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 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 $f \colon U \to \mathbb{C}$. Given holomorphic functions $f_n \colon U \to \mathbb{C}$ for each $n \in \mathbb{N}$, if $f_n \to f$ 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 $\gamma \colon [0,1] \to U$, we would like to show

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

Note $\operatorname{im}\gamma$ is compact, so $f_n \to f$ 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

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

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

Proposition 1.3. Let $f \colon \mathbb{N} \to \mathbb{C}$ 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 $|f(n)| \le Cn^\sigma$ for some $C > 0$. Thus, showing the absolute convergence is direct: note

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

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 $D_n \to D$ 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

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

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.

Definition 1.4 (multiplicative)**.** Let $f\colon \mathbb{N}\to\mathbb{C}$ be a function. Then f is *multiplicative* if and only if $f(nm)=f(n)f(m)$ for any $n,m\in\mathbb{N}$ such that $\gcd(n,m)=1$.

Proposition 1.5. Let $f\colon \mathbb{N}\to\mathbb{C}$ be a multiplicative function such that $|f(n)|=O\left(n^\sigma\right)$. For any $s\in\mathbb{C}$ such that $\operatorname{Re} s>\sigma+1$, we have

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

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

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

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

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

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

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

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

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

which now vanishes as $M\to\infty$ 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 $N\to\infty$ to finish the proof. For any $N>0$, we use the claim to note

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

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

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

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

Corollary 1.6. We have

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

Proof. By Proposition 1.5, 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 1.6 to give a proof of the infinitude of primes.

Theorem 1.7. 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

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

which goes to $+\infty$ as $s\to1^+$. In particular, $\log\zeta(s)\to+\infty$ as $s\to1^+$.

The last ingredient we need is to bound the Euler product of Corollary 1.6. In particular, we see

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

(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

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

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

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

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 $s\to1^+$, we see $\log\zeta(s)-S(s)\to+\infty$, so the theorem follows. ■

The proof of Theorem 1.1 more or less imitates the argument of Theorem 1.7. 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 1.8. 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 1.9. 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 1.10 (dual group)**.** Let G be a group. Then the *dual group* is $\widehat{G}:=\operatorname{Hom}(G,\mathbb{C}^\times)$, where the operation is pointwise. Its elements are called *characters*.

Notation 1.11 (principal character)**.** 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*; we might also denote 1 by χ_0.

Notation 1.12 (conjugate character)**.** If $\chi\colon G\to\mathbb{C}^\times$ is a character, then note that $\overline{\chi}\colon G\to\mathbb{C}^\times$ defined by $\overline{\chi}(g):=\overline{\chi(g)}$ is also a character. Indeed, conjugation is a field homomorphism.

Remark 1.13. If G is a finite group, we note that any $\chi\in\widehat{G}$ 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 1.14. We might write $e\colon\mathbb{C}\to\mathbb{C}$ for the function $e(z):=\exp(2\pi iz)$.

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

Lemma 1.15. Suppose G and H are groups. Then $\widehat{G}\times\widehat{H}\cong\widehat{G\times H}$ by sending (χ_G,χ_H) to $(g,h)\mapsto\chi_G(g)\chi_H(g)$.

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

- Well-defined: given $(\chi_G,\chi_H)\in\widehat{G}\times\widehat{H}$, 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 $\chi_G(g)\coloneqq\chi(g,e_H)$ and $\chi_H(h)\coloneqq\chi(e_G,h)$. 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 1.16. Suppose $G=\mathbb{Z}/n\mathbb{Z}$ for a positive integer n. Then $\chi_\bullet\colon\mathbb{Z}/n\mathbb{Z}\cong\widehat{G}$ 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 $\chi_\bullet\colon\mathbb{Z}\to\widehat{G}$ 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 $\chi_\bullet$ produces a homomorphism $\chi_\bullet\colon\mathbb{Z}/n\mathbb{Z}\to\widehat{G}$.

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

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 1.15 and Lemma 1.16, we compute

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

which is what we wanted. ■

Proposition 1.17 might look like we now understand dual groups perfectly, but the isomorphism given there is non-canonical because the isomorphism of Lemma 1.16 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 $G \to \widehat{\widehat{G}}$ which is an isomorphism.

Proposition 1.18. Fix a finite abelian group G. Define the map $\operatorname{ev}_\bullet \colon G \to \widehat{\widehat{G}}$ by sending $g \in G$ to the map $\operatorname{ev}_g \in \widehat{\widehat{G}}$ 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 $\operatorname{ev}_g \colon \widehat{G} \to \mathbb{C}^\times$ 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 $|G| = |\widehat{\widehat{G}}|$ by Proposition 1.17.

For this, we appeal to the following lemma.

Lemma 1.19. 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 $\chi\left((g_i)_{i=1}^n\right) \neq 1$. Without loss of generality, suppose that $g_1 \neq 0$ and define χ by

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

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 1.15, 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 1.19. 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 $\mathrm{ev}_\bullet \colon G \to \widehat{\widehat{G}}$ 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 1.20. We can write general functions $G \to \mathbb{C}$ as linear combinations of characters.

Remark 1.21. 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 1.22. Let G be a finite abelian group. Given a function $f \colon G \to \mathbb{C}$, we define $\widehat{f} \colon \widehat{G} \to \mathbb{C}$ by

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

Recall $\overline{\chi(g)} = \chi\left(g^{-1}\right)$ by Remark 1.13.

To manifest Idea 1.20 properly, we need the following orthogonality relations.

Proposition 1.23. 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

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

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 $\sum_{\chi \in \widehat{G}} \chi(g) = \#(\widehat{G})$, which is $\#G$ by Proposition 1.17.
Otherwise, $g \neq e$, so by Lemma 1.19, there exists χ_0 such that $\chi_0(g) \neq 1$. Employing the same trick, it follows

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

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

Now here is our result.

Theorem 1.24 (Fourier inversion)**.** Let G be a finite abelian group. For any $f\colon G \to \mathbb{C}$, we have

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

for any $g \in G$.

Proof. This is direct computation with Proposition 1.23. Indeed, for any $g_0 \in G$, we see

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

Now using Proposition 1.23, 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

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

which is exactly what we wanted. ■

Here is our chief application.

Corollary 1.25. 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

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

because all terms except $g = g_0$ vanish. The result now follows from Theorem 1.24. ■

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 1.26 (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 $\chi \pmod q$. The Dirichlet character corresponding to 1 is denoted χ_0 and still called the *principal character*.

Remark 1.27. Note χ is periodic with period q.

We can finally define our generalization of ζ.

