathbb{A}_{\mathbb{R}}^1$ is the red set, as follows.

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

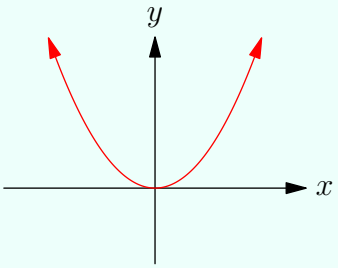
Example 24. Set $K = \mathbb{R}$ and $d = 1$, with $S = \{(x-1)(x-2)(x-3), (x-1)(x-2)(x-4)\}$. Then $V(S)$ is the red set.



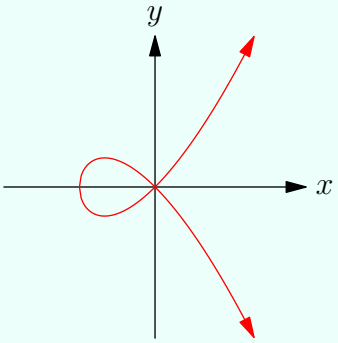
Example 25. Set $K = \mathbb{R}$ and $d = 2$, with $S = \{(x-1)(x-2)(x-3), (x-1)(x-2)(x-4)\}$. Then $V(S)$ is the red set.



Example 26. Set $K = \mathbb{R}$ and $d = 2$, with $S = \{y - x^2\} \subseteq \mathbb{R}[x, y]$. Then $V(S)$ is the red set.



Example 27. Set $K = \mathbb{R}$ and $d = 2$, with $S = \{y^2 - x^2(x+1)\} \subseteq \mathbb{R}[x, y]$. Then $V(S)$ is the red set.



3.2 The ζ-Function

Let q be a fixed prime-power and d a positive integer. Then we can construct a variety $V \subseteq \mathbb{A}^d_{\mathbb{F}_q}$ by choosing some subset of polynomials $S \subseteq \mathbb{F}_q[x_1, \ldots, x_d]$. In a field like arithmetic geometry, we are interested in counting the number of points on V.

It turns out to be relatively difficult to study V in isolation. To help with this, we will employ the following trick: note that we can embed $\mathbb{F}_q$ into $\mathbb{F}_{q^n}$ for any positive integer n, so we can view $S \subseteq \mathbb{F}_{q^m}[x_1, \ldots, x_d]$, allowing us to define another perhaps larger variety in $\mathbb{A}^d_{\mathbb{F}_q^n}$.

With this in mind, we will let $X(K)$ denote the variety defined by S in a field K containing $\mathbb{F}_q$; we will mostly be concerned with $K = \mathbb{F}_{q^n}$ for some positive integer n or $K = \overline{\mathbb{F}_q}$. In practice,

$$X(\mathbb{F}_{q^n}) = \{(a_1, \ldots, a_d) \in \mathbb{F}_{q^n} : f(a_1, \ldots, a_n) \text{ for all } f \in S\}.$$

In particular, instead of trying to count just $|X(\mathbb{F}_q)|$, it will be convenient to count all $|X(\mathbb{F}_{q^n})|$ at once. To see why, we define our ζ function to be the generating function

$$\zeta_X(T) \coloneqq \exp\left(\sum_{n=1}^{\infty} |X(\mathbb{F}_{q^n})| \frac{T^n}{n}\right) \in \mathbb{Q}[\![T]\!].$$

The following will be our main example.

Example 28. Take $S = \varnothing$ so that $X\left(\mathbb{F}_{q^n}\right) = \mathbb{A}^d_{\mathbb{F}_q^n}$ for all positive integers n. Then

$$\zeta_X(T) = \exp\left(\sum_{n=1}^{\infty} q^{nd} \cdot \frac{T^n}{n}\right) = \exp\left(\sum_{n=1}^{\infty} \frac{\left(q^d T\right)^n}{n}\right) = \frac{1}{1-q^d T},$$

where we have used the Taylor expansion $-\log(1-T) = \sum_{n=1}^{\infty} \frac{T^n}{n}$.

It will be enlightening to recast ζ_X as an arithmetic ζ-function, in the sense of Remark 7. This will be a little technical, but the details are not so important. The reader is encouraged to set $d = 1$ in what follows because it simplifies many parts of the discussion.

The relevant ring is $R \coloneqq \mathbb{F}_q[x_1, \ldots, x_d]/(S)$, where (S) is the ideal generated by the elements of S, as discussed in Remark 21. We will use the following idea.

