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]

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 Primer on Infinite Primes

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 $\operatorname{Re} s > 1$. The following factorization is due to Euler.

Proposition 1.2. For $s \in \mathbb{C}$ such that $\operatorname{Re} s > 1$, we have

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

Proof. Roughly speaking, we use unique prime factorization in $\mathbb{Z}$, writing

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \prod_{p \text{ prime}} \sum_{k=1}^{\infty} \frac{1}{p^{-ks}} = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

which is what we wanted. Rigorously, one ought to bound the size of our primes to get the required convergence. ■

Remark 1.3. Note that

$$\lim_{s \to 1^+} \zeta(s) = +\infty,$$

so the factorization of Proposition 1.2 requires there to be infinitely many primes. In fact, by taking logarithms of the factorization, we can see $\sum_p \frac{1}{p} = +\infty$.

The proof of Theorem 1.1 more or less imitates the argument of Remark 1.3. 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.

1.1.3 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 1.4. 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 1.5. 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 $n = \prod_{p \mid n} p^{\nu_p(n)}$, there is an isomorphism of rings

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{p \mid n} \left(\mathbb{Z}/p^{\nu_p(n)}\right)$$

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 1.6 (dual group)**.** Let G be a group. Then the *dual group* is $G^* := \operatorname{Hom}(G, \mathbb{C}^\times)$, where the operation is pointwise. Its elements are called *characters*. Note there is a "trivial" character $1\colon G \to \mathbb{C}^\times$ sending $g \mapsto 1$, which is the identity. We might call 1 the *principal character*.

Remark 1.7. If G is a finite group, we note that any $\chi \in G^*$ and $g \in G$ has

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

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

It will be helpful to have the following notation.

Notation 1.8. We might write $e \colon \mathbb{C} \to \mathbb{C}$ for the function $e(z) := \exp(2\pi i z)$.

We now begin computing G^* for finite abelian groups.

Lemma 1.9. Suppose G and H are groups. Then $G^* \times H^* \cong (G \times H)^*$ by sending (χ_G, χ_H) to $(g,h) \mapsto \chi_G(g)\chi_H(g)$.

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

- Well-defined: given $(\chi_G, \chi_H) \in G^* \times H^*$, define $\varphi(\chi_G, \chi_H) \colon G \times H \to \mathbb{C}^\times$ by $\varphi(\chi_G, \chi_H) \colon (g,h) \mapsto \chi_G(g)\chi_H(h)$. 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

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

  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 $\chi \colon (G \times H) \to \mathbb{C}^\times$, 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 1.10. Suppose $G = \mathbb{Z}/n\mathbb{Z}$ for a positive integer n. Then $\chi_\bullet \colon \mathbb{Z}/n\mathbb{Z} \cong G^*$ by sending $[k]$ to the character $\chi_k \colon [\ell] \mapsto e(k\ell/n)$.

Proof. To begin, note $\chi_k \colon \mathbb{Z} \to \mathbb{C}^\times$ 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 $\chi_k \colon G \to \mathbb{C}^\times$.

We now note that $\chi_\bullet \colon \mathbb{Z} \to G^*$ 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 $\chi_\bullet$ produces a homomorphism $\chi_\bullet \colon \mathbb{Z}/n\mathbb{Z} \to G^*$.

It remains to show that $\chi_\bullet$ 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 $\chi \colon G \to \mathbb{C}^\times$, we note $\chi([1])^n = \chi([0]) = 1$, so $\chi([1])$ is an nth root of unity. Thus, there exists k such that $\chi([1]) = e(k/n) = \chi_k([1])$. Thus, for any $\ell \in \{0, 1, \ldots, n-1\}$, we see

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

  so $\chi = \chi_k$ follows. ■

Proposition 1.11. Let G be a finite abelian group. Then $G \cong G^*$.

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 1.9 and Lemma 1.10, we compute

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

which is what we wanted. ■

Proposition 1.11 might look like we now understand dual groups perfectly, but the isomorphism given there is non-canonical because the isomorphism of Lemma 1.10 is non-canonical. In other words, given some $g \in G$, there is in general no good way to produce character $\chi \in G^*$.

However, there is a natural map $G \to G^{**}$ which is an isomorphism.

Proposition 1.12. Fix a finite abelian group G. Define the map $\operatorname{ev}_\bullet \colon G \to G^{**}$ by sending $g \in G$ to the map $\operatorname{ev}_g \in G^{**}$ defined by $\operatorname{ev}_g \colon \chi \mapsto \chi(g)$. Then $\operatorname{ev}_\bullet$ is an isomorphism.

Proof. We begin by checking that $\operatorname{ev}_\bullet$ is a well-defined homomorphism. For each $g \in G$, we see $\operatorname{ev}_g \colon G^* \to \mathbb{C}^\times$ is a homomorphism because

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

Further, $\operatorname{ev}_\bullet$ is a homomorphism because

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

It remains to show that $\operatorname{ev}_\bullet$ is an isomorphism. We claim that $\operatorname{ev}_\bullet$ is injective, which will be enough because $|G| = |G^{**}|$ by Proposition 1.11.

