

191: Analytic Number Theory

Nir Elber

Spring 2023

CONTENTS

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

—Neal Shusterman, [Shu16]

Contents	2
1 Arithmetic Progressions	4
1.1 January 18	4
1.1.1 House-Keeping	4
1.1.2 Facts about Dirichlet Series	4
1.1.3 The Euler Product	6
1.1.4 Characters	8
1.1.5 Finite Fourier Analysis	11
1.1.6 Dirichlet Characters	12
1.2 January 20	13
1.2.1 Continuing $L(s, \chi)$	13
1.2.2 Reducing to $L(1, \chi)$	18
1.3 January 23	21
1.3.1 The Dirichlet Convolution	21
1.3.2 The Mellin Transform	23
1.3.3 Finishing Dirichlet's Theorem	25
1.3.4 A Little on Quadratic Forms	27
1.3.5 The Upper-Half Plane	29
1.4 January 25	31
1.4.1 A Fundamental Domain	31
1.4.2 Gauss Reduced Forms	31
1.4.3 Dirichlet's Class Number Formula	32
2 The Prime Number Theorem	33
2.1 January 25	33
2.1.1 The Statement	33
2.1.2 Poisson Summation	36
2.2 January 27	37
2.2.1 An Abstract Functional Equation	38

2.2.2	Facts about Γ	39
2.2.3	Bounds on Γ	44
2.2.4	The Functional Equation	44
2.2.5	Corollaries of the Functional Equation	47
2.3	January 30	49
2.3.1	Zeroes of ζ	49
2.4	February 1	51
2.4.1	Zeroes of ζ , Again	51
2.4.2	The Explicit Formula	52
2.5	February 3	53
2.5.1	The Explicit Formula, Continued	53
2.5.2	A Zero-Free Region	54
2.6	February 6	55
2.6.1	A General Lemma	55
2.6.2	The Prime Number Theorem, Finally	57
2.7	February 8	57
2.7.1	Quadratic Residue Speedrun	58
2.7.2	Gauss Sums	59
2.8	February 10	60
2.8.1	The Pólya–Vinogradov Inequality	60
2.8.2	A Functional Equation for $L(s, \chi)$	61
2.9	February 13	62
2.9.1	All Functional Equations	63
2.9.2	A Zero-Free Region for Complex Characters	64
2.9.3	The Quadratic Gauss Sum	64
2.10	February 15	65
2.10.1	Counting Zeroes of $L(s, \chi)$	66
2.10.2	Solovay–Strassen Primality Testing	66
2.11	February 17	68
2.11.1	Deterministic Solovay–Strassen	68
2.11.2	Imprimitive Characters	69
A	Fourier Analysis	71
A.1	The Fourier Transform	71
A.2	Fourier Inversion	74
A.3	Fourier Coefficients	76
A.4	Fourier Series	80
	Bibliography	82
	List of Definitions	83

THEME 1

ARITHMETIC PROGRESSIONS

1.1 January 18

Here we go.

1.1.1 House-Keeping

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

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

1.1.2 Facts about Dirichlet Series

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

converges by our absolute convergence.

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

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

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

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

which is what we wanted. ■

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

1.1.3 The Euler Product

The following factorization is due to Euler.

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

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

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

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

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

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

To begin, we fix N and claim

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The proof of Theorem 1.1 more or less imitates the argument of Theorem 1.7. 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 $n = \prod_{p|n} p^{\nu_p(n)}$, there is an isomorphism of rings

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

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 $\widehat{G} := \text{Hom}(G, \mathbb{C}^\times)$, where the operation is pointwise. Its elements are called *characters*.

Notation 1.11 (principal character). There is a "trivial" character $1: G \rightarrow \mathbb{C}^\times$ sending $g \mapsto 1$, which is the identity. We might call 1 the *principal character*; we might also denote 1 by χ_0 .

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

Remark 1.13. If G is a finite group, we note that any $\chi \in \widehat{G}$ and $g \in G$ has

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

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

It will be helpful to have the following notation.

Notation 1.14. We might write $e: \mathbb{C} \rightarrow \mathbb{C}$ for the function $e(z) := \exp(2\pi iz)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This completes the proof. ■

Lemma 1.16. Suppose $G = \mathbb{Z}/n\mathbb{Z}$ for a positive integer n . Then $\chi_\bullet: \mathbb{Z}/n\mathbb{Z} \cong \widehat{G}$ by sending $[k]$ to the character $\chi_k: [\ell] \mapsto e(k\ell/n)$.

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

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

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

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

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

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

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

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

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

which forces $n \mid k$.

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

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

so $\chi = \chi_k$ follows. ■

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

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

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

for some positive integers n_i . Thus, using Lemma 1.15 and Lemma 1.16, we compute

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

which is what we wanted. ■

Proposition 1.17 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 $G \rightarrow \widehat{\widehat{G}}$ which is an isomorphism.

Proposition 1.18. Fix a finite abelian group G . Define the map $\text{ev}_\bullet: G \rightarrow \widehat{\widehat{G}}$ by sending $g \in G$ to the map $\text{ev}_g \in \widehat{\widehat{G}}$ defined by $\text{ev}_g: \chi \mapsto \chi(g)$. Then ev_\bullet is an isomorphism.

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

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

Further, ev_\bullet is a homomorphism because

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

It remains to show that ev_\bullet is an isomorphism. We claim that ev_\bullet is injective, which will be enough because $|G| = |\widehat{\widehat{G}}|$ by Proposition 1.17.

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

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

Certainly $\chi((g_i)_{i=1}^n) = e(g_1/n_1) \neq 1$, so it remains to show that χ is a character. This technically follows from Lemma 1.15, but we can see it directly by computing

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

This completes the proof. ■

The proof now follows quickly from Lemma 1.19. 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 $\text{ev}_\bullet: G \rightarrow \widehat{\widehat{G}}$ is injective. ■

1.1.5 Finite Fourier Analysis

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



Idea 1.20. We can write general functions $G \rightarrow \mathbb{C}$ as linear combinations of characters.

Remark 1.21. When G is not abelian, one must work with function $G \rightarrow \mathbb{C}$ which are “locally constant” on conjugacy classes of G .

Here is our Fourier transform.

Notation 1.22. Let G be a finite abelian group. Given a function $f: G \rightarrow \mathbb{C}$, we define $\widehat{f}: \widehat{G} \rightarrow \mathbb{C}$ by

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

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

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

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

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

- (b) If $g = e$, then the sum is $\sum_{\chi \in \widehat{G}} \chi(e) = \#(\widehat{G})$, which is $\#G$ by Proposition 1.17.

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

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

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

Now here is our result.

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

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

for any $g \in G$.

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

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

Now using Proposition 1.23, 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

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

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

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

for any $g \in G$.

Proof. Note

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

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

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* $(\bmod q)$ is a function $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ such that there exists a character $\tilde{\chi}: (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ for which

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

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

Remark 1.27. 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

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

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

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

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

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

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

upon summing over n yields

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

To finish, we see

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

which when combined with the previous equality finishes. ■

Remark 1.31. 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. We will need the following result, from [Mat01].

Proposition 1.32 (Differentiation under the integral sign). Let (X, \mathcal{S}, μ) be a measurable space, and let $U \subseteq \mathbb{C}$ be open, and let $f : U \times X \rightarrow \mathbb{C}$ and $g : X \rightarrow X$ be functions satisfying the following properties.

- The function g is integrable; namely, $\int_X g(t) dt < \infty$.
- For fixed x , the function $z \mapsto f(z, x)$ is holomorphic on U and has $|f(z, x)| \leq g(x)$ for all s .
- For fixed z , the function $x \mapsto f(z, x)$ is measurable.

Then the function $F : U \rightarrow \mathbb{C}$ given by $F(z) := \int_X f(z, x) dx$ is holomorphic on U and satisfies

$$F'(z) = \int_X \frac{\partial f}{\partial z}(z, x) dx.$$

Proof. We use Morera's theorem to show F is holomorphic and the Cauchy integral formula to compute the derivative. The intuition here is that we can control integrals of F easier than its derivatives, so we will try to turn everything into an integral. For clarity, we proceed in steps.

1. We show F is continuous on U . Well, fix some $w \in U$, and we show F is continuous at w ; for concreteness, again find $r > 0$ such that $B(w, r) \subseteq U$. Indeed, for some distinct $w' \in B(w, r)$, we let $\gamma : [0, 1] \rightarrow U$ denote the straight line from w to w' . Thus, the Fundamental theorem of calculus and Cauchy's integral formula grants

$$\begin{aligned} F(w') - F(w) &= \int_X (f(w', x) - f(w, x)) dx \\ &= \int_X \left(\int_{\gamma} \frac{\partial f}{\partial z}(z, x) dz \right) dx \\ &= \frac{1}{2\pi i} \int_X \left(\int_{\gamma} \int_{\gamma_z} \frac{f(z', x)}{(z - z')^2} dz' dz \right) dx, \end{aligned}$$

where γ_z denotes the counterclockwise circle around z of radius $r - \frac{1}{2}|w - w'|$, which is inside $B(w, r) \subseteq U$ because z is on the line connecting w to w' . Now, taking absolute values everywhere, we see

$$|F(w') - F(w)| \leq \frac{1}{2\pi} \int_X \left(\int_{\gamma} \int_{\gamma_z} \frac{g(t)}{|r - \frac{1}{2}|w - w'||^2} dz' dz \right) dx \leq \frac{1}{2\pi} \int_X g(t) dt \cdot \frac{\ell(\gamma) \cdot 2\pi |r - \frac{1}{2}|w - w'||}{|r - \frac{1}{2}|w - w'|^2},$$

where we have used the computation $\ell(\gamma_z) = 2\pi |r - \frac{1}{2}|w - w'||$ for each z . Now, as $w' \rightarrow w$, we see $\ell(\gamma) = |w - w'|$ goes to 0, so the entire right-hand side goes to 0. This completes the proof of continuity at w .

2. We show F is holomorphic on U . It suffices to show that F is differentiable at some fixed $w \in U$ and has the given derivative. As such, we find $r > 0$ such that $B(w, r) \subseteq U$ and replace f with its restriction to $B(w, r) \times X$ and F with its restriction to $B(w, r)$. In particular, we have reduced to the case where U is open and convex.

Now, we already know F is continuous, so we may use Morera's theorem. Well, let $\gamma: [0, 1] \rightarrow U$ be some closed curve, and we want to show

$$\int_{\gamma} F(z) dz = \int_{\gamma} \int_X f(z, x) dx dz \stackrel{?}{=} 0.$$

We would like to exchange the two integrals, so we note we have absolute convergence because

$$\int_{\gamma} \int_X |f(z, x)| dx dz \leq \int_{\gamma} \int_X g(x) dx dz \leq \ell(\gamma) \int_X g(x) dx < \infty.$$

Thus, Fubini's theorem lets us write

$$\int_{\gamma} F(z) dz = \int_X \int_{\gamma} f(z, x) dz dx = \int_X 0 dx = 0,$$

where we have used Cauchy's theorem to evaluate $\int_{\gamma} f(z, x) dz = 0$; recall we reduced to the case where U is convex above!

3. It remains to compute the derivative of F . Because F is holomorphic, we may use the Cauchy integral formula: for any $w \in U$, find r such that $B(w, r) \subseteq U$, and let γ be the loop of radius $r/2$ around w . Then

$$F'(w) = \frac{1}{2\pi i} \int_{\gamma} \frac{F(z)}{(z-w)^2} dz = \frac{1}{2\pi i} \int_{\gamma} \int_X \frac{f(z, x)}{(z-w)^2} dx dz.$$

As usual, we would like to exchange the two integrals, so we note that we have absolute convergence because

$$\int_{\gamma} \int_X \left| \frac{f(z, x)}{(z-w)^2} \right| dx dz \leq \int_{\gamma} \int_X \frac{g(x)}{(r/2)^2} dx dz \leq \frac{\ell(\gamma)}{(r/2)^2} \int_X g(x) dx < \infty.$$

Thus, Fubini's theorem lets us write

$$F'(w) = \int_X \left(\frac{1}{2\pi i} \int_{\gamma} \frac{f(z, x)}{(z-w)^2} dz \right) dx = \int_X \frac{\partial f}{\partial z}(w, x) dx,$$

where we have again applied the Cauchy integral formula. ■

Remark 1.33. Proposition 1.32 might look like needless abstract nonsense with the measure space floating around, but the point here is that we will be able to flexibly apply this result to exchange derivatives with both usual integrals and infinite sums.

Proposition 1.34. Let $\chi \pmod{q}$ be a non-principal Dirichlet character. Then the function $L(s, \chi)$ admits an analytic continuation to $\{s : \operatorname{Re} s > 0\}$.

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

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

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

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

Now, finally using Theorem 1.30, we see

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

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

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

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

Roughly speaking, we want to write

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

for any $\operatorname{Re} s > 0$, meaning that the integral converges, so we ought to have a holomorphic function. To make this computation rigorous, we will show that $I(s)$ is holomorphic on $\{s : \operatorname{Re} s > \sigma\}$ for any $\sigma > 0$, which will be enough by taking the union over all σ . Indeed, for some fixed σ , we define $g : [1, \infty)$ by $g(t) := q/t^{\sigma+1}$ for $t > 2$ and 0 elsewhere so that

$$\left| \frac{A(t)}{t^{s+1}} \right| = \left| \frac{A(t)}{t^{s+1}} \right| \leq g(t)$$

for $\operatorname{Re} s > \sigma$, and

$$\int_{\mathbb{R}} g(t) dt = q \int_1^{\infty} t^{-\sigma-1} dt < \infty$$

because $\sigma > 0$. Thus, Proposition 1.32 implies that $I(s)$ is holomorphic on $\{s : \operatorname{Re} s > \sigma\}$, finishing the proof. ■

Remark 1.35. Using the notions and notations of the above proof, we see that

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

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

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

Lemma 1.36. Let $\chi_0 \pmod{q}$ be the principal Dirichlet character. Then for $\operatorname{Re} s > 1$, we have

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

Proof. By Remark 1.29, 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 1.34, 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 1.37. The function $\zeta(s)$ has a meromorphic continuation to $\{s : \operatorname{Re} s > 0\}$. It is holomorphic everywhere except at $s = 1$, where it has a simple pole of residue 1.

Proof. For given s with $\operatorname{Re} s > 1$, set $a_n := 1$ and $f(x) := 1/x^s$. Then the partial sums $A(t) := \sum_{1 \leq n \leq t} a_n$ have $A(t) = [t]$, so Theorem 1.30 grants

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

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

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

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

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

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

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

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

so the integral converges and ought to define a holomorphic function. To make this computation rigorous, we will show that $I(s)$ is holomorphic on $\{s : \operatorname{Re} s > \sigma\}$ for any $\sigma > 0$, which will be enough by taking the union over all σ . Indeed, for some fixed σ , we set $g(t) := 1/t^{\sigma+1}$ for $t > 1$ and 0 elsewhere so that

$$\left| \frac{\{t\}}{t^{s+1}} \right| \leq g(t)$$

for $\operatorname{Re} s > \sigma$, and

$$\int_{\mathbb{R}} g(t) dt = \int_1^{\infty} t^{-\sigma-1} dt < \infty$$

because $\sigma > 0$. Thus, Proposition 1.32 implies that $I(s)$ is holomorphic on $\{s : \operatorname{Re} s > \sigma\}$, finishing the proof. ■

Remark 1.38. Using the notions and notation of the above proof, we see that

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

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

Remark 1.39. 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 1.40. 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 1.36 and Proposition 1.37 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 1.41. Let $\chi \pmod{q}$ be a Dirichlet character. For any s with $\operatorname{Re} s > 1$, we have

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

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

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

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

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

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

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

As an aside, we note that Lemma 1.41 provides us with a relatively large zero-free region for $L(s, \chi)$.

Corollary 1.42. Let $\chi \pmod{q}$ be a Dirichlet character. For any s with $\operatorname{Re} s > 1$, we have $L(s, \chi) \neq 0$.

Proof. By Lemma 1.41, we see

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

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

We now see that we can use Lemma 1.41 and Corollary 1.25 to extract a particular congruence class.

Lemma 1.43. Let q be an integer. For brevity, set $G := (\mathbb{Z}/q\mathbb{Z})^\times$, and fix some $a \in G$. For any s with $\operatorname{Re} s > 1$, we have

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

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

Proof. Corollary 1.25 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 1.41, 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 1.44. 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 1.34.

Let χ_0 denote the principal character. By Corollary 1.40, we see $L(s, \chi_0) \rightarrow +\infty$ as $s \rightarrow 1^+$: indeed, we know $L(s, \chi_0)$ must go to something in $\mathbb{R}_{\geq 0} \cup \{\infty\}$ because $L(s, \chi_0) \geq 1$ when $s > 1$ is real. But $L(s, \chi_0)$ cannot go to a finite value because then $L(s, \chi_0)$ would only have a removable singularity at $s = 1$.

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

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

so the result follows from Lemma 1.43. ■

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 1.45. 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 1.43 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 1.40 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 1.34, and $v(\chi)$ is finite because $L(s, \chi)$ is not constantly zero by Corollary 1.42.

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 1.43, 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 1.43 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 $s \rightarrow 1^+$, the left-hand side remains nonnegative. On the right-hand side, the middle and right terms both remain finite, so the left term must also remain finite. However, $\log(s-1) \rightarrow -\infty$ as $s \rightarrow 1^+$, so we must have $\sum_{\chi} v(\chi) \leq 0$ to ensure this term is nonnegative.

We now show the last sentence. Indeed, we have

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

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

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

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

But this grants two distinct characters χ and $\bar{\chi}$ with $L(1, \chi) = L(1, \bar{\chi}) = 0$, violating Lemma 1.45. ■

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

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 1.47 (Dirichlet convolution). Fix functions $f, g: \mathbb{N} \rightarrow \mathbb{C}$. Then the *Dirichlet convolution* $(f * g): \mathbb{N} \rightarrow \mathbb{C}$ is defined by

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

And we may now take products of Dirichlet series.

Proposition 1.48. Fix functions $f, g: \mathbb{N} \rightarrow \mathbb{C}$ such that $|f(n)|, |g(n)| = O(n^\sigma)$ for some $\sigma \in \mathbb{R}$. Then define the series

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

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 n th partial sums. Then we see

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

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

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

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

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

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

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

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

Example 1.49. 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, $1: \mathbb{N} \rightarrow \mathbb{C}$ 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 1.50. Let $f, g: \mathbb{N} \rightarrow \mathbb{C}$ be multiplicative functions. Then $(f * g): \mathbb{N} \rightarrow \mathbb{C}$ 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 $d_n d_m \mid nm$.
- Injective: suppose $d_n d_m = d'_n d'_m$ 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

$$\nu_p(d_n) = \nu_p(d_n d_m) = \nu_p(d'_n d'_m) = \nu_p(d'_n)$$

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 $d = d_n d_m$. 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 $\nu_p(d_m) = \nu_p(d)$. Because each prime $p \mid nm$ divides exactly one of n or m , we see that

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

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

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

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

Here, we have used the multiplicativity at $*$, 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 1.51 (decaying). A function $\varphi: (0, \infty) \rightarrow \mathbb{C}$ is *decaying at a rate of (α, β)* for real numbers $\alpha < \beta$ if and only if the functions $x^\alpha \varphi(x)$ and $x^\beta \varphi(x)$ are bounded.

Example 1.52. If $\varphi: (0, \infty) \rightarrow \mathbb{C}$ has compact support, then φ decays at a rate of (α, β) for all $\alpha < \beta$. Indeed, for any γ , the function $x^\gamma \varphi(x)$ is a continuous function supported on a compact set and is thus bounded.

Definition 1.53 (Mellin transform). Let $\varphi: (0, \infty) \rightarrow \mathbb{C}$ be a continuous function decaying at a rate of (α, β) . Then the *Mellin transform* is the function $\mathcal{M}\varphi$ given by

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

for $\alpha < \operatorname{Re} s < \beta$.

Remark 1.54. We quickly check that the integral $\mathcal{M}\varphi$ (absolutely) converges for $\alpha < \operatorname{Re} s < \beta$. For each $\gamma \in \{\alpha, \beta\}$, find a constant $C_\gamma \in \mathbb{R}$ such that $|x^\gamma \varphi(x)| \leq C_\gamma$ for all $x \in (0, \infty)$. For our absolute convergence, we set $\sigma := \operatorname{Re} s \in (\alpha, \beta)$ and compute

$$\int_0^\infty |\varphi(x) x^s| \frac{dx}{x} \leq \int_0^1 C_\alpha x^{-\alpha+\sigma-1} dx + \int_1^\infty C_\beta x^{-\beta+\sigma-1} dx,$$

so both of the right-hand integrals converge because $-\alpha + \sigma - 1 > -1$ and $-\beta + \sigma - 1 < -1$. Notably, this shows that $(\mathcal{M}\varphi)$ is uniformly bounded by

$$\int_0^1 C_\alpha x^{-\alpha+\alpha_0-1} dx + \int_1^\infty C_\beta x^{-\beta+\beta_0-1} dx$$

whenever $\sigma \in [\alpha_0, \beta_0]$.

Remark 1.55. Fixing some $\sigma \in (\alpha, \beta)$, let $\psi(u) := e^{-\sigma u} \varphi(e^{-u})$. Provided that ψ is Schwarz, changing variables by $x = e^{-u}$ gives

$$(\mathcal{M}\varphi)(\sigma + 2\pi it) = \int_0^\infty \varphi(x) x^{\sigma+2\pi it} \frac{dx}{x} = \int_{\mathbb{R}} \varphi(e^{-u}) e^{-\sigma u - 2\pi i t u} du = (\mathcal{F}\psi)(t).$$

Here is a basic result on the Mellin transform.

Lemma 1.56. Fix a differentiable function $\varphi: (0, \infty) \rightarrow \mathbb{C}$ such that φ decays at a rate of (α, β) . Defining $\psi(x) := x\varphi'(x)$, for any $\alpha < \operatorname{Re} s < \beta$, the integral defining $(\mathcal{M}\psi)(s)$ converges, and

$$(\mathcal{M}\psi)(s) = -s(\mathcal{M}\varphi)(s).$$

Proof. This is by integration by parts. Indeed, we compute

$$\begin{aligned} (\mathcal{M}\psi)(s) &= \int_0^\infty x\varphi'(x)x^s \frac{dx}{x} \\ &= x^s\varphi(x) \Big|_0^\infty - s \int_0^\infty \varphi(x)x^s \frac{dx}{x} \\ &= -s(\mathcal{M}\varphi)(s), \end{aligned}$$

which is what we wanted. Note, $x^s\varphi(x) \rightarrow 0$ as $x \rightarrow 0^+$ and $x \rightarrow \infty$ because φ decays at a rate of (α, β) and $\operatorname{Re} s \in (\alpha, \beta)$. ■

We will need two key properties of the Mellin transform.