Idea 29. Points on varieties correspond to maximal ideals of rings.

Indeed, to interface with an arithmetic ζ-function, we need to understand the maximal ideals of R; in some sense it is not too surprising that these maximal ideals are about to be able to let us count points on varieties, but the exact translation requires some care.

It turns out that these are in bijection with the maximal ideals of $\mathbb{F}_q[x_1, \ldots, x_d]$ which contain S. So let's begin by finding some maximal ideals. Well, given a point $p = (a_1, \ldots, a_d) \in X\left(\overline{\mathbb{F}_q}\right)$, observe that there is a map

$$\varphi\colon \mathbb{F}_q[x_1, \ldots, x_d] \to \overline{\mathbb{F}_q}$$

sending $x_i \mapsto a_i$ for all i. In particular, we get an embedding

$$\varphi\colon \frac{\mathbb{F}_q[x_1, \ldots, x_d]}{\ker \varphi} \hookrightarrow \overline{\mathbb{F}_q},$$

which implies that $\mathbb{F}_q[x_1, \ldots, x_d]/\ker\varphi$ is a field and hence $\ker\varphi$ is maximal. Additionally, requiring that $(a_1, \ldots, a_d) \in X\left(\overline{\mathbb{F}_q}\right)$ ensures that $S \subseteq \ker\varphi$. For notational convenience, we let $\mathfrak{m}_p \coloneqq \ker\varphi$.

It turns out that all maximal ideals of $\mathbb{F}_q[x_1, \ldots, x_d]/(S)$ take the form $\mathfrak{m}_p$ for some $p \in X\left(\overline{\mathbb{F}_q}\right)$. To see this, the key ingredient is Hilbert's Nullstellensatz.

Theorem 30 (Hilbert's Nullstellensatz)**.** Let K be a field and d a positive integer. If $\mathfrak{m} \subseteq K[x_1, \ldots, x_d]$ is a maximal ideal, then $K[x_1, \ldots, x_d]/\mathfrak{m}$ is a finite field extension of K.

Proof. Take a course in algebraic geometry. ∎

Remark 31. Many approximately equivalent statements are given the name Hilbert's Nullstellensatz, but we will only need the one of the above form.

Applied to our context, we are being told that all maximal ideals $\mathfrak{m} \subseteq \mathbb{F}_q[x_1, \ldots, x_d]$ come equipped with an isomorphism

$$\varphi\colon \frac{\mathbb{F}_q[x_1, \ldots, x_d]}{\mathfrak{m}} \to \mathbb{F}_{q^n}$$

for some positive integer n. We can then use φ to read off a d-tuple $p \coloneqq (a_1, \ldots, a_d) = (\varphi(x_1), \ldots, \varphi(x_d))$ in $\mathbb{A}^d_{\mathbb{F}_{q^n}}$, which lives in $X\left(\mathbb{F}_{q^n}\right)$ if and only if $S \subseteq \ker\varphi$. Thus, $\mathfrak{m} = \ker\varphi = \mathfrak{m}_p$.

Even though we have constructed all maximal ideals $\mathfrak{m}$ from points in $p \in X\left(\overline{\mathbb{F}_q}\right)$, some care is still required because it is possible for two points to give the same maximal ideal. Fixing this requires us to venture a little too far afield, so we will relegate the technicalities to an exercise.

Exercise 32. Fix a maximal ideal $\mathfrak{m} \subseteq \mathbb{F}_q[x_1, \dots, x_d]/(S)$. Additionally, we define the Frobenius automorphism $F : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$, which acts as $F(x) \coloneqq x^p$, and extend F to $X\left(\overline{\mathbb{F}_q}\right)$ coordinate-wise.

(a) Use Theorem 30 show that there is a positive integer n such that q^n equals the cardinality of the field $\mathbb{F}_q[x_1, \dots, x_d]/\mathfrak{m}$.

(b) If $p \in X\left(\overline{\mathbb{F}_q}\right)$ has $\mathfrak{m} = \mathfrak{m}_p$, then actually $p \in X\left(\mathbb{F}_{q^n}\right)$.

(c) Show that any $p \in X\left(\mathbb{F}_{q^n}\right)$ has $\mathfrak{m}_p = \mathfrak{m}_{Fp}$. (Hint: $\mathfrak{m}_p$ is the set of polynomials in $\mathbb{F}_q[x_1, \dots, x_d]$ which vanish at p.)