Definition 1.28 (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 1.29. Continuing in the context of the definition, we note Proposition 1.5 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 1.30 (Abel summation)**.** Let $\{a_n\}_{n\in\mathbb{N}}$ be a sequence of complex numbers, and define the partial sums be given by

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

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

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

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

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

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

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

To finish, we see

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

which when combined with the previous equality finishes. ■

Remark 1.31. One can use the theory of Riemann–Stieltjes integration to turn Theorem 1.30 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 1.32. 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 $A(t) := \sum_{1\le n\le t} a_n$ have

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

for any $k \ge 0$, where in the last equality we have used Proposition 1.23. Thus, for any $t\ge 0$, find $k\in\mathbb{Z}$ such that $kq \le t < k(q+1)$, and we see

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

Now, finally using Theorem 1.30, we see

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

Because $\operatorname{Re} s > 1$, we see $|A(x)x^{-s}| \le qx^{-\operatorname{Re} s}$ goes to 0 as $x\to\infty$. 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

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

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 $I_N(s) \to I(s)$ as $N \to \infty$ 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 $I_n(s) \to I(s)$ uniformly on compact sets as $n \to \infty$. The main computation is to note that for each s with $\operatorname{Re} s > 0$ and n, we may upper-bound

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

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

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

which completes the proof. ■

Remark 1.33. Using the notions and notations of the above proof, we see that

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

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

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

Proof. By Remark 1.29, 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

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

by Corollary 1.6, which finishes. ■

Thus, we are interested in continuing ζ. With a little more effort than Proposition 1.32, 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 1.35. 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 $A(t) := \sum_{1 \le n \le t} a_n$ have $A(t) = \lfloor t \rfloor$, so Theorem 1.30 grants

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

Because $\operatorname{Re} s > 1$, we see $|\lfloor x \rfloor \cdot x^{-s}| \le x^{1-\operatorname{Re} s}$ goes to 0 as $x \to \infty$. 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

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

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 $I_N(s) \to I(s)$ as $N \to \infty$ 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 $I_n(s) \to I(s)$ uniformly on compact sets as $n \to \infty$. The main computation is to note that for each s with $\operatorname{Re} s > 0$ and n, we may upper-bound

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

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

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

which completes the proof. ■

Remark 1.36. Using the notions and notation of the above proof, we see that

$$|\zeta(s)| \le \frac{|s|}{|s-1|} + \left|s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,dt\right| \le \frac{|s|}{|s-1|} + \frac{|s|}{\operatorname{Re} s}.$$

For example, if $\operatorname{Re} s > 1$, then we get $|\zeta(s)| \le 1 + \frac{|s|}{\operatorname{Re} s} < |s| + 1$.

Remark 1.37. 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 1.38. 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 1.34 and Proposition 1.35 completes the proof. ■

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

We now attack Theorem 1.1 directly. As in Theorem 1.7, we will want to understand $\log L(s,\chi)$.

Lemma 1.39. 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 $|E(s,\chi)| \le 1$.

Proof. Fix s with $\operatorname{Re} s > 1$. Applying $\log$ to the Euler product of Remark 1.29, we see

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

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

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

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

As an aside, we note that Lemma 1.39 provides us with a relatively large zero-free region for $L(s,\chi)$.

Corollary 1.40. Let $\chi \pmod q$ be a Dirichlet character. For any s with $\operatorname{Re} s > 1$, we have $L(s,\chi) \ne 0$.

Proof. By Lemma 1.39, we see

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

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 $L(s,\chi) \ne 0$. ■

We now see that we can use Lemma 1.39 and Corollary 1.25 to extract a particular congruence class.

Lemma 1.41. 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 $|E(s)| \le 1$.

Proof. Corollary 1.25 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 1.39, 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 1.17, 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 1.42. 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 1.32.

Let χ_0 denote the principal character. By Corollary 1.38, we see $L(s,\chi_0)\to+\infty$ as $s\to 1^+$: 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 $\log L(s,\chi_0)\to+\infty$ as $s\to 1^+$. However, $\log L(s,\chi)\to\log L(1,\chi)$ as $s\to 1^+$ for non-principal characters χ, and by hypothesis, this is a finite limit. It follows that

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

so the result follows from Lemma 1.41. ■

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 1.43. 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 1.41 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 1.38 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 1.32, and $v(\chi)$ is finite because $L(s,\chi)$ is not constantly zero by Corollary 1.40.

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 1.41, 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 1.41 with $a := 1$ so that $\overline{\chi(a)} = 1$ for all χ, giving

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

for $\operatorname{Re} s > 0$. As $s \to 1^+$, 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, $\log(s-1) \to -\infty$ as $s \to 1^+$, so we must have $\sum_\chi v(\chi) \le 0$ to ensure this term is nonnegative.

We now show the last sentence. Indeed, we have

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

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

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

Lemma 1.44. Let q be an integer. If $\chi \pmod q$ is a non-principal Dirichlet character with $\chi \ne \overline{\chi}$, then $L(1,\chi) \ne 0$.

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

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

But this grants two distinct characters χ and $\overline{\chi}$ with $L(1,\chi) = L(1,\overline{\chi}) = 0$, violating Lemma 1.43. ■

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

1.3 January 23

Today we finish the proof of Theorem 1.1.

1.3.1 The Dirichlet Convolution

As motivation, we might be interested in the product of two Dirichlet series. Formally, we might write

$$\left(\sum_{k=1}^\infty \frac{a_k}{k^s}\right)\left(\sum_{\ell=1}^\infty \frac{b_\ell}{\ell^s}\right) = \sum_{k=1}^\infty\sum_{\ell=1}^\infty \frac{a_k b_\ell}{(k\ell)^s} = \sum_{n=1}^\infty\left(\sum_{k\ell=n} a_k b_\ell\right)\frac{1}{n^s}.$$

Of course, we will want to formalize this intuitive argument to give the corresponding series the correct analytic properties, but we have at least arrived at the correct definition.

Definition 1.45 (Dirichlet convolution)**.** Fix functions $f, g\colon \mathbb{N} \to \mathbb{C}$. Then the *Dirichlet convolution* $(f * g)\colon \mathbb{N} \to \mathbb{C}$ is defined by

$$(f*g)(n) := \sum_{k\ell=n} f(k)g(\ell) = \sum_{d\mid n} f(d)g(n/d).$$

And we may now take products of Dirichlet series.

Proposition 1.46. Fix functions $f, g\colon \mathbb{N} \to \mathbb{C}$ such that $|f(n)|, |g(n)| = O(n^\sigma)$ for some $\sigma \in \mathbb{R}$. Then define the series

$$F(s) := \sum_{n=1}^\infty \frac{f(n)}{n^s}, \qquad G(s) := \sum_{n=1}^\infty \frac{g(n)}{n^s}, \qquad D(s) := \sum_{n=1}^\infty \frac{(f*g)(n)}{n^s}.$$

Then D converges absolutely for $\operatorname{Re} s > \sigma + 1$, where it defines a holomorphic function given by $D(s) = F(s)G(s)$.

Proof. Fix s with $\operatorname{Re} s > \sigma + 1$. We show that $D(s)$ converges absolutely and yields $D(s) = F(s)G(s)$, from which it follows that $D(s)$ is holomorphic over the region by using Proposition 1.3 on F and G. Let $F_n(s)$, $G_n(s)$, and $D_n(s)$ denote the nth partial sums. Then we see

$$F_N(s)G_N(s) = \left(\sum_{k=1}^N \frac{f(k)}{k^s}\right)\left(\sum_{\ell=1}^N \frac{g(\ell)}{\ell^s}\right) = \underbrace{\sum_{n=1}^N \left(\sum_{k\ell=n} f(k)g(\ell)\right)\frac{1}{n^s}}_{D_N(s)} + \underbrace{\sum_{\substack{1\le k,\ell\le N\\ k\ell>N}} \frac{f(k)g(\ell)}{(k\ell)^s}}_{R_N(s):=}.$$

Thus, the key claim is that $R_N(s) \to 0$ as $N \to \infty$. The main point is that $k\ell > N$ requires $k > \sqrt{N}$ or $\ell > \sqrt{N}$, so

$$|R_N(s)| \le \sum_{\substack{1\le k,\ell\le N\\ k\ell>N}} \frac{|f(k)|\cdot|g(\ell)|}{(k\ell)^{\operatorname{Re} s}} \le \left(\sum_{k>\sqrt{N}} \frac{|f(k)|}{k^{\operatorname{Re} s}}\right)\left(\sum_{\ell\ge1} \frac{|g(\ell)|}{\ell^{\operatorname{Re} s}}\right) + \left(\sum_{k\ge1} \frac{|f(k)|}{k^{\operatorname{Re} s}}\right)\left(\sum_{\ell>\sqrt{N}} \frac{|g(\ell)|}{\ell^{\operatorname{Re} s}}\right).$$

