191: Analytic Number Theory
For the Very Patient

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 **6**
1.1 January 18 . . . 6
1.1.1 House-Keeping . . . 6
1.1.2 Facts about Dirichlet Series . . . 6
1.1.3 The Euler Product . . . 7
1.1.4 Characters . . . 10
1.1.5 Finite Fourier Analysis . . . 13
1.1.6 Dirichlet Characters . . . 15
1.2 January 20 . . . 16
1.2.1 Abel Summation . . . 16
1.2.2 Continuing $L(s, \chi)$ . . . 17
1.2.3 Reducing to $L(1, \chi)$ . . . 20
1.3 January 23 . . . 23
1.3.1 The Dirichlet Convolution . . . 23
1.3.2 The Mellin Transform . . . 25
1.3.3 Finishing Dirichlet's Theorem . . . 27
1.3.4 A Little on Quadratic Forms . . . 30
1.3.5 The Upper-Half Plane . . . 31
1.4 January 25 . . . 33
1.4.1 A Fundamental Domain . . . 33
1.4.2 Gauss Reduced Forms . . . 34
1.4.3 Dirichlet's Class Number Formula . . . 34

2 The ζ-Function **35**
2.1 January 25 . . . 35
2.1.1 The Statement . . . 35
2.1.2 Poisson Summation . . . 38
2.2 January 27 . . . 40

2.2.1 An Abstract Functional Equation . . . 40
2.2.2 Facts about Γ . . . 41
2.2.3 Bounds on Γ . . . 46
2.2.4 The Functional Equation . . . 53
2.2.5 Corollaries of the Functional Equation . . . 57
2.3 January 30 . . . 59
2.3.1 Counting Zeroes of ζ . . . 59
2.4 February 1 . . . 61
2.4.1 Zeroes of ζ, Again . . . 61
2.4.2 The Explicit Formula . . . 62
2.5 February 3 . . . 64
2.5.1 The Explicit Formula, Continued . . . 64
2.5.2 A Zero-Free Region . . . 65
2.6 February 6 . . . 65
2.6.1 A General Lemma . . . 65
2.6.2 The Prime Number Theorem, Finally . . . 67

3 Dirichlet L-Functions **69**
3.1 February 8 . . . 69
3.1.1 Quadratic Residues . . . 69
3.1.2 Primitive Characters . . . 75
3.1.3 Gauss Sums . . . 76
3.2 February 10 . . . 79
3.2.1 The Pólya–Vinogradov Inequality . . . 79
3.2.2 The Functional Equation for $L(s, \chi)$ . . . 80
3.3 February 13 . . . 85
3.3.1 All Functional Equations . . . 85
3.3.2 The Sign of the Gauss Sum . . . 86
3.3.3 A Zero-Free Region for Complex Characters . . . 87
3.4 February 15 . . . 88
3.4.1 Counting Zeroes of $L(s, \chi)$ . . . 88
3.4.2 Solovay–Strassen Primality Testing . . . 88
3.5 February 17 . . . 90
3.5.1 Deterministic Solovay–Strassen . . . 90
3.5.2 Imprimitive Characters . . . 91
3.6 February 22 . . . 92
3.6.1 Real Primitive Characters . . . 92
3.6.2 Zero-Free Regions for $L(s, \chi)$ . . . 93
3.7 February 24 . . . 94
3.7.1 Siegel's Theorem . . . 94
3.8 February 27 . . . 95
3.8.1 The Burgess Bound . . . 95
3.8.2 A Little on Curves . . . 96
3.9 March 1 . . . 97
3.9.1 Proving the Burgess Bound . . . 97
3.10 March 3 . . . 100
3.10.1 The Prime Number Theorem in Arithmetic Progressions . . . 100

4 Introduction to Sieve Theory **102**
4.1 March 6 . . . 102
4.1.1 Elementary Sieve Theory . . . 102
4.2 March 8 . . . 105
4.2.1 Bounding the Main Term . . . 105
4.3 March 10 . . . 106

