

191: Analytic Number Theory

Nir Elber

Spring 2023

CONTENTS

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Contents	2
1 Arithmetic Progressions	3
1.1 January 18	3
1.1.1 House-Keeping	3
1.1.2 Facts about Dirichlet Series	3
1.1.3 The Euler Product	5
1.1.4 Characters	7
1.1.5 Finite Fourier Analysis	10
1.1.6 Dirichlet Characters	11
1.2 January 20	12
1.2.1 Continuing $L(s, \chi)$	12
1.2.2 Reducing to $L(1, \chi)$	16
Bibliography	19
List of Definitions	20

THEME 1

ARITHMETIC PROGRESSIONS

1.1 January 18

Here we go.

1.1.1 House-Keeping

We're teaching analytic number theory. Here are some notes.

- We will be referencing [Dav80] mostly, but we will do some things that Davenport does not do. For example, we will discuss the circle method, for which we refer to [Dav05].
- We will assume complex analysis, at the level of Math 185. We will use some Fourier analysis, but we will discuss the relevant parts as we need them. Of course, because this is number theory, we will assume some algebra, such as characters on abelian groups.
- There is a website [here](#), which includes a list of topics. Notably, there is a website for a previous version of the course.
- Grading is still up in there, as is the syllabus. Tentatively, grading will be as follows: by around the middle of the semester, there will be a list of recommended papers to read. Then we will write a 2–6-page report and present it to Professor Zhang. We will not have problem sets.
- Tentatively, office hours will be 90 minutes before lecture on Monday and Wednesday, in Evans 813.
- We should all write an email to Professor Zhang to introduce ourselves; for example, say what you're looking forward to in the course.

1.1.2 Facts about Dirichlet Series

In this first part of the course, we will be moving towards the following result.

Theorem 1.1 (Dirichlet). Fix nonzero integers $a, q \in \mathbb{Z}$ such that $\gcd(a, q) = 1$. Then there exist infinitely many primes p such that $p \equiv a \pmod{q}$.

The statement of Theorem 1.1 is purely elementary, but the standard proof uses complex analysis. The functions we will do analysis on are generalizations of the Riemann ζ function, defined as

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

which converges absolutely for $s \in \mathbb{C}$ such that $\operatorname{Re} s > 1$. Indeed, we can show this.

Lemma 1.2. Fix some open, connected subset $U \subseteq \mathbb{C}$ and some function $f: U \rightarrow \mathbb{C}$. Given holomorphic functions $f_n: U \rightarrow \mathbb{C}$ for each $n \in \mathbb{N}$, if $f_n \rightarrow f$ uniformly on all compact subsets $D \subseteq U$, then f is holomorphic.

Proof. The point is to use Morera's theorem. Each f_n is continuous, so we see f is continuous as well. Thus, fixing any closed piecewise C^1 path $\gamma: [0, 1] \rightarrow U$, we would like to show

$$\oint_{\gamma} f(z) dz \stackrel{?}{=} 0.$$

Note $\operatorname{im} \gamma$ is compact, so $f_n \rightarrow f$ uniformly on $\operatorname{im} \gamma$. Thus, fixing any $\varepsilon > 0$, we can find some N such that

$$|f(z) - f_n(z)| < \varepsilon$$

for all $n > N$. Fixing any $n > N$, we find

$$\left| \oint_{\gamma} f(z) dz \right| = \left| \oint_{\gamma} f(z) dz - \oint_{\gamma} f_n(z) dz \right| \leq \oint_{\gamma} |f(z) - f_n(z)| dz \leq \varepsilon \ell(\gamma),$$

where $\ell(\gamma)$ is the length of γ . (Note $\ell(\gamma)$ is finite because γ is piecewise C^1 .) Sending $\varepsilon \rightarrow 0^+$ finishes the proof. ■

Proposition 1.3. Let $f: \mathbb{N} \rightarrow \mathbb{C}$ denote a sequence of complex numbers such that $|f(n)| = O(n^{\sigma})$ for some $\sigma \in \mathbb{R}$. Then the series

$$D(s) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

converges absolutely for $s \in \mathbb{C}$ such that $\operatorname{Re} s > \sigma + 1$. Thus, $D(s)$ defines a holomorphic function in this region.

Proof. We are given $|f(n)| \leq Cn^{\sigma}$ for some $C > 0$. Thus, showing the absolute convergence is direct: note

$$\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right| \leq C \sum_{n=1}^{\infty} \frac{1}{n^{\operatorname{Re}(s) - \sigma}},$$

which converges because $\operatorname{Re}(s) - \sigma > 1$.

We can now convert absolute convergence to uniform convergence of the partial sums $\{D_n\}_{n \in \mathbb{N}}$ of D , from which Lemma 1.2 will finish. Fix some compact subset $D \subseteq U$, and we want to show $D_n \rightarrow D$ uniformly on D . Because D is compact, there exists $s_0 \in D$ with minimal $\operatorname{Re} s_0$; define $\sigma_0 := \operatorname{Re} s_0$. Now, the series

$$\sum_{n=1}^{\infty} \frac{|f(n)|}{n^{\sigma_0}}$$

converges by our absolute convergence.

As such, for any $\varepsilon > 0$, select N such that $n_0 > N$ implies

$$\sum_{n > n_0} \frac{|f(n)|}{n^{\sigma_0}} < \varepsilon.$$

Thus, for any $s \in \mathbb{C}$ and $n_0 > N$, we see

$$|D(s) - D_{n_0}(s)| = \left| \sum_{n > n_0} \frac{f(n)}{n^s} \right| \leq \sum_{n > n_0} \frac{|f(n)|}{n^{\operatorname{Re} s}} \leq \sum_{n > n_0} \frac{|f(n)|}{n^{\sigma_0}} < \varepsilon,$$

which is what we wanted. ■

It follows from Proposition 1.3 that $\zeta(s)$ defines a holomorphic function on $\operatorname{Re} s > 1$.

1.1.3 The Euler Product

The following factorization is due to Euler.

