8. PRIMES IN ARITHMETIC PROGRESSION

ROBERT J. LEMKE OLIVER AND FRANK THORNE

8. Dirichlet L-functions

In the last chapter, we introduced the *Dirichlet characters*, defined as homomorphisms $(\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$, or alternatively as the functions $\mathbb{Z}^+ \to \mathbb{C}$ which correspond to these homomorphisms. For each Dirichlet character χ we introduced its *L-function*

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

and we proved, for each arithmetic progression $a \pmod q$ with $(a,q) = 1$, that there are infinitely many primes $p \equiv a \pmod q$.

Our proof, however, rested on an IOU: that the limit $\lim_{s\to 1^+} L(s,\chi)$ exists and is nonzero. We will prove both of these facts in this chapter. We will also give an overview of the analytic behavior of these L-functions: they, too, have analytic continuation to $\mathbb{C}$ and satisfy a functional equation, and they are also expected to satisfy the Riemann hypothesis.

But before jumping into the weeds of complex analysis, let us look at what we are trying to persuade, so that we can convince ourselves that it should be true. We return to our old friend χ_4, given by

$$\chi_4(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \\ 0 & \text{if } n \text{ is even} \end{cases}. \tag{8.1}$$

Then we have

$$L(s,\chi_4) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots,$$

which doesn't look so scary. The series converges *absolutely* only for $\Re(s) > 1$, but (as we will prove in more generality) it converges and defines a holomorphic function for $\Re(s) > 0$, with

$$L(1,\chi_4) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

That is easily seen to converge, by the alternating series test. Indeed, you might remember from freshman calculus that

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}.$$

so that the 'special value' $L(1,\chi_4)$ is not only something nonzero, but something nice!

Date: February 25, 2025.

As another example, let χ_7 be the character[1]

$$\chi_7(n) = \left(\frac{\cdot}{7}\right) = \begin{cases} 1 & \text{if } n \equiv 1, 2, 4 \pmod 7 \\ -1 & \text{if } n \equiv 3, 5, 6 \pmod 7 \\ 0 & \text{if } 7 \mid n \end{cases}. \tag{8.2}$$

This is the unique nonprincipal character $(\mathrm{mod}\, 7)$ which takes values in ± 1. We have

$$L(1, \chi_7) = 1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} - \frac{1}{6} + \frac{1}{8} + \dots,$$

which converges because "the average value of the numerator equals 0", and which in fact equals $\frac{\pi}{\sqrt{7}}$.

Here is how to use the fact that the average value of the numerator equals 0.

Theorem 8.1. *Let χ be a Dirichlet character $(\mathrm{mod}\, q)$. If χ is nontrivial, then $L(s, \chi)$ converges if $\Re(s) > 0$ and can be extended to an analytic function in that region.*

Proof. Assume $\Re(s) > 0$. By Riemann-Stieltjes integration, we may write

$$L(s, \chi) = \int_{1^-}^{\infty} \frac{1}{t^s}\, d \sum_{n \le t} \chi(n).$$

By the orthogonality relations, the sum $\sum_{n \le t} \chi(n)$ is 0 whenever t is a multiple of q, which implies that its maximum absolute value for $t \in \mathbb{R}$ is bounded by $q/2$. Thus, by integration by parts,

$$\begin{aligned} L(s, \chi) &= \frac{1}{t^s} \sum_{n \le t} \chi(n) \Big|_{1^-}^{\infty} + s \int_1^{\infty} \frac{\sum_{n \le t} \chi(n)}{t^{s+1}}\, dt \\ &= s \int_1^{\infty} \frac{\sum_{n \le t} \chi(n)}{t^{s+1}}\, dt, \end{aligned}$$

which establishes the claim, since the integral converges. □

It is possible to prove, in an analogous manner as was done for the Riemann zeta function, that $L(s, \chi)$ analytically continues to a holomorphic function on all of $\mathbb{C}$. We will instead hit these L-functions with the sledgehammer of harmonic analysis behind the scenes, and present the resulting functional equation.