Proposition 1.57. Let $\varphi: (0, \infty) \rightarrow \mathbb{C}$ be a continuous function decaying at a rate of (α, β) .

- (a) The function $\mathcal{M}\varphi$ is holomorphic on $\{s : \alpha < \operatorname{Re} s < \beta\}$.
- (b) Suppose that φ is infinitely differentiable, and the n th derivatives decays at a rate of $(\alpha - n, \beta - n)$. Then for any integer $A \geq 0$ and $[\alpha_0, \beta_0] \subseteq (\alpha, \beta)$, the set

$$\{|s|^A (\mathcal{M}\varphi)(s) : \alpha_0 \leq \operatorname{Re} s \leq \beta_0\}$$

is bounded.

Proof. These are essentially bounding results.

- (a) We use Proposition 1.32. Here, $f(s, t) := \varphi(x)x^{s-1}$. We will show that $\mathcal{M}\varphi$ is holomorphic on the vertical strip $U := \{s : -\alpha_0 < \operatorname{Re} s < \beta_0\}$ for any $\alpha < \alpha_0 < \beta_0 < \beta$, and the result will follow by taking the union over all α_0 and β_0 .

By hypothesis on φ , we can find a constant C such that $|x^\alpha\varphi(x)| \leq C$ and $|x^\beta\varphi(x)| \leq C$ for each x . As such, we define $g: (0, \infty) \rightarrow \mathbb{R}$ by

$$g(t) := \begin{cases} Cx^{-\alpha+\alpha_0-1} & \text{if } x \leq 1, \\ Cx^{-\beta+\beta_0-1} & \text{if } x > 1. \end{cases}$$

Note $\int_{\mathbb{R}} g(t) dt < \infty$ because $-\alpha + \alpha_0 - 1 > -1$ and $-\beta + \beta_0 - 1 < -1$. Thus, we see that $x \in (0, 1]$ gives

$$|\varphi(x)x^{s-1}| \leq Cx^{-\alpha+\operatorname{Re} s-1} \leq Cx^{-\alpha+\alpha_0+1},$$

and similar for $x \in (1, \infty)$ comparing with β_0 . The result now follows from Proposition 1.32.

- (b) This follows from Lemma 1.56. Define $\varphi_0 := \varphi$ and $\varphi_{n+1}(x) := x\varphi'_n(x)$ for each n . By induction, φ_n decays at a rate of (α, β) for each n , and for each n , we see

$$|s^n (\mathcal{M}\varphi)(s)| = |(\mathcal{M}\varphi_n)(s)|$$

by Lemma 1.56. However, for each n , we see that $(\mathcal{M}\varphi_n)$ is uniformly bounded on $[\alpha_0, \beta_0]$ by Remark 1.54, which is what we wanted. ■

Remark 1.58. The condition that $\varphi^{(n)}$ decay at a rate of $(\alpha - n, \beta - n)$ is essentially requiring that φ behave like a polynomial somewhat. These sorts of conditions more or less vanish for sufficiently good functions; for example, if φ is infinitely differentiable and has compact support, then all the derivatives have compact support, so $\varphi^{(n)}$ always decays at a rate of (α, β) for all $\alpha < \beta$ by Example 1.52.

Theorem 1.59. Let $\varphi: (0, \infty) \rightarrow \mathbb{C}$ be a function such that $\psi(u) := e^{-\sigma u} \varphi(e^{-u})$ is Schwarz. For any $\sigma \in \mathbb{R}$ and $x \in (0, \infty)$, we have

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

Proof. We translate everything to the Fourier setting with Remark 1.55, where Theorem A.10 finishes. Following this outline, we compute

$$\begin{aligned} \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} (\mathcal{M}\varphi)(s) x^{-s} ds &= \int_{\mathbb{R}} (\mathcal{M}\varphi)(\sigma + 2\pi it) x^{-\sigma-2\pi it} dt \\ &= x^{-\sigma} \int_{\mathbb{R}} (\mathcal{F}\psi)(t) e^{2\pi i(-\log x)t} dt \\ &= x^{-\sigma} \cdot \psi(-\log x) \\ &= \varphi(x), \end{aligned}$$

which is what we wanted. ■

1.3.3 Finishing Dirichlet's Theorem

We finish the proof of Theorem 1.1. By Proposition 1.44 and Lemma 1.46, we have left to show $L(1, \chi) \neq 0$ for real characters χ . We provide a slick proof of this result.

Lemma 1.60. Let $\chi \pmod{q}$ be a “real” non-principal Dirichlet character, meaning $\chi = \bar{\chi}$. 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 1.34 and 1.37.

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 1.48. Note $(1 * \chi)$ is multiplicative by Lemma 1.50.

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

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

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

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

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 $(1 * \chi)(p^\nu) = \nu + 1 \geq 1$ always. On the other hand, if $\chi(p) = -1$, then $(1 * \chi)(p^\nu)$ is 1 when ν is even and 0 if ν is odd. The claim follows.

To finish, our positivity claim is that

$$\sum_{x < n \leq 2x} (1 * \chi)(n) \geq \sum_{x < n^2 \leq 2x} (1 * \chi)(n^2) \geq \sum_{\sqrt{x} < n \leq \sqrt{2x}} 1 = \lfloor \sqrt{2x} \rfloor - \lfloor \sqrt{x} \rfloor \geq (\sqrt{2} - 1)\sqrt{x} - 2.$$

Thus, for x large enough, we see

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

2. We now apply smoothing Let $\varphi: (0, \infty) \rightarrow (0, \infty)$ be an infinitely differentiable function with support contained in $[0.9, 2.1]$ such that $\varphi(x) = 1$ for $x \in [1, 2]$. Then one sees

$$\sum_{n=1}^{\infty} \varphi(n/x) (1 * \chi)(n) \geq \sum_{x < n \leq 2x} (1 * \chi)(n) \geq \frac{1}{3} \sqrt{x}.$$

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

We now use the Mellin transform $\mathcal{M}\varphi$. Indeed, note that φ is decaying at a rate of (α, β) for any $\alpha < \beta$ by Remark 1.58. Further, for any $\sigma > 0$, the function $\psi(u) := e^{-\sigma u} \varphi(e^{-u})$ has compact support and is infinitely differentiable, so $x^k \psi^{(\ell)}(x)$ is continuous of compact support for all k and ℓ and hence bounded. Thus, ψ is Schwarz, so we can use Theorem 1.59 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

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

by Proposition 1.48. To bound this, we see $|x^s| \leq x^{\operatorname{Re} s} = x^{\sigma}$ and

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

by Remarks 1.35 and 1.38, where $C_0(q, \sigma)$ is some constant. Thus,

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

However, by Proposition 1.57 (and Remark 1.58), there is C such that $|(\mathcal{M}\varphi)(s)| \leq C|s|^{-4} \leq C(\operatorname{Im} s)^{-4}$ on the vertical strip of interest, so we bound

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

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

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

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

3. Anyway, we now know we can write

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

by exchanging the sum and the integral and using Proposition 1.48. 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

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

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

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

Because $(\mathcal{M}\varphi)(s)$ is rapidly decaying as $\operatorname{Im} s \rightarrow \infty$ (recall Proposition 1.57), we see that this indeed goes to 0 as $\operatorname{Im} s \rightarrow \infty$.

In total, we see

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

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

Remark 1.61. The product $\zeta(s)L(s,\chi)$ 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 1.62 (binary quadratic form). A *binary quadratic form* is a function $f: \mathbb{Z}^2 \rightarrow \mathbb{Z}$ 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 1.63. 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 1.64. 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 1.65 (equivalent). Two binary quadratic forms $f_1, f_2: \mathbb{Z}^2 \rightarrow \mathbb{Z}$ 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 1.66. For a binary quadratic form $f(x, y) := ax^2 + bxy + cy^2$, note that

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

for any $v = (x, y) \in \mathbb{Z}^2$. In fact, this symmetric matrix M is unique to f : if $v^T M v = v^T M' v$ for all $v = (x, y) \in \mathbb{Z}^2$, then writing $M = (a_{ij})$ and $M' = (a'_{ij})$, we see

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 = v^T M v = v^T M' v = a'_{11}x^2 + 2a'_{12}xy + a'_{22}y^2.$$

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

Remark 1.67. Associate a binary quadratic form f the matrix M as in Remark 1.66. Thus, for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$,

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

so we can associate $\gamma \cdot f$ to the matrix $\gamma^{-T} M \gamma^{-1}$. (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 1.68 (discriminant). The *discriminant* of the binary quadratic form $f(x, y) := ax^2 + bxy + cy^2$ is given by $\mathrm{disc} f := b^2 - 4ac$. The number of equivalence classes of quadratic forms of discriminant d is notated by $h(-d)$.

Remark 1.69. 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 1.66. Using Remark 1.67, we see that the discriminant of $\gamma \cdot f$ is thus

$$4 \det (\gamma^{-T}) \det(M) \det (\gamma^{-1}) = 4 \det M$$

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

Remark 1.69 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 $\text{disc } f = d^2$. 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 1.70. Let $d < 0$ be an integer. Then $h(d)$ is finite.

Remark 1.71. 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 1.70, we will want to relate the action of $\text{SL}_2(\mathbb{Z})$ on quadratic forms with the action of $\text{SL}_2(\mathbb{R})$ on $\mathbb{H} := \{z \in \mathbb{C} : \text{Im } z > 0\}$ given by

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

Here are some checks on this action.

Lemma 1.72. Let $\mathbb{H} := \{z \in \mathbb{C} : \text{Im } z > 0\}$ denote the upper-half plane.

(a) The group $\text{SL}_2(\mathbb{R})$ 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 $\text{SL}_2(\mathbb{R})$ is all of \mathbb{H} .

(c) The stabilizer of $i \in \mathbb{H}$ is $\text{SO}_2(\mathbb{R})$, 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 $\gamma \in \text{SL}_2(\mathbb{R})$. Well, giving coefficients to γ , we compute

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

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

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

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

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

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 1.73. Parts (b) and (c) of Lemma 1.72 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 1.73 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 1.74. Define the subset

$$D := \{z \in \mathbb{H} : |z| > 1, -1/2 \leq \operatorname{Re} z < 1/2\} \cup \{z \in \mathbb{H} : |z| = 1, -1/2 \leq \operatorname{Re} z \leq 0\}.$$

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

$$S := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{and} \quad T := \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}.$$

Then one can use T to push all elements of \mathbb{H} to $\{z \in \mathbb{H} : -1 \leq \operatorname{Re} z < 1\}$ 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 1.74 for fun and profit.

Theorem 1.70. Let $d < 0$ be an integer. Then $h(d)$ is finite.

Proof. Roughly speaking, a quadratic form $f(x, y) := ax^2 + bxy + cy^2$ 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 1.74, we know there is some γ_f 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 $|z_f| \geq 1$ implies that

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

so $a \leq c$. Further, the condition $-1/2 \leq \operatorname{Re} z \leq 1/2$ implies $|b| \leq 2a$. Thus, we are counting the number of triples (a, b, c) with $a, c > 0$ such that $b^2 - 4ac = d$ and $|b| \leq a \leq c$, which we can see immediately is finite. Indeed, $b^2 \leq d$, 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 1.75. 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 1.76 (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 $d = -4$ 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 1.77. 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 1.37, 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.

$$\begin{aligned} \pi(x) &:= \sum_{p \leq x} 1, \\ \vartheta(x) &:= \sum_{p \leq x} \log p, \\ \Lambda(n) &:= \begin{cases} \log p & \text{if } n = p^\nu \text{ for } \nu \in \mathbb{Z}^+, \\ 0 & \text{else,} \end{cases} \\ \psi(x) &:= \sum_{n \leq x} \Lambda(n). \end{aligned}$$

Quickly, we note that the prime-powers we have included in $\Lambda(n)$ and $\psi(x)$ don't actually matter.

Lemma 2.3. For any $x \geq 2$, we have

$$\psi(x) = \vartheta(x) + O(\sqrt{x}(\log x)^2).$$

Proof. Note

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{k=1}^{\infty} \left(\sum_{p^k \leq x} \log p \right).$$

Now, note $k \geq \log_2 x$ implies that $p^k \geq 2^k \geq x$ for all primes p , so we only need to sum up to $\log_2 x$. As such, we upper-bound the $k > 1$ sum as

$$\left| \sum_{k=2}^{\log_2 x} \left(\sum_{p^k \leq x} \log p \right) \right| \leq |\log_2 x - 1| \cdot \left| \sum_{n \leq \sqrt{x}} \log(\sqrt{n}) \right| \leq \frac{\sqrt{x}(\log x)^2}{2 \log 2}.$$

Adding the $k = 1$ sum back in, we see that

$$\psi(x) = \sum_{p \leq x} \log p + O(\sqrt{x}(\log x)^2),$$

which is what we wanted. ■

Remark 2.4. Doing logarithmic differentiation, one finds

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

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

Now, here is our statement.

Theorem 2.5 (Prime number). We have $\pi(x) \sim x/\log x$ as $x \rightarrow \infty$.

Here is why we mentioned ϑ and ψ .

Lemma 2.6. Define $g(x) := \vartheta(x) - x$. Then

$$\pi(x) = \int_2^x \frac{1}{\log t} dt + \frac{2}{\log 2} + \frac{g(x)}{\log x} + \int_2^x \frac{g(t)}{t(\log t)^2} dt.$$

Proof. This is summation by parts. Let $a_n = \log n$ be 1 if n is prime and 0 otherwise so that the partial sum up to x of a_n is given by $\vartheta(x)$. Further, let $f(n) := 1/\log n$ if $n > 1$ and 0 at $n = 1$. Then Theorem 1.30 tells us

$$\begin{aligned} \pi(x) &= \sum_{n \leq x} a_n f(n) \\ &= \vartheta(x)f(x) - \int_0^x \vartheta(t)f'(t) dt \\ &= \frac{x}{\log x} + \int_2^x \frac{t}{t(\log t)^2} dt + \frac{g(x)}{\log x} + \int_2^x \frac{g(t)}{t(\log t)^2} dt \\ &= \int_2^x \frac{1}{\log t} dt + \frac{2}{\log 2} + \frac{g(x)}{\log x} + \int_2^x \frac{g(t)}{t(\log t)^2} dt, \end{aligned}$$

which is what we wanted. ■

Proposition 2.7. The following are equivalent.

- (a) $\pi(x) \sim x/\log x$ as $x \rightarrow \infty$.
- (b) $\vartheta(x) \sim x$ as $x \rightarrow \infty$.
- (c) $\psi(x) \sim x$ as $x \rightarrow \infty$.

Proof. By Lemma 2.3, we see

$$\frac{\vartheta(x)}{x} - \frac{\psi(x)}{x} = O\left(x^{-1/2}(\log x)^2\right) = o(1),$$

so

$$\lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = \lim_{x \rightarrow \infty} \frac{\psi(x)}{x},$$

provided that either limit exists. The equivalence of (b) and (c) follows.

We now show that (a) and (b) are equivalent to finish.

- Showing (a) implies (b) is by summation by parts. Let a_n denote the prime indicator at n so that the partial sum up to x is $\pi(x)$. Further, define $f(x) := \log x$ for $x \geq 1$ and 0 otherwise. Thus, Theorem 1.30 implies

$$\begin{aligned} \vartheta(x) &= \sum_{n \leq x} a_n f(n) \\ &= \pi(x)f(x) - \int_0^x \pi(t)f'(t) dt \\ &= \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt, \end{aligned}$$

so

$$\frac{\vartheta(x)}{x} = \frac{\pi(x)}{x/\log x} - \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt.$$

Given $\pi(x) \sim x/\log x$, the main term here has $\pi(x)/(x/\log x) \rightarrow 1$ as $x \rightarrow \infty$, so we have left to show that the right term vanishes. Well, $|\pi(x)/(x/\log x)| \rightarrow 1$ as $x \rightarrow \infty$ implies that this function has a maximum on $[2, \infty)$, so we let M denote the maximum. Thus,

$$\left| \int_2^x \frac{\pi(t)}{t} dt \right| \leq M \int_2^x \frac{\log t}{t} dt.$$

To finish, we use L'Hôpital's rule to note

$$\lim_{x \rightarrow \infty} \frac{M \int_2^x \log t/t dt}{x} = \lim_{x \rightarrow \infty} \frac{M \log x}{x} = 0.$$

- Showing (b) implies (a) follows from Lemma 2.6. Indeed, note

$$\frac{\pi(x)}{x/\log x} = \frac{\int_2^x 1/\log t dt}{x/\log x} + \frac{g(x)}{x} + \frac{\log x}{x} \int_2^x \frac{g(t)}{t(\log t)^2} dt, \quad (2.1)$$

where $g(x) := \theta(x) - x$. Using L'Hôpital's rule, the main term has

$$\lim_{x \rightarrow \infty} \frac{\int_2^x 1/\log t dt}{x/\log x} = \lim_{x \rightarrow \infty} \frac{1/\log x}{(\log x - 1)/(\log x)^2} = \lim_{x \rightarrow \infty} \frac{1}{1 - 1/\log x} = 1.$$

It remains to show that everything else on the right-hand side of (2.1) vanishes. We are given $g(x)/x \rightarrow 0$ as $x \rightarrow \infty$, so we have nothing to worry about there. For the last term, $g(x)/x \rightarrow 0$ implies that we can choose N so that $x > N$ enforces $|g(x)| \leq 2x$, meaning

$$\left| \int_2^x \frac{g(t)}{t(\log t)^2} dt \right| \leq \left| \int_2^N \frac{g(t)}{t(\log t)^2} dt \right| + \int_N^x \frac{1}{(\log t)^2} dt.$$

The left term is constant so vanishes as $x \rightarrow \infty$ when multiplied through by $\log x/x$. The right term will also vanish similarly: by L'Hôpital's rule, we see

$$\lim_{x \rightarrow \infty} \frac{\int_N^x \frac{1}{(\log t)^2} dt}{x/\log x} = \lim_{x \rightarrow \infty} \frac{1/(\log x)^2}{(\log x - 1)/(\log x)^2} = \lim_{x \rightarrow \infty} \frac{1}{\log x - 1} = 0.$$

This completes the proof. ■

2.1.2 Poisson Summation

Starting with the easier parts of Riemann's paper, we will show the functional equation for $\zeta(s)$. For this, we use the Poisson summation formula.

Theorem 2.8 (Poisson summation). Let $f: \mathbb{R} \rightarrow \mathbb{C}$ be a Schwarz function. Then

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} (\mathcal{F}f)(n),$$

and both sums converge absolutely.

Proof. Consider the function

$$F(x) := \sum_{n \in \mathbb{Z}} f(x+n).$$

The point is to compute the Fourier series of $F: \mathbb{R} \rightarrow \mathbb{C}$. Thus, we divide the proof into steps.

1. Note that F is continuous. Indeed, we will essentially see that the series (absolutely) converges uniformly on compact sets: let F_N denote the N th partial sum, where $N \geq 1$. Thus, to show that F is continuous on some closed interval $[a, b]$, it suffices to show that $F_N \rightarrow F$ uniformly on $[a, b]$ because each F_N is continuous. This will be enough because each $x \in \mathbb{R}$ is contained in some closed interval $[x-1, x+1]$, so F is continuous at each $x \in \mathbb{R}$.

Before doing anything, note $x \in [a, b]$ implies $|x| \leq m$ where $m := \max\{|a|, |b|\}$, so we will take $N > 2m$ throughout. Now, the Schwartz condition on f lets us find a constant $C \in \mathbb{R}$ such that $|x^2 f(x)| \leq C$, so

$$|F(x) - F_N(x)| \leq \sum_{|n| > N} |f(x+n)| \leq 2C \sum_{|n| > N} \frac{1}{(x+n)^2}.$$

The sum now splits into

$$|F(x) - F_N(x)| \leq \sum_{n < -N} \frac{1}{(x+n)^2} + \sum_{n > N} \frac{1}{(x+n)^2} = \sum_{n > N} \left(\frac{1}{(n-x)^2} + \frac{1}{(n+x)^2} \right).$$

The summand is now decreasing in n , so we may upper-bound this by the integral test, writing

$$|F(x) - F_N(x)| \leq \int_{N-1}^{\infty} \left(\frac{1}{(t-x)^2} + \frac{1}{(t+x)^2} \right) dt = \frac{1}{2(N-1-x)} + \frac{1}{2(N-1+x)},$$

which does vanish as $N \rightarrow \infty$.

As an aside, note that the above bounding has also shown that the series $F(x)$ absolutely converges because we showed that $\sum_{|n| > N} |f(x+n)|$ converges for some N depending on x (though this dependency is irrelevant here).

2. Note F is 1-periodic because rearranging the sum gives

$$F(x+1) = \sum_{n \in \mathbb{Z}} f(x+n+1) = \sum_{n \in \mathbb{Z}} f(x+n) = F(x).$$

3. The next step is compute the Fourier coefficients of F , which for some $n \in \mathbb{Z}$ is

$$a_n(F) = \int_0^1 \left(\sum_{k \in \mathbb{Z}} f(x+k) e^{-2\pi i n x} \right) dx.$$

We would like to exchange the integral and the sum, so we check the absolute convergence as

$$\int_0^1 \left(\sum_{k \in \mathbb{Z}} |f(x+k) e^{-2\pi i n x}| \right) dx = \int_0^1 \left(\sum_{k \in \mathbb{Z}} |f(x+k)| \right) dx.$$

Now, we showed that the series $x \mapsto \sum_{k \in \mathbb{Z}} |f(x+k)|$ converges uniformly on compact closed intervals $[a, b]$, so it defines a continuous function on the closed interval $[0, 1]$, so this integral converges. As such, we may now apply Fubini's theorem to get

$$a_n(F) = \sum_{k \in \mathbb{Z}} \int_0^1 f(x+k) e^{-2\pi i n x} dx = \sum_{k \in \mathbb{Z}} \int_k^{k+1} f(x) e^{-2\pi i n x} dx = \int_{-\infty}^{\infty} f(x) e^{-2\pi i n x} dx = (\mathcal{F}f)(n).$$

4. We would like to build the Fourier series using Theorem A.20, but for this we must show that S_F converges absolutely and uniformly. Well, by Lemma A.6, we see that $n \neq 0$ have

$$(\mathcal{F}f)(n) = \frac{1}{2\pi i n} \cdot (\mathcal{F}f')(n) = \frac{1}{-4\pi^2 n^2} \cdot (\mathcal{F}f'')(n).$$

Now, $(\mathcal{F}f'')$ is bounded by Remark A.5, so find M such that $|(\mathcal{F}f'')(s)| \leq M$ for all s . Checking the absolute and uniform convergence, we see $N > 0$ lets us upper-bound

$$\sum_{|n| > N} |a_n(F) e^{2\pi i n x}| \leq \frac{M}{4\pi^2} \sum_{|n| > N} \frac{1}{n^2} = \frac{2M}{4\pi^2} \sum_{n > N} \frac{1}{n^2} = \frac{2M}{4\pi^2} \int_N^{\infty} \frac{1}{x^2} dx = \frac{2M}{4\pi^2 N},$$

which does vanish as $N \rightarrow \infty$.