4.3.1 The Sieve Dimension . . . 107
4.3.2 Twin Primes . . . 108
4.4 March 13 . . . 108
4.4.1 The Brun Sieve . . . 108
4.4.2 Twin Primes . . . 110
4.5 March 15 . . . 111
4.5.1 More Counting by Geometry . . . 111
4.6 March 17 . . . 113
4.6.1 Introducing the Circle Method . . . 113
4.7 March 20 . . . 114
4.7.1 Partitions via the Circle Method . . . 114
4.7.2 Overview of the Circle Method . . . 115
4.7.3 Beginning Vinogradov's Theorem . . . 116
4.8 March 22 . . . 116
4.8.1 Major Arcs . . . 116
4.9 March 24 . . . 118
4.9.1 Singular Things . . . 118
4.10 April 3 . . . 120
4.10.1 How to Bound Minor Arcs . . . 120
4.10.2 Sieving in Minor Arcs: Type I . . . 121
4.11 April 5 . . . 123
4.11.1 Sieving in Minor Arcs: Type II . . . 123
4.11.2 Vinogradov's Sieve . . . 123
4.12 April 7 . . . 123
4.12.1 Using Vaughan's Identity . . . 124
4.13 April 10 . . . 126
4.13.1 A Duality Theorem . . . 126
4.14 April 12 . . . 127
4.14.1 The Large Sieve Inequality . . . 127
4.14.2 Quick Applications . . . 129
4.15 April 17 . . . 129
4.15.1 The Bombieri–Vinogradov Theorem . . . 130
4.16 April 19 . . . 131
4.16.1 Using the Large Sieve . . . 131
4.16.2 Using the Bilinear Method . . . 133
4.17 April 21 . . . 133
4.17.1 Continuing the Bilinear Method . . . 133
4.18 April 24 . . . 135
4.18.1 Least Nonquadratic Residues . . . 135
4.19 April 26 . . . 136
4.19.1 Reyni's Theorem . . . 136
4.19.2 Smooth Numbers . . . 138
4.20 April 28 . . . 139
4.20.1 Hua's Inequality . . . 139

A Complex Analysis **141**
A.1 Holomorphic Functions . . . 141
A.2 Path Integrals . . . 142
A.3 The Cauchy Integral Formula . . . 142
A.4 Building Primitives . . . 144
A.5 Differentiation Under the Integral . . . 146
A.6 Infinite Products . . . 147

B Entire Functions **152**
B.1 Counting Zeroes 152
B.2 Functions of Bounded Order 155
B.3 Elementary Factors 158
B.4 Hadamard Factorization 160

C Fourier Analysis **166**
C.1 The Fourier Transform 166
C.2 Fourier Inversion 169
C.3 Fourier Coefficients 172
C.4 Fourier Series 176

Bibliography **178**

List of Definitions **179**

Theme 1
Arithmetic Progressions

it looked like only a hop, skip, and jump on the map, but the drive took six hours

—Merriam-Webster Dictionary, [Mer23]

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

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

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

Proposition 1.2. Let $f \colon \mathbb{N} \to \mathbb{C}$ denote a sequence of complex numbers such that $|f(n)| = O(n^\sigma)$ for some $\sigma \in \mathbb{R}$. Then the series

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

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

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

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

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

We can now convert absolute convergence to uniform convergence of the partial sums $\{D_n\}_{n \in \mathbb{N}}$ of D, from which Lemma A.15 will finish. Fix some compact subset $D \subseteq U$, and we want to show $D_n \to D$ uniformly on D. Because D is compact, there exists $s_0 \in D$ with minimal $\operatorname{Re} s_0$; define $\sigma_0 \coloneqq \operatorname{Re} s_0$. Now, the series

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

converges by our absolute convergence.

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

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

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

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

which is what we wanted. ∎

It follows from Proposition 1.2 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 1.3 (multiplicative)**.** Let $f \colon \mathbb{N} \to \mathbb{C}$ be a function. Then f is *multiplicative* if and only if $f(nm) = f(n)f(m)$ for any $n, m \in \mathbb{N}$ such that $\gcd(n,m) = 1$.

Proposition 1.4. Let $f\colon \mathbb{N} \to \mathbb{C}$ 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

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

In fact, the product converges absolutely and uniformly on compacts.

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

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

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

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

To begin, we fix N and claim

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

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

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

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

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

which now vanishes as $M \to \infty$ because $\sum_{n=1}^{\infty} f(n)/n^s$ converges absolutely by Proposition 1.2. This completes the proof of the claim.

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

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

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

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

and now we see that the right-hand side goes to 0 as $N \to \infty$ because $\sum_{n=1}^{\infty} f(n)/n^s$ converges absolutely by Proposition 1.2. The equality follows.