For each primitive character χ, we define the *Gauss sum*

$$\tau(\chi) = \sum_{a (\mathrm{mod}\, q)} \chi(a) e^{2\pi i a/q},$$

The function $e^{-2\pi i \cdot/q}$ is a *character* of the additive group $\mathbb{Z}/q\mathbb{Z}$. (We write $e^{-2\pi i \cdot/q}$ as a shorthand for the function $a \mapsto e^{-2\pi i a/q}$.) Thus the Gauss sum measures the correlation between the multiplicative character χ and the additive character $e^{-2\pi i \cdot/q}$. In the exercises, you will prove that $|\tau(\chi)| = q^{1/2}$.

We also define a quantity

$$\mathfrak{a} = \mathfrak{a}(\chi) := \begin{cases} 0 & \text{if } \chi(-1) = 1, \\ 1 & \text{if } \chi(-1) = -1. \end{cases}$$

[1] In fact, this would usually be denoted χ_{-7}, as it describes the splitting of primes in the quadratic field $\mathbb{Q}(\sqrt{-7})$. But that is a lengthy digression...

We call the character χ *even* in the first case and *odd* in the second.

Theorem 8.2 (Functional equation for $L(s,\chi)$)**.** *Let $\chi \pmod q$ be a nonprincipal primitive character, and define the completed L-function $\xi(s,\chi)$ by*

$$\xi(s,\chi) = (q/\pi)^{(s+\mathfrak{a})/2}\Gamma\left(\frac{s+\mathfrak{a}}{2}\right)L(s,\chi). \tag{8.3}$$

Then $\xi(s,\chi)$ is an everywhere holomorphic function satisfying

$$\xi(1-s,\chi) = \frac{i^{\mathfrak{a}}q^{1/2}}{\tau(\overline{\chi})}\xi(s,\overline{\chi}). \tag{8.4}$$

An exercise will ask you to fill in the last step of the proof of this functional equation: the bare result of Poisson summation will be presented as a black box, and you will manipulate them to conclude the above. This will give the reader some intuition for why the Gauss sum appears, for why it matters whether χ is even or odd, and why we assumed that χ is primitive.

Corollary 8.3 (Trivial zeros)**.** *If χ is a primitive Dirichlet character $\pmod q$, then $L(s,\chi) \neq 0$ in the region $\Re(s) > 1$. In the region $\Re(s) < 0$, $L(s,\chi) \neq 0$ except for the trivial zeroes:*

- *When χ is even, $L(s,\chi) = 0$ when $s \leq 0$ is an even integer;*
- *When χ is odd, $L(s,\chi) = 0$ when $s \leq 0$ is an odd integer.*

Proof. Non-vanishing in the region $\Re(s) > 1$ follows from the absolute convergence of the Euler product for $L(s,\chi)$. The claim about the region $\Re(s) < 0$ is a fairly straightforward exercise – use the facts that $\Gamma(s)$ is everywhere non-vanishing and that it has poles exactly at the non-positive integers. □

We will prove[2] that $L(s,\chi) \neq 0$ for $\Re(s) = 1$, in which case the functional equation also proves that $L(s,\chi) \neq 0$ for $\Re(s) = 0$, except that $L(0,\chi) = 0$ for an even character χ.

These L-functions are also expected to satisfy a version of the Riemann hypothesis – namely, that all zeros lie on the line of symmetry of the functional equation, $\Re(s) = 1/2$.

Conjecture 8.4 (The Generalized Riemann Hypothesis)**.** *If ρ_χ is a non-trivial zero of $L(s,\chi)$ for some primitive character $\chi \pmod q$, then $\Re(\rho_\chi) = 1/2$.*

This is no more proved than the ordinary Riemann hypothesis.

We now return to a proof that $L(1,\chi) \neq 0$, which will break up into two cases: the case where χ is nonprincipal and real-valued, and the case where it is not. The second case is, in our opinion, the most interesting. Let's eat our vegetables first.