5. The previous step gives our absolute and uniform convergence, so Theorem A.20 tells us

$$\sum_{n \in \mathbb{Z}} f(x+n) = F(x) = \sum_{n \in \mathbb{Z}} a_n(F) e^{2\pi i n x} = \sum_{n \in \mathbb{Z}} (\mathcal{F}f)(n) e^{-2\pi i n x}$$

for all $x \in \mathbb{R}$. Setting $x = 0$ completes the proof. ■

Example 2.9. Let f be a Schwarz function, and define $f_x(t) := f(tx)$ for any $x > 0$. Then $(\mathcal{F}f_x)(s) = \frac{1}{x} (\mathcal{F}f)\left(\frac{s}{x}\right)$, so Theorem 2.8 yields

$$\sum_{n \in \mathbb{Z}} f(nx) = \sum_{n \in \mathbb{Z}} f_x(n) = \sum_{n \in \mathbb{Z}} (\mathcal{F}f_x)(n) = \frac{1}{x} \sum_{n \in \mathbb{Z}} (\mathcal{F}f)(n/x)$$

for any $x > 0$.

2.2 January 27

We began class finishing the proof of Theorem 2.8. I have edited directly into that proof for continuity.

2.2.1 An Abstract Functional Equation

We now use Theorem 2.8 in order to show the functional equation for ζ , which provides us with its meromorphic continuation.

There is a usual functional equation, but we will take a moment to point out that there is nothing particularly special about the functional equation we are about to construct. Indeed, we can build a family of functional equations as follows.

Proposition 2.10. Call a Schwarz function $f: \mathbb{R} \rightarrow \mathbb{R}$ “slow” if and only if the function

$$S_f(x) := \sum_{n \in \mathbb{Z}} f(nx)$$

is defined on $(0, \infty)$ and decays at a rate of (α, β) for all $0 < \alpha < \beta$. If f is slow, then $I(f, s) := (\mathcal{M}S_f)(s)$ converges absolutely to a holomorphic function on $\{s : \operatorname{Re} s > 0\}$. In fact, if $\mathcal{F}f$ is also slow, then

$$I(\mathcal{F}f, 1 - s) = I(f, s)$$

for $0 < \operatorname{Re} s < 1$.

Proof. The second sentence follows from Proposition 1.57.

It remains to show the last sentence. By Example 2.9, we see

$$\sum_{n \in \mathbb{Z}} f(nx) = \frac{1}{x} \sum_{n \in \mathbb{Z}} (\mathcal{F}f)(n/x)$$

for any $x > 0$. It follows that

$$\begin{aligned} I(f, s) &= \int_0^\infty \left(\sum_{n \in \mathbb{Z}} f(nx) \right) x^s \frac{dx}{x} \\ &= \int_0^\infty \left(\sum_{n \in \mathbb{Z}} (\mathcal{F}f)(n/x) \right) x^{s-1} \frac{dx}{x} \\ &= \int_0^\infty \left(\sum_{n \in \mathbb{Z}} (\mathcal{F}f)(nx) \right) x^{1-s} \frac{dx}{x} \\ &= I(\mathcal{F}f, 1 - s), \end{aligned}$$

which is what we wanted. ■

Corollary 2.11. Continue in the context of Proposition 2.10, but further assume that the (double) integrals $I(f, s)$ and $I(\mathcal{F}f, s)$ both absolutely converge for $\operatorname{Re} s > 0$. Then

$$\zeta(s)(\mathcal{M}f)(s) = (\mathcal{M}\mathcal{F}f)(1 - s)\zeta(1 - s).$$

Proof. Because the (double) integral $I(f, s)$ absolutely converges, we may use Fubini's theorem to write

$$\begin{aligned} I(f, s) &= \int_0^\infty \left(\sum_{n \in \mathbb{Z}} f(nx) \right) x^s \frac{dx}{x} \\ &= \sum_{n \in \mathbb{Z}} \left(\int_0^\infty f(nx) x^s \frac{dx}{x} \right) \\ &\stackrel{*}{=} 2 \sum_{n=1}^\infty \left(\frac{1}{n^s} \int_0^\infty f(x) x^s \frac{dx}{x} \right) \\ &= 2\zeta(s)(\mathcal{M}f)(s), \end{aligned}$$

Note at $\stackrel{*}{=}$ we have assumed that $f(0) = 0$, which holds because $S_f(x)$ converges absolutely. (Indeed, if $|f(0)| > 0$, then as $x \rightarrow 0^+$, we would have $S_f(x)$ diverge: we may say $|f(x)| > |f(0)|/2$ for $|x| < \delta$, but then the absolute sum is bounded below by $n|f(0)|/2$ at $x = \delta/n$.) To finish, we plug into the functional equation of Proposition 2.10. ■

Remark 2.12. We could spend time searching for a function f satisfying all of our various hypotheses, but we are about to show a more concrete functional equation, so there is little point.

2.2.2 Facts about Γ

In this subsection, we will collect a few facts about Γ which will be helpful shortly. We will loosely follow [Tao14, Section 1].

Definition 2.13. For $\operatorname{Re} s > 0$, we define

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

Remark 2.14. 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 2.15. Define $f: [0, \infty) \rightarrow \mathbb{R}$ by $f(t) := e^{-t}$ so that $\Gamma = \mathcal{M}f$ by definition. Notably, for any $c > 0$, the function $t \mapsto t^c f(t)$ is bounded on $[0, \infty)$ because

$$\lim_{t \rightarrow \infty} t^c f(t) = \lim_{t \rightarrow \infty} \frac{t^c}{e^t} = 0.$$

(Explicitly, find N such that $|t^c f(t)| < 1$ for any $x > N$; for $x \leq N$, note $t \mapsto t^c f(t)$ has a maximum on the compact set $[0, N]$.) Thus, f decays at a rate of (α, β) for any $0 < \alpha < \beta$, so Proposition 1.57 implies that Γ converges absolutely and is a holomorphic function on $\{s : \operatorname{Re} s > 0\}$ by taking the union over all such (α, β) .

Remark 2.15 assures us that Γ is holomorphic on $\operatorname{Re} s > 0$, but we quickly note that we can provide Γ with a meromorphic continuation to the left, at the cost of some poles.

Lemma 2.16. For any $\operatorname{Re} s > 0$, we have $\Gamma(s+1) = s\Gamma(s)$.

Proof. This is integration by parts. Indeed, we compute

$$\begin{aligned}
 \Gamma(s+1) &= \int_0^\infty e^{-t} t^s dt \\
 &= -e^{-t} t^s \Big|_0^\infty + \int_0^\infty e^{-t} s t^{s-1} dt \\
 &= 0 + s \int_0^\infty e^{-t} t^{s-1} dt \\
 &= s \Gamma(s),
 \end{aligned}$$

which is what we wanted. ■

Example 2.17. For any positive integer n , applying Lemma 2.16 inductively yields

$$\Gamma(n) = (n-1)\Gamma(n-1) = (n-1)(n-2)\Gamma(n-2) = \cdots = (n-1)\Gamma(1).$$

Notably, $\Gamma(1) = \int_0^\infty e^{-t} dt = 1$, so we see $\Gamma(n) = (n-1)!$ for any positive integer n .

Remark 2.18. We now describe how to (inductively) continue Γ using Lemma 2.16. Fix some $n \in \mathbb{N}$ and set $U_n := \{s : \operatorname{Re} s > -n, -s \notin \mathbb{Z}_{\geq 0}\}$. Then we define $\Gamma_n := U_n \rightarrow \mathbb{C}$ by

$$\Gamma_n(s) := \frac{\Gamma(s+n)}{s(s+1)(s+2)\cdots(s+n-1)}.$$

Because Γ is holomorphic on $\operatorname{Re} s > 0$, we see Γ_n is holomorphic on U_n . Further, Lemma 2.16 implies that $\Gamma_n(s) = \Gamma(s)$ for $\operatorname{Re} s > 0$, so we have indeed defined a continuation of Γ . Sending $n \rightarrow \infty$ provides our meromorphic continuation of Γ to all of \mathbb{C} .

Remark 2.18 is in some sense analogous to defining a continuation for $\zeta(s)$ to all of \mathbb{C} using the repeated integration by parts mentioned in Remark 1.39. However, just as with ζ , there is a “functional equation” for Γ which does not require the sort of inductive arguments of Remark 2.18. We begin by upgrading Lemma 2.16.

Lemma 2.19. For any $s_1, s_2 \in \mathbb{C}$ such that $\operatorname{Re} s_1, \operatorname{Re} s_2 > 0$, we have

$$\Gamma(s_1 + s_2) \int_0^1 u^{s_1-1} (1-u)^{s_2-1} du = \Gamma(s_1) \Gamma(s_2).$$

Proof. Remark 2.15 tells us that the integral defining Γ converges absolutely, so Fubini’s theorem lets us write

$$\Gamma(s_1) \Gamma(s_2) = \int_0^\infty \int_0^\infty e^{-t_1-t_2} t_1^{s_1-1} t_2^{s_2-1} dt_1 dt_2.$$

We would like to combine the t_1 and t_2 into a single t . Thus, we set $t_1 = ut$ and $t_2 = (1-u)t$ for $u \in [0, 1]$ and $t \in (0, \infty]$. More precisely, for $t_1, t_2 > 0$, we have $u = t_1/(t_2 + t_1)$ and $t = t_1 + t_2$, which makes our Jacobian

$$\det \begin{pmatrix} \partial t_1 / \partial u & \partial t_1 / \partial t \\ \partial t_2 / \partial u & \partial t_2 / \partial t \end{pmatrix} = \det \begin{pmatrix} t & u \\ -t & 1-u \end{pmatrix} = t.$$

Thus,

$$\Gamma(s_1) \Gamma(s_2) = \int_0^1 \int_0^\infty e^{-t} t^{s_1+s_2-1} u^{s_1-1} (1-u)^{s_2-1} dt du.$$

This still absolutely converges (indeed, we can just change coordinates back to $dt_1 dt_2$ to see this), so a last application of Fubini's theorem reveals

$$\Gamma(s_1)\Gamma(s_2) = \left(\int_0^1 u^{s_1-1} (1-u)^{s_2-1} du \right) \left(\int_0^1 e^{t} t^{s_1+s_2-1} dt \right) = \Gamma(s_1 + s_2) \int_0^1 u^{s_1-1} (1-u)^{s_2-1} du,$$

which is what we wanted. ■

Remark 2.20. Because $\Gamma(1) = 1$ and $\int_0^1 u^s du = \frac{1}{s+1}$ for $\operatorname{Re} s > -1$, we see Lemma 2.19 implies

$$\Gamma(s) = \Gamma(s)\Gamma(1) = \Gamma(s+1) \int_0^1 u^s du = \frac{1}{s+1} \Gamma(s+1),$$

thus recovering Lemma 2.16.

Proposition 2.21 (Functional equation for Γ). For any s with $0 < \operatorname{Re} s < 1$, we have

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

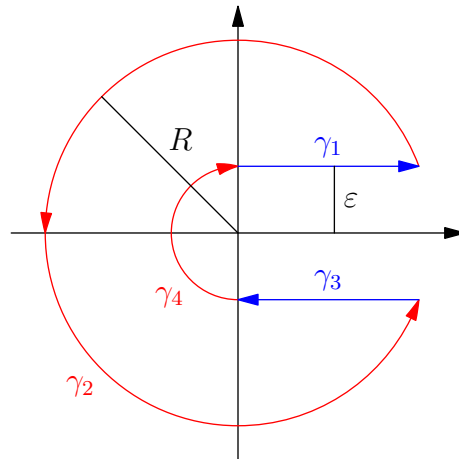
Proof. By Lemma 2.19, we see

$$\Gamma(s)\Gamma(1-s) = \Gamma(1) \int_0^1 u^{s-1} (1-u)^{-s} du = \int_0^1 (1-u) \left(\frac{u}{1-u} \right)^{s-1} du.$$

As such, we have reduced to compute some integral. This is done via contour integration. Thus, we set $t := \frac{u}{1-u} = \frac{1}{1-u} - 1$ so that $u = \frac{t}{t+1}$ and $dt = \frac{1}{(1-u)^2} du = (1+t)^2 du$, which gives

$$\Gamma(s)\Gamma(1-s) = \int_0^\infty \frac{t^{s-1}}{1+t} dt.$$

We are now ready to use contour integration. Being careful, the function $t \mapsto t^{s-1}$ is given a meromorphic continuation to $\mathbb{C} \setminus \mathbb{R}_{\geq 0}$ by $t \mapsto \exp((s-1)\log t)$, where $\log t$ has a branch cut at $\mathbb{R}_{\geq 0}$; explicitly, $\operatorname{Im}(\log t) \in [0, 2\pi)$. Now, for fixed R, ε with $R > 1 > \varepsilon > 0$, draw the following contour γ , split into four pieces.



Notably, the function $f(z) := z^{s-1}/(1+z)$ is meromorphic on $\mathbb{C} \setminus \mathbb{R}_{\geq 0}$ with a single simple pole at $z = -1$, with residue $(-1)^{s-1} = e^{\pi i(s-1)}$. Thus, the Residue theorem yields

$$\frac{1}{2\pi i} \oint_\gamma f(z) dz = e^{\pi i(s-1)} = -e^{\pi i s}$$

because $z = -1$ lies within the interior of γ . We now compute the integral $\oint_{\gamma} f(z) dz$ on each of the γ_i independently.

- For $i \in \{1, 3\}$, we compute

$$\int_{\gamma_i} f(z) dz = \int_0^R \frac{\lambda_i(t \pm \varepsilon i)^{s-1}}{1 + (t \pm \varepsilon i)} (\pm dt),$$

where $\lambda_i = 1$ (and we use $+$) if $i = 1$, and $\lambda_i = e^{2\pi i(s-1)} = e^{2\pi i s}$ (and we use $-$) if $i = 3$. Now, for each $\varepsilon \in (0, 1)$, we see

$$\left| \frac{(t \pm \varepsilon i)^{s-1}}{1 + (t \pm \varepsilon i)} \right| \leq \frac{(t+1)^{\operatorname{Re} s - 1}}{1+t},$$

and the right-hand function has finite integral over $[0, R]$ because $\operatorname{Re} s > 0$. Thus, we may apply the Dominated convergence theorem to see that sending $\varepsilon \rightarrow 0^+$ tells us that

$$\lim_{R \rightarrow \infty} \lim_{\varepsilon \rightarrow 0^+} \int_{\gamma_i} f(z) dz = \lim_{R \rightarrow \infty} \pm \lambda_i \int_0^R \frac{t^{s-1}}{1+t} dt = \pm \lambda_i \int_0^{\infty} \frac{t^{s-1}}{1+t} dt.$$

- On γ_2 , we bound

$$\left| \int_{\gamma_2} f(z) dz \right| \leq 2\pi R \cdot \max_{z \in \operatorname{im} \gamma_2} |f(z)|.$$

To compute this maximum, we use the fact that $|z| = R > 1$ to see

$$\left| \frac{z^{s-1}}{1+z} \right| \leq \frac{R^{\operatorname{Re} s - 1}}{R-1},$$

so

$$\left| \int_{\gamma_2} f(z) dz \right| \leq \frac{2\pi R^{\operatorname{Re} s}}{R-1} = \frac{2\pi R^{\operatorname{Re} s - 1}}{1 - 1/R}.$$

Sending $R \rightarrow \infty$ has this integral go to 0/1 because $\operatorname{Re} s < 1$.

- On γ_4 , we bound

$$\left| \int_{\gamma_4} f(z) dz \right| \leq \pi \varepsilon \cdot \max_{z \in \operatorname{im} \gamma_4} |f(z)|.$$

To compute this maximum, we use the fact that $|z| = \varepsilon < 1$ to see

$$\left| \frac{z^{s-1}}{1+z} \right| \leq \frac{\varepsilon^{\operatorname{Re} s - 1}}{1 - \varepsilon},$$

so

$$\left| \int_{\gamma_4} f(z) dz \right| \leq \frac{\pi \varepsilon^{\operatorname{Re} s}}{1 - \varepsilon}.$$

Sending $\varepsilon \rightarrow 0^+$ has this integral go to 0/1 because $\operatorname{Re} s > 0$.

Combining the above integrals, we see

$$-2\pi i e^{\pi i s} = \oint_{\gamma} f(z) dz = (1 - e^{2\pi i s}) \int_0^{\infty} \frac{t^{s-1}}{1+t} dt$$

upon sending $\varepsilon \rightarrow 0^+$ and then $R \rightarrow \infty$. Rearranging,

$$\Gamma(s)\Gamma(1-s) = \int_0^{\infty} \frac{t^{s-1}}{1+t} dt = \frac{-2\pi i e^{\pi i s}}{1 - e^{2\pi i s}} = \frac{\pi}{(e^{-\pi i s} - e^{\pi i s})/(2i)} = \frac{\pi}{\sin(\pi s)},$$

which is what we wanted. ■

Example 2.22. Plugging in $s = 1/2$ into Proposition 2.21, we see $\Gamma(1/2)^2 = \pi$. However, the definition of Γ surely has $\Gamma(1/2) > 0$, so we must have $\Gamma(1/2) = \sqrt{\pi}$.

Corollary 2.23. The function Γ has a meromorphic continuation to all \mathbb{C} , and Γ has no zeroes. The only poles are simple poles occurring at all nonpositive integers, and the residue of the pole at $-n$ is $(-1)^n/n!$ for each positive integer n .

Proof. For completeness, we use the functional equation to produce an analytic continuation. Let Z be the zeroes of Γ in $\{s : \operatorname{Re} s > 0\}$, which we know is an isolated set because Γ is a nonconstant holomorphic function. Now, define $U := \mathbb{C} \setminus (\mathbb{Z}_{\leq 0} \cup \{s : 1 - s \in Z\})$, and define a function $U \rightarrow \mathbb{C}$ by

$$s \mapsto \begin{cases} \Gamma(s) & \text{if } \operatorname{Re} s > 0, \\ \pi/(\Gamma(1-s)\sin(\pi s)) & \text{if } \operatorname{Re} s < 1. \end{cases}$$

Note Proposition 2.21 tells us that this function is well-defined on the overlapping region $\{s : 0 < \operatorname{Re} s < 1\}$. Thus, gluing these meromorphic functions together, we define a single meromorphic function $\Gamma : U \rightarrow \mathbb{C}$.

It remains to show the other listed properties of Γ . Note that $\Gamma(s+1) = s\Gamma(s)$ holds on $\{s : \operatorname{Re} s > 0\}$ and hence everywhere by analytic continuation. Thus, for the residue computation, we fix some nonnegative integer n and write

$$\lim_{s \rightarrow 0} s\Gamma(s-n) = \lim_{s \rightarrow 0} \frac{s\Gamma(s-n+1)}{(s-n)} = \cdots = \lim_{s \rightarrow 0} \frac{s\Gamma(s+1)}{(s-n)(s-n+1)\cdots(s-1)(s)} = \frac{\Gamma(1)}{(-1)^n n!}.$$

Thus, Γ has a pole of residue $(-1)^n/n!$ at $-n$ for each nonnegative integer n .

Lastly, we show that Γ has no zeroes. Note Γ has no zeroes on the positive integers by Example 2.17, and Γ isn't even defined on the nonpositive integers, so Γ has no zeroes on \mathbb{Z} . Additionally, we note that we surely have an analytic continuation of Γ by $\mathbb{C} \setminus \mathbb{Z}_{\leq 0}$ by Remark 2.18. Thus, we see each $s \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$ has $1-s \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$, thus giving

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)} \neq 0,$$

which forces $\Gamma(s) \neq 0$. (Note this functional equation extends from $\{s : 0 < \operatorname{Re} s < 1\}$ to all $\mathbb{C} \setminus \mathbb{Z}$ by uniqueness of analytic continuation.) ■

Remark 2.24. Corollary 2.23 tells us that $1/\Gamma(s)$ is an entire function. Indeed, the poles of Γ becomes 0s, and Γ has no zeroes to become poles!

While we're here, we give another application of Lemma 2.19.

Proposition 2.25. For any $s \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$, we have

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) = \sqrt{\pi}2^{1-s}\Gamma(s).$$

Proof. By the uniqueness of analytic continuation, it suffices to show this for $0 < \operatorname{Re} s < 1$. Now Lemma 2.19

lets us write

$$\begin{aligned}
 \frac{\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}\right)}{\Gamma(s)} &= \int_0^1 u^{s-1}(1-u)^{s-1} du \\
 &= \int_{-1}^1 \left(\frac{1+t}{2}\right)^{s/2-1} \left(\frac{1-t}{2}\right)^{s/2-1} \frac{dt}{2} \\
 &= \frac{1}{2^{s-1}} \int_{-1}^1 (1-t^2)^{s/2-1} dt \\
 &= \frac{1}{2^s} \int_0^1 (1-t^2)^{s/2-1} dt \\
 &= \frac{1}{2^{s-1}} \int_0^1 u^{1/2-1}(1-u)^{s/2-1} dt \\
 &= \frac{1}{2^{s-1}} \cdot \frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{s}{2}\right)}{\Gamma\left(\frac{s+1}{2}\right)}.
 \end{aligned}$$

By Corollary 2.23, $\Gamma(s/2) \neq 0$ for all s , so we may rearrange the above into

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) = \Gamma\left(\frac{1}{2}\right) 2^{1-s}\Gamma(s).$$

Plugging in $\Gamma(1/2) = \sqrt{\pi}$ from Example 2.22 completes the proof. ■

2.2.3 Bounds on Γ

While Γ is still fresh in our mind, we will prove a few bounds about it. We continue to roughly follow [Tao14].

2.2.4 The Functional Equation

We now return to discussing the functional equation for ζ . Being concrete, we will want to fix a particular Schwarz function $f: \mathbb{R} \rightarrow \mathbb{R}$. Staring at Corollary 2.11, we see that it will be helpful to have control over both f and $\mathcal{F}f$, so we will take $f(x) := e^{-\pi x^2}$, even this of course does not satisfy all the hypotheses. The associated function S_f has a name.