It remains to show that the product converges absolutely and uniformly on compacts. We use Proposition A.25. Indeed, fix some compact $D \subseteq \{s : \operatorname{Re} s > \sigma + 1\}$. Now, we want to upper-bound

$$a_p(s) = -1 + \sum_{k=0}^{\infty} \frac{f\left(p^k\right)}{p^{ks}} = \sum_{k=1}^{\infty} \frac{f\left(p^k\right)}{p^{ks}}$$

on D. Well, let σ_0 denote the (achieved!) minimum of the continuous function $\operatorname{Re}\colon D \to \mathbb{R}$, and note that $\sigma_0 > \sigma + 1$. Now, $f(n) = O\left(n^\sigma\right)$ promises some constant C such that $|f(n)| \le Cn^\sigma$ for all n. Thus, we see

$$|a_p(s)| \le \sum_{k=1}^{\infty} \left| \frac{f\left(p^k\right)}{p^{ks}} \right| \le C \sum_{k=1}^{\infty} \frac{p^{k\sigma}}{p^{k\sigma_0}} = C \cdot \frac{p^{\sigma-\sigma_0}}{1-p^{\sigma-\sigma_0}} < Cp^{\sigma-\sigma_0}.$$

Notably, the geometric series converges because $p^{\sigma-\sigma_0} < p^{-1} < 1$. However, this finishes our check of absolute convergence by Proposition A.25 because

$$\sum_{p \text{ prime}} Cp^{\sigma-\sigma_0} < C \sum_{n=1}^{\infty} \frac{1}{n^{\sigma_0-\sigma}}$$

converges because $\sigma_0 - \sigma > 1$. ∎

Corollary 1.5. We have

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

Proof. By Proposition 1.4, we see

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

which is what we wanted. ∎

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.1.4 Characters

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

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

Remark 1.8. It is a fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for any prime p. This is nontrivial to prove; we will show it later in Proposition 3.2.

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

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

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

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

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

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

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

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

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

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

It will be helpful to have the following notation.

Notation 1.13. We might write $e\colon \mathbb{C} \to \mathbb{C}$ for the function $e(z) \coloneqq \exp(2\pi i z)$.

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

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

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

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

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

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

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

  so $\varphi((\chi_G, \chi_H)\cdot(\chi_G', \chi_H')) = \varphi(\chi_G, \chi_H)\cdot\varphi(\chi_G', \chi_H')$.

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

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

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

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

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

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

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

  This completes the proof. ∎

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

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

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

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

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

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

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

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

- Injective: suppose $\chi_k = 1$ for $k \in \mathbb{Z}$. We must show $k \in n\mathbb{Z}$. Well, we must then have
$$1 = \chi_k([1]) = e(k/n),$$
which forces $n \mid k$.
- Surjective: given some character $\chi \colon G \to \mathbb{C}^\times$, we note $\chi([1])^n = \chi([0]) = 1$, so $\chi([1])$ is an nth root of unity. Thus, there exists k such that $\chi([1]) = e(k/n) = \chi_k([1])$. Thus, for any $\ell \in \{0, 1, \dots, n-1\}$, we see
$$\chi([\ell]) = \chi(\underbrace{[1] + \cdots + [1]}_{\ell}) = \underbrace{\chi([1]) \cdot \ldots \cdot \chi([1])}_{\ell} = \underbrace{\chi_k([1]) \cdot \ldots \cdot \chi_k([1])}_{\ell} = \chi_k([\ell]),$$
so $\chi = \chi_k$ follows. ∎

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

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

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

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

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

which is what we wanted. ∎

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

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

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

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

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

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

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

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

For this, we appeal to the following lemma.

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

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

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

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

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

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

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

This completes the proof. ∎

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

1.1.5 Finite Fourier Analysis

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

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

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

Here is our Fourier transform.

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

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

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

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

Proposition 1.22. Let G be a finite abelian group.

- For any fixed $\chi \in \widehat{G}$, we have
$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq 1, \\ \#G & \text{if } \chi = 1. \end{cases}$$
- For any $g \in G$, we have
$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} 0 & \text{if } g \neq e, \\ \#G & \text{if } g = e. \end{cases}$$

Proof. We show these directly.

(a) If $\chi = 1$, then the sum is $\sum_{g\in G} 1 = \#G$.
Otherwise, $\chi \neq 1$, so there exists $g_0 \in G$ such that $\chi(g_0) \neq 1$. It follows

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

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

(b) If $g = e$, then the sum is $\sum_{\chi\in\widehat{G}}\chi(g) = \#(\widehat{G})$, which is $\#G$ by Proposition 1.16.
Otherwise, $g \neq e$, so by Lemma 1.18, there exists χ_0 such that $\chi_0(g) \neq 1$. Employing the same trick, it follows

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

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

Now here is our result.

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

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

for any $g \in G$.

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

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

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

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

which is exactly what we wanted. ■

Here is our chief application.

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

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

for any $g \in G$.