Proposition 1.4. Let $f: \mathbb{N} \rightarrow \mathbb{C}$ be a multiplicative function such that $|f(n)| = O(n^\sigma)$. For any $s \in \mathbb{C}$ such that $\operatorname{Re} s > \sigma + 1$, we have

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

Proof. Fix $s \in \mathbb{C}$ with $\operatorname{Re} s > \sigma + 1$. Roughly speaking, this follows from unique prime factorization in \mathbb{Z} . For and N and M to be fixed later, define

$$P_{N,M} := \prod_{p < N} \left(\sum_{k=0}^{M-1} \frac{f(p^k)}{p^{ks}} \right),$$

and define $P_{N,\infty}$ analogously. Define $A_{N,M}$ to be the set of integers n such that the prime factorization of n includes primes less than N each to a power less than M , and define $A_{N,\infty}$ analogously. Note $A_{N,M}$ is a finite set, so the distributive law implies

$$P_{N,M} = \sum_{n \in A_{N,M}} \frac{f(n)}{n^s}.$$

To begin, we fix N and claim

$$P_{N,\infty} \stackrel{?}{=} \sum_{n \in A_{N,\infty}} \frac{f(n)}{n^s}.$$

Note $P_{N,\infty} = \lim_{M \rightarrow \infty} P_{N,M}$, so we fix some $M > 0$ and compute

$$\left| P_{N,M} - \sum_{n \in A_{N,\infty}} \frac{f(n)}{n^s} \right| = \left| \sum_{n \in A_{N,\infty} \setminus A_{N,M}} \frac{f(n)}{n^s} \right| \leq \sum_{n \notin A_{N,M}} \left| \frac{f(n)}{n^s} \right|.$$

Now, the smallest n such that $n \notin A_{N,M}$ is at least 2^M , so we see

$$\left| P_{N,M} - \sum_{n \in A_{N,\infty}} \frac{f(n)}{n^s} \right| \leq \sum_{n \geq 2^M} \left| \frac{f(n)}{n^s} \right|,$$

which now vanishes as $M \rightarrow \infty$ because $\sum_{n=1}^{\infty} f(n)/n^s$ converges absolutely by Proposition 1.3. This completes the proof of the claim.

We now send $N \rightarrow \infty$ to finish the proof. For any $N > 0$, we use the claim to note

$$\left| P_{N,\infty} - \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \right| = \left| \sum_{n \notin A_{N,\infty}} \frac{f(n)}{n^s} \right| \leq \sum_{n \notin A_{N,\infty}} \left| \frac{f(n)}{n^s} \right|.$$

Now, we note that the smallest $n \notin A_{N,\infty}$ is at least N because any $n < N$ has a prime factor less than N , so

$$\left| P_{N,\infty} - \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \right| \leq \sum_{n \geq N} \left| \frac{f(n)}{n^s} \right|,$$

and now we see that the right-hand side goes to 0 as $N \rightarrow \infty$ because $\sum_{n=1}^{\infty} f(n)/n^s$ converges absolutely by Proposition 1.3. The proposition follows. \blacksquare

Corollary 1.5. We have

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

Proof. By Proposition 1.4, we see

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

which is what we wanted. ■

We can now use Corollary 1.5 to give a proof of the infinitude of primes.

Theorem 1.6. There are infinitely many primes. In fact,

$$\sum_{p \text{ prime}} \frac{1}{p} = +\infty.$$

Proof. Throughout the proof, s will be a real number greater than 1. The key estimate is to note

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \geq \int_1^{\infty} x^{-s} dx = -\frac{1}{1-s},$$

which goes to $+\infty$ as $s \rightarrow 1^+$. In particular, $\log \zeta(s) \rightarrow +\infty$ as $s \rightarrow 1^+$.

The last ingredient we need is to bound the Euler product of Corollary 1.5. In particular, we see

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

(Formally, one should cap the number of factors and then send the number of factors to infinity.) Using the Taylor expansion of $-\log(1 - x)$, we now see

$$\log \zeta(s) = \sum_{p \text{ prime}} \left(\sum_{k=1}^{\infty} \frac{1}{k p^{ks}} \right) = \left(\sum_{p \text{ prime}} \frac{1}{p^s} \right) + \sum_{p \text{ prime}} \left(\sum_{k=2}^{\infty} \frac{1}{k p^{ks}} \right).$$

We would like to focus on $\sum_p 1/p^s$, so we quickly show that the other sum converges. All terms are positive, so it suffices to show that it is bounded above, for which we see

$$\sum_{p \text{ prime}} \left(\sum_{k=2}^{\infty} \frac{1}{k p^{ks}} \right) \leq \sum_{p \text{ prime}} \left(\sum_{k=2}^{\infty} \frac{1}{p^k} \right) = \sum_{p \text{ prime}} \frac{1/p^2}{1 - 1/p} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) = 1,$$

where we have telescoped in the last equality. Letting the value of this sum be $S(s)$, we see

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

Now, as $s \rightarrow 1^+$, we see $\log \zeta(s) - S(s) \rightarrow +\infty$, so the theorem follows. ■

The proof of Theorem 1.1 more or less imitates the argument of Theorem 1.6. Roughly speaking, we will show that

$$\sum_{\substack{p \text{ prime} \\ p \equiv a \pmod{q}}} \frac{1}{p} = +\infty,$$

from which our infinitude follows. Finding a way to extract out the equivalence class $a \pmod{q}$ will use a little character theory.

1.1.4 Characters

Throughout, our groups will be finite and abelian, and actually we will be most interested in the abelian groups $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^\times$ for integers n . Formally, here is our definition.

Definition 1.7. Fix a positive integer n . Then we define $(\mathbb{Z}/n\mathbb{Z})^\times$ as the units in $\mathbb{Z}/n\mathbb{Z}$, which is $\{a \pmod n : \gcd(a, n) = 1\}$.

Remark 1.8. It is a fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for any prime p . This is nontrivial to prove, but we will not show it here.

Notably, given a prime factorization $n = \prod_{p|n} p^{\nu_p(n)}$, there is an isomorphism of rings

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{p|n} (\mathbb{Z}/p^{\nu_p(n)})$$

and hence also an isomorphism of multiplicative groups, upon taking units.

Having said all that, the theory is most cleanly build working with general finite abelian groups.

Definition 1.9 (dual group). Let G be a group. Then the *dual group* is $\widehat{G} := \text{Hom}(G, \mathbb{C}^\times)$, where the operation is pointwise. Its elements are called *characters*.

Notation 1.10 (principal character). There is a "trivial" character $1: G \rightarrow \mathbb{C}^\times$ sending $g \mapsto 1$, which is the identity. We might call 1 the *principal character*; we might also denote 1 by χ_0 .

Notation 1.11 (conjugate character). If $\chi: G \rightarrow \mathbb{C}^\times$ is a character, then note that $\overline{\chi}: G \rightarrow \mathbb{C}^\times$ defined by $\overline{\chi}(g) := \overline{\chi(g)}$ is also a character. Indeed, conjugation is a field homomorphism.