Definition 2.26 (Θ). Define the function $\Theta: (0, \infty) \rightarrow \mathbb{R}$ by

$$\Theta(t) := \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t}.$$

Remark 2.27. Note that series defining Θ converges absolutely and uniformly on any interval $[\varepsilon, 0)$ for $\varepsilon > 0$ by the Weierstrass M -test: indeed, we may upper-bound

$$\sum_{n \in \mathbb{Z}} e^{-\pi n^2 t} \leq 1 + 2 \sum_{n=1}^{\infty} e^{-\pi \varepsilon n^2} \leq 1 + 2 \sum_{n=1}^{\infty} e^{-\pi \varepsilon n} = 1 + 2 \cdot \frac{e^{-\pi \varepsilon}}{1 - e^{-\pi \varepsilon}} < \infty.$$

In particular, the uniform convergence confirms that Θ defines a continuous function $(0, \infty) \rightarrow \mathbb{R}$.

The functional equation for ζ will come from the following functional equation for Θ .

Proposition 2.28. For any $t > 0$, we have

$$\Theta(t) = \frac{1}{\sqrt{t}} \Theta\left(\frac{1}{t}\right).$$

Proof. For fixed $t > 0$, define $f(x) := e^{-\pi(\sqrt{t}x)^2}$, which is Schwarz by Lemma A.6 and Exercise A.7; in particular, $(\mathcal{F}f)(s) = \frac{1}{\sqrt{t}}f(s)$. Thus, Theorem 2.8 implies that $\Theta(t)$ converges absolutely, and

$$\Theta(t) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t} = \sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} (\mathcal{F}f)(n) = \sum_{n \in \mathbb{Z}} \frac{1}{\sqrt{t}} e^{-\pi n^2 / t} = \frac{1}{\sqrt{t}} \Theta\left(\frac{1}{t}\right),$$

which is what we wanted. ■

Remark 2.29. For $z \in \mathbb{H}$, set $q := e^{2\pi iz}$ so that $|q| < 1$. Then

$$f(z) := \sum_{n \in \mathbb{Z}} q^{n^2/2} = \sum_{n \in \mathbb{Z}} e^{\pi i n^2 z}$$

converges absolutely and satisfies $f(it) = \Theta(t)$. One can check, for example using Proposition 1.32, that f is holomorphic on \mathbb{H} . In fact, f is a modular form: note that $f(z+2) = f(z)$. Further, hitting Proposition 2.28 with the uniqueness of analytic continuation, we see that $f(-1/z) = (z/i)^{1/2} f(z)$ for $z \in \mathbb{H}$, for suitably defined square root. Thus, (with a growth condition we haven't mentioned) f is a modular form of weight $1/2$ and level

$$\left\langle \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

We next describe how ζ relates Θ . This requires us to “complete” ζ , as follows.

Definition 2.30 (ξ). For $\mathrm{Re} s > 0$, we define

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

Remark 2.31. Note ξ is meromorphic on $\{s : \mathrm{Re} s > 0\}$ with only a simple pole at $s = 1$ because $s \mapsto \pi^{-s/2} \Gamma(s/2)$ is holomorphic here (see Remark 2.15), and ζ is meromorphic with only a simple pole at $s = 1$ (see Proposition 1.37).

Remark 2.32. 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 [Tat10].

Now here is how Θ enters the picture.

Lemma 2.33. For $\mathrm{Re} s > 1$, we have

$$\xi(s) = \int_0^\infty \left(\frac{\Theta(t) - 1}{2} \right) t^{s/2} \frac{dt}{t}.$$

Proof. This argument is similar to Corollary 2.11. Note

$$\frac{\Theta(t) - 1}{2} = \sum_{n=1}^\infty e^{-\pi n^2 t}$$

for any $t > 0$, so we are looking at

$$\int_0^\infty \left(\sum_{n=1}^\infty e^{-\pi n^2 t} t^{(s-2)/2} \right) dt.$$

We would like to switch the sum and integral, so we check for absolute convergence. Well, to check absolute convergence, it's enough to check after we exchange the integral and sum, so we compute

$$\begin{aligned} \sum_{n=1}^\infty \left(\int_0^\infty \left| e^{-\pi n^2 t} t^{s/2} \cdot \frac{1}{t} \right| dt \right) &= \sum_{n=1}^\infty \left(\int_0^\infty e^{-\pi n^2 t} t^{\operatorname{Re} s/2} \frac{dt}{t} \right) \\ &= \sum_{n=1}^\infty \left(\int_0^\infty e^{-t} \left(\frac{t}{\pi n^2} \right)^{\operatorname{Re} s/2} \frac{dt}{t} \right) \\ &= \pi^{-\operatorname{Re} s/2} \sum_{n=1}^\infty \left(\frac{1}{n^{\operatorname{Re} s}} \int_0^\infty e^{-\pi t} t^{\operatorname{Re} s/2} \frac{dt}{t} \right) \\ &= \pi^{-\operatorname{Re} s/2} \zeta(\operatorname{Re} s) \Gamma(\operatorname{Re} s/2). \end{aligned}$$

Now, $\operatorname{Re} s > 1$, so all terms are finite, so we have absolute convergence. Thus, our integral converges absolutely, so we can exchange the integral and sum. Repeating the above equalities but removing the absolute value signs (and hence removing $\operatorname{Re} s$ with just s everywhere) shows

$$\int_0^\infty \left(\sum_{n=1}^\infty e^{-\pi n^2 t} t^{(s-2)/2} \right) dt = \sum_{n=1}^\infty \left(\int_0^\infty e^{-\pi n^2 t} t^{s/2} \frac{dt}{t} \right) = \pi^{-s/2} \Gamma(s/2) \zeta(s) = \xi(s)$$

for $\operatorname{Re} s > 1$, which is what we wanted. ■

We are now ready to prove our functional equation.

Theorem 2.34 (Functional equation for ξ). The function ξ has a meromorphic continuation to all \mathbb{C} , with only simple poles at $s = 1$ and $s = 0$ of residue 1 and -1 , respectively. In fact, ξ satisfies the equation

$$\xi(s) = \xi(1-s)$$

for $s \in \mathbb{C} \setminus \{0, 1\}$.

Proof. We combine Proposition 2.28 with Lemma 2.33. We proceed in steps.

1. The integral in Lemma 2.33 is poorly behaved for $\operatorname{Re} s < 1$ because of the integral over $t \in (0, 1)$, so we define

$$I(s) := \int_1^\infty \left(\frac{\Theta(t) - 1}{2} \right) t^{s/2} \frac{dt}{t}.$$

We claim that $I(s)$ defines an entire function; more precisely, we will show that $I(s)$ defines holomorphic function on $\{s : \operatorname{Re} s > \sigma\}$ for any $\sigma \in \mathbb{R}$, and taking the union over all σ will finish.

We use Proposition 1.32. For one, the function $t \mapsto \left(\frac{\Theta(t) - 1}{2} \right) t^{s/2}$ is continuous (recall Θ is continuous by Remark 2.27) and hence measurable. Lastly, we must upper-bound

$$\begin{aligned} \int_1^\infty \left| \left(\frac{\Theta(t) - 1}{2} \right) t^{s/2} \right| \frac{dt}{t} &= \frac{1}{2} \int_1^\infty \left(\sum_{n=1}^\infty e^{-\pi n^2 t} \right) t^{\sigma/2} \frac{dt}{t} \\ &\leq \frac{1}{2} \int_1^\infty \left(\sum_{n=1}^\infty e^{-\pi n t} \right) t^{\sigma/2} \frac{dt}{t} \\ &= \frac{1}{2} \int_1^\infty \frac{e^{-\pi t} t^{\sigma/2}}{1 - e^{-\pi t}} \frac{dt}{t} \\ &\leq \frac{1}{2(1 - e^{-\pi})} \int_1^\infty e^{-\pi t} t^{\sigma/2} \frac{dt}{t}. \end{aligned}$$

Thus, we take $g: (1, \infty) \rightarrow \mathbb{C}$ by $g(t) := e^{-\pi t} t^{\sigma/2-1} / (2(1 - e^{-\pi}))$. Using Proposition 1.32, it remains to show that $\int_1^\infty g(t) dt < \infty$. Well, $e^{-\pi t} t^{\sigma/2+1} \rightarrow 0$ as $t \rightarrow \infty$, so this function achieves a maximum on $[1, \infty)$,¹ which we will call M . It follows

$$\int_1^\infty g(t) dt \leq \frac{1}{2(1 - e^{-\pi})} \int_1^\infty \frac{M}{t} \frac{dt}{t} < \infty.$$

2. Having controlled the $(1, \infty)$ part of the integral in Lemma 2.33, we turn to the $(0, 1)$ part. The idea here is to use Proposition 2.28 to transform the $(0, 1)$ part back into a well-behaved $(1, \infty)$ part. Indeed, for $\operatorname{Re} s > 1$, we may evaluate

$$\begin{aligned} \int_0^1 \left(\frac{\Theta(t) - 1}{2} \right) t^{s/2} \frac{dt}{t} &= \int_1^\infty \left(\frac{\Theta(1/t) - 1}{2} \right) t^{-s/2} \frac{dt}{t} \\ &= \int_1^\infty \left(\frac{\sqrt{t}\Theta(t) - 1}{2} \right) t^{-s/2} \frac{dt}{t} \\ &= \int_1^\infty \left(\frac{\sqrt{t}\Theta(t) - \sqrt{t}}{2} \right) t^{-s/2} \frac{dt}{t} - \frac{1}{2} \int_1^\infty t^{-s/2} \frac{dt}{t} + \frac{1}{2} \int_1^\infty t^{(1-s)/2} \frac{dt}{t} \\ &= \int_1^\infty \left(\frac{\Theta(t) - 1}{2} \right) t^{(1-s)/2} \frac{dt}{t} - \int_1^\infty t^{-s} \frac{dt}{t} + \int_1^\infty t^{1-s} \frac{dt}{t} \\ &= I(1-s) - \frac{1}{s} - \frac{1}{1-s}. \end{aligned}$$

3. Synthesizing the previous steps, Lemma 2.33 grants

$$\xi(s) = I(s) + I(1-s) - \frac{1}{s} - \frac{1}{1-s}$$

on $\operatorname{Re} s > 1$. However, $I(s)$ is fully entire, so the right-hand side is a meromorphic function on \mathbb{C} with simple poles at $s = 1$ (of residue $\operatorname{Res}_{s=1} -\frac{1}{1-s} = \operatorname{Res}_{s=1} \frac{1}{s-1} = 1$) and at $s = 0$ (of residue $\operatorname{Res}_{s=1} -\frac{1}{s} = -1$). Viewing the right-hand side as our continuation of ξ completes the analysis of ξ . Lastly, the above equation tells us that

$$\xi(s) = \xi(1-s)$$

for $s \in \mathbb{C} \setminus \{0, 1\}$, which completes the proof. ■

2.2.5 Corollaries of the Functional Equation

We quickly establish the following more asymmetric version of the functional equation.

Corollary 2.35 (Functional equation for ζ). The function ζ has a meromorphic continuation to \mathbb{C} with only a simple pole at $s = 1$ of residue 1. In fact, for $s \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$, we have the functional equation

$$\zeta(1-s) = 2(2\pi)^{-s} \cos\left(\frac{\pi s}{2}\right) \Gamma(s) \zeta(s).$$

Proof. We begin by discussing the meromorphic continuation of ζ . Note Theorem 2.34 lets us continue ζ by writing

$$\zeta(s) = \frac{\xi(s)}{\pi^{-s/2} \Gamma(s/2)}$$

for any $s \in \mathbb{C} \setminus \{0, 1\}$. Notably, the denominator is never nonzero, and even though $\Gamma(s/2)$ has a simple pole at nonpositive even integers $-2n$ by Corollary 2.23 at these points $\xi(s)$ will have at worst simple pole by Theorem 2.34 as well, so we can just multiply the numerator and denominator by $(s - 2n)$ until the denominator is nonzero.

¹ Find N such that $g(t) < g(1)$ for $t < N$. Then the maximum of g is its maximum on $[1, N]$.

It remains to deal with $s \in \{0, 1\}$. At $s = 0$, we write

$$\zeta(s) = \frac{s\xi(s)}{\pi^{-s/2} \cdot s\Gamma(s/2)}$$

so that we have written $\zeta(s)$ as the quotient of holomorphic functions nonzero at $s = 0$. (Note $s \cdot \Gamma(s/2)$ has no pole and is nonzero at $s = 0$ by Corollary 2.23.) However, at $s = 1$, we already know that ζ has a simple pole of residue 1 by Proposition 1.37.

To finish the proof, we must produce the functional equation. By uniqueness of the functional equation, it suffices to focus on $0 < \operatorname{Re} s < 1$. Here, Theorem 2.34 grants

$$\pi^{-(1-s)/2} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s) = \xi(1-s) = \xi(s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s). \quad (2.2)$$

Multiplying both sides by $\Gamma\left(\frac{1+s}{2}\right)$, we see Proposition 2.21 implies

$$\Gamma\left(\frac{1+s}{2}\right) \Gamma\left(\frac{1-s}{2}\right) = \frac{\pi}{\sin\left(\pi \cdot \frac{1+s}{2}\right)} = \frac{\pi}{\cos(\pi s/2)}.$$

On the other hand, Proposition 2.25 implies

$$\Gamma\left(\frac{s}{2}\right) \Gamma\left(\frac{s+1}{2}\right) = \sqrt{\pi} 2^{1-s} \Gamma(s).$$

In total, we may rearrange (2.2) into

$$\frac{\pi^{-(1-s)/2+1} \zeta(1-s)}{\cos(\pi s/2)} = \pi^{1/2-s/2} \cdot 2^{1-s} \zeta(s),$$

which rearranges into the desired equation. ■

Example 2.36. Note

$$\zeta(0) = \lim_{s \rightarrow 1} \zeta(1-s) = \lim_{s \rightarrow 1} \left(2(2\pi)^{-s} \cdot \frac{\cos(\pi s/2)}{s-1} \cdot \Gamma(s) \cdot (s-1)\zeta(s) \right).$$

Using L'Hôpital's rule, we see $\cos(\pi s/2)/(s-1) \rightarrow -\pi/2$ as $s \rightarrow 1$. By Proposition 1.37, we see $(s-1)\zeta(s) \rightarrow 1$ as $s \rightarrow 1$. Plugging everything else in, we see $\zeta(0) = 2 \cdot (2\pi)^{-1} \cdot (\pi/2) \cdot 1 \cdot 1 = -1/2$.

This functional equation grants us some basic knowledge about the zeroes of ζ .

Corollary 2.37. We have the following.

- (a) Conjugate symmetry: if $\zeta(s) = 0$, then $\zeta(\bar{s}) = 0$.
- (b) Trivial zeroes: the function ζ is zero at $-2n$ for each positive integer n .
- (c) Critical strip: if $\zeta(s) = 0$ and $-s/2 \notin \mathbb{N}$, then $0 \leq \operatorname{Re} s \leq 1$.
- (d) Horizontal symmetry: if $\zeta(s) = 0$ and $0 \leq \operatorname{Re} s \leq 1$, then $\zeta(1-s) = 0$.

Proof. Here we go.

- (a) More generally, we claim that $\overline{\zeta(\bar{s})} = \zeta(s)$ for $s \in \mathbb{C} \setminus \{1\}$, from which the claim will follow.

Because ζ is holomorphic in this region, we see that $s \mapsto \overline{\zeta(\bar{s})}$ is also holomorphic. (Formally, we can just check that $\zeta(x+yi) = u(x+yi) + iv(x+yi)$ satisfying the Cauchy–Riemann equations implies that $u(x-yi) - iv(x-yi)$ does as well.) So by the uniqueness of analytic continuation, it suffices to check the result for $s \in \mathbb{R}_{>1}$, which is clear because ζ is real on this line, so

$$\zeta(s) = \zeta(\bar{s}) = \overline{\zeta(\bar{s})}.$$

(b) For any positive integer n , write

$$\zeta(s) = \frac{(s+2n)\xi(s)}{\pi^{-s/2} \cdot (s+2n)\Gamma(s/2)}.$$

As $s \rightarrow -2n$, the numerator vanishes because ξ is holomorphic at $s = -2n$ by Theorem 2.34. However, the denominator is finite and nonzero: $\pi^{-s/2}$ vanishes nowhere, and $\Gamma(s/2)$ has a simple pole at $s = -2n$ by Corollary 2.23 which is cancelled by the factor of $(s+2n)$. In total, we conclude

$$\zeta(-2n) = \lim_{s \rightarrow -2n} \zeta(s) = 0.$$

(c) If $\operatorname{Re} s > 1$, then $\zeta(s) \neq 0$ by Corollary 1.42 already. Thus, it remains to discuss $\operatorname{Re} s < 0$. Well, for $\operatorname{Re} s > 1$, we see

$$\zeta(1-s) = 2(2\pi)^{-s} \cos\left(\frac{\pi s}{2}\right) \Gamma(s) \zeta(s),$$

and for $\operatorname{Re} s > 1$ this right-hand side will only vanish when $\cos(\pi s/2) = 0$, which is equivalent to $s \in 2\mathbb{Z}_{\geq 0} + 1$. (Namely, $\Gamma(s)$ never vanishes by Corollary 2.23, and $\zeta(s)$ does not vanish in this region as just discussed.) Unwinding, we see that $\zeta(s) = 0$ and $\operatorname{Re} s < 0$ implies that $1-s \in 2\mathbb{Z}_{\geq 0} + 1$, which is equivalent to $s \in -2\mathbb{Z}_{\leq 0}$. This is what we wanted.

(d) Note that $\zeta(1)$ isn't defined, and $\zeta(0) \neq 0$ by Example 2.36, so we may safely ignore $s \in \{0, 1\}$. Otherwise, we stare at

$$\zeta(1-s) = 2(2\pi)^{-s} \cos\left(\frac{\pi s}{2}\right) \Gamma(s) \zeta(s),$$

which is valid on $\{s : 0 \leq \operatorname{Re} s \leq 1\} \setminus \{0, 1\}$. (In particular, Γ is holomorphic here by Corollary 2.23.) Thus, $\zeta(s) = 0$ implies $\zeta(1-s) = 0$. ■

2.3 January 30

Today we began by completing the proof of the functional equation. I have directly edited into last class's notes for continuity reasons.

2.3.1 Zeroes of ζ

We would like to understand the zeroes of $\zeta(s)$, for which we use Cauchy's formula. Roughly speaking, we will study integrals

$$\frac{1}{2\pi i} \oint_{\gamma} \frac{\zeta'(s)}{\zeta(s)} ds,$$

where γ is a contour over a very tall vertical strip in \mathbb{C} .

We will want the following bounds.

Lemma 2.38 (Stirling). We have

$$\log \Gamma(s) = \left(s - \frac{1}{2}\right) \log s + \frac{1}{2} \log 2\pi + O_{\delta}(1/|s|),$$

and

$$\frac{\Gamma'(s)}{\Gamma(s)} = \log s + O_{\delta}(1/|s|)$$

as $|s| \rightarrow \infty$ for $-\pi + \delta < \arg s < \pi - \delta$.

Proof. Omitted. ■

Remark 2.39. For $\sigma \in [a, b]$ for some fixed $a < b$, we have $\Gamma(\sigma + it) \sim e^{-\pi|t|/2} |t|^{\sigma-1/2}$ as $t \rightarrow \infty$. Again, we omit this proof.

We also want access to the Hadamard factorization theorem.

Theorem 2.40. Fix an entire function $\varphi: \mathbb{C} \rightarrow \mathbb{C}$. Let $n(r)$ denote the number of zeroes z such that $|z| < r$ and α the order of an entire function φ , one has $n(R) = O_\varepsilon(R^{\alpha+\varepsilon})$ for any $\varepsilon > 0$.

Notably, for $\operatorname{Re} s > 1/2$, one has $|s(s-1)\zeta(s)| \ll |s|^3$. Further, one can check that Γ has order 1 as an entire function, so $s(1-s)\xi(s)$ has order at most 1. Thus, Hadamard's factorization theorem enforces

$$s(1-s)\xi(s) = e^{A+Bs} \prod_{\zeta(\rho)=0} \left(\left(1 - \frac{s}{\rho}\right) e^{s/\rho} \right).$$

Notably, this product will converge absolutely. For example, absolute convergence tells us

$$\sum_{\zeta(\rho)=0} \frac{1}{|\rho|^{1+\varepsilon}} < \infty$$

for any $\varepsilon > 0$. One also has the following result on the distribution of our ρ .

Theorem 2.41. Define

$$N(T) := \#\{\rho : 0 \leq \operatorname{Re} \rho \leq 1, \operatorname{Im} \rho \geq 0, \zeta(\rho) = 0\}.$$

Then

$$N(T) = \frac{T}{2\pi} \log \left(\frac{T}{2\pi} \right) - \frac{T}{2\pi} + O(\log T)$$

as $T \rightarrow \infty$.

We will first show the following lemma.

Lemma 2.42. We have

$$\sum_{\rho} \frac{1}{1 + |\operatorname{Im} \rho - T|^2} \ll \log(T+3).$$

Proof. This is by smoothing. By taking logarithmic differentiation

$$\frac{\Xi'(s)}{\Xi(s)} = B + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right).$$

However, by using the above estimates, we see

$$\frac{\Xi'(s)}{\Xi(s)} = \frac{1}{s} - \frac{1}{1-s} - \frac{1}{2} \log \pi + \frac{1}{2} \frac{\Gamma'(s/2)}{\Gamma(s/2)} + \frac{\zeta'(s)}{\zeta(s)}$$

by definition of ξ . Now, the term ζ'/ζ is well-behaved for $\operatorname{Re} s$ large: we set $s := 2 + it$, and one can see that $|\zeta'(s)/\zeta(s)|$ is bounded by an absolute constant. Thus, we understand on the right-hand side here.

Continuing, we see

$$\operatorname{Re} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right) = \frac{2 - \operatorname{Im} s}{(2 - \operatorname{Im} s)^2 + (T - \operatorname{Im} s)^2} + \frac{\beta}{(\operatorname{Re} s + \operatorname{Im} s)^2} \gg \frac{1}{1 + |T - \operatorname{Im} s|^2}.$$

However, $\Gamma'(s)/\Gamma(s) \ll \log(T+3)$ by Stirling, so the result follows. ■

2.4 February 1

Today we move towards a proof of the explicit formula.

Notation 2.43. A sum/product over ρ is over the zeroes of $\zeta(s)$.

2.4.1 Zeroes of ζ , Again

Let's provide a few applications of Lemma 2.42.