For this, we appeal to the following lemma.

Lemma 1.13. Fix a finite abelian group G with identity e. If $g \neq e$, then there exists $\chi \in G^*$ 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 $\chi\left((g_i)_{i=1}^n\right) \neq 1$. Without loss of generality, suppose that $g_1 \neq 0$ and define χ by

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

Certainly $\chi\left((g_i)_{i=1}^n\right) = e(g_1/n_1) \neq 1$, so it remains to show that χ is a character. This technically follows from Lemma 1.9, but we can see it directly by computing

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

This completes the proof. ■

The proof now follows quickly from Lemma 1.13. By contraposition, we see that any $g \in G$ such that $\chi(g) = 1$ for all $\chi \in G^*$ and must have $g = e$. But this is exactly the statement that $\operatorname{ev}_\bullet \colon G \to G^{**}$ is injective. ■

1.1.4 Finite Fourier Analysis

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

Idea 1.14. We can write general functions $G \to \mathbb{C}$ as linear combinations of characters.

Remark 1.15. When G is not abelian, one must work with function $G \to \mathbb{C}$ which are "locally constant" on conjugacy classes of G.

Here is our Fourier transform.

Notation 1.16. Let G be a finite abelian group. Given a function $f \colon G \to \mathbb{C}$, we define $f^* \colon G^* \to \mathbb{C}$ by

$$f^*(\chi) \coloneqq \sum_{g \in G} f(g)\overline{\chi(g)}.$$

Recall $\overline{\chi(g)} = \chi\left(g^{-1}\right)$ by Remark 1.7.

To manifest Idea 1.14 properly, we need the following orthogonality relations.

Proposition 1.17. Let G be a finite abelian group.

- For any fixed $\chi \in G^*$, 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
$$\sum_{\chi\in G^*}\chi(g) = \begin{cases} 0 & \text{if } g \neq e, \\ \#G & \text{if } g = e. \end{cases}$$

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
$$\chi(g_0)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(g_0 g) \overset{*}{=} \sum_{g\in G}\chi(g),$$
so we must have $\sum_{g\in G}\chi(g) = 0$. Note that we have re-indexed the sum at $\overset{*}{=}$.

(b) If $g = e$, then the sum is $\sum_{\chi\in G^*}\chi(g) = \#(G^*)$, which is $\#G$ by Proposition 1.11.

Otherwise, $g \neq e$, so by Lemma 1.13, there exists χ_0 such that $\chi_0(g) \neq 1$. Employing the same trick, it follows
$$\chi_0 \sum_{\chi\in G^*}\chi(g) = \sum_{\chi\in G^*}(\chi_0\chi)(g) \overset{*}{=} \sum_{\chi\in G^*}\chi(g),$$
so we must have $\sum_{\chi\in G^*}\chi(g) = 0$. Again, we re-indexed at $\overset{*}{=}$. ■

Now here is our result.

Theorem 1.18 (Fourier inversion)**.** Let G be a finite abelian group. For any $f\colon G \to \mathbb{C}$, we have
$$f(g) = \frac{1}{\#G}\sum_{\chi\in G^*} f^*(\chi)\chi(g)$$
for any $g \in G$.

Proof. This is direct computation with Proposition 1.17. Indeed, for any $g_0 \in G$, we see
$$\sum_{\chi\in G^*} f^*(\chi)\chi(g_0) = \sum_{\chi\in G^*}\sum_{g\in G} f(g)\chi\left(g^{-1}\right)\chi(g_0) = \sum_{g\in G}\left(f(g)\sum_{\chi\in G^*}\chi\left(g^{-1}g_0\right)\right).$$
Now using Proposition 1.17, 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
$$\frac{1}{\#G}\sum_{\chi\in G^*} f^*(\chi)\chi(g_0) = f(g_0),$$
which is exactly what we wanted. ■

Here is our chief application.

Corollary 1.19. Let G be a finite abelian group. Fixing some $g_0 \in G$, we have

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

for any $g \in G$.

Proof. Note

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

because all terms except $g = g_0$ vanish. The result now follows from Theorem 1.18. ■

1.1.5 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 1.20 (Dirichlet character)**.** Let q be a nonzero integer. A *Dirichlet character* $\pmod q$ is a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ such that there exists a character $\widetilde{\chi}\colon (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ for which

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

We might write this situation as $\chi \pmod q$.

Remark 1.21. Note χ is periodic with period q.

We can finally define our generalization of ζ.

Definition 1.22 (Dirichlet L-function)**.** Fix a Dirichlet character $\chi \pmod q$. Then we define the *Dirichlet L-function* as

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

Note we have absolute convergence for $\operatorname{Re} s > 1$.

In fact, these definitions work for $\operatorname{Re} s > 0$, which we will talk about later.

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