Remark 1.12. If G is a finite group, we note that any $\chi \in \widehat{G}$ and $g \in G$ has

$$\chi(g)^{\#G} = \chi(g^{\#G}) = 1,$$

so $\chi(g)$ is a $(\#G)$ th root of unity. In particular, $|\chi(g)| = 1$, so $\overline{\chi(g)} = \chi(g)^{-1} = \chi(g^{-1})$.

It will be helpful to have the following notation.

Notation 1.13. We might write $e: \mathbb{C} \rightarrow \mathbb{C}$ for the function $e(z) := \exp(2\pi iz)$.

We now begin computing \widehat{G} for finite abelian groups.

Lemma 1.14. Suppose G and H are groups. Then $\widehat{G} \times \widehat{H} \cong \widehat{G \times H}$ by sending (χ_G, χ_H) to $(g, h) \mapsto \chi_G(g)\chi_H(h)$.

Proof. We have the following checks. Let e_G and e_H be the identities of G and H , respectively.

- Well-defined: given $(\chi_G, \chi_H) \in \widehat{G} \times \widehat{H}$, define $\varphi(\chi_G, \chi_H): G \times H \rightarrow \mathbb{C}^\times$ by $\varphi(\chi_G, \chi_H): (g, h) \mapsto \chi_G(g)\chi_H(h)$. Note $\varphi(\chi_G, \chi_H)$ is a homomorphism: we have

$$\begin{aligned} \varphi(\chi_G, \chi_H)((g, h) \cdot (g', h')) &= \varphi(\chi_G, \chi_H)(gg', hh') \\ &= \chi_G(gg')\chi_H(hh') \\ &= \chi_G(g)\chi_H(h)\chi_G(g')\chi_H(h') \\ &= \varphi(\chi_G, \chi_H)(g, h) \cdot \varphi(\chi_G, \chi_H)(g', h'). \end{aligned}$$

- Homomorphism: to show φ is a homomorphism, we have

$$\varphi((\chi_G, \chi_H) \cdot (\chi'_G, \chi'_H))(g, h) = \chi_G(g)\chi'_G(g)\chi_H(h)\chi'_H(h) = \varphi(\chi_G, \chi_H)(g, h) \cdot \varphi(\chi'_G, \chi'_H)(g, h),$$

$$\text{so } \varphi((\chi_G, \chi_H) \cdot (\chi'_G, \chi'_H)) = \varphi(\chi_G, \chi_H) \cdot \varphi(\chi'_G, \chi'_H).$$

- Injective: if $\varphi(\chi_G, \chi_H) = 1$, then

$$\chi_G(g)\chi_H(h) = \varphi(\chi_G, \chi_H)(g, h) = 1$$

for all $g \in G$ and $h \in H$. Setting $g = e_G$ shows that $\chi_H = 1$, and similarly setting $h = e_H$ shows that $\chi_G = 1$. Thus, $(\chi_G, \chi_H) = (1, 1)$.

- Surjective: given a character $\chi: (G \times H) \rightarrow \mathbb{C}^\times$, define $\chi_G(g) := \chi(g, e_H)$ and $\chi_H(h) := \chi(e_G, h)$. Note χ_G is a character because

$$\chi_G(gg') = \chi(gg', e_H) = \chi(g, e_H)\chi(g', e_H) = \chi_G(g)\chi_G(g').$$

Switching the roles of G and H shows that χ_H is also a character. Lastly, we note $\varphi(\chi_G, \chi_H) = \chi$ because

$$\varphi(\chi_G, \chi_H)(g, h) = \chi(g, e_H)\chi(e_G, h) = \chi(g, h).$$

This completes the proof. ■

Lemma 1.15. Suppose $G = \mathbb{Z}/n\mathbb{Z}$ for a positive integer n . Then $\chi_\bullet: \mathbb{Z}/n\mathbb{Z} \cong \widehat{G}$ by sending $[k]$ to the character $\chi_k: [\ell] \mapsto e(k\ell/n)$.

Proof. To begin, note $\chi_k: \mathbb{Z} \rightarrow \mathbb{C}^\times$ defines a homomorphism because

$$\chi_k(\ell + \ell') = e\left(\frac{k(\ell + \ell')}{n}\right) = e\left(\frac{k\ell}{n}\right)e\left(\frac{k\ell'}{n}\right) = \chi_k(\ell)\chi_k(\ell').$$

Further, note $\chi_k(n\ell) = e(k\ell) = 1$ for any $n\ell \in \mathbb{Z}$, so $n\mathbb{Z} \subseteq \ker \chi_k$. It follows that χ_k produces a homomorphism $\chi_k: G \rightarrow \mathbb{C}^\times$.

We now note that $\chi_\bullet: \mathbb{Z} \rightarrow \widehat{G}$ defines a homomorphism: for any $[\ell] \in G$, we see

$$\chi_{k+k'}([\ell]) = e\left(\frac{(k+k')\ell}{n}\right) = e\left(\frac{k\ell}{n}\right)e\left(\frac{k'\ell}{n}\right) = \chi_k([\ell])\chi_{k'}([\ell]).$$

Additionally, $\chi_{nk}([\ell]) = e(k\ell) = 1$, so $\chi_{nk} = 1$, so $nk \in \ker \chi_\bullet$. It follows that χ_\bullet produces a homomorphism $\chi_\bullet: \mathbb{Z}/n\mathbb{Z} \rightarrow \widehat{G}$.

It remains to show that χ_\bullet is a bijection. We have two checks.

- Injective: suppose $\chi_k = 1$ for $k \in \mathbb{Z}$. We must show $k \in n\mathbb{Z}$. Well, we must then have

$$1 = \chi_k([1]) = e(k/n),$$

which forces $n \mid k$.

- Surjective: given some character $\chi: G \rightarrow \mathbb{C}^\times$, we note $\chi([1])^n = \chi([0]) = 1$, so $\chi([1])$ is an n th root of unity. Thus, there exists k such that $\chi([1]) = e(k/n) = \chi_k([1])$. Thus, for any $\ell \in \{0, 1, \dots, n-1\}$, we see

$$\chi([\ell]) = \chi(\underbrace{[1] + \dots + [1]}_\ell) = \underbrace{\chi([1]) \cdot \dots \cdot \chi([1])}_\ell = \underbrace{\chi_k([1]) \cdot \dots \cdot \chi_k([1])}_\ell = \chi_k([\ell]),$$

so $\chi = \chi_k$ follows. ■

Proposition 1.16. Let G be a finite abelian group. Then $G \cong \widehat{\widehat{G}}$.