Corollary 2.44. We have

$$\#\{\rho : \zeta(\rho) = 0, \operatorname{Im} \rho \in [T, T+1], \operatorname{Re} \rho \in (0, 1)\} = O(\log T).$$

Proof. This follows from Lemma 2.42 by separating out our zeroes into intervals. ■

We will be interested in contours γ_T which look like large vertical rectangles; namely, they are the boundary of the rectangle $[-\varepsilon, 1+\varepsilon] \times [-T, T]$. Notably, the top and bottom of the rectangle's contours will cancel out by the functional equation, so we only need to pay attention to the vertical parts of this contour.

Lemma 2.45. For $t > 3$, we have

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_{|\operatorname{Im} \rho - t| \leq 1} \frac{1}{s - \rho} + O(\log t)$$

for $\operatorname{Re} s \in [-1, 2]$.

Proof. We consider

$$\frac{\zeta'(s)}{\zeta(s)} - \frac{\zeta'(2+it)}{\zeta(2+it)}.$$

Thus, we recall

$$\frac{\Xi'(s)}{\Xi(s)} = \frac{1}{s} - \frac{1}{s-1} - \frac{1}{2} \log \pi + \frac{1}{2} \frac{\Gamma'(s/2)}{\Gamma(s/2)} + \frac{\zeta'(s)}{\zeta(s)},$$

so we can just bound everything. Notably, we can use the infinite product to bound Ξ'/Ξ and then compare everything. For example,

$$\frac{\zeta'(s)}{\zeta(s)} - \frac{\zeta'(2+it)}{\zeta(2+it)} = \sum_{\rho} \left(\frac{1}{s - \rho} - \frac{1}{2 + it - \rho} \right) + O(\log t),$$

where the $O(\log t)$ includes the trivial zeroes of ζ . Now, we notice

$$\left| \frac{1}{s - \rho} - \frac{1}{2 + it - \rho} \right| \ll \frac{1}{|\operatorname{Im} \rho - t|^2}$$

for $|\operatorname{Im} \rho - t| \geq 1$, so we can use Lemma 2.42 to absorb most terms into $O(\log t)$. In total, we see

$$\frac{\zeta'(s)}{\zeta(s)} - \frac{\zeta'(2+it)}{\zeta(2+it)} = \sum_{|\operatorname{Im} \rho - t| \leq 1} \frac{1}{s - \rho} + O(\log t),$$

and now the $2 + it$ term can also be absorbed to $O(\log t)$. ■

Remark 2.46. One can give more accurate bounding than the above, but we will not need it.

We now return to the proof of Theorem 2.41.

Proof of Theorem 2.41. Use the argument principle on Ξ on the box $[-1, 2] \times [-T, T]$. In particular, by the functional equation, it suffices to just look at the right and top edges of this box. The hope is that we can use Lemma 2.45 and the ideas in its proof to do the bounding for us. In particular, we will be working with the equation

$$\frac{\Xi'(s)}{\Xi(s)} = \frac{1}{s} - \frac{1}{1-s} - \frac{1}{2} \log \pi + \frac{1}{2} \frac{\Gamma'(s/2)}{\Gamma(s/2)} + \frac{\zeta'(s)}{\zeta(s)}.$$

Now, the main term in the argument will come from $\Gamma'(s)/\Gamma(s)$, which one can see using Stirling's asymptotics. Most of these terms are not going to matter on our contour. It turns out that the only difficulty is integrating ζ'/ζ over the line $\{a + Ti : a \in [-1, 2]\}$. Well, using the above estimates, we recall

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_{|\operatorname{Im} \rho - T| \leq 1} \frac{1}{s - \rho} + O(\log T),$$

where now the integral of the $1/(s - \rho)$ term is bounded by a constant, and the number of terms is $O(\log T)$ by Corollary 2.44, so everything is absorbed into the error term. ■

2.4.2 The Explicit Formula

Let's move towards the explicit formula. Here is our statement.

Theorem 2.47. When x is not a prime-power, we have

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2} \log(1 - x^{-2}).$$

Remark 2.48. Ignoring convergence issues, we may compute

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

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.

Here is a lemma.

Lemma 2.49. We have

$$\psi(x) - \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)} x^s ds = O(x(\log x)^2/T).$$

Proof. We first describe a heuristic. The main idea is to use contour integration, noting that

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} y^s \frac{ds}{s} = \begin{cases} 0 & \text{if } y < 1, \\ 1 & \text{if } y > 1, \end{cases} \quad (2.3)$$

where $c > 1$ and $y \in (0, \infty) \setminus \{1\}$. The proof of this is essentially complex analysis where we “complete the contour” of this vertical line either off to $-\infty$ or off to $+\infty$ depending on $y < 1$ or $y > 1$.

Now, the point is that we can write

$$\psi(x) = \sum_{n \leq x} \Lambda(n) \approx \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)} x^s \frac{ds}{s},$$

where we have ignored convergence issues to exchange the Dirichlet series for ζ'/ζ with this integral. The point now is that we can integrate ζ'/ζ appropriately to give the formula.

To make this more rigorous, we need to do only finite computations. Thus, we define

$$I(y, T) := \frac{1}{2\pi i} \int_{c-iT}^{c+iT} y^s \frac{ds}{s}.$$

We now note that our extra variable c will be later set to $1 + 1/\log T$, so it is important to have this degree of freedom. Now, the proof of (2.3) grants

$$|I(y, T) - 1_{>1}(y)| \ll y^c \min\{1, 1/|T \log y|\},$$

where the implied constant is absolute. Integrating over this, we see

$$\left| \psi(x) - \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)} x^s ds \right| \leq \left(\sum_{n=1}^{\infty} \Lambda(n) (x/n)^c \min \left\{ 1, \frac{1}{|T \log(x/n)|} \right\} \right).$$

Now, setting $c = 1 + 1/\log T$, we get an upper-bound of $O(x(\log x)^2/T)$. Roughly speaking, we note that x away from particular n are small; however, when n is close to x , we can explicitly evaluate the logarithm as about $1/(n-x)$, and there the sum is roughly harmonic and thus grants a logarithmic growth. ■

2.5 February 3

Last time we were in the middle of the proof of the explicit formula. I have edited directly into yesterday's notes for continuity reasons.

2.5.1 The Explicit Formula, Continued

We now do a contour shift on the integral

$$\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)} x^s ds.$$

Roughly speaking, we will expand our box to look like $[-U, c] \times [-T, T]$, sending $U \rightarrow \infty$ for fixed T . We will then send $T \rightarrow \infty$, always remembering to choose T avoiding zeroes of $\zeta(s)$. In particular, by Corollary 2.44, we can be at least $1/\log T$ away from any particular zeroes. We will finish the proof next lecture.

On this contour, the point is that $|x^s| \leq x^{\operatorname{Re} s}$, so for most of this contour, we don't have to care. For example, it will be enough to only care about $\operatorname{Re} s > -1$. By the functional equation, it's enough to just look at the integral from $c + iT$ to $-1 + iT$. To bound the size here, we change T so that $\operatorname{Im} s = T$ is at most $\gg 1/\log T$ away from zeroes. Now, to bound, we see

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{|\operatorname{Im} \rho - T| \leq 1} \underbrace{\frac{1}{s - \rho}}_{O(\log T)} + O(\log T)$$

for, say, $-1 \leq \sigma \leq 2$. Thus, the contribution of the integral over $-1 \leq \sigma \leq c$ is given by

$$O\left((\log T)^2 \int_{-1}^c \frac{x^{\sigma+iT}}{|\sigma+iT|} d\sigma\right) = O\left(\frac{x(\log T)^2}{T}\right),$$

so this also goes to 0 as $T \rightarrow \infty$.

Remark 2.50. It is helpful for computations to have the functional equation

$$\zeta(1-s) = 2^{1-s} \pi^{-s} \cos(\pi s/2) \Gamma(s) \zeta(s),$$

where we have notably used the reflection formula for Γ .

As such, the value of ζ'/ζ on $\{s : \operatorname{Re} s \leq -1\}$ is bounded by

$$\left| \frac{\zeta'(s)}{\zeta(s)} \right| \ll \log |s| + 1,$$

where s avoids circle of radius $1/2$ around the zeroes (including the trivial ones). (Note because the trivial zeroes only occur at the negative even integers, we can indeed choose U at odd integers to be okay here.)

We now report the bounds on the other parts of the contour, for completeness. Indeed, the entire contribution for $\operatorname{Re} s \leq -1$ is given by

$$O\left(\frac{x(\log T)^2}{T}\right),$$

where U is a very large odd positive integer. Thus, we use residue calculus to see

$$\psi(x) = x - \sum_{|\operatorname{Im} s| \leq T} \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2} \log(1-x^{-s}) + O\left(\frac{x \log(xT)^2}{T}\right),$$

where x is not a prime power. Note the contributions of $-\frac{1}{2} \log(1-x^{-s})$ are coming from the trivial zeroes of ζ . This completes the proof.

2.5.2 A Zero-Free Region

We are going to construct a zero-free region slightly to the left of (and including) $\operatorname{Re} s = 1$. In some sense, the explicit formula tells us that the Prime number theorem is equivalent to requiring $\zeta(1+it) \neq 0$ for $t \in \mathbb{R}$, where the point of the zero-free region is to control the nontrivial zeroes in the explicit formula.

We are going to use positivity to create our zero-free region. We begin with a slick but weak proof.

Proposition 2.51. Fix some $t_0 \in \mathbb{R}$ and $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$. Defining $\sigma_z(n) := \sum_{d|n} d^z$, we have

$$\sum_{n=1}^{\infty} \frac{|\sigma_{it_0}(n)|^2}{n^s} = \frac{\zeta(s)^2 \zeta(s+it_0) \zeta(s-it_0)}{\zeta(2s)}$$

Proof. Direct expansion with Euler factors. ■

The point is that we can provide a meromorphic continuation of this function to $s \in \mathbb{C}$, whose power we can plug into the following result.

Lemma 2.52 (Landau). Let $\{a_n\}_{n \in \mathbb{N}}$ be a sequence of nonnegative real numbers, and define

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

Further, let $\sigma_0 \in \mathbb{R}$ be the smallest real numbers such that D absolutely converges on $\operatorname{Re} s > \sigma_0$. Then D does not extend to an analytic function past σ_0 .

Proof. This is just complex analysis, so we omit it. ■

Thus, if we can find t_0 such that $\zeta(1 + it_0) = 0$, then we also have a zero at $\zeta(1 - it_0)$, so in fact the function

$$\frac{\zeta(s)^2 \zeta(s + it_0) \zeta(s - it_0)}{\zeta(2s)}$$

is analytic on $\operatorname{Re} s > 1/2$ and is zero at $1/2$. But this is an obvious contradiction because the series must absolutely converge by Lemma 2.52, but we cannot vanish at $s = 1/2$ by just staring at it. Thus, we could not actually have continued it any further.

Remark 2.53. Essentially the same proof can show that $L(s, \chi)\zeta(s)$ does not vanish at $s = 0$, provided we give $L(s, \chi)$ an analytic continuation. We will do this later.

2.6 February 6

Today we construct our zero-free region for ζ .

2.6.1 A General Lemma

The above zero-free region is technically enough to prove the Prime number theorem, but to get an error term, we will want to do better. As such, we pick up the following lemma.

Lemma 2.54. Let $\{a_n\}_{n \in \mathbb{N}}$ be a sequence of nonnegative real numbers, and define

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

Suppose D satisfies the following conditions.

- $D(s)$ converges absolutely on $\operatorname{Re} s > 1$.
- $D(s)$ has a pole of order $m > 0$ at $s = 1$.
- We can define

$$\Xi(s) := (s(1-s))^m D^s \left(\prod_{i=1}^{\ell} \Gamma_{\mathbb{R}}(s + \alpha_j) \right) D(s)$$

for some D and m . Here, $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2} \Gamma(s/2)$. Then $\Xi(s)$ is entire, order 1, and satisfies $\Xi(s) = \Xi(1-s)$.

Then D has at most m zeroes in $(1 - c(\ell, m)/\log M, 1) \subseteq \mathbb{R}$, where $M := (D + 1) \prod_{i=1}^{\ell} (|\alpha_i| + 1)$ is the “analytic conductor,” and $c(\ell, m)$ is a constant computable from ℓ and m .

Remark 2.55. More complex L -functions might have “complex” Γ -factors $\Gamma_{\mathbb{C}}$. Roughly speaking, such factors arise from taking the Mellin transform of a Gaussian, so over \mathbb{R} we get $\Gamma_{\mathbb{R}}$, but over \mathbb{C} we will get something a little different. For details, see [Tat10].

It might look concerning that Lemma 2.54 only gives us an interval in the real numbers, but we can more carefully select our $D(s)$ to get a more comprehensive region.

Example 2.56. Given some $t_0 \in \mathbb{R}$, set

$$D(s) := \zeta(s)^3 \zeta(s + it_0)^2 \zeta(s - it_0)^2 \zeta(s + 2it_0) \zeta(s - it_0).$$

Some trigonometry shows that $D(s)$ has nonnegative coefficients. Then one can use Lemma 2.54 on $D(s)$: note $m = 3$, $\ell = 9$, so $M \ll \log(|t_0| + 1)$, meaning that we have at most 3 zeroes in the interval $(1 - c/\log(|t_0| + 1), 1)$ for some computable constant c . However, given $\beta \in (1 - c/\log(|t_0| + 1), 1)$, if $\zeta(\beta + it_0) = 0$, then $\zeta(\beta - it_0) = 0$ as well, so D actually gets four zeroes, which is contradiction. In particular, we get a zero-free region which looks like

$$\left\{ s = \sigma + it : \sigma > 1 - \frac{c}{\log(|t| + 1)} \right\}.$$

Remark 2.57. The magical $D(s)$ from Example 2.56 does come from a larger structure, but it is somewhat advanced to explain.

Remark 2.58. It might look upsetting that Example 2.56 does not achieve a full zero-free region of the form $\{s : \operatorname{Re} s > c\}$ for some $c > 0$, but the proof of such a region is not known.

Now that we care about Lemma 2.54, let's prove it.

Proof of Lemma 2.54. Note $\Xi(0) \neq 0$ by the functional equation. Now, factoring, we see

$$\Xi(s) = e^{A+Bs} \prod_{\Xi(\rho)=0} \left(1 - \frac{s}{\rho}\right) e^{s/\rho}.$$

Taking the logarithmic derivative, we see

$$\frac{\Xi'(s)}{\Xi(s)} = B + \sum_{\Xi(\rho)=0} \left(\frac{1}{s - \rho} + \frac{1}{\rho} \right).$$

As an intermediate step, we claim

$$\operatorname{Re} B = - \sum_{\Xi(\rho)=0} \operatorname{Re}(1/\rho).$$

Note that summing over these zeroes in conjugate pairs will give us absolute convergence. Anyway, this follows from the functional equation: note $\Xi(s) = \Xi(1 - s)$ grants

$$B + \sum_{\Xi(\rho)=0} \left(\frac{1}{1 - s - \rho} + \frac{1}{\rho} \right) = -B - \sum_{\Xi(\rho)=0} \left(\frac{1}{s - \rho} + \frac{1}{\rho} \right).$$

The zeroes are symmetric by the functional equation, so the contribution given by $1/(1 - s - \rho) = -1/(s - (1 - \rho))$ and $1/(s - \rho)$ will cancel. This completes the proof of the claim.

As such, the product definition of Ξ allows us to expand

$$\sum_{\Xi(\rho)=0} \frac{1}{s - \rho} = \frac{m}{s} + \frac{m}{s - 1} + \frac{G'(s)}{G(s)} + \frac{D'(s)}{D(s)},$$

where

$$G(s) := D^s \left(\prod_{i=1}^{\ell} \Gamma_{\mathbb{R}}(s + \alpha_j) \right).$$

Now, for $s > 1$, we know $D'(s)/D(s) < 0$ by hypothesis on $D(s)$. As such, we are now in good shape because we more or less understand everything on our right-hand side, so we can translate it into knowledge about Ξ . In particular, we can show

$$\sum_{\Xi(\rho)=0} \frac{1}{s-\rho} \leq \frac{m}{s-1} + \frac{m}{s} + C_1 \log M,$$

where C_1 is some constant depending on ℓ and m . In particular, if we send $s \rightarrow 1^+$ and have too many zeroes of Ξ close to 1, then the left-hand side should explode while the right-hand side grows slower.

As such, let

$$R_c := \{\rho \in (1 - c/\log M) : \Xi(\rho) = 0\},$$

where $c > 0$ is some constant we will fix later. We see

$$\sum_{\rho \in R_c} \frac{m}{s-\rho} \leq \frac{m}{s-1} + C_2 \log M$$

as $s \rightarrow 1^+$, for some perhaps different constant C_2 . As such, for some $\delta > 0$ we will fix later, we set $s := 1 + \delta/\log M$ so that

$$\sum_{\rho \in R_c} \frac{1}{c + \delta} \leq \frac{m}{\delta} + C_2$$

after cancelling out C_2 . But taking, say, $c < 1/(100mC_2)$ and $\delta < 1/2C_2$ will enforce $\#R_c < m + 1$, which is what we wanted. ■

2.6.2 The Prime Number Theorem, Finally

We are now ready to prove the Prime number theorem.

Theorem 2.5 (Prime number). We have $\pi(x) \sim x/\log x$ as $x \rightarrow \infty$.

Proof. We show $\psi(x) \sim x$, which is one of our equivalent formulations; we use the explicit formula. Namely, taking $T > 3$, we recall

$$\psi(x) = x - \sum_{|\operatorname{Im} \rho| \leq T} \frac{x^\rho}{\rho} + O(1) + O\left(\frac{x(\log T)^2}{T}\right).$$

However, we can upper-bound

$$\left| \sum_{|\operatorname{Im} \rho| \leq T} \frac{x^\rho}{\rho} \right| \leq \sum_{|\operatorname{Im} \rho| \leq T} \frac{x^\rho}{|\rho|} \leq x \sum_{|\operatorname{Im} \rho| \leq T} \frac{x^{-c/\log(|t|+1)}}{|\rho|} \ll x^{1-c/\log T} (\log T)^2.$$

Here, this last inequality follows from “dyadic decomposition.” Note that the number of terms is $\ll T \log T$; then decomposing \mathbb{R}^+ into $\bigcup_{k \in \mathbb{Z}} (2^k, 2^{k+1}]$, the number of roots here is $\ll 2^k k$, so we get that our sum is bounded by

$$\sum_{\substack{k \geq 0 \\ 2^k \leq T}} 2^{-k} \cdot 2^k k + O(1) \ll (\log T)^2.$$

Now, taking $T = e^{c\sqrt{\log x}}$ gets a bound $|\psi(x) - x| \ll x \exp(-c\sqrt{\log x})$, which is enough. ■

2.7 February 8

We began class by proving the Prime number theorem. I have edited directly into those notes for continuity.

2.7.1 Quadratic Residue Speedrun

Fix a prime p , for simplicity. Let $\chi \pmod{p}$ be a Dirichlet character. Our goal is to prove an analytic continuation and functional equation for $L(s, \chi)$.

Proposition 2.59. Fix a prime p . Then \mathbb{F}_p^\times is cyclic.

Proof. Standard. ■

Corollary 2.60. Fix a prime p and some $d \in \mathbb{Z}^+$.

- (a) If $\gcd(d, p-1) = 1$, then the function $\mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times$ defined by $x \mapsto x^d$ is an isomorphism.
- (b) If $d \mid p-1$, then each $a \in \mathbb{F}_p^\times$ makes $x^d \equiv a \pmod{p}$ with either 0 or d solutions.

Proof. Here we go.

- (a) Let g be a generator of \mathbb{F}_p^\times . Then g^d is also a generator and lives in the image of the map.
- (b) The map $x \mapsto x^d$ has kernel of size d . Thus, any element of the image has d solutions to the equation; otherwise there are no solutions. ■

This motivates the Legendre symbol.

Definition 2.61 (quadratic residue). Fix an odd prime p . And some $a \in \mathbb{Z}$ not divisible by p .

- If $x^2 \equiv a \pmod{p}$ has a solution, then a is a *quadratic residue*.
- If $x^2 \equiv a \pmod{p}$ does not have a solution, then a is a *nonquadratic residue*.

We will be silent about the case of $p \mid a$.

Definition 2.62. Fix an odd prime p and some $a \in \mathbb{Z}$. Then we define the *Legendre symbol* by

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue,} \\ -1 & \text{if } a \text{ is a nonquadratic residue.} \end{cases}$$

Proposition 2.63 (Euler's criterion). Fix an odd prime p . For any $a \in \mathbb{Z}$, we have

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Proof. If $a \equiv 0 \pmod{p}$, there is nothing to say. If $a \equiv x^2 \pmod{p}$ for some x , then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1$. Lastly, if a is a nonquadratic residue, then we see

$$\left(a^{(p-1)/2} - 1\right) \left(a^{(p-1)/2} + 1\right) \equiv 0 \pmod{p},$$

but $x^{(p-1)/2} \equiv 1 \pmod{p}$ has already been granted $(p-1)/2$ roots as the quadratic residues, so we must instead have $a^{(p-1)/2} \equiv -1 \pmod{p}$. ■

Corollary 2.64. Fix an odd prime p . Then $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod{4}$, and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv -1 \pmod{4}$.

Proof. Use Proposition 2.63. ■

Remark 2.65. Note that $\left(\frac{\bullet}{p}\right)$ is the unique non-principal real character \pmod{p} . One can see this because the characters $\mathbb{F}_p^\times \rightarrow \{\pm 1\}$ must have order 2, so we are looking for elements of order 2 in $\widehat{\mathbb{F}_p^\times} \cong \mathbb{F}_p^\times$. But \mathbb{F}_p^\times has only one element of order 2, so we know we have found the only such real non-principal character.

Remark 2.66. More generally studying when $f(x) \equiv 0 \pmod{p}$ has solutions (and how it factors) has connections directly with the Langlands program and similar. We will not say more because this is (very) far outside the scope of the course.

2.7.2 Gauss Sums

We mentioned in Remark 2.14 that Γ is more or less a continuous version of a Gauss sum: it's some kind of multiplicative Fourier transform of an additive character. Well, here are the usual Gauss sums.

Definition 2.67 (Gauss sum). Fix a prime p and integer m . Then the *Gauss sum* is

$$\tau(\chi, m) := \sum_{n \in \mathbb{F}_p^\times} e\left(\frac{nm}{p}\right) \chi(n).$$

Namely, $\psi_m: n \mapsto e\left(\frac{nm}{p}\right)$ is our additive character, our measure is the counting measure, so we are indeed just looking at the multiplicative Fourier transform of an additive character.