The absolute convergence of F and G at s now causes the right-hand side to be

$$\left(\sum_{k=1}^\infty \frac{|f(k)|}{k^{\operatorname{Re} s}}\right)\cdot 0 + 0 \cdot \left(\sum_{\ell=1}^\infty \frac{|g(\ell)|}{\ell^{\operatorname{Re} s}}\right) = 0$$

as $N \to \infty$, so we conclude $R_N(s) \to 0$ as $N \to \infty$. Thus, we conclude

$$F(s)G(s) = \lim_{N\to\infty} (F_N(s)G_N(s)) = \lim_{N\to\infty} D_N(s) + \lim_{N\to\infty} R_N(s) = D(s).$$

Lastly, we need to show that $D(s)$ actually converges absolutely. Well, we note that we can replace f with $|f|$ and g with $|g|$ and s with $\operatorname{Re} s$ everywhere in the above bounding to show that

$$\sum_{n=1}^\infty \left|\frac{(f*g)(n)}{n^s}\right| \le \sum_{n=1}^\infty \frac{(|f|*|g|)(n)}{n^{\operatorname{Re} s}} = \left(\sum_{k=1}^\infty \frac{|f(k)|}{k^{\operatorname{Re} s}}\right)\left(\sum_{\ell=1}^\infty \frac{|g(\ell)|}{\ell^{\operatorname{Re} s}}\right),$$

and the right-hand side converges because $F(s)$ and $G(s)$ converge absolutely. Thus, $D(s)$ converges absolutely. ■

Example 1.47. Let $d(n)$ denote the number of divisors of n. Then we see

$$\zeta(s)^2 = \sum_{n=1}^\infty \frac{(1*1)(n)}{n^s} = \sum_{n=1}^\infty \frac{d(n)}{n^s}.$$

Here, $1\colon \mathbb{N} \to \mathbb{C}$ is the function which constantly returns 1.

We might be interested in an Euler product factorization for a product of two Dirichlet series (as in Proposition 1.5), but this notably requires the relevant functions to be multiplicative. Thus, we now show that the Dirichlet convolution sends multiplicative functions to multiplicative functions.

Lemma 1.48. Let $f, g\colon \mathbb{N} \to \mathbb{C}$ be multiplicative functions. Then $(f * g)\colon \mathbb{N} \to \mathbb{C}$ is still multiplicative.

Proof. Let n and m be coprime positive integers. We must show $(f*g)(nm) = (f*g)(n)\cdot(f*g)(m)$. The key point is that there is a bijection between divisors $d \mid nm$ and pairs of divisors $d_n \mid n$ and $d_m \mid m$ by sending (d_n, d_m) to d. We quickly show formally that this is a bijection.

- Well-defined: certainly $d_n \mid n$ and $d_m \mid m$ implies $d_nd_m \mid nm$.
- Injective: suppose $d_nd_m = d_n'd_m'$ for $d_n, d_n' \mid n$ and $d_m, d_m' \mid m$. We show $d_n = d_n'$, and $d_m = d_m'$ follows by symmetry. Well, for each $p \mid n$, we see $p \nmid m$ because $\gcd(n,m) = 1$, so $p \nmid d_m, d_m'$ as well, meaning

  $$\nu_p(d_n) = \nu_p(d_nd_m) = \nu_p(d_n'd_m') = \nu_p(d_n')$$

  for all $p \mid n$. However, $p \mid d_n, d_n'$ implies $p \mid n$, so we see that the prime factorizations of d_n and d_n' are the same, so $d_n = d_n'$.
- Surjective: for each $d \mid nm$, define $d_n := \gcd(d,n)$ and $d_m := \gcd(d,m)$. Certainly $d_n \mid n$ and $d_m \mid m$, so it remains to show $d = d_nd_m$. Well, for each $p \mid n$, we see $\nu_p(d_n) = \nu_p(d)$ because $d \mid n$; and similarly, each $p \mid m$ has $\nu_p(d_m) = \nu_p(m)$. Because each prime $p \mid nm$ divides exactly one of n or m, we see that

  $$\nu_p(d_nd_m) = \nu_p(d_n) + \nu_p(d_m) = \nu_p(d)$$

  by doing casework on $p \mid n$ or $p \mid m$.

We have written down all of this so that we may compute

$$\begin{aligned}(f*g)(nm) &= \sum_{d\mid nm} f(d)g(nm/d)\\ &= \sum_{d_n\mid n}\sum_{d_m\mid m} f(d_nd_m)g\left(\frac{n}{d_n}\cdot\frac{m}{d_m}\right)\\ &\overset{*}{=} \left(\sum_{d_n\mid n} f(d_n)g(n/d_n)\right)\left(\sum_{d_m\mid m} f(d_m)g(m/d_m)\right)\\ &= (f*g)(n)\cdot(f*g)(m).\end{aligned}$$

Here, we have used the multiplicativity at $\overset{*}{=}$, noting that $d_n \mid n$ and $d_m \mid m$ implies $\gcd(d_n, d_m) = 1$ because $\gcd(n,m) = 1$. ■

1.3.2 The Mellin Transform

In this subsection, we pick up a few facts about the Mellin transform. Roughly speaking, we are doing Fourier analysis on the group $\mathbb{R}^+$ whose operation is multiplication. As such, the Haar measure is dx/x: for any Borel set $S \subseteq \mathbb{R}^+$ and $a \in \mathbb{R}^+$, we see

$$\int_{aS}\frac{dx}{x} = \int_S \frac{d(ax)}{ax} = \int_S \frac{a}{a}\cdot\frac{dx}{x} = \int_S\frac{dx}{x},$$

so dx/x is in fact a translation-invariant measure on $\mathbb{R}^+$. Anyway, here is our definition of the Mellin transform.

Definition 1.49 (rapidly decaying)**.** A function $\varphi\colon \mathbb{R}_{\ge 0} \to \mathbb{C}$ is *rapidly decaying* at 0 and ∞ if and only if $x^A \cdot \varphi(x)$ is bounded for all $A \in \mathbb{R}$.

Definition 1.50 (Mellin transform)**.** Let $\varphi\colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ be a continuous function rapidly decaying at 0 and ∞. Then the *Mellin transform* is the function $\mathcal{M}\varphi\colon \mathbb{C} \to \mathbb{C}$ given by

$$(\mathcal{M}\varphi)(s) := \int_0^\infty \varphi(x)x^s \,\frac{dx}{x}.$$

We quickly check that the integral converges for any $s \in \mathbb{C}$. Indeed, fixing $A, B > 0$, we show that $\mathcal{M}\varphi$ converges for $-A < \operatorname{Re} s < B$. Find constants C_A and C_B such that $\varphi(x) \leq x^A C_A$ and $\varphi(x) \leq x^{-B}C_B$. Now, it suffices to show that the integral absolutely converges, so upon setting $\sigma := \operatorname{Re} s$, we are showing

$$\int_0^\infty \varphi(x)x^\sigma \,\frac{dx}{x}$$

converges. Now, we split this integral into

$$\int_0^1 \varphi(x)x^{\sigma-1}\,dx + \int_1^\infty \varphi(x)x^{\sigma-1}\,dx \leq C_A\int_0^1 x^{A+\sigma-1}\,dx + C_B\int_1^\infty x^{-B+\sigma-1}\,dx,$$

both of which converge because $A+\sigma-1 > -1$ and $-B+\sigma-1 < -1$.