Proof. By the Fundamental theorem of finitely generated abelian groups, we may write

$$G \cong \prod_{i=1}^n \mathbb{Z}/n_i\mathbb{Z}$$

for some positive integers n_i . Thus, using Lemma 1.14 and Lemma 1.15, we compute

$$\widehat{G} \cong \left(\prod_{i=1}^n \widehat{\mathbb{Z}/n_i\mathbb{Z}} \right) = \prod_{i=1}^n \widehat{\mathbb{Z}/n_i\mathbb{Z}} \cong \prod_{i=1}^n \mathbb{Z}/n_i\mathbb{Z} \cong G,$$

which is what we wanted. ■

Proposition 1.16 might look like we now understand dual groups perfectly, but the isomorphism given there is non-canonical because the isomorphism of Lemma 1.15 is non-canonical. In other words, given some $g \in G$, there is in general no good way to produce character $\chi \in \widehat{G}$.

However, there is a natural map $G \rightarrow \widehat{\widehat{G}}$ which is an isomorphism.

Proposition 1.17. Fix a finite abelian group G . Define the map $\text{ev}_\bullet: G \rightarrow \widehat{\widehat{G}}$ by sending $g \in G$ to the map $\text{ev}_g \in \widehat{\widehat{G}}$ defined by $\text{ev}_g: \chi \mapsto \chi(g)$. Then ev_\bullet is an isomorphism.

Proof. We begin by checking that ev_\bullet is a well-defined homomorphism. For each $g \in G$, we see $\text{ev}_g: \widehat{G} \rightarrow \mathbb{C}^\times$ is a homomorphism because

$$\text{ev}_g(\chi\chi') = \chi(g)\chi'(g) = \text{ev}_g(\chi)\text{ev}_g(\chi').$$

Further, ev_\bullet is a homomorphism because

$$\text{ev}_{gg'}(\chi) = \chi(g)\chi(g') = \text{ev}_g(\chi)\text{ev}_{g'}(\chi).$$

It remains to show that ev_\bullet is an isomorphism. We claim that ev_\bullet is injective, which will be enough because $|G| = |\widehat{\widehat{G}}|$ by Proposition 1.16.

For this, we appeal to the following lemma.

Lemma 1.18. Fix a finite abelian group G with identity e . If $g \neq e$, then there exists $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$.

Proof. Using the Fundamental theorem of finitely generated abelian groups, we may write

$$G \cong \prod_{i=1}^n \mathbb{Z}/n_i\mathbb{Z}$$

for positive integers $n_i \geq 2$. Moving our problem from G to the right-hand side, we are given some $(g_i)_{i=1}^n$ such that $[g_i] \neq [0]$ for at least one i , and we want a character χ such that $\chi((g_i)_{i=1}^n) \neq 1$. Without loss of generality, suppose that $g_1 \neq 0$ and define χ by

$$\chi((k_i)_{i=1}^n) := e(k_1/n_1).$$

Certainly $\chi((g_i)_{i=1}^n) = e(g_1/n_1) \neq 1$, so it remains to show that χ is a character. This technically follows from Lemma 1.14, but we can see it directly by computing

$$\chi((k_i)_{i=1}^n + (k'_i)_{i=1}^n) = e(k_1/n_1)e(k'_1/n_1) = \chi((k_i)_{i=1}^n)\chi((k'_i)_{i=1}^n).$$

This completes the proof. ■

The proof now follows quickly from Lemma 1.18. By contraposition, we see that any $g \in G$ such that $\chi(g) = 1$ for all $\chi \in \widehat{G}$ and must have $g = e$. But this is exactly the statement that $\text{ev}_\bullet: G \rightarrow \widehat{\widehat{G}}$ is injective. ■

1.1.5 Finite Fourier Analysis

We now proceed to essentially do Fourier analysis for finite abelian groups. Here is the idea.



Idea 1.19. We can write general functions $G \rightarrow \mathbb{C}$ as linear combinations of characters.

Remark 1.20. When G is not abelian, one must work with function $G \rightarrow \mathbb{C}$ which are “locally constant” on conjugacy classes of G .

Here is our Fourier transform.

Notation 1.21. Let G be a finite abelian group. Given a function $f: G \rightarrow \mathbb{C}$, we define $\widehat{f}: \widehat{G} \rightarrow \mathbb{C}$ by

$$\widehat{f}(\chi) := \sum_{g \in G} f(g) \overline{\chi(g)}.$$

Recall $\overline{\chi(g)} = \chi(g^{-1})$ by Remark 1.12.

To manifest Idea 1.19 properly, we need the following orthogonality relations.

Proposition 1.22. Let G be a finite abelian group.

- For any fixed $\chi \in \widehat{G}$, we have

$$\sum_{g \in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq 1, \\ \#G & \text{if } \chi = 1. \end{cases}$$

- For any $g \in G$, we have

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} 0 & \text{if } g \neq e, \\ \#G & \text{if } g = e. \end{cases}$$

Proof. We show these directly.

- (a) If $\chi = 1$, then the sum is $\sum_{g \in G} 1 = \#G$.

Otherwise, $\chi \neq 1$, so there exists $g_0 \in G$ such that $\chi(g_0) \neq 1$. It follows

$$\chi(g_0) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g_0 g) \stackrel{*}{=} \sum_{g \in G} \chi(g),$$

so we must have $\sum_{g \in G} \chi(g) = 0$. Note that we have re-indexed the sum at $\stackrel{*}{=}$.

- (b) If $g = e$, then the sum is $\sum_{\chi \in \widehat{G}} \chi(e) = \#(\widehat{G})$, which is $\#G$ by Proposition 1.16.

Otherwise, $g \neq e$, so by Lemma 1.18, there exists χ_0 such that $\chi_0(g) \neq 1$. Employing the same trick, it follows

$$\chi_0 \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} (\chi_0 \chi)(g) \stackrel{*}{=} \sum_{\chi \in \widehat{G}} \chi(g),$$

so we must have $\sum_{\chi \in \widehat{G}} \chi(g) = 0$. Again, we re-indexed at $\stackrel{*}{=}$. ■

Now here is our result.

Theorem 1.23 (Fourier inversion). Let G be a finite abelian group. For any $f: G \rightarrow \mathbb{C}$, we have

$$f(g) = \frac{1}{\#G} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(g)$$

for any $g \in G$.