Let's show a few basic facts.

Lemma 2.68. Fix a prime p and integer m . Then for a nontrivial character χ , we have

$$\tau(\chi, m) = \bar{\chi}(m) \tau(\chi, 1).$$

Proof. This is just a change of variables. ■

Lemma 2.69. Fix a prime p . Then $|\tau(\chi, 1)|^2 = p$.

Proof. This is essentially the Plancherel formula. Namely, we see

$$\begin{aligned} (p-1)|\tau(\chi, 1)|^2 &= \sum_{m=0}^{p-1} |\tau(\chi, m)|^2 \\ &= \sum_{k, \ell \in \mathbb{F}_p^\times} \left(\chi(k) \bar{\chi}(\ell) \sum_{m=0}^{p-1} e\left(\frac{m(k-\ell)}{p}\right) \right) \\ &= p \sum_{k \in \mathbb{F}_p^\times} |\chi(k)|^2 \\ &= p(p-1), \end{aligned}$$

where we have used Corollary 1.25. ■

2.8 February 10

We continue discussing applications of the Gauss sum.

2.8.1 The Pólya–Vinogradov Inequality

As an aside, we set up the Pólya–Vinogradov inequality.

Theorem 2.70 (Pólya–Vinogradov inequality). Fix a prime p and a nontrivial character $\chi \pmod{p}$. Then for any a, b , we have

$$\left| \sum_{a \leq n \leq b} \chi(n) \right| \ll \sqrt{p} \log p,$$

where the implicit constant does not depend on anything.

Proof. Roughly speaking, we are computing the inner product of χ and the indicator function of an interval. Using “Plancherel’s formula” to bound completes the proof. The trick here is to “complete the sum.” Because $\sum_{n=0}^{p-1} \chi(n) = 0$, we may assume that $a, b \leq p$. (If shifting yields $a \leq p \leq b \leq p + a$, then we can flip the entire sum to make it $b - p \leq p - a \leq p$.)

Now, the main point is to take the Fourier transform

$$\widehat{1_{[a,b]}}(m) = \sum_{a \leq n \leq b} e\left(-\frac{mn}{p}\right) \ll \frac{p}{m},$$

where we have expanded out the geometric series to get this bound; namely, we are noting $\frac{1}{1-e(-1/p)} \approx p$. As such, we use the Fourier inversion formula Corollary 1.25 to see

$$\left| \sum_{x \in \mathbb{F}_p} 1_{[a,b]}(x) \chi(x) \right| = \frac{1}{p} \left| \sum_{m, x \in \mathbb{F}_p} \widehat{1_{[a,b]}}(m) e\left(\frac{mx}{p}\right) \chi(x) \right|.$$

Now, by Lemma 2.69, this is bounded above by

$$\frac{1}{p} \sum_{m=1}^{p-1} \widehat{1_{[a,b]}} \sqrt{p} \ll \frac{1}{\sqrt{p}} \cdot \sqrt{p} \sum_{m=1}^{p-1} \frac{1}{m} \ll \sqrt{p} \log p.$$

(Notably, the $m = 0$ term provides no contribution.) This completes the proof. ■

Corollary 2.71. The least nonquadratic residue is $O(\sqrt{x} \log x)$.

Proof. This is direct from Theorem 2.70. ■

Remark 2.72. For “short” intervals, one can do better, which is the point of the Burgess bound.

2.8.2 A Functional Equation for $L(s, \chi)$

Fix a prime p . Given a Dirichlet character $\chi \pmod{p}$, we would like to provide a functional equation akin to Theorem 2.34. Roughly speaking, there will be three cases.

- χ could be the trivial character χ_0 .
- χ could be the (unique) nontrivial real quadratic character $\left(\frac{\cdot}{p}\right)$.
- χ could be a complex character satisfying $\chi \neq \bar{\chi}$.

We separate out these cases because it turns out that our knowledge of the second case is the worst.

Remark 2.73. Note that the case of $\chi = \chi_0$ is essentially just ζ with a few Euler factors, so its functional equation can be derived directly from Theorem 2.34.

In light of Remark 2.73, we will focus on the case of $\chi \neq \chi_0$. Now, for $\alpha \in \mathbb{R}$, an argument similar to Example 2.9 yields

$$\sum_{n \in \mathbb{Z}} e^{-\pi(n+\alpha)^2/x} = x^{1/2} \sum_{n \in \mathbb{Z}} e^{-\pi n^2 x + 2\pi i n \alpha}.$$

In particular, taking $\alpha = m/p$ for $m \in \mathbb{Z}$ grants

$$\sum_{n \in \mathbb{Z}} e^{-\pi(n+m/p)^2/x} = \left(\frac{x}{p}\right)^{1/2} \sum_{n \in \mathbb{Z}} e^{-\pi n^2 x/p + 2\pi i n m/p}.$$

To continue, we will work with $\chi(-1) = 1$.² Here, we set

$$\Theta_\chi(x) := \sum_{n \in \mathbb{Z}} \chi(n) e^{-\pi n^2 x/p}.$$

Roughly speaking, in the case where $\chi(-1) = -1$, this sum would completely vanish, so we would have to add a factor of n or similar to make this summation behave. We will not say more about this case.

Using Corollary 1.25, we see

$$\begin{aligned} \Theta_\chi(x) &= \sum_{n \in \mathbb{Z}} \frac{1}{\tau(\bar{\chi}, 1)} \left(\sum_{m=0}^{p-1} \bar{\chi}(m) \right) e^{mn/p} e^{-\pi n^2 x/p} \\ &= \frac{1}{\tau(\bar{\chi}, 1)} \sum_{m=0}^{p-1} \chi(m) \sum_{n \in \mathbb{Z}} e^{2\pi i m n/p - \pi n^2 x/p} \\ &\stackrel{*}{=} \frac{1}{\tau(\bar{\chi}, 1)} \cdot \left(\frac{x}{p}\right)^{1/2} \sum_{m=0}^{p-1} \chi(m) \sum_{n \in \mathbb{Z}} e^{-\pi(n+m/p)^2 p/x} \\ &= \frac{1}{\tau(\bar{\chi}, 1)} \cdot \left(\frac{x}{p}\right)^{1/2} \sum_{m=0}^{p-1} \chi(m) \sum_{n \in \mathbb{Z}} e^{-\pi(pn+m)^2/(px)}, \end{aligned}$$

where we have applied Poisson summation at $\stackrel{*}{=}$. Now, the summations loop over all residue classes in $pn + m$, so we see

$$\Theta_\chi(x) = \frac{1}{\tau(\bar{\chi}, 1)} \cdot \left(\frac{x}{p}\right)^{1/2} \sum_{t \in \mathbb{Z}} \chi(t) e^{-\pi t^2/(px)} = \frac{1}{\tau(\bar{\chi}, 1)} \cdot \left(\frac{x}{p}\right)^{1/2} \Theta_{\bar{\chi}}(1/x),$$

where we are also using the fact that χ is periodic \pmod{p} .

² This is called the “unramified at ∞ case” because the place here at infinity is totally real.

Now, to find our functional equation, we write

$$\Xi_\chi(s) := p^{s/2} \pi^{-s/2} \Gamma(s/2) L(s, \chi).$$

Here, the factor of p roughly comes from some kind of conductor, and the $\pi^{-s/2} \Gamma(s/2)$ is our real Γ -factor. In particular, our functional equation will turn out to be the following result.

Theorem 2.74 (Functional equation for Ξ_χ). Fix a nontrivial Dirichlet character $\chi \pmod{p}$ such that $\chi(-1) = -1$. Then $\Xi_\chi(s)$ is entire and satisfies the functional equation

$$\Xi_\chi(s) = \varepsilon(\bar{\chi}) \Xi_{\bar{\chi}}(1-s),$$

where $\varepsilon_\chi := \sqrt{q}/\tau(\chi)$.

Proof. We follow the proof of Theorem 2.34. One can compute the integral

$$\Gamma(s/2) (p/\pi)^{s/2} n^{-s} = \int_0^\infty e^{-\pi n^2 x/p} x^{s/2} \frac{dx}{x}$$

for $\operatorname{Re} s > 1$. Summing, we see

$$\Xi_\chi(s) = \frac{1}{2} \int_0^\infty \Theta_\chi(x) x^{s/2} \frac{dx}{x}.$$

At this point, one can see directly that this right-hand side is entire for all $s \in \mathbb{C}$: indeed, $\Theta_\chi(x)$ rapidly decays at both 0 and ∞ , so its Mellin transform is safe for all $s \in \mathbb{C}$. Thus, we already see that Ξ_χ is entire. In particular, this equality now holds for all $s \in \mathbb{C}$.

Anyway, applying the usual variable change $x \mapsto 1/x$, we see

$$\begin{aligned} \Xi_\chi(s) &= \frac{1}{2} \int_0^\infty \Theta_\chi(1/x) x^{-s/2} \frac{dx}{x} \\ &= \frac{1}{2} \int_0^\infty \left(\frac{p^{1/2}}{\tau(\bar{\chi})} \Theta_{\bar{\chi}}(x) \right) x^{-s/2} \frac{dx}{x}, \end{aligned}$$

where we have used the functional equation for Θ_χ at the last equality. Upon using the analytic continuation for $\Xi_{\bar{\chi}}$ provided by the previous paragraph, we get

$$\Xi_\chi(s) = \varepsilon_{\bar{\chi}} \Xi_{\bar{\chi}}(1-s).$$

This completes the proof. ■

Remark 2.75. The element ε_χ in the functional equation is called “the root number.” There is a wealth of research trying to understand their behavior.

Remark 2.76. We omit the case of $\chi(-1) = -1$.

2.9 February 13

Today we conclude discussing the functional equation for $L(s, \chi)$.

2.9.1 All Functional Equations

We will want to state our functional equation for primitive Dirichlet characters, so here is the definition of primitive characters.

Definition 2.77 (primitive). A Dirichlet character $\chi \pmod{q}$ is *primitive* if and only if $\chi: (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ has no smaller period than q .

Remark 2.78. In more general contexts, q is called the “conductor” of χ .

Here is our statement.

Theorem 2.79. Fix a primitive Dirichlet character $\chi \pmod{q}$ for $q > 1$. Then set $a_\chi := \frac{1}{2}(1 - \chi(-1)) \in \{0, 1\}$, and define

$$\Xi_\chi(s) := \left(\frac{q}{\pi}\right)^{(s+a)/2} \Gamma\left(\frac{s+a}{2}\right) L(s, \chi).$$

Then Ξ_χ is entire and satisfies the functional equation

$$\Xi_\chi(s) = \varepsilon_\chi \Xi_{\bar{\chi}}(1-s),$$

where $\varepsilon_\chi := i^a q^{1/2} / \tau(\chi)$, where $\tau(\bar{\chi})$ is a Gauss sum.

Proof. Omitted. ■

We should probably say a few words about these more general Gauss sums.

Lemma 2.80. Fix a primitive Dirichlet character $\chi \pmod{q}$. Then $\tau(\chi, m) = \bar{\chi}(m) \tau(\chi, 1)$.

Proof. If $\gcd(m, q) = 1$, then the same proof from earlier goes through, so we may assume that $\gcd(m, q) > 1$. Further, if $q \mid m$, then everything vanishes, so we may assume that $q \nmid m$.

In this case, we would like to show that $\tau(\chi, m) = 0$, or in other words,

$$\sum_{k=0}^{q-1} \chi(k) e\left(\frac{mk}{q}\right) \stackrel{?}{=} 0.$$

For this, we must use the fact that χ is primitive. Now, take $d := \gcd(m, q)$ and $m' := m/d$ and $q' := q/d$ so that $\gcd(m', q') = 1$. As such, we compute

$$\begin{aligned} \tau(\chi, m) &= \sum_{k=0}^{q-1} \chi(k) e\left(\frac{m}{k} q\right) \\ &= \sum_{k=0}^{q'-1} \sum_{r=0}^{d-1} \chi(kq' + r) e\left(\frac{m'(kq' + r)}{q'}\right) \\ &= \sum_{r=0}^{d-1} \left(e\left(\frac{m'r}{q'}\right) \sum_{k=0}^{q'-1} \chi(kq' + r) \right). \end{aligned}$$

Because χ is primitive, $\chi \pmod{q'}$ is not periodic, so we can find $r_1 \equiv r_2 \pmod{q'}$ such that $\chi(r_1)$ and $\chi(r_2)$ are nonzero and not equal. It follows from the above expression that

$$\chi(r_1) \tau(\chi, m) = \chi(r_2) \tau(\chi, m)$$

by taking and then re-indexing the sums over r in our last summation.

Alternatively, if $\chi(tq' + 1) = 1$ for all $t \in \mathbb{Z}$, then it actually follows that χ is periodic $(\bmod q')$, which is a contradiction, so it is enough to check that

$$\tau(\chi, m) = \chi(tq' + 1)\tau(\chi, m)$$

for all t by again just re-indexing the relevant sum. ■

Lemma 2.81. Fix a primitive Dirichlet character $\chi \pmod{q}$. Then $|\tau(\chi)|^2 = \sqrt{q}$.

Proof. Again sum over the $\tau(\chi, m)$ as in Lemma 2.69. ■

The rest of the proof of Theorem 2.79 now follows exactly as we proceeded last class.

2.9.2 A Zero-Free Region for Complex Characters

We continue to let $\chi \pmod{q}$ be a primitive character.

Remark 2.82. When $\chi \pmod{q}$ is not primitive, then $L(s, \chi)$ is equal, up to a few Euler factors, to some $L(s, \chi')$, where χ' has smaller modulus. These finite Euler factors do not affect our zero-free region.

Example 2.83. Fix

$$D(s) := \zeta(s)^3 L(s, \chi)^2 L(s, \bar{\chi})^2 L(s, \chi^2) L(s, \bar{\chi}^2).$$

When χ is a complex character, one can check that this has nonnegative real coefficients, so Lemma 2.54 goes through and grants us a zero-free region using the same argument we used for ζ . Namely, we still get a zero-free region which looks like

$$\left\{ \sigma + it : \sigma > 1 - \frac{c}{\log |q|(|t| + 2)} \right\},$$

where c is some fixed constant. In particular, we get a smaller zero-free region for larger q .

2.9.3 The Quadratic Gauss Sum

We take a moment to evaluate some Gauss sums.

Lemma 2.84. Fix a prime p . Then

$$\tau := \sum_{k=1}^{p-1} \left(\frac{k}{p} \right) e \left(\frac{k}{p} \right) = \sum_{k=0}^{p-1} e \left(\frac{k^2}{p} \right).$$

Proof. Quickly, note that $\sum_{k=0}^{p-1} e(k/p) = 0$, so we can add this to our original sum to see

$$\tau = \sum_{k=0}^{p-1} e \left(\frac{k^2}{p} \right)$$

by counting the number of times quadratic and nonquadratic residues appear. Explicitly, $k^2 = 0$ happens once, k^2 hits quadratic residues twice, and k^2 hits nonquadratic residues zero times; this exactly matches $1 + \left(\frac{a}{p} \right)$. ■

The benefit of Lemma 2.84 is that we can use this as our “definition” of the Gauss sum, namely remove the hypothesis that p is prime.

Proposition 2.85. Fix some odd integer q . Then

$$\sum_{r=0}^{q-1} e\left(\frac{r^2}{q}\right) = \frac{1-i^q}{1-i} \cdot \sqrt{q}.$$

Proof. We will use Poisson summation; the point is to turn our Gauss sum into an infinite sum by adding some dampening factor. As such, define $f(t) := \Theta(t/\sqrt{\pi})$ so that Proposition 2.28 tells us that

$$f(t) = \left(\frac{\pi}{t}\right)^{1/2} f\left(\frac{\pi^2}{t}\right) \quad (2.4)$$

for $t > 0$. Everything here is holomorphic on $\operatorname{Re} s > 0$, so we can extend this identity to work for $\operatorname{Re} s > 0$ by the uniqueness of analytic continuation.

Notably, for $\varepsilon > 0$, we see

$$\begin{aligned} f\left(\varepsilon + \frac{2\pi i}{q}\right) &= 1 + 2 \sum_{n=1}^{\infty} e^{-n^2} e^{-2\pi i n^2/q} \\ &= 1 + 2 \sum_{r=0}^{q-1} \left(e^{-2\pi i r^2/q} \sum_{m=0}^{\infty} e^{-(r+mq)^2 \varepsilon} \right). \end{aligned}$$

Now, one can check that $\varepsilon \rightarrow 0^+$ enforces

$$\sum_{m=0}^{\infty} e^{-(r+mq)^2 \varepsilon} \sim \frac{\sqrt{\pi}}{2q\sqrt{\varepsilon}}$$

by doing Poisson summation and only focusing on the leading term. In particular, we see that

$$f\left(\varepsilon + \frac{2\pi i}{q}\right) \sim \frac{\sqrt{\pi}}{2q\sqrt{\varepsilon}} \sum_{r=1}^q e^{-2\pi i r^2/q}$$

as $\varepsilon \rightarrow 0^+$. As such, using the functional equation (2.4) for f , as well as the computation

$$\frac{\pi^2}{\varepsilon + 2\pi i/q} = -\frac{\pi i q}{2} + \frac{q^2}{4} \varepsilon + O(\varepsilon^2)$$

to take the asymptotics on the other side. This will complete the proof. ■

Remark 2.86. One can use Proposition 2.85 to prove the law of quadratic reciprocity, essentially by comparing Gauss sums $(\text{mod } p)$ and $(\text{mod } q)$ for distinct odd primes p and q . One can also use these techniques to prove the supplement $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

2.10 February 15

We open class by remarking that the arguments of Gauss sums turn out to be equidistributed. As references, we mention “Sato–Tate Theorems for Finite Field Mellin Transforms” and “Gauss sums, Kloosterman Sums, and Monodromy Groups.” Let’s give a quick algebraic proof of the supplement.

Proposition 2.87. Fix an odd prime p . Then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Proof. Let $\zeta \in \overline{\mathbb{F}_p}$ be an eighth root of unity. (We can also find ζ in \mathbb{F}_{p^4} because ζ is a root of the equation $\zeta^4 + 1 = 0$.) Because $\zeta^4 = -1$, we see $\zeta^2 = \zeta^{-2}$, so

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = 2.$$

Now, we see $\left(\frac{2}{p}\right) = 1$ is equivalent to having $\zeta + \zeta^{-1} \in \mathbb{F}_p$, which because $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is topologically generated by the Frobenius, is equivalent to

$$\zeta^p + \zeta^{-p} = (\zeta + \zeta^{-1})^p \stackrel{?}{=} \zeta + \zeta^{-1}.$$

Now, this is equivalent to $p \equiv \pm 1 \pmod{8}$; indeed, if $p \equiv \pm 3 \pmod{8}$, then we see $\zeta^3 + \zeta^{-3} = -\zeta - \zeta^{-1}$ is the negative root. ■

2.10.1 Counting Zeroes of $L(s, \chi)$

We would like to generalize Theorem 2.41. For this, we have the following definition.

Notation 2.88. Fix a primitive character $\chi \pmod{q}$. Then we define

$$N_\chi(T) := \#\{|\rho| \leq T : \Xi_\chi(\rho) = 0\}.$$

Remark 2.89. Note that the functional Theorem 2.79 does tell us that all zeroes live in the critical strip, but we no longer have conjugate symmetry because χ might not be real.

Arguing as before, the set

$$\left\{ \frac{L'(2 + iT, \chi)}{L(2 + iT, \chi)} : T \in \mathbb{R}, q, \chi \pmod{q} \right\}$$

is uniformly bounded above, and one can show as in Lemma 2.42 that

$$\sum_{\Xi_\chi(\rho)=0} \frac{1}{1 + |\text{Im } \rho - T|^2} \ll \log(|T| + 2) + \log q,$$

where the implied constant is absolute. Following the rest of the proof of Theorem 2.41 from the argument principle again gives us

$$\frac{1}{2} N_\chi(T) = \frac{T}{2\pi} \log \left(\frac{qT}{2\pi} \right) - \frac{T}{2\pi} + O(\log q(|T| + 2)),$$

where the implied constants are still absolute.

2.10.2 Solovay–Strassen Primality Testing

As an application of what we've done so far, we describe a primality test assuming the Generalized Riemann Hypothesis (GRH).

Question 2.90. Can one determine if an integer n is prime in $\text{Poly}(\log n)$ time?

This is known unconditionally (via the AKS algorithm), and there are fast probabilistic algorithms, but we describe an algorithm which works assuming GRH. Here is the statement of GRH.

Conjecture 2.91 (Generalized Riemann Hypothesis). For any primitive character $\chi \pmod{q}$, the zeroes of $\Xi_\chi(s)$ all lie on the vertical line

$$\operatorname{Re} s = \frac{1}{2}.$$

And now here is our result.

Theorem 2.92 (Miller–Rabin). Assume GRH. Then we can test if an integer n is prime in $\operatorname{Poly}(\log n)$ time.

For this, we describe the Miller–Rabin primality test, which is one of the more efficient probabilistic primality tests.

Lemma 2.93 (Fermat’s little theorem). Fix a prime p . If $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. This follows from Lagrange’s theorem: the order of $a \in \mathbb{F}_p^\times$ divides $|\mathbb{F}_p^\times| = p - 1$. ■

Remark 2.94. It turns out that there are infinitely many integers n such that

$$a^n \equiv a \pmod{n}.$$

For example, $n = 561$ works. Thus, one cannot really use Lemma 2.93 to test for primality.

Instead, we will want to use Proposition 2.63, which implies

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

for $\gcd(a, p) = 1$. In order to compute Legendre symbols efficiently, we must introduce the Jacobi symbol.

Definition 2.95 (Jacobi). Fix an odd integer n . Then for integers a , we define the *Jacobi symbol*

$$\left(\frac{a}{n}\right) = \prod_p \left(\frac{a}{p}\right)^{\nu_p(n)}.$$

Remark 2.96. The Jacobi symbol, like the Legendre symbol, is multiplicative in the numerator, but it is also multiplicative in the denominator. One can use this to show “Jacobi reciprocity,” which asserts that odd $a, b \in \mathbb{Z}$ grant

$$\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}.$$

One also gets the supplement $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

Remark 2.97. Remark 2.96 allows us to compute Jacobi symbols efficiently via reciprocity. Roughly speaking, we are basically just doing the Euclidean algorithm and keeping track of some signs.

We now do primality testing with the Euler criterion.