Theorem 8.5. *Let χ be a real-valued Dirichlet character $\pmod q$. Then $L(1,\chi) \neq 0$.*

Proof. If $L(1,\chi) = 0$, then the product $L(s,\chi)\zeta(s)$ is holomorphic for all of $\mathbb{C}$. Is this possible?

[2]At least for $s = 1$. Will we do it in this generality?

The product $L(s,\chi)\zeta(s)$ can be written as an infinite product over all p, and we write out the Euler factors explicitly. At primes p for which $\chi(p) = -1$, we have

$$\begin{aligned}\left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{\chi(p)}{p^s}\right)^{-1} &= \left(1-\frac{1}{p^s}\right)^{-1}\left(1+\frac{1}{p^s}\right)^{-1}\\ &= \left(1-\frac{1}{p^{2s}}\right)^{-1}\\ &= 1+\frac{1}{p^{2s}}+\frac{1}{p^{4s}}+\dots\end{aligned}$$

We observe two key facts about this Euler factor: for real $s > 0$, it is a positive real number, and as $s \to 0^+$, it tends to infinity monotonically. Now, if $\chi(p) = 1$, we have

$$\begin{aligned}\left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{\chi(p)}{p^s}\right)^{-1} &= \left(1-\frac{1}{p^s}\right)^{-2}\\ &= \left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots\right)^2,\end{aligned}$$

while if $\chi(p) = 0$,

$$\left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{\chi(p)}{p^s}\right)^{-1} = \left(1-\frac{1}{p^s}\right)^{-1} = 1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots,$$

and once again the Euler factor is positive for real $s > 0$ and tends to infinity monotonically as $s \to 0^+$. We conclude from these observations that for all real $s > 0$ for which the product

$$\zeta(s)L(s,\chi) = \prod_p \left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$

converges, $\zeta(s)L(s,\chi)$ will be positive, and that there is some $\sigma_c \geq 0$ such that

$$\lim_{s\to\sigma_c^+} \zeta(s)L(s,\chi) = +\infty.$$

But the product $\zeta(s)L(s,\chi)$ is analytic, and so cannot have a pole at $s = \sigma_c$. This provides the desired contradiction. □

A famous fast food TV commercial from the 1980's asked, "Where's the beef?" The commercial suggested that their competitors sold hamburgers with big, fancy buns – and not very much in the middle.

Such a question might be asked of the previous proof as well. But in this case the beef is there – hiding in plain sight. Our reader should ask herself *what just happened*. This sort of question is something of a Zen koan.[3] Any answer we provided would be useless and unenlightening, but the process of contemplating the question is not.

Now we come to the very interesting case where χ is complex. The principle of the proof is to prove the following statement:

If $L(s,\chi)$ has a zero at $s = 1$, then $L(s,\chi^2)$ has a pole at $s = 1$.

[3]e.g., 'What is the sound of one hand clapping?'

Now, if χ^2 is a nonprincipal character, then we proved that $L(s, \chi^2)$ does not have a pole at $s = 1$ – and so the matter is settled. And, if χ is complex, then so is χ^2 – so in particular it is not principal. (If χ is real, then χ^2 *is* principal – this is the reason that case required a separate proof.)

Earlier, when we sketched a proof that $\zeta(s)$ doesn't have any zeroes on the line $\Re(s) = 1$, that proof hinged on the following statement:

$$\boxed{\text{If } \zeta(s) \text{ has a zero at } s = 1 + it, \text{ then } \zeta(s) \text{ has a pole at } s = 1 + 2it.}$$

And we knew a priori that $\zeta(s)$ had no poles in $\Re(s) > 0$, apart from that at $s = 1$.

In fact, we shall unify the above statements, and generalize further by proving the folliowing:

Theorem 8.6. *Let χ be a Dirichlet character, possibly principal.*

If $L(s, \chi)$ has a zero at $s = 1 + it$, then the L-function $L(s, \chi^2)$ has a pole at $s = 1 + 2it$.