We will need two key properties of the Mellin transform, which we will not prove because they would take us too far afield.

Proposition 1.51. Let $\varphi\colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ be a continuous function rapidly decaying at 0 and ∞. Then $\mathcal{M}\varphi$ is entire. In fact, for any real number A and $a < b$, the set

$$\left\{|t|^A\mathcal{M}\varphi(\sigma+it) : \sigma \in [a,b], t \in \mathbb{R}\right\}$$

is bounded.

Proof. Omitted. ■

Theorem 1.52. Let $\varphi\colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ be a continuous function rapidly decaying at 0 and ∞. For any $\sigma \in \mathbb{R}$, we have

$$\varphi(x) = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} (\mathcal{M}\varphi)(s)x^{-s}\,ds.$$

Proof. Omitted. ■

1.3.3 Finishing Dirichlet's Theorem

We finish the proof of Theorem 1.1. By Proposition 1.42 and Lemma 1.44, we have left to show $L(1,\chi) \neq 0$ for real characters χ. We provide a slick proof of this result.

Lemma 1.53. Let $\chi \pmod q$ be a "real" non-principal Dirichlet character, meaning $\chi = \overline{\chi}$. We show

Proof. We combine two techniques called "positivity" and "smoothing." The main point is that $L(1,\chi) = 0$ implies that the zero of $L(s,\chi)$ at $s = 1$ is able to cancel the pole of $\zeta(s)$ as $s = 1$, implying that the function $\zeta(s)L(s,\chi)$ is holomorphic on $\{s : \operatorname{Re} s > 0\}$ by combining Propositions 1.32 and 1.35.

Anyway, we divide the proof in three steps.

1. Let's begin with our positivity result. Because we are interested in $\zeta(s)L(s,\chi)$, we will want to study the coefficients of this Dirichlet series, which are given by $(1*\chi)$ by Proposition 1.46. Note $(1*\chi)$ is multiplicative by Lemma 1.48.

   To set up our bounding, we claim that $(1*\chi)(n) \ge 0$ for all $n \in \mathbb{N}$, and $(1*\chi)\left(n^2\right) \ge 1$. Because $(1*\chi)$ is multiplicative, we may write

$$(1*\chi)(n) = (1*\chi)\left(\prod_{p\mid n} p^{\nu_p(n)}\right) = \prod_{p\mid n}(1*\chi)\left(p^{\nu_p(n)}\right).$$

   Thus, it suffices to show $(1*\chi)\left(p^k\right) \ge 0$ for each prime-power p^k, and $(1*\chi)\left(p^k\right) \ge 1$ when k is even. Well, we can compute this directly as

$$(1*\chi)\left(p^k\right) = \sum_{d\mid p^k}\chi(d) = \sum_{\nu=0}^{k}\chi\left(p^\nu\right) = \sum_{\nu=0}^{k}\chi(p)^\nu.$$

   Now, $\chi(p) = \overline{\chi(p)}$ by hypothesis on χ, so because $|\chi(p)| = 1$ by Remark 1.13, we conclude $\chi(p) \in \{\pm 1\}$. Thus, on one hand, if $\chi(p) = 1$, then $(1*\chi)\left(p^\nu\right) = \nu + 1 \ge 1$ always. On the other hand, if $\chi(p) = -1$, then $(1*\chi)\left(p^\nu\right)$ is 1 when ν is even and 0 if ν is odd. The claim follows.

   To finish, our positivity claim is that

$$\sum_{x<n\le 2x}(1*\chi)(n) \ge \sum_{x<n^2\le 2x}(1*\chi)\left(n^2\right) \ge \sum_{\sqrt{x}<n\le\sqrt{2x}} 1 = \left\lfloor\sqrt{2x}\right\rfloor - \left\lfloor\sqrt{x}\right\rfloor \ge (\sqrt{2}-1)\sqrt{x} - 2.$$

   Thus, for x large enough, we see

$$\sum_{x<n\le 2x}(1*\chi)(n) \ge \frac{1}{3}\sqrt{x}.$$

2. We now apply smoothing Let $\psi\colon (0,\infty) \to [0,\infty)$ be a continuous function with support contained in $[0.9, 2.1]$ such that $\psi(x) = 1$ for $x \in [1,2]$. Then one sees

$$\sum_{n=1}^{\infty}\psi(n/x)(1*\chi)(m) \ge \sum_{x<n\le 2x}(1*\chi)(n) \ge \frac{1}{3}\sqrt{x}.$$

   Note that this sum is finite because only finitely many n have $n/x \le 2.1$.

   We now use the Mellin transform $\mathcal{M}\varphi$. Indeed, note that φ is rapidly decaying at 0 and ∞ because φ actually vanishes for $x < 0.9$ and $x > 2.1$. Now, we use Theorem 1.52 to compute

$$\sum_{n=1}^{\infty}\psi(n/x)(1*\chi)(n) = \frac{1}{2\pi i}\sum_{n=1}^{\infty}\int_{2-i\infty}^{2+i\infty}\left((\mathcal{M}\varphi)(s)x^s \cdot \frac{(1*\chi)(n)}{n^s}\right)ds.$$

   Thus, we see that we would like to exchange the integral and the sum so that we can sum over $(1*\chi)$ to finally make $\zeta(s)L(s,\chi)$ appear. It suffices to show that this iterated "integral" absolutely converges, so for any $\sigma > 0$, we may compute

$$I_\sigma(x) := \int_{\sigma-i\infty}^{\sigma+i\infty}\sum_{n=1}^{\infty}\left|(\mathcal{M}\varphi)(s)x^s \cdot \frac{(1*\chi)(n)}{n^s}\right|ds = \int_{\sigma-i\infty}^{\sigma+i\infty}\left|(\mathcal{M}\varphi)(s)x^s \cdot \zeta(s)L(s,\chi)\right|ds$$

   by Proposition 1.46. To bound this, we see $|x^s| \le x^{\operatorname{Re} s} = x^\sigma$ and

$$|\zeta(s)L(s,\chi)| \le q \cdot \frac{|s|}{\sigma} \cdot |s|\left(\frac{1}{|1-\sigma|} + \frac{1}{\sigma}\right) = C_0(q,\sigma)|s|^2$$

by Remarks 1.33 and 1.36, where $C_0(q,\sigma)$ is some constant. Thus,

$$I_\sigma(x) \le C_0(q,\sigma)x^c \int_{\sigma-i\infty}^{\sigma+i\infty} (|(\mathcal{M}\varphi)(s)| \left(\sigma^2 + (\operatorname{Im} s)^2\right) \, ds.$$

However, by Proposition 1.51, there is C such that $|(\mathcal{M}\varphi)(s)| \le C(\operatorname{Im} s)^{-4}$, so we bound

$$\begin{aligned}\frac{I(x)}{C_0(q,\sigma)x^c} \le C\left(\int_{\sigma-i\infty}^{\sigma-i} \frac{\left(\sigma^2+(\operatorname{Im} s)^2\right)}{(\operatorname{Im} s)^4}\,ds\right) + C\left(\int_{\sigma+i}^{\sigma+i\infty} \frac{\left(\sigma^2+(\operatorname{Im} s)^2\right)}{(\operatorname{Im} s)^4}\,ds\right)\\ + \left(\int_{\sigma-i}^{2+i} (|(\mathcal{M}\varphi)(s)| \left(\sigma^2 + (\operatorname{Im} s)^2\right)\,ds\right).\end{aligned}$$

The integrals on the top row are finite by direct computation (they are improper integrals avoiding 0 of decaying on the order of x^{-2} or faster), and the bottom integral is finite because it is a finite integral of a continuous function. We conclude that $I(x)$ converges, so we have absolute convergence.