Lemma 2.98. Fix an odd integer n . If n is not prime, there exists some a such that

$$a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Proof. Omitted. The idea is to split this into two cases: if n is squarefree, one can divide the result via the Chinese remainder theorem into various $(\bmod p)$ statements; if n is not squarefree, then one can look $(\bmod p^2)$ somewhere to get the result. ■

This suggests the following algorithm to test if n an odd integer n is prime.

1. Choose some random $a \in [1, n)$.
2. Compute the Jacobi symbol $\left(\frac{a}{n}\right)$. Via the Euclidean algorithm, one can compute this in $O((\log n)^2)$ time.
3. Compute $a^{(n-1)/2} \pmod n$ using exponentiation by repeated squaring. This will run in $O((\log n)^3)$ time.
4. If the above do not match, then n is not prime. If the above match, then return to step 1 and try and another a .

In fact, we will show (using GRH), that one only has to check $a \ll (\log n)^2$, so the entire algorithm runs in $O((\log n)^5)$.

2.11 February 17

The next two classes (Wednesday and Friday) will be recorded and posted online.

2.11.1 Deterministic Solovay–Strassen

Here is our main theorem, which tells us that the Solovay–Strassen primality test can be made deterministic.

Theorem 2.99. Suppose that q is an odd integer which is not prime. Assuming GRH, then there exists $a \ll (\log q)^2$ such that

$$\left(\frac{a}{q}\right) \not\equiv a^{(q-1)/2} \pmod q.$$

We will require the following result.

Proposition 2.100. Let q be an odd integer. Given a subgroup $A \subseteq (\mathbb{Z}/q\mathbb{Z})^\times$. Assuming GRH, there exists an absolute constant c such that

$$\{[k] \in (\mathbb{Z}/n\mathbb{Z})^\times : k \leq c(\log q)^2\} \subseteq A$$

implies $A = (\mathbb{Z}/q\mathbb{Z})^\times$.

One can quickly prove Theorem 2.99 from Proposition 2.100.

Proof of Theorem 2.99. Indeed, the set

$$A := \left\{ a \in (\mathbb{Z}/q\mathbb{Z})^\times : \left(\frac{a}{q}\right) \not\equiv a^{(n-1)/2} \pmod q \right\}$$

is a subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$. Because q is not prime, we know that $A \neq (\mathbb{Z}/q\mathbb{Z})^\times$, so it follows from Proposition 2.100 that A does not contain all $[k] \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that $k \leq c(\log q)^2$. The conclusion follows. ■

We now attack Proposition 2.100.

Proof of Proposition 2.100. Suppose for the sake of contradiction that $A \neq (\mathbb{Z}/q\mathbb{Z})^\times$. Now, the quotient $(\mathbb{Z}/q\mathbb{Z})^\times / A$ is nontrivial and abelian, so it has some nonzero character. Pulling this character to $(\mathbb{Z}/q\mathbb{Z})^\times$, we have a Dirichlet character $\chi \pmod{q}$ such that

$$\chi(k) = 1$$

for each $0 \leq k \leq c(\log q)^2$ coprime to n .

As in the proof of the Prime number theorem, we want to consider the infinite sum

$$\sum_{n \leq x} \Lambda(n) \chi(n) = \frac{1}{2\pi i} \int_{\operatorname{Re} s = c} \left(-\frac{L'(s, \chi)}{L(s, \chi)} \right) x^s \frac{ds}{s}$$

and shift the contour over to the left. To do this, we apply smoothing ψ to get a smooth function compactly supported on $[1/4, 3/4]$. Arguing as in Dirichlet's theorem, we see

$$\sum_{n \geq 0} \Lambda(n) \chi(n) \psi\left(\frac{n}{x}\right) = \frac{1}{2\pi i} \int_{\operatorname{Re} s = 2} \left(-\frac{L'(s, \chi)}{L(s, \chi)} \right) (\mathcal{M}\psi)(s) x^s ds.$$

Shifting the contour is somewhat delicate, but it can be done similarly as in our proof of the Prime number theorem. This gives

$$\sum_{n \geq 0} \Lambda(n) \chi(n) \psi\left(\frac{n}{x}\right) = - \sum_{L(\rho, \chi) = 0} (\mathcal{M}\psi)(\rho_\chi) x^{\rho_\chi}$$

plus some smaller error terms. By GRH, we may assume that all the roots lie on $\operatorname{Re} s = \frac{1}{2}$, so this is bounded (up to a constant) by

$$\sqrt{x} \log q.$$

Notably, the number of zeroes does not increase very much, especially in comparison to the rapid decay of $\mathcal{M}\psi$. As such, we see

$$x \ll \left| \sum_{n \geq 0} \Lambda(n) \chi(n) \psi\left(\frac{n}{x}\right) \right| \ll \sqrt{x} \log q,$$

so $x \ll (\log q)^2$. However, setting $x = c(\log q)^2$ for c large enough will break this bound, which is our contradiction. ■

2.11.2 Imprimitive Characters

Let's talk a little more about our characters.

Definition 2.101 (conductor). Fix a Dirichlet character $\chi \pmod{q}$. Then the *conductor* $f(\chi)$ is the minimal period of χ restricted $\{n \in \mathbb{Z} : \gcd(n, q) = 1\}$. If $f(\chi) \neq q$, then χ is said to be *imprimitive*.

Roughly speaking, one can take characters and reduce them to the primitive case by pretending they are Dirichlet characters modulo their conductor.

Definition 2.102 (induces). Fix a Dirichlet character $\chi \pmod{q}$ with conductor f . Then the Dirichlet character " $\chi \pmod{f}$ " is primitive (by construction) and is said to *induce* $\chi \pmod{q}$.

Example 2.103. The principal Dirichlet characters are induced by the constantly 1 character.

Remark 2.104. The point is that a Dirichlet character $\chi \pmod{q}$ induced by a primitive Dirichlet character $\chi' \pmod{f}$ has L -function given by

$$L(s, \chi') = L(s, \chi) \prod_{\substack{p \nmid f \\ p|q}} \frac{1}{1 - \chi'(p)p^{-s}}.$$

Note that these finitely many Euler factors do not add any zeroes or poles or similar.

Remark 2.105. Under our philosophy that the real characters are the hard ones. By the Chinese remainder theorem, it suffices to understand characters modulo prime powers p^ν . If p is odd, then $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ is cyclic, so the only real characters are either principal or is $\left(\frac{\cdot}{p}\right)$ depending on if the generator $g \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times$ gets sent to -1 or 1 . If $p = 2$, then $(\mathbb{Z}/2^\nu\mathbb{Z}) \cong \langle -1 \rangle \times \langle 5 \rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}\mathbb{Z}$ for $\nu \geq 2$, and we can decompose this as one might expect. Namely, there is one modulo 4 and two modulo 8.

APPENDIX A

FOURIER ANALYSIS

*Ring around the rosie,
A pocket full of posies.
Ashes! Ashes!
We all fall down!*

—“Ring Around the Rosie”

A.1 The Fourier Transform

It will pay off for us later to have established a little Fourier analysis right now. Our exposition follows [SS03, Chapter 5].

Definition A.1 (Schwarz). A function $f: \mathbb{R} \rightarrow \mathbb{C}$ is *Schwarz* if and only if f is infinitely differentiable and the n th derivative $f^{(n)}$ satisfies that the function $x^A \cdot f^{(n)}(x)$ is bounded for all nonnegative integers A .

Remark A.2. Because the linear combination of bounded sets remains bounded, we see that Schwarz functions form a \mathbb{C} -vector space. Also, by definition, if f is Schwarz, then any derivative is also Schwarz.

Remark A.3. If $f: \mathbb{R} \rightarrow \mathbb{R}$ is Schwarz, we note that $|x^A f(x)|$ is integrable over \mathbb{R} for any $A \geq 0$. Indeed, let k be an integer greater than $A + 2$, and we are granted a constant C such that $|x^k f(x)| \leq C$. Thus,

$$\int_{\mathbb{R}} |x^A f(x)| \, dx \leq \int_{[-1,1]} |x^A f(x)| \, dx + \int_{|x| \geq 1} \frac{C}{x^{A-k}} \, dx,$$

which is finite because $A - k < -2$.

Definition A.4 (Fourier transform). Let $f: \mathbb{R} \rightarrow \mathbb{C}$ be a Schwarz function. Then we define the *Fourier transform* to be the function $\mathcal{F}f: \mathbb{R} \rightarrow \mathbb{C}$ given by

$$(\mathcal{F}f)(s) := \int_{\mathbb{R}} f(x) e^{-2\pi i s x} \, dx.$$

Remark A.5. The integral converges because it absolutely converges: we note

$$\int_{\mathbb{R}} |f(x)e^{-2\pi isx}| dx = \int_{\mathbb{R}} |f(x)| dx$$

is finite by Remark A.3. In fact, this shows that $\mathcal{F}f$ is bounded.

We now run some quick checks on the Fourier transform.

Lemma A.6. Let $f: \mathbb{R} \rightarrow \mathbb{C}$ be a Schwartz function.

- (a) For some $\lambda > 0$, define $f_{\lambda}(x) := f(\lambda x)$. Then $f_{\lambda}: \mathbb{R} \rightarrow \mathbb{C}$ is Schwartz, and $(\mathcal{F}f_{\lambda})(s) = \frac{1}{\lambda}(\mathcal{F}f)\left(\frac{s}{\lambda}\right)$.
- (b) We have $(\mathcal{F}f')(s) = 2\pi is(\mathcal{F}f)(s)$.
- (c) The function $\mathcal{F}f$ is differentiable, and $(\mathcal{F}f)'(s)$ is the Fourier transform of the function $g(x) := -2\pi ix f(x)$.
- (d) The function $\mathcal{F}f$ is Schwarz.

Proof. We show these one at a time.

- (a) To show f_{λ} is Schwarz, we note $f_{\lambda}^{(n)}(x) = \lambda^n f^{(n)}(\lambda x)$ for all $n \geq 0$, so $x^n \cdot f_{\lambda}^{(n)}(x)$ is bounded because $(\lambda x)^n f^{(n)}(\lambda x)$ is. The last equality is a direct computation. We see

$$\begin{aligned} (\mathcal{F}f_{\lambda})(s) &= \int_{\mathbb{R}} f_{\lambda}(x)e^{-2\pi isx} dx \\ &= \int_{\mathbb{R}} f(\lambda x)e^{-2\pi i(s/\lambda)\lambda x} dx \\ &= \frac{1}{\lambda} \int_{\mathbb{R}} f(x)e^{-2\pi i(s/\lambda)x} dx \\ &= \frac{1}{\lambda}(\mathcal{F}f)\left(\frac{s}{\lambda}\right). \end{aligned}$$

- (b) Note f' is Schwarz by Remark A.2, so the statement at least makes sense. Now, by integration by parts, we see

$$\begin{aligned} (\mathcal{F}f')(s) &= \int_{\mathbb{R}} f'(x)e^{-2\pi isx} dx \\ &= f(x)e^{-2\pi isx} \Big|_{-\infty}^{\infty} - \int_{\mathbb{R}} f(x)(2\pi is e^{-2\pi isx}) dx \\ &= 2\pi is(\mathcal{F}f)(s). \end{aligned}$$

To justify the last equality, we see that $f(x)e^{-2\pi isx} \rightarrow 0$ as $x \rightarrow \pm\infty$ because f is Schwarz: note $|f(x)e^{-2\pi isx}| = |f(x)|$, and $|xf(x)|$ is bounded, so there is a constant C such that $f(x) \leq C/|x|$ for all $x \neq 0$, meaning that $|f(x)| \rightarrow 0$ as $x \rightarrow \pm\infty$.

- (c) Note g is the product of infinitely differentiable functions and thus infinitely differentiable. Further, by induction, derivatives of g are the \mathbb{C} -linear of terms of the form $x^k f^{(\ell)}(x)$. Thus, for any integers $k, \ell \geq 0$, the function $|x|^k |g^{(k)}(x)|$ is a \mathbb{C} -linear combination of bounded functions because f is Schwarz, so it follows that $|x|^k |g^{(\ell)}(x)|$ is bounded, so g is Schwarz.

The rest of the proof is a direct computation. For $t, t' \in \mathbb{R}$, we see

$$\int_t^{t'} (\mathcal{F}g)(s) ds = \int_t^{t'} \left(\int_{\mathbb{R}} -2\pi ix f(x)e^{-2\pi isx} dx \right) ds.$$

We would like to exchange the two integrals. Well, by Fubini's theorem, we note that $\int_{\mathbb{R}} |xf(x)| dx < \infty$ is finite by Remark A.3, so

$$\int_t^{t'} \left(\int_{\mathbb{R}} |-2\pi i x f(x) e^{-2\pi i s x}| dx \right) ds \leq 2\pi |t' - t| \int_{\mathbb{R}} |xf(x)| dx < \infty.$$

Thus, we may write

$$\begin{aligned} \int_t^{t'} (\mathcal{F}g)(s) ds &= \int_{\mathbb{R}} \left(\int_t^{t'} -2\pi i x f(x) e^{-2\pi i s x} ds \right) dx \\ &= \int_{\mathbb{R}} f(x) \left(e^{-2\pi i t' x} - e^{-2\pi i t x} \right) dx \\ &= (\mathcal{F}f)(t') - (\mathcal{F}f)(t). \end{aligned}$$

Thus, by the Fundamental theorem of calculus, we see

$$(\mathcal{F}f)'(t) = \lim_{t' \rightarrow t} \frac{(\mathcal{F}f)(t') - (\mathcal{F}f)(t)}{t' - t} = \lim_{t' \rightarrow t} \left(\frac{1}{t' - t} \int_t^{t'} (\mathcal{F}g)(s) ds \right) = (\mathcal{F}g)(t).$$

- (d) By Remark A.5, the Fourier transform of a Schwarz function is bounded. Thus, it suffices to note that, for any nonnegative integers k and ℓ , the function $s \mapsto s^k (\mathcal{F}f)^{(\ell)}(s)$ is the Fourier transform of the function

$$x \mapsto \frac{1}{(2\pi i)^k} \left(\frac{d}{dx'} \right)^{(k)} \left((-2\pi i x')^{\ell} f(x') \right) \Big|_{x'=x}$$

by combining (b) and (c). This completes the proof. ■

As an application, we can compute the Fourier transform of the Gaussian.

Exercise A.7 (Gaussian). Define $g: \mathbb{R} \rightarrow \mathbb{R}$ by $g(x) := e^{-\pi x^2}$. Then g is Schwarz, and $(\mathcal{F}g)(x) = g(x)$.

Proof. We build a differential equation that $\mathcal{F}g$ solves, and then we solve that differential equation. Namely, by using Lemma A.6 repeatedly, we see

$$\begin{aligned} (\mathcal{F}g)'(s) &= \int_{\mathbb{R}} -2\pi i x g(x) e^{-2\pi i s x} dx \\ &= i \int_{\mathbb{R}} g'(x) e^{-2\pi i s x} dx \\ &= i(\mathcal{F}g')(s) \\ &= -2\pi x (\mathcal{F}g)(s), \end{aligned}$$

so $(\mathcal{F}g)$ solves the differential equation $y' + 2\pi y = 0$. To solve this differential equation, we define $f(x) := (\mathcal{F}g)(x)e^{\pi x^2}$ and use the differential equation to write

$$f'(x) = (\mathcal{F}g)(x) \cdot 2\pi x e^{\pi x^2} - 2\pi x (\mathcal{F}g)(x) \cdot e^{\pi x^2} = 0.$$

Thus, f is a constant function, so there exists $a \in \mathbb{C}$ such that $(\mathcal{F}g)(x) = a e^{-\pi x^2}$ for all $x \in \mathbb{R}$.

To finish, we need to introduce an initial condition. Well, we compute $(\mathcal{F}g)(0) = 1$ in the usual way,

writing

$$\begin{aligned}
 (\mathcal{F}g)(0)^2 &= \left(\int_{\mathbb{R}} e^{-\pi x^2} dx \right)^2 \\
 &= \int_{\mathbb{R}} \int_{\mathbb{R}} e^{-\pi(x^2+y^2)} dx dy \\
 &= \int_0^{2\pi} \int_0^\infty e^{-\pi r^2} r dr d\theta \\
 &= \int_0^{2\pi} \frac{1}{2\pi} d\theta \\
 &= 1.
 \end{aligned}$$

However, surely $(\mathcal{F}g)(0) \geq 0$, so we conclude $(\mathcal{F}g)(0) = 1$. It follows that $a = 1$, so $(\mathcal{F}g)(x) = e^{-\pi x^2}$ for all $x \in \mathbb{R}$. ■

A.2 Fourier Inversion

The goal of this subsection is to prove the Fourier inversion theorem; we continue to roughly follow [SS03, Chapter 5]. Roughly speaking, this will follow from understanding the Gaussian. Here are the necessary tools.

Lemma A.8. Define the Gaussian $g: \mathbb{R} \rightarrow \mathbb{R}$ by $g(x) := e^{-\pi x^2}$. For any $\delta > 0$, we have

$$\lim_{\varepsilon \rightarrow 0^+} \frac{1}{\varepsilon} \int_{|t| \geq \delta} g(t/\varepsilon) dt = 0.$$

Proof. Changing variables, we see

$$\lim_{\varepsilon \rightarrow 0^+} \int_{|t| \geq \delta} g(t/\varepsilon) dt = \lim_{\varepsilon \rightarrow 0^+} \int_{|t| \geq \delta/\varepsilon} g(t) dt = \lim_{N \rightarrow \infty} \int_{|t| \geq N} g(t) dt,$$

where $N = \delta/\varepsilon$ in the last equality. However, g is Schwarz by Exercise A.7, so $\int_{\mathbb{R}} g(t) dt$ is finite by Remark A.3, so

$$\lim_{N \rightarrow \infty} \int_{|t| \leq N} g(t) dt = \int_{\mathbb{R}} g(t) dt.$$

Rearranging, we see

$$\lim_{N \rightarrow \infty} \int_{|t| \geq N} g(t) dt = 0,$$

which is what we wanted. ■

Lemma A.9. Define the Gaussian $g: \mathbb{R} \rightarrow \mathbb{R}$ by $g(x) := e^{-\pi x^2}$. For any bounded and continuous function $f: \mathbb{R} \rightarrow \mathbb{R}$, we have

$$f(0) = \lim_{\varepsilon \rightarrow 0^+} \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t) g(t/\varepsilon) dt.$$

Proof. The point here is that, for any $\varepsilon > 0$, we have

$$\frac{1}{\varepsilon} \int_{\mathbb{R}} g(t/\varepsilon) dt = \int_{\mathbb{R}} g(t) dt = (\mathcal{F}g)(0) = g(0) = 1 \tag{A.1}$$

by Exercise A.7. However, the functions $t \mapsto g(t/\varepsilon)$ concentrate at $t = 0$ as $\varepsilon \rightarrow 0^+$, so we expect that adding in an $f(t)$ to our integral will force the output to be $f(0)$.

As an aside, we go ahead and check that these integrals converge for each $\varepsilon > 0$. Indeed, they absolutely converge: because f is bounded, we may find $M_f \in \mathbb{R}$ such that $|f(x)| \leq M_f$ for each $x \in \mathbb{R}$, which gives

$$\int_{\mathbb{R}} |f(t)g(t/\varepsilon)| dt \leq M_f \int_{\mathbb{R}} g(t/\varepsilon) dt = \varepsilon M_f,$$

where we have used (A.1).

We now proceed with the proof, which is somewhat technical. For psychological reasons, we set $h(x) := f(x) - f(0)$ for all $x \in \mathbb{R}$. Note h is still bounded and continuous (it's a shift away from f). Further, for each $\varepsilon > 0$, we see

$$\frac{1}{\varepsilon} \int_{\mathbb{R}} h(t)g(t/\varepsilon) dt = \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t)g(t/\varepsilon) dt - \frac{f(0)}{\varepsilon} \int_{\mathbb{R}} g(t/\varepsilon) dt = \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t)g(t/\varepsilon) dt - f(0),$$

where we have used (A.1) in the last equality, so it suffices to show

$$\lim_{\varepsilon \rightarrow 0^+} \frac{1}{\varepsilon} \int_{\mathbb{R}} h(t)g(t/\varepsilon) dt \stackrel{?}{=} 0.$$

Well, fix any $\delta > 0$. Note h is continuous at 0 and has $h(0) = 0$, so we may find $\delta_0 > 0$ such that $|h(t)| < \delta$ for $|t| < \delta_0$. For the other values of t , we note h is bounded, so we may find $M_h \geq 0$ such that $|h(t)| < M_h$ for all t . Thus, we upper-bound

$$\begin{aligned} \left| \frac{1}{\varepsilon} \int_{\mathbb{R}} h(t)g(t/\varepsilon) dt \right| &\leq \frac{1}{\varepsilon} \int_{|t| \leq \delta_0} |h(t)g(t/\varepsilon)| dt + \frac{1}{\varepsilon} \int_{|t| \geq \delta_0} |h(t)g(t/\varepsilon)| dt \\ &\leq \frac{\delta}{\varepsilon} \int_{|t| \leq \delta_0} g(t/\varepsilon) dt + \frac{M_h}{\varepsilon} \int_{|t| \geq \delta_0} g(t/\varepsilon) dt \\ &\leq \frac{\delta}{\varepsilon} \int_{\mathbb{R}} g(t/\varepsilon) dt + \frac{M_h}{\varepsilon} \int_{|t| \geq \delta_0} g(t/\varepsilon) dt \\ &= \delta + \frac{M_h}{\varepsilon} \int_{|t| \geq \delta_0} g(t/\varepsilon) dt. \end{aligned}$$

(As usual, we have used (A.1) in the last equality.) Thus, using Lemma A.8, sending $\varepsilon \rightarrow 0^+$ shows that

$$\lim_{\varepsilon \rightarrow 0^+} \left| \frac{1}{\varepsilon} \int_{\mathbb{R}} h(t)g(t/\varepsilon) dt \right| \leq \delta$$

for any $\delta > 0$, so sending $\delta \rightarrow 0^+$ completes the proof. ■

And here is our main attraction.

Theorem A.10 (Fourier inversion). Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a Schwarz function. For any $x \in \mathbb{R}$, we have

$$f(x) = \int_{\mathbb{R}} (\mathcal{F}f)(s) e^{2\pi i x s} ds.$$

Proof. Expanding out the definition of $\mathcal{F}f$, we are computing

$$\int_{\mathbb{R}} \left(\int_{\mathbb{R}} f(t) e^{-2\pi i t s} dt \right) e^{2\pi i x s} ds.$$

We would like to exchange the two integrals, but we do not have absolute convergence. As such, we employ a trick: fix some $\varepsilon > 0$, and define the integral

$$f_{\varepsilon}(x) := \int_{\mathbb{R}} \int_{\mathbb{R}} f(t) e^{2\pi i (x-t)s} e^{-\pi \varepsilon^2 s^2} dt ds.$$

Notably, we expect $f_\varepsilon(x) \rightarrow \int_{\mathbb{R}} (\mathcal{F}f)(s) e^{2\pi i x s} ds$ as $\varepsilon \rightarrow 0^+$. As such, we compute the behavior of $\varepsilon \rightarrow 0^+$ in two ways.