We regard the constant function 1 as a Dirichlet character $\chi_1 \pmod 1$, with $\zeta(s) = L(s, \chi_1)$. Thus the theorem above applies to both the Riemann zeta function and to 'nontrivial' Dirichlet L-functions. The theorem contains both of the above boxed statements, as well as the statement that if $L(1 + it, \chi) = 0$, then $L(s, \chi^2)$ has a pole at $s = 1 + 2it$.

Of course, we know that the only poles of $L(s, \chi^2)$ on the line $\Re(s) = 1$ (or, indeed, anywhere in $\mathbb{C}$) lie at the point $\Re(s) = 1$, and then only for χ^2 principal – equivalently, for χ real. So the theorem asserts that no L-function $L(s, \chi)$ has a zero on the 1-line, except for the special case which we singled out and handled earlier.

Here is the principle of the proof. Write

$$L(1 + it, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n) n^{-it}}{n} =: \sum_{n=1}^{\infty} \frac{\alpha(n)}{n}.$$

Then we have

$$L(1 + 2it, \chi^2) = \sum_{n=1}^{\infty} \frac{\chi^2(n) n^{-2it}}{n} =: \sum_{n=1}^{\infty} \frac{\alpha^2(n)}{n}.$$

Now, if $L(s + it, \chi)$ has a zero at $s = 1$, then we will see that $\alpha(p)$ 'will usually be close to -1', as p ranges over the set of primes. But then $\alpha^2(p)$ will be close to 1, which will imply that $L(s + 2it, \chi^2)$ will have a pole at $s = 1$.

Write $L(s, \alpha) := L(s + it, \chi)$ and $L(s, \alpha^2) := L(s + 2it, \chi^2)$ for these two L-functions. Since α and α^2 are multiplicative, we have

$$L(s, \alpha^k) = \prod_p \left(1 - \frac{\alpha(p)}{p^s}\right)^{-1}$$

and (after taking logarithms and a Taylor expansion as usual)

$$\log L(s, \alpha^k) = \sum_p \frac{\alpha(p)}{p^s} + O(1),$$

uniformly throughout the domain of absolute convergence.

Here is the key step of the proof:

Lemma 8.7 (Analytic rigidity lemma)**.** *Let $L(s, \alpha^k)$ be above, and write*

$$\delta := \mathrm{ord}_{s=1} L(s, \alpha^k) \in \mathbb{Z}$$

for the order of vanishing of $L(s, \alpha^k)$ at $s = 1$. Then, we have

$$\lim_{s \to 1^+} \sum_p \frac{\alpha(p)^k + \delta}{p^s} = O_\alpha(1).$$

Proof. Our proof will use the fact that $L(s, \alpha^k)$ has meromorphic continuation to an open neighborhood of $\Re(s) \geq 1$. Consider first the special case $\delta = 0$, i.e. where $L(s, \alpha^k)$ is holomorphic and nonzero in a neighborhood of $s = 1$. Then the logarithm $\log L(s, \alpha^k)$ extends to a holomorphic function in this same neighborhood, and we have

$$\lim_{s \to 1^+} \sum_p \frac{\alpha(p)^k}{p^s} = \log L(1, \alpha_k) + O(1),$$

establishing the claim in this case.

Suppose now that $L(s, \alpha^k)$ has a zero of order δ at $s = 1$. (If $\delta < 0$, this means that $L(s, \alpha^k)$ has a pole of order $-\delta$.) Then, we 'calibrate' by considering the function $L(s, \alpha^k)\zeta(s)^\delta$: since $\zeta(s)$ has a simple pole at $s = 1$, the product $f(s) := L(s, \alpha^k)\zeta(s)^\delta$ is holomorphic and nonzero in a neighborhood of $s = 1$.