Proof. Note

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

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

1.1.6 Dirichlet Characters

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

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

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

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

Remark 1.26. Note χ is periodic with period q.

We can finally define our generalization of ζ.

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

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

By Proposition 1.2, we have absolute convergence for $\operatorname{Re} s > 1$, and $L(s,\chi)$ defines a holomorphic function there.

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

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

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

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

1.2 January 20

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

1.2.1 Abel Summation

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

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

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

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

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

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

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

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

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

To finish, we see

$$A(\lfloor x\rfloor)f(\lfloor x\rfloor) = A(x)f(x) + A(\lfloor x\rfloor)\big(f(\lfloor x\rfloor) - f(x)\big) = A(x)f(x) - \int_{\lfloor x\rfloor}^x A(t)f'(t)\,dt,$$

which when combined with the previous equality finishes. ∎

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

Here is a quick application of Theorem 1.29.

Proposition 1.31. The limit

$$\lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k}-\log n\right)$$

converges to a finite value.

Proof. Set $a_n = 1$ for each n and $f(t) \coloneqq 1/t$ so that $A(t) = \lfloor t \rfloor$. Then Theorem 1.29 tells us

$$\begin{aligned}\sum_{0<k\le n}\frac{1}{k} &= \frac{\lfloor n\rfloor}{n}+\int_0^n \frac{\lfloor t\rfloor}{t^2}\,dt\\ &= 1+\int_1^x \frac{\lfloor t\rfloor}{t^2}\,dt\\ &= 1+\int_1^x \frac{1}{t}\,dt-\int_1^x\frac{\{t\}}{t^2}\,dt\\ &= \log x+1-\int_1^x\frac{\{t\}}{t^2}\,dt.\end{aligned}$$

Thus,

$$\lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k}-\log n\right)=1-\int_1^\infty\frac{\{t\}}{t^2}\,dt,$$

and this integral converges because it is bounded above by $\int_1^\infty 1/t^2\,dt = 1$. ∎

Definition 1.32 (Euler–Mascheroni constant)**.** The *Euler–Mascheroni constant* γ is the limit

$$\gamma \coloneqq \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k}-\log n\right).$$

1.2.2 Continuing $L(s,\chi)$

As an example application of Theorem 1.29, we may give $L(s,\chi)$ an analytic continuation to $\{s : \operatorname{Re} s > 0\}$ when χ is not the principal character.

Proposition 1.33. 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 $a_n \coloneqq \chi(n)$ and $f(x) \coloneqq 1/x^s$. Then the partial sums $A(t) \coloneqq \sum_{1\le n\le t} a_n$ have

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

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

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

Now, finally using Theorem 1.29, we see

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

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

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

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

Roughly speaking, we want to write

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

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 $g \colon [1, \infty)$ by $g(t) \coloneqq q/t^{\sigma+1}$ 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 A.18 implies that $I(s)$ is holomorphic on $\{s : \operatorname{Re} s > \sigma\}$, finishing the proof. ∎

Remark 1.34. 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 1.35. Let $\chi_0 \pmod q$ be the principal Dirichlet character. Then for $\operatorname{Re} s > 1$, we have

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

Proof. By Remark 1.28, we see

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

so

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

by Corollary 1.5, which finishes. ∎

Thus, we are interested in continuing ζ. With a little more effort than Proposition 1.33, 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 1.36. The function $\zeta(s)$ has a meromorphic continuation to $\{s : \operatorname{Re} s > 0\}$. It is holomorphic everywhere except at $s = 1$, where it has a simple pole of residue 1.

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

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

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

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

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

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

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

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

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

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

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

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 A.18 implies that $I(s)$ is holomorphic on $\{s : \operatorname{Re} s > \sigma\}$, finishing the proof. ∎

Remark 1.37. Using the notions and notation of the above proof, we see that

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

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

Remark 1.38. 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 1.39. 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 $\prod_{p \mid q} (1 - p^{-s})$ is entire and has its only zero at $s = 0$. Combining Lemma 1.35 and Proposition 1.36 completes the proof. ∎

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

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

Lemma 1.40. Let $\chi \pmod q$ be a Dirichlet character. For any s with $\operatorname{Re} s > 1$, we have

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

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

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

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

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

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

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

As an aside, we note that Lemma 1.40 provides us with a relatively large zero-free region for $L(s,\chi)$.

Corollary 1.41. 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 1.40, we see

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

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

Remark 1.42. Alternatively, we can recall from Proposition 1.4 that the Euler product for $L(s,\chi)$ converges absolutely for $\operatorname{Re} s > 1$, and in particular $L(s,\chi) = 0$ would require one of the Euler factors

$$\frac{1}{1-\chi(p)p^{-s}}$$

to vanish by Remark A.24. However, none of these Euler factors vanish.