In fact, the entire right-hand side of the above bound is merely some function of σ, so we have actually shown that

$$\int_{\sigma-i\infty}^{\sigma+i\infty} |(\mathcal{M}\varphi)(s)x^s \cdot \zeta(s)L(s,\chi)|\,ds \le C(q,\sigma)x^c \tag{1.1}$$

for some constant $C(q,\sigma)$.

3. Anyway, we now know we can write

$$\frac{1}{3}\sqrt{x} \le \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \underbrace{(\mathcal{M}\varphi)(s)x^s\zeta(s)L(s,\chi)}_{D(s)}\,ds$$

by exchanging the sum and the integral and using Proposition 1.46. In order to use (1.1), we would like to push the vertical line left from $\operatorname{Re} s = 2$ to $\operatorname{Re} s = 1/3$ (for example).

We will be allowed to do this by Cauchy's theorem because the function $D(s) = (\mathcal{M}\varphi)(s)x^s\zeta(s)L(s,\chi)$ is holomorphic on $\{s : \operatorname{Re} s > 0\}$. Indeed, the only possible pole among these functions is the pole of order 1 at $s = 1$ for $\zeta(s)$, but $L(s,\chi)$ has a zero there by assumption and thus cancels this out!

We now apply Cauchy's theorem. For any $T > 0$, we see

$$\left|\int_{1/3-iT}^{1/3+iT} D(s)\,ds - \int_{2-iT}^{2+iT} D(s)\,ds\right| \le \int_{1/3+iT}^{2+iT} |D(s)|\,ds + \int_{1/3-iT}^{2-iT} |D(s)|\,ds.$$

We would like to show that this right-hand side vanishes as $T \to \infty$. Because the length of each of these paths is finite, it suffices to show that $|D(s)|$ vanishes as $\operatorname{Im} s \to \infty$ on these paths. Well, utilizing our bounds from before, we see

$$|D(s)| \le |(\mathcal{M}\varphi)(s)| \cdot x^2 \cdot C_0(q,\sigma)\left(4 + (\operatorname{Im} s)^2\right).$$

Because $(\mathcal{M}\varphi)(s)$ is rapidly decaying as $\operatorname{Im} s \to \infty$ (recall Proposition 1.51), we see that this indeed goes to 0 as $\operatorname{Im} s \to \infty$.

In total, we see

$$\frac{1}{3}\sqrt{x} \le \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} D(s)\,ds = \frac{1}{2\pi i}\int_{1/3-i\infty}^{1/3+i\infty} D(s)\,ds \le C(q,1/3)x^{1/3},$$

where we have used (1.1) at the end. However, for x large enough, this is impossible: $x^{1/2-1/3} \to \infty$ as $x \to \infty$. So we have hit our contradiction. ■

Remark 1.54. The product $L(s,\chi)\zeta(s)$ is the Dedekind ζ-function associated to a real quadratic field.

1.3.4 A Little on Quadratic Forms

To say something in the direction of Dirichlet's class number formula, we discuss quadratic forms. In particular, we will discuss the reduction theory, which shows that there are finitely many classes of binary quadratic forms of given discriminant.

Definition 1.55 (binary quadratic form)**.** A *binary quadratic form* is a function $f\colon \mathbb{Z}^2 \to \mathbb{Z}$ where $f(x,y) := ax^2 + bxy + cy^2$ where $a,b,c \in \mathbb{Z}$. If $\gcd(a,b,c) = 1$, then we call the quadratic form *primitive*.

It is a problem of classical interest to determine when a quadratic form achieves a particular integer.

It is another problem of classical interest to count the number of binary quadratic forms. However, some binary quadratic forms are "the same," in the sense that they are just a variable change away.

Example 1.56. The quadratic forms $x_1^2 + x_2^2$ and $y_1^2 + 2y_1y_2 + 2y_2^2$ are roughly the same by the change of variables given by

$$(y_1, y_2) = (x_1 - x_2, x_2).$$

To define this correctly, we define a group action on the set of quadratic forms.

Lemma 1.57. Let $\mathcal{Q}$ be the set of binary quadratic forms. Then $\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms by

$$(\gamma \cdot f) := f \circ \gamma^{-1},$$

where $f \in \mathcal{Q}$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Proof. We have the following checks.

- Identity: note $(\mathrm{id} \cdot f) = f \circ \mathrm{id}^{-1} = f \circ \mathrm{id} = f$.
- Composition: note $((\gamma\gamma') \cdot f) = f \circ (\gamma\gamma')^{-1} = f \circ (\gamma')^{-1} \circ \gamma^{-1} = \gamma \cdot (\gamma' \cdot f)$. ■

Definition 1.58 (equivalent)**.** Two binary quadratic forms $f_1, f_2\colon \mathbb{Z}^2 \to \mathbb{Z}$ are *equivalent* if and only if f_1 and f_2 live in the same orbit under the $\mathrm{SL}_2(\mathbb{Z})$-action. In other words, f_1 and f_2 are equivalent if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$f_1 = f_2 \circ \gamma.$$

Note that this is in fact an equivalence relation because the orbits of a group action form a partition.

Remark 1.59. For a binary quadratic form $f(x,y) := ax^2 + bxy + cy^2$, note that

$$f(v) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \underbrace{\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}}_{M:=} \begin{bmatrix} x \\ y \end{bmatrix} = v^\intercal M v$$

for any $v = (x,y) \in \mathbb{Z}^2$. In fact, this symmetric matrix M is unique to f: if $v^\intercal M v = v^\intercal M' v$ for all $v = (x,y) \in \mathbb{Z}^2$, then writing $M = (a_{ij})$ and $M' = (a'_{ij})$, we see

$$a_{11}x^2 + 2a_{12}xy + a_{22}^2 = v^\intercal M v = v^\intercal M' v = a'_{11}x^2 + 2a'_{12}xy + a'_{22}y^2.$$

Plugging in $(x,y) \in \{(1,0),(0,1),(1,1)\}$ shows $M = M'$.

Remark 1.60. Associate a binary quadratic form f the matrix M as in Remark 1.59. Thus, for any $\gamma \in \operatorname{SL}_2(\mathbb{Z})$,

$$(\gamma \cdot f)(v) = f\left(\gamma^{-1}v\right) = \left(\gamma^{-1}v\right)^\intercal M\gamma^{-1}v = v^\intercal\left(\gamma^{-\intercal}M\gamma^{-1}\right)v,$$

so we can associate $\gamma \cdot f$ to the matrix $\gamma^{-\intercal}M\gamma^{-1}$. (Notably, this is still a symmetric matrix!) This allows for relatively easy computation of $\gamma \cdot f$.

So we would like to count the number of quadratic forms, up to equivalence. However, we will soon see that there are still infinitely many of equivalence classes, so we will want some stronger invariant to distinguish between them.

Definition 1.61 (discriminant)**.** The *discriminant* of the binary quadratic form $f(x,y) := ax^2 + bxy + cy^2$ is given by $\operatorname{disc} f := b^2 - 4ac$. The number of equivalence classes of quadratic forms of discriminant d is notated by $h(-d)$.