(d) It turns out that any $p, p' \in X\left(\mathbb{F}_{q^n}\right)$ with $\mathfrak{m}_p = \mathfrak{m}_{p'}$ has $p = F^k q$ for some integer k. Show this for $d = 1$, but feel free to use this fact for any positive integer d later on.

(e) Suppose that $\mathfrak{m} = \mathfrak{m}_p$ for $p \in X\left(\mathbb{F}_{q^n}\right)$. Use the previous two parts to show that

$$\left\{p' \in X\left(\mathbb{F}_{q^n}\right) : \mathfrak{m} = \mathfrak{m}_{p'}\right\} = \left\{F^k p : k \in \mathbb{Z}\right\}$$

has cardinality n. (Hint: F^n is the identity on $\mathbb{F}_{q^n}$.)

We are now ready to talk about our arithmetic ζ-function ζ_R, where $R = \mathbb{F}_q[x_1, \dots, x_d]/(S)$. Given two points $p, p' \in X\left(\overline{\mathbb{F}_q}\right)$, say $p \sim p'$ if and only if there exists $k \in \mathbb{Z}$ such that $p = F^k p'$. Then our work above combined with Exercise 32 tells us that maximal ideals $\mathfrak{m}$ of R are in bijection with equivalence classes of points $[p]$ in $X\left(\overline{\mathbb{F}_q}\right) / \sim$.

Now that we understand maximal ideals, the rest of the argument is just a computation. For convenience, we will write

$$\deg p \coloneqq \left[\frac{\mathbb{F}_q[x_1, \dots, x_d]}{\mathfrak{m}_p} : \mathbb{F}_q\right]$$

so that the equivalence class $[p] \subseteq$ has $\deg p$ points in it, using Exercise 32. Intuitively, we can think of the coordinates of p as generating a (finite) field extension of $\mathbb{F}_q$, and we have let n be the degree of this extension. In other words, the least n for which the coordinates of p live in $\mathbb{F}_{q^n}$ is $n = \deg p$, so translating this into Galois theory we have that the least n for which $F^n p = p$ is $n = \deg p$ as well.

Now, our bijection between maximal ideals and equivalence classes of points gives

$$\zeta_R(s) = \prod_{\substack{\text{maximal } \mathfrak{m} \subseteq R \\ |R/\mathfrak{m}| < \infty}} \frac{1}{1 - |R/\mathfrak{m}|^{-s}} = \prod_{[p] \in X\left(\overline{\mathbb{F}_q}\right)/\sim} \frac{1}{1 - q^{-s \cdot \deg p}}.$$

Already we see that we might as well set $T \coloneqq q^{-s}$ to abstract away the q from our ζ-function. As such, we write

$$\zeta_R(T) = \prod_{[p] \in X\left(\overline{\mathbb{F}_q}\right)/\sim} \frac{1}{1 - T^n}.$$

To try to get closer to the definition of $\zeta_X(T)$, we will want to apply logarithmic differentiation, so we write

$$\begin{aligned}
\frac{d}{dT} \log \zeta_R(T) &= \sum_{[p] \in X\left(\overline{\mathbb{F}_q}\right)/\sim} \frac{d}{dT} - \log\left(1 - T^{\deg p}\right) \\
&= \sum_{[p] \in X\left(\overline{\mathbb{F}_q}\right)/\sim} \frac{(\deg p) T^{\deg p - 1}}{1 - T^{\deg p}} \\
&= \sum_{[p] \in X\left(\overline{\mathbb{F}_q}\right)/\sim} \sum_{k=1}^{\infty} (\deg p) T^{(\deg p)k - 1} \\
&= \sum_{p \in X\left(\overline{\mathbb{F}_q}\right)} \sum_{k=1}^{\infty} T^{(\deg p)k - 1},
\end{aligned}$$

where at the end we used the fact that $[p]$ has $\deg p$ points in it. To help us out a little, we multiply both sides by T, giving

$$\begin{aligned} T \cdot \frac{d}{dT} \log \zeta_R(T) &= \sum_{p \in X\left(\overline{\mathbb{F}_q}\right)} \sum_{k=1}^{\infty} T^{(\deg p)k} \\ &= \sum_{n=1}^{\infty} \left(\sum_{d \mid n} \left| \{p \in X(\overline{\mathbb{F}_q}) : \deg p = d\} \right| \right) T^n \end{aligned}$$