- We integrate over dt first. Namely, we would like to send $\varepsilon \rightarrow 0^+$, for which we use the Dominated convergence theorem. For each $\varepsilon > 0$, note that we have the bound

$$\left| \int_{\mathbb{R}} f(t) e^{2\pi i(x-t)s} e^{-\pi \varepsilon^2 s^2} dt \right| \leq e^{-\pi \varepsilon^2 s^2} \int_{\mathbb{R}} |f(t)| dt.$$

Now, $s \mapsto e^{-\pi \varepsilon^2 s^2}$ is Schwarz by Exercise A.7 (combined with (a) of Lemma A.6), so we may integrate the right-hand function over all $s \in \mathbb{R}$ by Remark A.3.

Thus, our integrand in $f_\varepsilon(x)$ is dominated by an integrable function, so the Dominated convergence theorem implies

$$\lim_{\varepsilon \rightarrow 0^+} f_\varepsilon(x) = \int_{\mathbb{R}} \left(\lim_{\varepsilon \rightarrow 0^+} e^{-\pi \varepsilon^2 s^2} \int_{\mathbb{R}} f(t) e^{2\pi i(x-t)s} dt \right) ds = \int_{\mathbb{R}} (\mathcal{F}f)(s) e^{2\pi i x s} ds.$$

- We integrate over ds first. As such, we begin by justifying our application of Fubini's theorem: checking for absolute convergence, we compute

$$\int_{\mathbb{R}} \int_{\mathbb{R}} |f(t) e^{2\pi i(x-t)s} e^{-\pi \varepsilon^2 s^2}| dt ds = \left(\int_{\mathbb{R}} |f(t)| dt \right) \left(\int_{\mathbb{R}} e^{-\pi \varepsilon^2 s^2} ds \right).$$

Now, f is Schwarz by hypothesis, as is $s \mapsto e^{-\pi \varepsilon^2 s^2}$ by Exercise A.7, so both of these integrals are finite by Remark A.3.

Thus, we may switch the order of our integration. Setting up notation, we let $g(x) := e^{-\pi x^2}$ denote the Gaussian (so that $(\mathcal{F}g)(s) = g(s)$ for all $s \in \mathbb{R}$) and $g_\varepsilon(x) := g(\varepsilon x)$. Then we see

$$\begin{aligned} f_\varepsilon(x) &= \int_{\mathbb{R}} \int_{\mathbb{R}} f(t) e^{2\pi i(x-t)s} e^{-\pi \varepsilon^2 s^2} ds dt \\ &= \int_{\mathbb{R}} f(t) \left(\int_{\mathbb{R}} e^{-\pi(\varepsilon s)^2} e^{-2\pi i(t-x)s} ds \right) dt \\ &= \int_{\mathbb{R}} f(t) (\mathcal{F}g_\varepsilon)(t-x) dt \\ &\stackrel{*}{=} \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t) g\left(\frac{t-x}{\varepsilon}\right) dt \\ &= \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t+x) g(t/\varepsilon) dt, \end{aligned}$$

where we have used part (a) of Lemma A.6 at $\stackrel{*}{=}$. Sending $\varepsilon \rightarrow 0^+$, Lemma A.9 tells us that

$$f(x) = \lim_{\varepsilon \rightarrow 0^+} \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t+x) g(t/\varepsilon) dt = \lim_{\varepsilon \rightarrow 0^+} f_\varepsilon(x).$$

Combining the above two computations completes the proof. ■

A.3 Fourier Coefficients

In order to say that we've done some Fourier analysis, we will also say a few things about Fourier series. We follow [SS03, Chapter 2].

The idea here is that the functions $e_n: x \mapsto e^{2\pi i n x}$ for $n \in \mathbb{Z}$ form an orthonormal set of continuous functions $\mathbb{R} \rightarrow \mathbb{C}$, where our (Hermitian) inner product is given by

$$\langle f, g \rangle := \frac{1}{2\pi i} \int_0^1 f(x) \overline{g(x)} dx.$$

Indeed, for any $n, m \in \mathbb{Z}$, we see

$$\langle e_n, e_m \rangle = \int_0^1 e^{2\pi i n x} \overline{e^{2\pi i m x}} dx = \int_0^1 e^{2\pi i (m-n)x} dx = \begin{cases} 1 & \text{if } m = n, \\ 0 & \text{if } m \neq n. \end{cases} \quad (\text{A.2})$$

Now, the functions e_n are varied enough that we might hope that all sufficiently smooth 1-periodic functions $f: \mathbb{R} \rightarrow \mathbb{C}$ can be written in terms of our orthonormal functions as

$$f(x) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n x}$$

for some coefficients $a_n \in \mathbb{C}$. Thus, we might hope we can extract out the n th coefficient by

$$\langle f, e_n \rangle = \int_0^1 f(x) e^{-2\pi i n x} dx.$$

This motivates the following definition.

Definition A.11 (Fourier coefficient). Fix a continuous 1-periodic function $f: \mathbb{R} \rightarrow \mathbb{C}$. Then we define the n th Fourier coefficient as

$$a_n(f) := \int_0^1 f(x) e^{-2\pi i n x} dx.$$

Remark A.12. Note that the integral defining $a_n(f)$ converges absolutely. Indeed, f is continuous on $[0, 1]$ and hence bounded because $[0, 1]$ is compact. Thus, we may find M such that $|f(x)| \leq M$ for $x \in [0, 1]$, which implies

$$|a_n(f)| \leq \int_0^1 |f(x) e^{-2\pi i n x}| dx \leq M \int_0^1 dx = M.$$

Of course, one can weaken the requirement that f be continuous, but we will have no need for these levels of generality.

Remark A.13. In fact, we note

$$a_n(f) = \int_t^{t+1} f(x) e^{2\pi i n x} dx$$

for any $t \in \mathbb{R}$. Because $x \mapsto f(x) e^{2\pi i n x}$ is 1-periodic, it suffices to show this for $t \in [0, 1)$. Then the integral over $[t, t+1) = [t, 1) \sqcup [1, t+1)$ is equal to the integral over $[0, t) \sqcup [t, 1) = [0, 1)$, where we have used the 1-periodicity.

Here is some basic arithmetic with these coefficients.

Lemma A.14. Fix continuous 1-periodic functions $f, g: \mathbb{R} \rightarrow \mathbb{C}$.

- (a) For any $z, w \in \mathbb{C}$ and $n \in \mathbb{Z}$, we see $a_n(zf + wg) = za_n(f) + wa_n(g)$.
- (b) For any $n \in \mathbb{Z}$, we see $a_n(\bar{f}) = \overline{a_{-n}(f)}$.
- (c) Given $x_0 \in \mathbb{R}$, define $g(x) := f(x + x_0)$. Then $a_n(g) = e^{-2\pi i n x_0} a_n(f)$.

Proof. Here we go.

(a) This follows from the fact that $\langle \cdot, \cdot \rangle$ is an inner product. Indeed,

$$a_n(zf + wg) = z \int_0^1 f(x) e^{-2\pi i n x} dx + w \int_0^1 g(x) e^{-2\pi i n x} dx = za_n(f) + wa_n(g).$$

(b) We compute

$$a_n(\bar{f}) = \int_0^1 \overline{f(x)} e^{-2\pi i n x} dx = \overline{\int_0^1 f(x) e^{2\pi i n x} dx} = \overline{a_{-n}(f)}.$$

(c) We compute

$$a_n(g) = \int_0^1 f(x + x_0) e^{2\pi i n x} dx = e^{-2\pi i n x_0} \int_0^1 f(x + x_0) e^{2\pi i n (x + x_0)} dx = e^{-2\pi i n x_0} a_n(f),$$

where the last inequality used Remark A.13. ■

Here is a slightly harder computation, still akin to Lemma A.6.

Lemma A.15. Fix a continuously differentiable 1-periodic function $f: \mathbb{R} \rightarrow \mathbb{C}$. For $n \neq 0$, we have

$$a_n(f') = -2\pi i n a_n(f).$$

Proof. This is by integration by parts. Indeed, we compute

$$\begin{aligned} a_n(f') &= \int_0^1 f'(x) e^{-2\pi i n x} dx \\ &= \left. \frac{f(x) e^{-2\pi i n x}}{-2\pi i n} \right|_0^1 - \frac{1}{-2\pi i n} \int_0^1 f(x) e^{-2\pi i n x} dx \\ &= 0 + \frac{1}{2\pi i n} \cdot a_n(f), \end{aligned}$$

which is what we wanted. ■

The following is our key result.

Lemma A.16. Fix a continuous 1-periodic function $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $f(0) \neq 0$. Then $a_n(f) \neq 0$ for some $n \in \mathbb{Z}$.

Proof. Define the function $p: \mathbb{R} \rightarrow \mathbb{C}$ by $p(x) := e^{-2\pi i n x}$. Roughly speaking, the idea is that $a_n(f) = 0$ for all $n \in \mathbb{Z}$ implies that any “polynomial in p ” named $q \in \mathbb{C}[p, p^{-1}]$ written as

$$q := \sum_{n \in \mathbb{Z}} q_n p^n,$$

where all but finitely many of the q_n vanish, will have

$$\int_{-1/2}^{1/2} f(x) q(x) dx = \sum_{n \in \mathbb{Z}} \left(q_n \int_{-1/2}^{1/2} f(x) e^{2\pi i n x} dx \right) = \sum_{n \in \mathbb{Z}} q_n a_n(f) = 0$$

by Remark A.13. Indeed, we will be able to build a function $q \in \mathbb{C}[p, p^{-1}]$ which is “concentrated at 0” so that $f(0) \neq 0$ is incompatible with all these integrals vanishing.

We now proceed with the proof. Quickly, we replace $f(x)$ with $f(x)/f(0)$, which is still continuous, 1-periodic, and has $a_n(f/f(0)) = a_n(f)/f(0)$ for all $n \in \mathbb{Z}$, so $a_n(f/f(0)) \neq 0$ implies $a_n(f) \neq 0$. Thus, we may assume $f(0) = 1$, and we still want to show $a_n(f) \neq 0$ for some n .

We now set up some bounding, in steps.

1. Note f is continuous on the compact set $[-1/2, 1/2]$, so we may find some M_f such that $|f(x)| \leq M_f$ for all $x \in [-1/2, 1/2]$.

2. Because f is continuous, we may find $\delta_f > 0$ such that $|f(x) - 1| \leq 1/2$ for $|x| < \delta_f$. In particular, we see $f(x) \geq 1/2$ for $|x| < \delta_f$. By making δ_f smaller if necessary, we will enforce $\delta_f \leq 1/4$.
3. Now, define $q_1(x) := 2\varepsilon + p(x) + p(x)^{-1} = 2\varepsilon + \cos(2\pi x)$, for $\varepsilon := \frac{2}{3}(1 - \cos(2\pi\delta_f))$. Note $\cos(2\pi x)$ is decreasing in the region in $[\delta_f, 1/2]$, so in fact

$$\varepsilon \leq \frac{1}{3}(1 - \cos(2\pi\delta_f))$$

for $x \in [\delta_f, 1/2]$. Rearranging, we see

$$q_1(x) = 2\varepsilon + \cos(2\pi x) \leq 1 - \varepsilon$$

for $x \in [\delta_f, 1/2]$. In fact, because $q_1(x) \geq -1 + 2\varepsilon$, we see that $|q_1(x)| \leq 1 - \varepsilon$ for $x \in [\delta_f, 1/2]$. Lastly, because q_1 is even, these inequalities hold on $[-1/2, -\delta_f] \cup [\delta_f, 1/2]$.

4. Lastly, choose $\delta_q > 0$ such that $|q_1(x) - q_1(0)| \leq \varepsilon$ for $|x| < \delta_q$. In particular, $q_1(x) \geq 1 - \varepsilon$ for $|x| < \delta_q$. By making δ_q smaller if necessary, we may assume $\delta_q < \delta_f$, though this is actually implied.

To finish, we define $q_N := q_1^N$ for $N \in \mathbb{N}$. (Notably, $q_1 = q_1^1$.) The point is that $k \rightarrow \infty$ makes q_N blow up at 0 around points where f is bounded below by $1/2$, but q_N will vanish elsewhere. Indeed, using Remark A.13, we compute

$$\begin{aligned} \int_{-1/2}^{1/2} f(x)q_N(x) dx &= \int_{|x| \leq \delta_q} f(x)q_N(x) dx + \int_{\delta_q \leq |x| \leq \delta_f} f(x)q_N(x) dx + \int_{\delta_f \leq |x| \leq 1/2} f(x)q_N(x) dx \\ &\geq 2\delta_q \cdot \frac{1}{2} (1 + \varepsilon)^N + 2(\delta_f - \delta_q) \cdot \frac{1}{2} \cdot 0 - 2 \left(\frac{1}{2} - \delta_f \right) B (1 - \varepsilon)^N \\ &\geq \delta_q (1 + \varepsilon)^N - \delta_f B (1 - \varepsilon)^N. \end{aligned}$$

Thus, as $N \rightarrow \infty$, the integral goes to $+\infty$. In particular, we can (in theory) find an (explicit) N such that $\int_{-1/2}^{1/2} f(x)q_N(x) dx > 0$. Now, we may write

$$q_N = (2\varepsilon + p + p^{-1})^N = \sum_{n=-N}^N q_{N,n} p^n$$

for some coefficients $q_{N,n} \in \mathbb{R}$. Thus,

$$0 < \int_{-1/2}^{1/2} f(x)q_N(x) dx = \sum_{n=-N}^N \left(q_{N,n} \int_{-1/2}^{1/2} f(x) e^{-2\pi i n x} dx \right) = \sum_{n=-N}^N q_{N,n} a_n(f),$$

where we have used Remark A.13. Thus, there exists n with $|n| \leq N$ such that $a_n(f) \neq 0$. ■

Proposition A.17. Fix a continuous 1-periodic function $f: \mathbb{R} \rightarrow \mathbb{C}$ such that $a_n(f) = 0$ for all $n \in \mathbb{N}$. Then $f(x) = 0$ for all $x \in \mathbb{R}$.

Proof. This follows from Lemma A.16 and the following reductions.

- It suffices to show the result for real-valued functions f . Indeed, we may write $f(x) := u(x) + iv(x)$ for some real-valued, continuous, and 1-periodic functions $u, v: \mathbb{R} \rightarrow \mathbb{R}$. (Namely, $u = \operatorname{Re} f$ and $v = \operatorname{Im} f$, and each adjective is inherited from f .) However, for each $n \in \mathbb{N}$, we use Lemma A.14 to see

$$a_n(u) = a_n \left(\frac{f + \bar{f}}{2} \right) = \frac{1}{2} \left(a_n(f) + \overline{a_{-n}(f)} \right) = 0,$$

and

$$a_n(v) = a_n\left(\frac{f - \bar{f}}{2i}\right) = \frac{1}{2i} \left(a_n(f) - \overline{a_{-n}(f)} \right) = 0.$$

Thus, if we can prove the result for real-valued functions, we see $a_n(u) = a_n(v) = 0$ for all $n \in \mathbb{Z}$ forces $u = v = 0$, so $f = u + iv = 0$ also.

- It suffices to show that $f(0) = 0$, which is Lemma A.16. Indeed, for some fixed $x_0 \in \mathbb{R}$, we define $g(x) := f(x + x_0)$. Note g is still continuous and 1-periodic. Further, Lemma A.14 tells us that $a_n(g) = e^{2\pi i n x_0} a_n(f) = 0$ for each $n \in \mathbb{Z}$. Thus, Lemma A.16 implies $g(0) = 0$, so $f(x_0) = g(0) = 0$ follows. ■

The point is that we know the linear transformation sending a continuous 1-periodic function f to the tuple of its coefficients $\{a_n(f)\}_{n \in \mathbb{N}}$ is injective. We now expect that we can construct a partial inverse map by sending the tuple of coefficients to the corresponding Fourier series, which is what we show next.

A.4 Fourier Series

Now that we have our coefficients, we can define our Fourier series. We continue to follow [SS03, Chapter 2].

Definition A.18 (Fourier series). Fix a continuous 1-periodic function $f: \mathbb{R} \rightarrow \mathbb{C}$. Then we define the N th partial sum of the *Fourier series* of f as

$$S_{f,N}(x) := \sum_{n=-N}^N a_n(f) e^{2\pi i n x}.$$

The *Fourier series* is defined as $S_f(x) := \lim_{N \rightarrow \infty} S_{f,N}(x)$, when this limit converges.

The main goal of this subsection is to provide smoothness conditions on f which will imply $f(x) = S(x)$ for all $x \in \mathbb{R}$.

We will begin by figuring out when this series will converge.

Lemma A.19. Fix a twice continuously differentiable 1-periodic function $f: \mathbb{R} \rightarrow \mathbb{C}$. Then the series $S_f(x)$ converges absolutely and uniformly.

Proof. This follows from Lemma A.15. Indeed, for $n \neq 0$, we see that

$$a_n(f) = \frac{1}{-2\pi i n} \cdot a_n(f') = \frac{a_n(f'')}{4\pi^2 n^2}.$$

Because f'' is continuous, Remark A.12 grants $M \in \mathbb{R}$ such that $|a_n(f'')| \leq M$, so it follows that $|a_n(f)| \leq M/(4\pi^2 n^2)$ for $n \neq 0$. Thus, we see the series S_f converges absolutely because

$$\sum_{n \in \mathbb{Z}} |a_n(f) e^{2\pi i n x}| \leq a_0(f) + \frac{2M}{4\pi^2} \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty$$

for any $x \in \mathbb{R}$. To get the uniform convergence, for any $N \in \mathbb{N}$, we compute

$$|S_f(x) - S_{f,N}(x)| = \left| \sum_{|n| > N} a_n(f) e^{2\pi i n x} \right| \leq \sum_{|n| > N} \frac{M}{4\pi^2 n^2} = \frac{2M}{4\pi^2} \sum_{n > N} \frac{1}{n^2} < \frac{2M}{4\pi^2} \int_N^{\infty} \frac{1}{t^2} dt = \frac{2M}{4\pi^2 N},$$

which does vanish as $N \rightarrow \infty$. ■

And in this situation, we can show that our Fourier series is well-behaved.

Theorem A.20. Fix a continuous 1-periodic function $f: \mathbb{R} \rightarrow \mathbb{C}$. If the series S_f converges absolutely and uniformly, then $S_f(x) = f(x)$ for all $x \in \mathbb{R}$.

Proof. The point is to show that $a_n(S_f) = a_n(f)$ for all $n \in \mathbb{Z}$ so that the result will follow from Proposition A.17.

Quickly, note that the uniform convergence provided by hypothesis implies that S_f is a continuous function because the partial sums $S_{f,N}$ are continuous. Further, S_f is 1-periodic: for any $x \in \mathbb{R}$, we see

$$S_f(x+1) = \lim_{N \rightarrow \infty} \sum_{n=-N}^N a_n(f) e^{2\pi i n(x+1)} = \lim_{N \rightarrow \infty} \sum_{n=-N}^N a_n(f) e^{2\pi i n x} = S_f(x).$$

Thus, we are allowed to compute the Fourier coefficients

$$a_n(S_f) = \int_0^1 \left(\sum_{m \in \mathbb{Z}} a_m(f) e^{2\pi i(m-n)x} \right) dx$$

for $n \in \mathbb{Z}$. We would like to exchange the sum and the integral, for which we use Fubini's theorem. Indeed, we see

$$\int_0^1 \left(\sum_{m \in \mathbb{Z}} |a_m(f) e^{2\pi i(m-n)x}| \right) dx = \left(\int_0^1 dx \right) \sum_{m \in \mathbb{Z}} |a_m(f)| = \sum_{m \in \mathbb{Z}} |a_m(f)|,$$

which converges because $S_f(0)$ converges absolutely by hypothesis. Thus, Fubini's theorem lets us write

$$a_n(S_f) = \sum_{m \in \mathbb{Z}} \left(\int_0^1 a_m(f) e^{2\pi i(m-n)x} dx \right) = a_n(f),$$

where we have used (A.2) in the last equality. To finish the proof, we note $a_n(S_f - f) = 0$ by Lemma A.14. As such, $S_f - f = 0$ by Proposition A.17, which finishes the proof. ■

BIBLIOGRAPHY

- [Dav80] Harold Davenport. *Multiplicative number theory*. eng. Second Edition. Vol. 74. Graduate Texts in Mathematics. New York, NY: Springer, 1980. ISBN: 9781475759297.
- [Mat01] Lutz Mattner. "Complex differentiation under the integral". In: *Nieuw Archief voor Wiskunde* 2.1 (2001), pp. 32–35.
- [SS03] Elias M. Stein and Rami Shakarchi. *Fourier Analysis: An Introduction*. Vol. 1. Princeton University Press, 2003. URL: <https://books.google.com/books?id=I6CJngEACAAJ>.
- [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.
- [Tat10] John T. Tate. "Fourier Analysis in Number Fields and Hecke's Zeta-Functions". In: *Algebraic Number Theory: Proceedings of an Instructional Conference*. Ed. by J. W. S. Cassels and A. Fröhlich. 2nd ed. London Mathematical Society, 2010.
- [Ser12] Jean-Pierre Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer New York, 2012. URL: <https://books.google.com/books?id=8fPTBwAAQBAJ>.
- [Tao14] Terence Tao. 254A, Supplement 3: The Gamma function and the functional equation (optional). 2014. URL: <https://terrytao.wordpress.com/2014/12/15/254a-supplement-3-the-gamma-function-and-the-functional-equation-optional/>.
- [Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

LIST OF DEFINITIONS

binary quadratic form, [27](#)

character, [8](#)

conductor, [69](#)

decaying, [23](#)

Dirichlet L -function, [13](#)

Dirichlet character, [12](#)

Dirichlet convolution, [21](#)

discriminant, [28](#)

dual group, [8](#)

equivalent, [28](#)

Fourier coefficient, [77](#)

Fourier series, [80](#)

Fourier transform, [71](#)

Γ , [44](#)

Gauss sum, [59](#)

imprimitive, [69](#)

induces, [69](#)

Jacobi, [67](#)

Mellin transform, [23](#)

multiplicative, [6](#)

primitive, [63](#)

quadratic residue, [58](#)

Schwarz, [71](#)

ξ , [45](#)