Remark 1.62. By definition, note that the discriminant of the binary quadratic form f is $4\det M$, where M is the matrix associated to f as in Remark 1.59. Using Remark 1.60, we see that the discriminant of $\gamma \cdot f$ is thus

$$4\det\left(\gamma^{-\intercal}\right)\det(M)\det\left(\gamma^{-1}\right) = 4\det M$$

for any $\gamma \in \operatorname{SL}_2(\mathbb{Z})$.

Remark 1.62 shows that the discriminant is invariant to equivalence class. Thus, for example, for each $d \in \mathbb{Z}$, we set

$$f_d(x,y) := dxy$$

so that $\operatorname{disc} f = d^2$. Now letting d vary of $\mathbb{Z}$, we see that there are infinitely many equivalence classes of quadratic forms.

But once we bound our discriminant, there will be finitely many quadratic forms. Here is our goal.

Theorem 1.63. Let $d < 0$ be an integer. Then $h(d)$ is finite.

Remark 1.64. It is also true that $h(d)$ is finite when $d \geq 0$, but we will not show it here.

1.3.5 The Upper-Half Plane

To show Theorem 1.63, we will want to relate the action of $\operatorname{SL}_2(\mathbb{Z})$ on quadratic forms with the action of $\operatorname{SL}_2(\mathbb{R})$ on $\mathbb{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z := \frac{az+b}{cz+d}.$$

Here are some checks on this action.

Lemma 1.65. Let $\mathbb{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ denote the upper-half plane.

(a) The group $\operatorname{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z := \frac{az+b}{cz+d}.$$

(b) The orbit of $i \in \mathbb{H}$ under $\operatorname{SL}_2(\mathbb{R})$ is all of $\mathbb{H}$.

(c) The stabilizer of $i \in \mathbb{H}$ is $\operatorname{SO}_2(\mathbb{R})$, the group of rotations.

Proof. We show the parts one at a time.

(a) To begin, we show that the action is well-defined: given z with $z \in \mathbb{H}$, we need to show that $\gamma \cdot z \in \mathbb{H}$ for any $\gamma \in \mathrm{SL}_2(\mathbb{R})$. Well, giving coefficients to γ, we compute

$$\gamma \cdot z = \begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az+b}{cz+d} = \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{\big(ac|z|^2+bd\big)+(adz+bc\overline{z})}{|cz+d|^2}.$$

To check $\gamma \cdot z \in \mathbb{H}$, we must check that the imaginary part here is positive. Well, we see

$$\operatorname{Im}(\gamma \cdot z) = \frac{(ad-bc)\operatorname{Im}(z)}{|cz+d|^2} = \frac{\operatorname{Im}(z)}{|cz+d|^2},$$

where the last equality is because $\det \gamma = 1$.

We now run our checks to have a group action.

- Identity: we compute
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} z = \frac{z+0}{0+1} = z.$$
- Composition: we compute
$$\begin{aligned}
\begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} z \right) &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{a'z+b'}{c'z+d'} \\
&= \frac{a \cdot \frac{a'z+b'}{c'z+d'} + b}{c \cdot \frac{a'z+b'}{c'z+d'} + d} \\
&= \frac{a(a'z+b')+b(c'z+d')}{c(a'z+b')+d(c'z+d')} \\
&= \frac{(aa'+bc')z+(ab'+bd')}{(ca'+dc')z+(cb'+dd')} \\
&= \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix} z \\
&= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \right) z.
\end{aligned}$$

(b) Giving coefficients to some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we use the computation in (a) to see

$$\gamma \cdot i = \begin{bmatrix} a & b \\ c & d \end{bmatrix} i = \frac{\big(ac|i|^2+bd\big)+(adi+bc\overline{i})}{|ci+d|^2} = \frac{(ac+bd)+(ad-bc)i}{c^2+d^2} = \frac{(ac+bd)+i}{c^2+d^2}.$$

Thus, for any $a+bi \in \mathbb{H}$, we see

$$\begin{bmatrix} \sqrt{b} & a/\sqrt{b} \\ 0 & 1/\sqrt{b} \end{bmatrix} i = \frac{a/b+i}{1/b} = a+bi,$$

so the orbit of i is indeed all of $\mathbb{H}$.

(c) Using the computation of (b), we see that $\gamma \cdot i = i$ if and only if the usual coefficients of γ have $ac+bd=0$ and $c^2+d^2=1$. Thus, we see that any $\theta \in [0, 2\pi)$ will give

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} i = i$$

because $(\cos\theta)(\sin\theta)+(\cos\theta)(-\sin\theta)=0$ and $(\cos\theta)^2+(\sin\theta)^2=1$. It follows that $\mathrm{SO}_2(\mathbb{R})$ is certainly contained in the stabilizer of i.

Conversely, suppose γ stabilizes i and has the usual coefficients. Note that the pair (c,d) with $c^2+d^2=1$ has a unique $\theta \in [0, 2\pi)$ such that $c = \sin\theta$ and $d = \cos\theta$. To solve for a and b, we divide our work in two cases.

- If $c \neq 0$, then we see $a = -bd/c$. Further, $ad - bc = 1$, so we see $-bd^2/c - bc = 1$, which gives
$$b = -\frac{1}{d^2/c + c} = -\frac{c}{c^2 + d^2} = -c = -\sin\theta.$$
Thus, we see $a = -bd/c = d = \cos\theta$. Plugging everything in, we see $\gamma \in \mathrm{SO}_2(\mathbb{R})$.
- If $c = 0$, then $d \neq 0$, so we see $b = -ac/d$. Thus, $ad - bc = 1$, so we see $ad + ac^2/d = 1$, which gives
$$a = \frac{1}{d + c/d} = \frac{d}{c^2 + d^2} = d = \cos\theta.$$
Thus, we see $b = -ac/d = -c = -\sin\theta$. Plugging everything in, we again see $\gamma \in \mathrm{SO}_2(\mathbb{R})$.

The above cases complete the proof. ■

Remark 1.66. Parts (b) and (c) of Lemma 1.65 roughly show
$$\frac{\mathrm{SL}_2(\mathbb{R})}{\mathrm{SO}_2(\mathbb{R})} \cong \mathbb{H}.$$

Next class we will discuss how to build a fundamental domain for the induced action of $\mathrm{SL}_2(\mathbb{Z}) \subseteq \mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$.

1.4 January 25

Today we continue discussing quadratic forms.

1.4.1 A Fundamental Domain

Recall from Remark 1.66 that
$$\frac{\mathrm{SL}_2(\mathbb{Z})}{\mathrm{SO}_2(\mathbb{R})} \cong \mathbb{H}.$$
Now, $\mathrm{SL}_2(\mathbb{Z}) \subseteq \mathrm{SL}_2(\mathbb{R})$ has a natural action on $\mathbb{H}$; this is a "discrete subgroup," so one might say that the action is discrete. (Concretely, we can see that the orbit of any $z \in \mathbb{H}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$ is a discrete set.) We will be interested in a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. Here is an example.

Proposition 1.67. Define the subset
$$D := \{z \in \mathbb{H} : |z| > 1, -1/2 \le \operatorname{Re} z < 1/2\} \cup \{z \in \mathbb{H} : |z| = 1, -1/2 \le \operatorname{Re} z \le 0\}.$$
Then D is a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. In other words, for each $z \in \mathbb{H}$, there exists a unique $z_0 \in \mathbb{H}$ such that there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $z = \gamma \cdot z_0$.