Proof. This is direct computation with Proposition 1.22. Indeed, for any $g_0 \in G$, we see

$$\sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(g_0) = \sum_{\chi \in \hat{G}} \sum_{g \in G} f(g) \chi(g^{-1}) \chi(g_0) = \sum_{g \in G} \left(f(g) \sum_{\chi \in \hat{G}} \chi(g^{-1} g_0) \right).$$

Now using Proposition 1.22, given $g \in G$, we see that the inner sum will vanish whenever $g \neq g_0$ and returns $\#G$ when $g = g_0$. In total, it follows

$$\frac{1}{\#G} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(g_0) = f(g_0),$$

which is exactly what we wanted. ■

Here is our chief application.

Corollary 1.24. Let G be a finite abelian group. Fixing some $g_0 \in G$, we have

$$1_{g_0}(g) = \frac{1}{\#G} \sum_{\chi \in \hat{G}} \overline{\chi(g_0)} \chi(g)$$

for any $g \in G$.

Proof. Note

$$\hat{1}_{g_0}(\chi) = \sum_{g \in G} 1_{g_0}(g) \overline{\chi(g)} = \overline{\chi(g_0)}$$

because all terms except $g = g_0$ vanish. The result now follows from Theorem 1.23. ■

1.1.6 Dirichlet Characters

We want to extend our characters on $(\mathbb{Z}/q\mathbb{Z})^\times$ to work on all \mathbb{Z} , but this requires some trickery because, for example, 0 is not in general represented in $(\mathbb{Z}/q\mathbb{Z})^\times$. Here is our definition.

Definition 1.25 (Dirichlet character). Let q be a nonzero integer. A *Dirichlet character* $(\bmod q)$ is a function $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ such that there exists a character $\tilde{\chi}: (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ for which

$$\chi(a) = \begin{cases} 0 & \text{if } \gcd(a, q) > 1, \\ \tilde{\chi}([a]) & \text{if } \gcd(a, q) = 1. \end{cases}$$

We might write this situation as $\chi \pmod{q}$. The Dirichlet character corresponding to 1 is denoted χ_0 and still called the *principal character*.

Remark 1.26. Note χ is periodic with period q .

We can finally define our generalization of ζ .

Definition 1.27 (Dirichlet L -function). Fix a Dirichlet character $\chi \pmod{q}$. Then we define the *Dirichlet L -function* as

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

By Proposition 1.3, we have absolute convergence for $\operatorname{Re} s > 1$, and $L(s, \chi)$ defines a holomorphic function there.

Remark 1.28. Continuing in the context of the definition, we note Proposition 1.4 gives

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

for $\operatorname{Re} s > 1$.

In fact, the summation for $L(s, \chi)$ defines a holomorphic function for $\operatorname{Re} s > 0$, but seeing this requires a little care.

1.2 January 20

A syllabus was posted. There are some extra references posted.

1.2.1 Continuing $L(s, \chi)$

We are going to need the following technical result. Roughly speaking, it allows us to estimate infinite sums with a discrete part and a continuous part by summing the discrete part and integrating the continuous part. Oftentimes, a sum is difficult because of the way it mixes discrete and continuous portions, so it is useful to be able to separate them.

Theorem 1.29 (Abel summation). Let $\{a_n\}_{n \in \mathbb{N}}$ be a sequence of complex numbers, and define the partial sums be given by

$$A(t) := \sum_{1 \leq n \leq t} a_n.$$

For any real numbers $x, y \in \mathbb{R}$ with $x < y$ and continuously differentiable function $f: (0, x] \rightarrow \mathbb{C}$, we have

$$\sum_{0 < n \leq x} a_n f(n) = A(x)f(x) - \int_0^x A(t)f'(t) dt.$$

Proof. The idea is to write $a_n = A(n) - A(n-1)$, so we write

$$\begin{aligned} \sum_{n \leq x} a_n f(n) &= \sum_{n \leq x} A(n)f(n) - \sum_{n \leq x} A(n-1)f(n) \\ &= \sum_{0 < n \leq x} A(n)f(n) - \sum_{-1 < n \leq x-1} A(n)f(n+1) \\ &= A(\lfloor x \rfloor)f(\lfloor x \rfloor) - A(-1)f(0) - \sum_{0 < n \leq x-1} A(n)(f(n+1) - f(n)). \end{aligned}$$

Note $A(-1) = 0$. We now introduce an integral by noting $A(n)(f(n+1) - f(n)) = \int_n^{n+1} A(t)f'(t) dt$, which

upon summing over n yields

$$\sum_{0 < n \leq x} a_n f(n) = A(\lfloor x \rfloor) f(\lfloor x \rfloor) - \int_0^{\lfloor x \rfloor} A(t) f'(t) dt.$$

To finish, we see

$$A(\lfloor x \rfloor) f(\lfloor x \rfloor) = A(x) f(x) + A(\lfloor x \rfloor) (f(\lfloor x \rfloor) - f(x)) = A(x) f(x) - \int_{\lfloor x \rfloor}^x A(t) dt,$$

which when combined with the previous equality finishes. ■

Remark 1.30. One can use the theory of Riemann–Stieltjes integration to turn Theorem 1.29 into just an application of integration by parts, but we will not need this.

As an example application, we may give $L(s, \chi)$ an analytic continuation to $\{s : \operatorname{Re} s > 0\}$ when χ is not the principal character.

Proposition 1.31. Let $\chi \pmod{q}$ be a non-principal Dirichlet character. Then the function $L(s, \chi)$ admits an analytic continuation to $\{s : \operatorname{Re} s > 0\}$.

Proof. For given s with $\operatorname{Re} s > 1$, set $a_n := \chi(n)$ and $f(x) := 1/x^s$. Then the partial sums $A(t) := \sum_{1 \leq n \leq t} a_n$ have

$$\sum_{n=1}^{kq} \chi(n) = \sum_{a=0}^{k-1} \sum_{r=1}^q \chi(aq+r) = k \sum_{r=1}^q \chi(r) = k \sum_{\substack{1 \leq r \leq q \\ \gcd(r,q)=1}} \chi(r) = k \cdot 0$$

for any $k \geq 0$, where in the last equality we have used Proposition 1.22. Thus, for any $t \geq 0$, find $k \in \mathbb{Z}$ such that $kq \leq t < k(q+1)$, and we see

$$|A(t)| = \left| \sum_{1 \leq n \leq t} \chi(n) \right| = \left| \sum_{1 \leq n \leq kq} \chi(n) + \sum_{kq < n \leq t} \chi(n) \right| \leq \sum_{kq < n \leq t} |\chi(n)| \leq t - kq \leq q.$$

Now, finally using Theorem 1.29, we see

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \left(\lim_{x \rightarrow \infty} A(x) x^{-s} \right) - \lim_{x \rightarrow \infty} \int_0^x (A(t) \cdot -s t^{-s-1}) dt.$$

Because $\operatorname{Re} s > 1$, we see $|A(x) x^{-s}| \leq q x^{-\operatorname{Re} s}$ goes to 0 as $x \rightarrow \infty$. Thus, we are left with

$$L(s, \chi) = s \int_0^{\infty} \frac{A(t)}{t^{s+1}} dt = s \underbrace{\int_1^{\infty} \frac{A(t)}{t^{s+1}} dt}_{I(s)}.$$

We claim that the right-hand side provides our analytic continuation to $\{s : \operatorname{Re} s > 0\}$. Indeed, it suffices to show that $I(s)$ is analytic on $\{s : \operatorname{Re} s > 0\}$. This is technical.