This time we have

$$\begin{aligned} \log f(1) &= \lim_{s \to 1^+} \Big(\log L(s, \alpha^k) + \delta \log \zeta(s) \Big) \\ &= \lim_{s \to 1^+} \Big(\sum_p \Big(\frac{\alpha(p)^k}{p^s} + \delta \frac{1}{p^s} \Big) \Big) + O(1), \end{aligned}$$

and upon writing $f(1) = O_\alpha(1)$ we are done. □

We now finish the proof. Suppose that $L(s, \alpha)$ has a zero at $s = 1$. Then, by analytic rigidity, we have

$$\lim_{s \to 1^+} \sum_p \frac{\alpha(p) + 1}{p^s} = O_\alpha(1).$$

In particular, assuming now that $s = \sigma$ is real, and taking real parts in the above, we have

$$\lim_{\sigma \to 1^+} \sum_p \frac{\Re(\alpha(p) + 1)}{p^\sigma} = O_\alpha(1), \tag{8.5}$$

and we wish to show that

$$\lim_{\sigma \to 1^+} \sum_p \frac{\Re(\alpha(p)^2 - 1)}{p^\sigma} = O_\alpha(1), \tag{8.6}$$

As an exercise, you might show that (8.5) does *not*, on its own, imply (8.6). We need analytic rigidity – namely, we need to know that if (8.6) fails, then we must instead have

$$\lim_{\sigma \to 1^+} \sum_p \frac{\Re(\alpha(p)^2 + \nu)}{p^\sigma} = O_\alpha(1) \tag{8.7}$$

for some nonnegative integer ν. This can't happen, and showing a contradiction between (8.5) and (8.7) is an exercise in pure muscle: almost any plausible strategy for finishing the

proof will eventually work. Here is one example. As $|\alpha(p)| = 1$ for each p, write $\alpha(p) := e^{i\theta_p}$ with $\theta_p \in \mathbb{R}/(2\pi\mathbb{Z})$. Let $\mathcal{S}$ denote the subset of those primes with either $\theta_p \in (\frac{7\pi}{8}, \frac{9\pi}{8})$ or $(\frac{-\pi}{8}, \frac{\pi}{8})$. Then for each $p \notin \mathcal{S}$, we have $\Re(\alpha(p) + 1) \geq 1 - \cos(\frac{7\pi}{8}) \gg 1$. Hence, by (8.5), we have

$$\lim_{\sigma \to 1^+} \sum_{p \notin \mathcal{S}} \frac{1}{p^\sigma} = O_\alpha(1), \tag{8.8}$$

which is a quantitative assertion that the complement of $\mathcal{S}$ is very small.

Now, if $\alpha(p) := e^{i\theta_p}$, then $\alpha(p)^2 = e^{2i\theta_p}$, and we turn our attention to (8.7). We have

$$\lim_{\sigma \to 1^+} \sum_{p \notin \mathcal{S}} \frac{\Re(\alpha(p)^2 + \nu)}{p^\sigma} = O_\alpha(1) \tag{8.9}$$

by (8.8), simply because the numerator is bounded. So by (8.7) we must also have

$$\lim_{\sigma \to 1^+} \sum_{p \in \mathcal{S}} \frac{\Re(\alpha(p)^2 + \nu)}{p^\sigma} = O_\alpha(1) \tag{8.10}$$

But for each $p \in \mathcal{S}$, we have $2\theta_p \in (\frac{-\pi}{4}, \frac{\pi}{4})$. Since $\nu \geq 0$, we have $\Re(\alpha(p)^2 + \nu) \geq \frac{1}{\sqrt{2}}$ for each $p \in \mathcal{S}$, so that

$$\lim_{\sigma \to 1^+} \sum_{p \in \mathcal{S}} \frac{1}{p^\sigma} = O_\alpha(1), \tag{8.11}$$

which means that $\mathcal{S}$ is very small. But wait – where do all the primes live then? $\mathcal{S}$ and its complement cannot simultaneously be small. Since $\zeta(s)$ has a pole at $s = 1$, we know that

$$\lim_{\sigma \to 1^+} \sum_{p} \frac{1}{p^\sigma} = +\infty, \tag{8.12}$$

which means that (8.8) and (8.11) cannot both be true.

This is our desired contradiction. Backtracking, we see that (8.6) holds, which by analytic rigidity implies that $L(s, \alpha^2)$ has a pole at $s = 1$. This was the conclusion of the theorem.