Proof. Omitted. Roughly speaking, one has to show that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the elements
$$S := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \text{and} \qquad T := \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}.$$
Then one can use T to push all elements of $\mathbb{H}$ to $\{z \in \mathbb{H} : -1 \le \operatorname{Re} z < 1\}$ and use S to push what's left over to S. We refer to [Ser12] for details. ■

1.4.2 Gauss Reduced Forms

We now use Proposition 1.67 for fun and profit.

> **Theorem 1.63.** Let $d<0$ be an integer. Then $h(d)$ is finite.

Proof. Roughly speaking, a quadratic form $f(x,y):=ax^2+bxy+cz^2$ where $a,c>0$ without loss of generality, we can study $f(x,1)$ to have a root

$$z_f:=\frac{-b+\sqrt{b^2-4ac}}{2a}=\frac{-b+\sqrt{d}}{2a}.$$

Now, in our case of interest, we have $d<0$, so this describes an element of $\mathbb{H}$. (There is also a negative root, but we focus on z_f.) In fact, one can check that $z_{\gamma f}=\gamma z_f$, which is how we relate quadratic forms to $\mathbb{H}$.

In fact, by Proposition 1.67, we know there is some γf such that $z_{\gamma f}\in D$. The point here is that the number of quadratic forms up to equivalence is bounded above by the number of points in D with imaginary part $\sqrt{|d|}$. For example, the condition $|z_f|\ge 1$ implies that

$$\frac{b^2-d}{4a^2}=\frac{c}{a},$$

so $a\le c$. Further, the condition $-1/2\le\operatorname{Re}z\le 1/2$ implies $|b|\le 2a$. Thus, we are counting the number of triples (a,b,c) with $a,c>0$ such that $b^2-4ac=d$ and $|b|\le a\le c$, which we can see immediately is finite. Indeed, $b^2\le d$, so there are only finitely many possible b, but then for each b, we see $4ac=b^2-d$, so there are only finitely many possible a and c. ■

> **Remark 1.68.** A quadratic form satisfying the above conditions on a,b,c is called "Gauss reduced."

1.4.3 Dirichlet's Class Number Formula

We take a moment to record Dirichlet's class number formula for completeness, though we will not prove it.

> **Theorem 1.69** (class number formula)**.** Let d be a "fundamental discriminant," meaning that $d\equiv 1\pmod 4$ and is squarefree or $d=4q$ where $q\equiv 2,3\pmod 4$ and is squarefree. Let $\chi_d=\left(\frac{d}{\bullet}\right)$ be the Kronecker symbol.
>
> (a) If $d<0$,
>
> $$h(d)=\frac{w_d|d|^{1/2}}{2\pi}\cdot L(1,\chi_d),$$
>
> where $w_d=2$ if $d<-4$ and $w_d=4$ if $d=-r$ and $w_d=6$ if $d=-3$. (Namely, w_d is the number of roots of unity in $\mathbb{Q}(\sqrt{d})$.)
>
> (b) If $d>0$, then
>
> $$h(d)\log\varepsilon_d=|d|^{1/2}L(1,\chi_d),$$
>
> where ε_d is a fundamental unit for $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. (Namely, $\varepsilon_d=(t_0+u_0\sqrt{d})/2$ yields the least positive solution to $t_0^2-du_0^2=4$.)

The point behind the fundamental discriminant is that $\operatorname{disc}\mathcal{O}_{\mathbb{Q}(\sqrt{d})}=d$.

> **Remark 1.70.** The interested should now be able to do the first part of the first problem set.

Theme 2
The Prime Number Theorem

2.1 January 25

We now shift gears and move towards the Prime number theorem. Today, we begin by discussing Riemann's original paper on the topic.

> **Remark 2.1.** For the rest of this course, any sum or product over an unnamed p will be a sum over primes.

2.1.1 The Statement

So far we have established the following facts about ζ.

- By Corollary 1.6, for $\operatorname{Re} s > 1$, there is an Euler product factorization
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1-p^{-s}}.$$
- By Proposition 1.35, there is a meromorphic continuation of $\zeta(s)$ to $\operatorname{Re} s > 1$, where $\zeta(s)$ is analytic everywhere except for a pole of order 1 at $s = 1$.

Roughly speaking, we will show the Prime number theorem by being able to study $\zeta'(s)/\zeta(s) = \frac{d}{ds}\log\zeta(s)$. Let's establish some notation.

> **Definition 2.2.** For $x \in \mathbb{R}$, we define the following functions.
> $$\pi(x) \coloneqq \sum_{\substack{p \text{ prime} \\ p \leq x}} 1,$$
> $$\Lambda(x) \coloneqq \begin{cases} \log p & \text{if } n = p^\nu \text{ for } \nu \in \mathbb{Z}^+, \\ 0 & \text{else,} \end{cases}$$
> $$\psi(x) \coloneqq \sum_{n \leq x} \Lambda(n).$$

Remark 2.3. Note that

$$\psi(x) = \sum_{p\le x}\log p + \sum_{p\le x^{1/2}}\log p + \sum_{p\le x^{1/3}}\log p + \cdots = \sum_{p\le x}\log p + O_\varepsilon\left(x^{1/2+\varepsilon}\right).$$

The point is that the prime-powers don't actually contribute anything.

Now, here is our statement.

Theorem 2.4 (Prime number)**.** We have $\pi(x) \sim x/\log x$ as $x\to\infty$.

Here is why we mentioned ψ.

Proposition 2.5. The statement $\psi(x)\sim x$ as $x\to\infty$ is equivalent to $\pi(x)\sim x/\log x$ as $x\to\infty$.

Proof. Summation by parts. ■

2.1.2 Poisson Summation

Starting with the easier parts of Riemann's paper, we will use the Poisson summation formula. Let's state it. We will need to establish a little Fourier analysis.

Definition 2.6 (Schwarz)**.** Let $f\colon\mathbb{R}\to\mathbb{R}$ be an infinitely differentiable functions. Then f is *Schwarz* if and only if the nth derivative $f^{(n)}$ is rapidly decaying at $\pm\infty$ for all n.

Definition 2.7 (Fourier transform)**.** Let $f\colon\mathbb{R}\to\mathbb{R}$ be a Schwarz function. Then the *Fourier transform* is the function

$$\widehat{f}(s) := \int_{-\infty}^{\infty} f(x)x^{-2\pi its}\,dt.$$

Example 2.8. Fix $a>0$, and let $f\colon\mathbb{R}\to\mathbb{R}$ be a Schwarz function. Then define $f_a(t) := f(at)$ for $t\in\mathbb{R}$. One can compute that $\widehat{f_a}(s) = \frac{1}{a}\widehat{f}\left(\frac{s}{a}\right)$.

Theorem 2.9 (Poisson summation)**.** Let $f\colon\mathbb{R}\to\mathbb{R}$ be a Schwarz function. Then

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}}\widehat{f}(n).$$

Proof. We compute the trace of a special operator in two ways. Define

$$K(x,y) := \sum_{n\in\mathbb{Z}} f(x-y+n).$$

Note that K is 1-periodic in x and y, so K defines a smooth function on $(\mathbb{R}/\mathbb{Z})^2$. Then one can define the operator

$$T_Kf(x) := \int_{y\in\mathbb{R}/\mathbb{Z}} K(x,y)f(y)\,dy.$$

The point is that $T_K\colon L^2(\mathbb{R}/\mathbb{Z})\to L^2(\mathbb{R}/\mathbb{Z})$ defines a compact operator. We now compute the trace of T_K in two ways.