Roughly speaking, we want to write

$$\left| \int_1^{\infty} \frac{A(t)}{t^{s+1}} dt \right| \leq q \int_1^{\infty} \frac{1}{t^{\operatorname{Re} s + 1}} dt = q \cdot \left. \frac{t^{-\operatorname{Re} s}}{-\operatorname{Re} s} \right|_1^{\infty} = \frac{q}{\operatorname{Re} s}$$

for any $\operatorname{Re} s > 0$, meaning that the integral converges, so we ought to have a holomorphic function. Well, for each N , we define

$$I_N(s) := \int_1^N \frac{A(t)}{t^{s+1}} dt = \sum_{n=1}^{N-1} \left(A(n) \int_n^{n+1} t^{-s-1} dt \right) = \sum_{n=1}^{N-1} \left(A(n) \cdot \frac{(n+1)^{-s} - n^{-s}}{-s} \right)$$

so that $I_N(s) \rightarrow I(s)$ as $N \rightarrow \infty$ for each s with $\operatorname{Re} s > 0$. Notably, for each N , the above computation shows that I_N is holomorphic on $\{s : \operatorname{Re} s > 0\}$.

By Lemma 1.2, it thus suffices to show that $I_n(s) \rightarrow I(s)$ uniformly on compact sets as $n \rightarrow \infty$. The main computation is to note that for each s with $\operatorname{Re} s > 0$ and n , we may upper-bound

$$|I(s) - I_n(s)| = \left| \int_n^\infty \frac{A(t)}{t^{s+1}} dt \right| \leq q \int_n^\infty t^{-\operatorname{Re} s - 1} dt = \frac{qn^{-\operatorname{Re} s}}{\operatorname{Re} s}.$$

Now, select some compact $D \subseteq \{s : \operatorname{Re} s > 0\}$. Because D is compact, there exists $s \in D$ with minimal $\sigma := \operatorname{Re} s$. Note $\sigma > 0$, so using the above bound, for any $\varepsilon > 0$, select $N := (\sigma\varepsilon/q)^{-1/\sigma}$. Thus, for any $n > N$ and $s \in D$, we see

$$|I(s) - I_n(s)| \leq \frac{qn^{-\operatorname{Re} s}}{\operatorname{Re} s} < \frac{qN^{-\sigma}}{\sigma} = \varepsilon,$$

which completes the proof. ■

Remark 1.32. Using the notions and notations of the above proof, we see that

$$|L(s, \chi)| = \left| s \int_1^\infty \frac{A(t)}{t^{s+1}} dt \right| \leq \frac{q|s|}{\operatorname{Re} s}$$

for $\operatorname{Re} s > 0$. This upper-bound is occasionally helpful.

One might wonder what happens to the principal character χ_0 . It turns out its behavior is tied to ζ .

Lemma 1.33. Let $\chi_0 \pmod{q}$ be the principal Dirichlet character. Then for $\operatorname{Re} s > 1$, we have

$$L(s, \chi) = \left(\prod_{p|q} (1 - p^{-s}) \right) \zeta(s).$$

Proof. By Remark 1.28, we see

$$L(s, \chi) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}} = \prod_{p \nmid q} \frac{1}{1 - p^{-s}},$$

so

$$L(s, \chi) \prod_{p|q} \frac{1}{1 - p^{-s}} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} = \zeta(s)$$

by Corollary 1.5, which finishes. ■

Thus, we are interested in continuing ζ . With a little more effort than Proposition 1.31, we may provide $\zeta(s)$ a meromorphic continuation to $\{s : \operatorname{Re} s > 0\}$. The main difficulty here is that we have a pole to deal with.

Proposition 1.34. The function $\zeta(s)$ has a meromorphic continuation to $\{s : \operatorname{Re} s > 0\}$. It is holomorphic everywhere except at $s = 1$, where it has a simple pole of residue 1.

Proof. For given s with $\operatorname{Re} s > 1$, set $a_n := 1$ and $f(x) := 1/x^s$. Then the partial sums $A(t) := \sum_{1 \leq n \leq t} a_n$ have $A(t) = \lfloor t \rfloor$, so Theorem 1.29 grants

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \left(\lim_{x \rightarrow \infty} \lfloor x \rfloor \cdot x^{-s} \right) - \lim_{x \rightarrow \infty} \int_0^x (\lfloor t \rfloor \cdot -st^{-s-1}) dt.$$

Because $\operatorname{Re} s > 1$, we see $|\lfloor x \rfloor \cdot x^{-s}| \leq x^{1-\operatorname{Re} s}$ goes to 0 as $x \rightarrow \infty$. Thus, we are left with

$$\zeta(s) = s \int_0^\infty \frac{\lfloor t \rfloor}{t^{s+1}} dt = s \int_1^\infty \frac{\lfloor t \rfloor}{t^{s+1}} dt.$$

To extract out a main term, we write $\lfloor t \rfloor = t + \{t\}$, giving

$$\zeta(s) = s \int_1^\infty t^{-s} dt + s \int_1^\infty \frac{\{t\}}{t^{s+1}} dt = \frac{s}{s-1} + s \underbrace{\int_1^\infty \frac{\{t\}}{t^{s+1}} dt}_{I(s)}.$$

We claim that the above expression defines our meromorphic continuation. Notably, the function $s/(s-1) = 1 + 1/(s-1)$ is holomorphic everywhere except at $s = 1$, where it has a simple pole of residue 1.