And thus, putting everything together, we are able to conclude:

Corollary 8.8. *Dirichlet's theorem, Theorem 7.1, is true.*

Remark. The proof of Theorem 8.5 is inspired by a theorem of Landau, who showed that if

$$A(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

is a Dirichlet series with positive coefficients a_n and there is some $s_0 \in \mathbb{C}$ for which the series defining $A(s)$ does not converge, then there exists a real $\sigma_c \geq \Re(s_0)$ such that $A(s)$ has a pole at $s = \sigma_c$. By examining the Euler product, the proof of Theorem 8.5 shows that $\zeta(s)L(s, \chi)$ is a series of this form that manifestly diverges at $s = 0$. Thus, Landau's theorem implies that $\zeta(s)L(s, \chi)$ must have a pole at some real $\sigma_c > 0$. But now that we know that $L(1, \chi) \neq 0$, this statement is obvious! The pole is simply at $s = 1$, coming from the factor of $\zeta(s)$ in the product $\zeta(s)L(s, \chi)$. In other words, the proof of Theorem 8.5 only establishes exactly what it says, that $L(1, \chi) \neq 0$, but who knows beyond that? It is entirely possible that for the kinds of "exceptional" characters χ considered by Theorem 8.5, $L(\sigma, \chi) = 0$

for some real σ extraordinarily close to 1. *It is a fundamental problem in analytic number theory, called the "Landau-Siegel zero" problem, to show that such zeros cannot exist.*

(Though we will not pursue it here, it is possible to adapt the proof of Theorem **??**, and for that matter Theorem 5.1, to show that $L(s,\chi) \neq 0$ for any s sufficiently close to the one-line $\Re(s) = 1$. In other words, in stark contrast to Theorem 8.5, these proofs establish more than what they say.)

Exercises.

1. Let χ be a non-trivial Dirichlet character $(\mathrm{mod}\, q)$. Show that

$$L(0,\chi) = \frac{-1}{q}\sum_{a=1}^{q}\chi(a)a.$$

Note that $\chi(-1) = \pm 1$ for all characters χ. Show that if $\chi(-1) = 1$, then

$$\sum_{a\le q/2}\chi(a) = 0.$$

Conclude in this case that $L(0,\chi) = 0$.

If $\chi(-1) = -1$, is it possible that $L(0,\chi) = 0$?[4]

2. Let χ be a primitive character. Prove that the Gauss sum $\tau(\chi)$ satisfies $|\tau(\chi)| = \sqrt{q}$.

(Hint: prove that $\tau(\chi)\cdot\overline{\tau(\chi)} = q$.)

3. (To be checked!) Here is an alternative derivation of the functional equation for Dirichlet L-functions. Let $q \ge 2$ be an integer, let $\Phi_q : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be any function for which $\Phi_q(-a) = \Phi_q(a)$ for all a, and define

$$\zeta(s,\Phi_q) := \sum_{n\ge 1}\Phi_q(n)n^{-s}.$$

Define the *Fourier transform* $\widehat{\Phi_q} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ by

$$\widehat{\Phi_q}(x) := \frac{1}{q}\sum_{y\in\mathbb{Z}/q\mathbb{Z}}\Phi_q(y)\exp(2\pi i xy/p),$$

and define $\zeta(s,\widehat{\Phi_q})$ accordingly. Defining $\xi(s,\Phi_q)$ and $\xi(s,\widehat{\Phi_q})$ by (8.3), then the functional equation

$$\xi(1-s,\Phi_q) = q^s\xi(s,\widehat{\Phi_q}). \tag{8.13}$$

is known to hold. Prove, as a consequence, that the functional equation (8.4) holds for even primitive characters χ.

This exercise is inspired by the second author's work on prehomogeneous vector spaces. The advantage of (8.13) as opposed to (8.3) is that its origin in the land of Fourier analysis is (arguably) a little bit clearer.

[4]This part of the question isn't fair.