To finish up, $p \in X\left(\mathbb{F}_{q^n}\right)$ is equivalent to the coordinates of p living in $\mathbb{F}_{q^n}$, which is equivalent to $\mathbb{F}_{q^{\deg p}} \subseteq \mathbb{F}_{q^n}$, which is equivalent to $\deg p \mid n$. As such,

$$T \cdot \frac{d}{dT} \log \zeta_R(T) = \sum_{n=1}^{\infty} \left| X(\mathbb{F}_{q^n}) \right| T^n = T \cdot \frac{d}{dT} \log \zeta_X(T),$$

which shows that $\zeta_X(T) = \zeta_R(T)$ after integrating and exponentiating—note $T = 0$ gives $1 = 1$, so our constant term is correct. In other words,

$$\zeta_X\left(q^{-s}\right) = \zeta_R(T) \tag{3.1}$$

after substituting back for T.

3.3 The Prime Number Theorem

As an application of the theory we've built, let q be a prime-power, set $d = 1$, and $S = (0) \subseteq \mathbb{F}_q[x_1, \dots, x_d]$ so that $X(K) = \mathbb{A}_K^d$ is to the K-points of the variety $V(S) \subseteq \mathbb{A}_K^d$, where $\mathbb{F}_q \subseteq K$. Lastly, we see $R = \mathbb{F}_q[x]$.

The main benefit to (3.1) is that it gives us an Euler product

$$\zeta_R(T) = \prod_{\text{maximal } \mathfrak{m} \subseteq R} \frac{1}{1 - T^{[R/\mathfrak{m}:\mathbb{F}_q]}}$$

after messaging the definition of $\zeta_R(T)$. Because R is a principal ideal domain with units $\mathbb{F}_q^\times$, for each maximal ideal $\mathfrak{m}$, we can find a unique monic irreducible polynomial $\pi \in \mathbb{F}_q[x]$ with $\mathfrak{m} = (\pi)$. Then

$$R/\mathfrak{m} = \mathbb{F}_q[x]/(\pi) \cong \mathbb{F}_{q^{\deg \pi}},$$

so

$$\zeta_R(T) = \prod_{\text{monic } \pi} \frac{1}{1 - T^{\deg \pi}},$$

where the product is taken over monic irreducible polynomials $\pi \in \mathbb{F}_q[x]$.

Remark 33. We can use unique prime factorization in $\mathbb{F}_q[x]$ to expand out $\zeta_R(T)$ into the series

$$\zeta_R(T) = \sum_{\text{monic } f \in \mathbb{F}_q[x]} T^{\deg f},$$

where the sum is over monic polynomials $f \in \mathbb{F}_q[x]$.

For that matter, careful examination of the arguments made at the end of subsection 3.2 (or by direct logarithmic differentiation again), we deduce

$$T \cdot \frac{d}{dT} \log \zeta_R(T) = \sum_{n=1}^{\infty} \left(\sum_{d \mid n} d\pi_q(d) \right) T^n, \tag{3.2}$$

where $\pi_q(d)$ is the number of monic irreducible polynomials of degree d. On the other hand,

$$T \cdot \frac{d}{dT} \log \zeta_X(T) = \sum_{n=1}^{\infty} |X(\mathbb{F}_{q^n})| T^n = \sum_{n=1}^{\infty} q^n T^n,$$

so we conclude

$$\sum_{d|n} d\pi_q(d) = q^n.$$

Möbius inversion gives the following statement.

Theorem 34. Let q be a prime-power and n a positive integer. Letting $\pi_q(n)$ denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$, we have

$$\pi_q(n) = \frac{1}{n} \sum_{d|n} q^d \mu(n/d) = \frac{q^n}{n} + O\big(q^{n/2}\big).$$

Remark 35. The error bound of $O\left(q^{n/2}\right)$ is said to have Riemann hypothesis quality because the analogous bound for integers is equivalent to the Riemann hypothesis.

Remark 36. Importantly, the above proof is more or less the easy part of the proof of the Prime number theorem (notably taking logarithmic differentiation of our ζ function in (3.2)). But then things immediately collapse because $\zeta_X(T)$ has no zeroes at all, meaning that the difficult bounding of the proof of the Prime number theorem to establish zero-free regions may be omitted.