Thus, it remains to show that $s \cdot I(s)$ is a holomorphic function for $\operatorname{Re} s > 0$, where it suffices to show that $I(s)$ is a holomorphic function for $\operatorname{Re} s > 0$. This is mildly technical. At a high level, we would like to just note that

$$\left| \int_1^\infty \frac{\{t\}}{t^{s+1}} dt \right| \leq \int_1^\infty \frac{1}{t^{\operatorname{Re} s + 1}} dt = \frac{t^{-\operatorname{Re} s}}{-\operatorname{Re} s} \Big|_1^\infty = \frac{1}{\operatorname{Re} s},$$

so the integral converges and ought to define a holomorphic function. Being more formal, we work with the finite integrals

$$I_N(s) := \int_1^N \frac{\{t\}}{t^{s+1}} dt = \sum_{n=1}^{N-1} \left(\int_n^{n+1} \frac{t-n}{t^{s+1}} dt \right) = \sum_{n=1}^{N-1} \left(\frac{(n+1)^{-s+1} - n^{-s+1}}{-s+1} - n \cdot \frac{(n+1)^{-s} - n^{-s}}{-s} \right)$$

so that $I_N(s) \rightarrow I(s)$ as $N \rightarrow \infty$ for each s with $\operatorname{Re} s > 0$. Notably, for each N , the above computation shows that I_N is holomorphic on $\{s : \operatorname{Re} s > 0\}$.

By Lemma 1.2, it thus suffices to show that $I_n(s) \rightarrow I(s)$ uniformly on compact sets as $n \rightarrow \infty$. The main computation is to note that for each s with $\operatorname{Re} s > 0$ and n , we may upper-bound

$$|I(s) - I_n(s)| = \left| \int_n^\infty \frac{\{t\}}{t^{s+1}} dt \right| \leq \int_n^\infty \frac{1}{t^{\operatorname{Re} s}} dt = \frac{n^{-\operatorname{Re} s}}{\operatorname{Re} s},$$

arguing as before. Now, select some compact $D \subseteq \{s : \operatorname{Re} s > 0\}$. Because D is compact, there exists a minimal $\sigma := \operatorname{Re} s$ among all $s \in D$. Note $\sigma > 0$, so for any $\varepsilon > 0$, we use the above bounding to set $N := (\sigma\varepsilon)^{-1/\sigma}$. Thus, for any $n > N$ and $s \in D$, we see

$$|I(s) - I_n(s)| \leq \frac{n^{-\operatorname{Re} s}}{\operatorname{Re} s} < \frac{N^{-\sigma}}{\sigma} = \varepsilon,$$

which completes the proof. ■

Remark 1.35. Doing repeated integration by parts, one can extend the continuations above further to the left, but we will not do this. Instead, we will use a functional equation to continue to all \mathbb{C} in one fell swoop.

Corollary 1.36. Let $\chi_0 \pmod{q}$ denote the principal Dirichlet character. Then $L(s, \chi)$ has a meromorphic continuation to $\{s : \operatorname{Re} s > 0\}$. It is holomorphic everywhere except for a simple pole at $s = 1$.

Proof. Note that the function $\prod_{p|q} (1 - p^{-s})$ is entire and has its only zero at $s = 0$. Combining Lemma 1.33 and Proposition 1.34 completes the proof. ■

1.2.2 Reducing to $L(1, \chi)$

We now attack Theorem 1.1 directly. As in Theorem 1.6, we will want to understand $\log L(s, \chi)$.

Lemma 1.37. Let $\chi \pmod{q}$ be a Dirichlet character. For any s with $\operatorname{Re} s > 1$, we have

$$\log L(s, \chi) = \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} + E(s, \chi),$$

where $|E(s, \chi)| \leq 1$.

Proof. Fix s with $\operatorname{Re} s > 1$. Applying \log to the Euler product of Remark 1.28, we see

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

The $k = 1$ term of the right-hand sum is the main term present in the statement, so we need to bound the terms with $k > 1$. Thus, for $\operatorname{Re} s > 1$, we compute

$$\left| \sum_{p \text{ prime}} \left(\sum_{k=2}^{\infty} \frac{\chi(p)^k}{k p^{ks}} \right) \right| \leq \sum_{n=2}^{\infty} \left(\sum_{k=2}^{\infty} \frac{1}{n^k} \right) = \sum_{n=2}^{\infty} \frac{1/n^2}{1 - 1/n} = \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) = 1,$$

where we have telescoped in the last equality. This completes the proof. \blacksquare

As an aside, we note that Lemma 1.37 provides us with a relatively large zero-free region for $L(s, \chi)$.

Corollary 1.38. Let $\chi \pmod{q}$ be a Dirichlet character. For any s with $\operatorname{Re} s > 1$, we have $L(s, \chi) \neq 0$.

Proof. By Lemma 1.37, we see

$$|\log L(s, \chi)| \leq \sum_{p \text{ prime}} \left| \frac{\chi(p)}{p^s} \right| + 1 \leq \sum_{n=1}^{\infty} \frac{1}{n^{\operatorname{Re} s}} + 1,$$

which converges because $\operatorname{Re} s > 1$. Thus, $\log L(s, \chi)$ takes on a finite value for all s with $\operatorname{Re} s > 0$, which implies $L(s, \chi) \neq 0$. \blacksquare

We now see that we can use Lemma 1.37 and Corollary 1.24 to extract a particular congruence class.

Lemma 1.39. Let q be an integer. For brevity, set $G := (\mathbb{Z}/q\mathbb{Z})^\times$, and fix some $a \in G$. For any s with $\operatorname{Re} s > 1$, we have

$$\sum_{\substack{p \text{ prime} \\ p \equiv a \pmod{q}}} \frac{1}{p^s} = \frac{1}{\varphi(q)} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \log L(s, \chi) + E(s),$$

where $|E(s)| \leq 1$.

Proof. Corollary 1.24 tells us

$$1_{[a]}(p) = \frac{1}{\varphi(q)} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \chi(p),$$

so

$$\sum_{\substack{p \text{ prime} \\ p \equiv a \pmod{q}}} \frac{1}{p^s} = \frac{1}{\varphi(q)} \sum_{\chi \in \widehat{G}} \left(\overline{\chi(a)} \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} \right).$$

However, using the notation of Lemma 1.37, we see

$$\frac{1}{\varphi(q)} \sum_{\chi \in \widehat{G}} \left(\overline{\chi}(a) \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} \right) = \frac{1}{\varphi(q)} \sum_{\chi \in \widehat{G}} \overline{\chi}(a) \log L(s, \chi) + \frac{1}{\varphi(q)} \sum_{\chi \in \widehat{G}} \overline{\chi}(a) E(s, \chi).$$

Because $\#\widehat{G} = \#G = \varphi(q)$ by Proposition 1.16, we conclude that the right-hand error term has magnitude bounded by 1, which completes the proof. ■

We can now reduce Theorem 1.1 to analyzing $L(1, \chi)$.