- "Summing" along the diagonal, we see

  $$\operatorname{tr} K = \int_0^1 K(x,x)\,dx = \sum_{n\in\mathbb{Z}} f(n).$$

  More explicitly, K is a normal operator, so we can find an orthonormal basis $\{\varphi_i\}_i$ which are an eigenbasis for K, we let λ_i be the eigenvalue of φ_i, and we see

  $$K(x,y) = \sum_i \lambda_i\varphi_i(x)\overline{\varphi_j(y)}.$$

  Integrating appropriately completes the proof.

- We may use $\varphi_i(x) := e^{-2\pi inx}$ as an orthonormal basis so that $T_K f$ becomes a Fourier transform. Computing the trace in the same way as above, we see

  $$\operatorname{tr} K = \sum_{n\in\mathbb{Z}} \widehat{f}(n).$$

Equating the above two expressions for $\operatorname{tr} K$ completes the proof. ■

Remark 2.10. The above proof generalizes to the Selberg trace formula. In particular, we are interested in $L^2(\Gamma\backslash\operatorname{SL}_2(\mathbb{R}))$, where Γ is some subgroup of finite index. One recover the Selberg trace formula by computing the trace of the "point pair invariant."

Example 2.11. Let f be a Schwarz function. Then $x>0$ yields

$$\sum_{n\in\mathbb{Z}} f(nx) = \sum_{n\in\mathbb{Z}} f_x(n) = \sum_{n\in\mathbb{Z}} \widehat{f_x}(n) = \frac{1}{x}\sum_{n\in\mathbb{Z}} \widehat{f}(n/x) = \frac{\widehat{f}(0)}{x} + O_{f,A}\left(x^A\right).$$

2.2 January 27

We began class finishing the proof of Theorem 2.9. I have edited directly into that proof for continuity.

2.2.1 An Abstract Functional Equation

We now use Theorem 2.9 in order to show the functional equation for ζ, which provides us with its meromorphic continuation.

To work somewhat abstractly, suppose $f\colon\mathbb{R}\to\mathbb{R}$ is a Schwartz function which has both f and $\widehat{f}$ even and satisfies $f(0)=\widehat{f}(0)=0$. Now define

$$I(f,s) := \int_0^\infty \left(\sum_{n=1}^\infty f(nx)\right) x^s\,\frac{dx}{x}.$$

One can show by hand that $I(f,s)$ is absolutely convergent and then analytic for $\operatorname{Re} s>0$. However, if we take the Fourier transform and use Theorem 2.9, we are able to continue this to all of $\mathbb{C}$. Now, for $\operatorname{Re} s>1$, we have absolute convergence, so Fubini's theorem lets us write

$$I(f,s) = \sum_{n=1}^\infty \left(\int_0^\infty f(nx)x^s\,\frac{dx}{x}\right) = \sum_{n=1}^\infty \left(\frac{1}{n^s}\int_0^\infty f(x)x^s\,\frac{dx}{x}\right) = \zeta(s)(\mathcal{M}f)(s).$$

Notably, we used $\operatorname{Re} s > 1$ in order to write $\zeta(s)$ as the series. Now, everything has a continuation to $\operatorname{Re} s > 0$, so uniqueness of extension lets us extend to $\operatorname{Re} s > 0$.

However, we were able to continue $I(f, s)$ to all of $\mathbb{C}$ by applying Poisson summation. Indeed, Theorem 2.9 yields

$$I(f,s) = \int_0^\infty \left(\sum_{n=1}^\infty \widehat{f}(n/x)\right) x^{s-1}\,\frac{dx}{x}.$$

Now, $\widehat{f}$ is also Schwarz, so we have absolute convergence for $\operatorname{Re} s < 1$, so we have indeed produced our analytic continuation to all of $\mathbb{C}$. Manipulating, we see

$$I(f,s) = \int_0^\infty \left(\sum_{n=1}^\infty \widehat{f}(nx)\right) x^{1-s}\,\frac{dx}{x} = I(\widehat{f}, s-1).$$

Comparing, we see

$$(\mathcal{M}\widehat{f})(1-s)\zeta(1-s) = I(\widehat{f}, s-1) = I(f,s) = \zeta(s)(\mathcal{M}f)(s)$$

on $0 < \operatorname{Re} s < 1$. Thus, we see that we will have a good functional equation for ζ by choosing a sufficiently good f. Indeed, choosing f which is nonzero everywhere except for some finite set of points will grant us a meromorphic continuation of ζ to all of $\mathbb{C}$.

2.2.2 The Functional Equation

We now go back and use a specific value of f to give a functional equation we can really write down. In particular, we will know that ζ only has simple poles at $s = 0$ and $s = 1$, each of residue 1. Indeed, set $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) := e^{-\pi x^2}$ so that $\widehat{f}(x) = f(x)$. Motivated by the above work, we set

$$\Xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s),$$

where

$$\Gamma(s) = \int_0^\infty e^{-t}t^s\,\frac{dt}{t}$$

for $\operatorname{Re} s > 0$, and we can continue Γ to the left by the functional equation $\Gamma(s) = s\Gamma(s-1)$. (This functional equation is proven by integration by parts.)

Remark 2.12. In some sense, Γ is a continuous version of a Gauss sum: it's an integral of an additive character multiplied by a multiplicative character, over a suitable Haar measure.

Remark 2.13. Notably, $\Gamma(s)$ has simple poles for $s \in \{0, -1, -2, \ldots\}$. In fact, $1/\Gamma(s)$ is entire.

Remark 2.14. In some sense, we want to write

$$\Xi(s) = \pi^{-s/2}\Gamma(s/2)\prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

Here, $\pi^{-s/2}\Gamma(s/2)$ is an "archimedean local factor" corresponding to the infinite place ∞ of $\mathbb{Q}$, and each of the $(1-p^{-s})^{-1}$ are "nonarchimedean local factors." Roughly speaking, the rigorization of this intuition is Tate's thesis.

Now working through the arguments of the previous subsection, we see that $\Xi(s)$ is entire except for simple poles at $s \in \{0, 1\}$, and

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

Let's give a few consequences.

Remark 2.15. Doing logarithmic differentiation, one finds

$$\frac{d}{ds}(-\log\zeta(s)) = -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\Gamma(n)}{n^s}.$$

This explains why ψ is a “better” prime-counting function than π.

Remark 2.16. Ignoring convergence issues, we may compute

$$\psi(x) = \sum_{n\le x}\Gamma(n) = \sum_{n=1}^{\infty}1_{[0,1]}(n/x)\Gamma(n) = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)x^s\,\frac{ds}{s}.$$

Now, if we imagine that we could push this integral all the way to the left of $\mathbb{C}$, we will eventually vanish and only pick up on the poles of ζ'/ζ. As such, we expect to achieve a formula of the form

$$\psi(x) = x - \sum_{\rho}\frac{x^\rho}{\rho},$$

where the sum is over the roots ρ of ζ. Thus, we see that having more control over the zeroes of ζ will be able to get good bounds on $\psi(x)-x$. In particular, the Riemann hypothesis is equivalent to $\psi(x) = x + O(\sqrt{x})$. As another application, the discontinuity of ψ will imply that ζ must have infinitely many roots.

Remark 2.17. The previous remark, after some summation by parts, tells us that $\pi(x) - \operatorname{Li}(x)$ has a better error term than $\pi(x) - x/\log x$, where

$$\operatorname{Li}(x) = \int_2^x\frac{dt}{\log t}.$$

Next class we will show the functional equation.

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.

[Ser12] Jean-Pierre Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer New York, 2012. URL: https://books.google.com/books?id=8fPTBwAAQBAJ.

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

List of Definitions