Proposition 1.40. Let q be an integer. Suppose that $L(1, \chi) \neq 0$ for each non-principal Dirichlet character $\chi \pmod{q}$. Then, for all $a \in (\mathbb{Z}/q\mathbb{Z})^\times$, we have

$$\sum_{\substack{p \text{ prime} \\ p \equiv a \pmod{q}}} \frac{1}{p} = +\infty.$$

In particular, there are infinitely many primes $p \equiv a \pmod{q}$.

Proof. Note that $L(1, \chi)$ is at least a complex number for non-principal characters $\chi \pmod{q}$ by Proposition 1.31.

Let χ_0 denote the principal character. By Corollary 1.36, we see $L(s, \chi_0) \rightarrow +\infty$ as $s \rightarrow 1^+$: indeed, we know $L(s, \chi_0)$ must go to something in $\mathbb{R}_{\geq 0} \cup \{\infty\}$ because $L(s, \chi_0) \geq 1$ when $s > 1$ is real. But $L(s, \chi_0)$ cannot go to a finite value because then $L(s, \chi_0)$ would only have a removable singularity at $s = 1$.

Thus, we also have $\log L(s, \chi_0) \rightarrow +\infty$ as $s \rightarrow 1^+$. However, $\log L(s, \chi) \rightarrow \log L(1, \chi)$ as $s \rightarrow 1^+$ for non-principal characters χ , and by hypothesis, this is a finite limit. It follows that

$$\lim_{s \rightarrow 1^+} \frac{1}{\varphi(q)} \sum_{\chi \in \widehat{G}} \overline{\chi}(a) \log L(s, \chi) = +\infty,$$

so the result follows from Lemma 1.39. ■

So we want to understand $L(1, \chi)$ when χ is a non-principal character. By paying closer attention to the above proof, we can control most of our characters χ .

Lemma 1.41. Let q be an integer, and set $G := (\mathbb{Z}/q\mathbb{Z})^\times$ for brevity. For each Dirichlet character $\chi \pmod{q}$, let $v(\chi)$ denote the order of vanishing of $L(s, \chi)$ at $s = 1$. Then

$$\sum_{\chi \in \widehat{G}} v(\chi) \leq 0.$$

In other words, at most one non-principal character χ has $L(1, \chi) = 0$, in which case $L(s, \chi)$ has a simple zero at $s = 1$.

Proof. The idea here is that Lemma 1.39 has a certainly nonnegative sum on the left-hand side, so not too many of the $L(s, \chi)$ s on the right-hand side may be 0, for otherwise the right-hand side would go to $-\infty$.

We make a few quick remarks on $v(\chi)$. Note Corollary 1.36 implies $v(\chi_0) = -1$, where χ_0 is the principal character. Additionally, $v(\chi) \geq 0$ for all non-principal characters χ by Proposition 1.31, and $v(\chi)$ is finite because $L(s, \chi)$ is not constantly zero by Corollary 1.38.

Thus, for each character χ , we may write $L(s, \chi) = (s - 1)^{v(\chi)} L_0(s, \chi)$ for some function $L_0(s, \chi)$ holomorphic on $\{s : \operatorname{Re} s > 0\}$ with $L_0(1, \chi) \neq 0$. Setting up our application of Lemma 1.39, we see

$$\sum_{\chi \in \widehat{G}} \log L(s, \chi) = \left(\sum_{\chi \in \widehat{G}} v(\chi) \right) \log(s - 1) + \left(\sum_{\chi \in \widehat{G}} \log L_0(s, \chi) \right)$$

for $\operatorname{Re} s > 1$. However, we now plug into Lemma 1.39 with $a := 1$ so that $\overline{\chi(a)} = 1$ for all χ , giving

$$\sum_{\substack{p \text{ prime} \\ p \equiv 1 \pmod{q}}} \frac{1}{p^s} = \frac{1}{\varphi(q)} \left(\sum_{\chi \in \hat{G}} v(\chi) \right) \log(s-1) + \frac{1}{\varphi(q)} \left(\sum_{\chi \in \hat{G}} \log L_0(s, \chi) \right) + E(s)$$

for $\operatorname{Re} s > 0$. As $s \rightarrow 1^+$, the left-hand side remains nonnegative. On the right-hand side, the middle and right terms both remain finite, so the left term must also remain finite. However, $\log(s-1) \rightarrow -\infty$ as $s \rightarrow 1^+$, so we must have $\sum_{\chi} v(\chi) \leq 0$ to ensure this term is nonnegative.

We now show the last sentence. Indeed, we have

$$\sum_{\chi \in \hat{G} \setminus \{\chi_0\}} v(\chi) \leq -v(\chi_0) = 1,$$

so at most one $\chi \in \hat{G} \setminus \{\chi_0\}$ may have $v(\chi) > 0$, in which case χ has $v(\chi) = 1$. ■

For example, the above lemma lets us control “complex” characters.

Lemma 1.42. Let q be an integer. If $\chi \pmod{q}$ is a non-principal Dirichlet character with $\chi \neq \bar{\chi}$, then $L(1, \chi) \neq 0$.

Proof. If $L(1, \chi) = 0$, then we see

$$L(1, \bar{\chi}) = \lim_{s \rightarrow 1^+} \sum_{n=1}^{\infty} \frac{\bar{\chi}(n)}{n^s} = \overline{\lim_{s \rightarrow 1^+} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}} = \overline{L(s, \chi)} = 0.$$

But this grants two distinct characters χ and $\bar{\chi}$ with $L(1, \chi) = L(1, \bar{\chi}) = 0$, violating Lemma 1.41. ■

Thus, it remains to deal with the “real” non-principal characters χ with $\chi = \bar{\chi}$. This is genuinely difficult, so we will wait until next class for them.

BIBLIOGRAPHY

- [Dav80] Harold Davenport. *Multiplicative number theory*. eng. Second Edition. Vol. 74. Graduate Texts in Mathematics. New York, NY: Springer, 1980. ISBN: 9781475759297.
- [Dav05] Harold Davenport. *Analytic methods for Diophantine equations and Diophantine inequalities*. eng. 2nd ed. / this edition edited and prepared for publication by T, D. Browning. Cambridge mathematical library. Cambridge, UK ; Cambridge University Press, 2005. ISBN: 0521605830.
- [Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

LIST OF DEFINITIONS

character, [7](#)

Dirichlet L -function, [12](#)

Dirichlet character, [11](#)

dual group, [7](#)