We now see that we can use Lemma 1.40 and Corollary 1.24 to extract a particular congruence class.

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

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

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

Proof. Corollary 1.24 tells us

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

so

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

However, using the notation of Lemma 1.40, we see

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

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

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

Proposition 1.44. 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 1.33.

Let χ_0 denote the principal character. By Corollary 1.39, we see $L(s,\chi_0) \to +\infty$ as $s \to 1^+$: indeed, we know $L(s,\chi_0)$ must go to something in $\mathbb{R}_{\ge 0} \cup \{\infty\}$ because $L(s,\chi_0) \ge 1$ when $s > 1$ is real. But $L(s,\chi_0)$ cannot go to a finite value because then $L(s,\chi_0)$ would only have a removable singularity at $s = 1$.

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

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

so the result follows from Lemma 1.43. ■

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

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

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 1.39 implies $v(\chi_0) = -1$, where χ_0 is the principal character. Additionally, $v(\chi) \ge 0$ for all non-principal characters χ by Proposition 1.33, and $v(\chi)$ is finite because $L(s,\chi)$ is not constantly zero by Corollary 1.41.

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

We now show the last sentence. Indeed, we have

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

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

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

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

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

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

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

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

1.3 January 23

Today we finish the proof of Theorem 1.1.

1.3.1 The Dirichlet Convolution

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

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

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

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

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

And we may now take products of Dirichlet series.

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

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

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 1.2 on F and G. Let $F_n(s)$, $G_n(s)$, and $D_n(s)$ denote the nth partial sums. Then we see

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

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

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

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

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

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

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

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

Example 1.49. 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, $1\colon \mathbb{N} \to \mathbb{C}$ is the function which constantly returns 1.

We might be interested in an Euler product factorization for a product of two Dirichlet series (as in Proposition 1.4), 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 $f, g\colon \mathbb{N} \to \mathbb{C}$ be multiplicative functions. Then $(f*g)\colon \mathbb{N} \to \mathbb{C}$ is still multiplicative.

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

- Well-defined: certainly $d_n \mid n$ and $d_m \mid m$ implies $d_n d_m \mid nm$.
- 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 $d_n \coloneqq \gcd(d, n)$ and $d_m \coloneqq \gcd(d, m)$. 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 $\nu_p(d_m) = \nu_p(m)$. 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

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

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

1.3.2 The Mellin Transform

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

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

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

Definition 1.51 (decaying)**.** A function $\varphi\colon (0,\infty)\to\mathbb{C}$ 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 $\varphi\colon (0,\infty)\to\mathbb{C}$ 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 $\varphi\colon (0,\infty)\to\mathbb{C}$ be a continuous function decaying at a rate of (α,β). Then the *Mellin transform* is the function $\mathcal{M}\varphi$ given by

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

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 $|x^\gamma \varphi(x)| \le C_\gamma$ for all $x \in (0,\infty)$. For our absolute convergence, we set $\sigma \coloneqq \operatorname{Re} s \in (\alpha,\beta)$ and compute

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

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 $\psi(u) \coloneqq e^{-\sigma u}\varphi(e^{-u})$. Provided that ψ is Schwarz, changing variables by $x = e^{-u}$ gives

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

Here is a basic result on the Mellin transform.

Lemma 1.56. Fix a differentiable function $\varphi\colon (0,\infty)\to\mathbb{C}$ such that φ decays at a rate of (α,β). Defining $\psi(x) \coloneqq x\varphi'(x)$, 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, $x^s\varphi(x)\to 0$ as $x\to 0^+$ and $x\to\infty$ 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 $\varphi\colon (0,\infty)\to\mathbb{C}$ 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 nth derivatives decays at a rate of $(\alpha-n,\beta-n)$. Then for any integer $A \ge 0$ and $[\alpha_0,\beta_0] \subseteq (\alpha,\beta)$, the set

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

is bounded.

Proof. These are essentially bounding results.

(a) We use Proposition A.18. Here, $f(s,t) \coloneqq \varphi(x)x^{s-1}$. We will show that $\mathcal{M}\varphi$ is holomorphic on the vertical strip $U \coloneqq \{s : -\alpha_0 < \operatorname{Re} s < \beta_0\}$ 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 $|x^\alpha \varphi(x)| \le C$ and $\left|x^\beta \varphi(x)\right| \le C$ for each x. As such, we define $g\colon (0,\infty) \to \mathbb{R}$ by

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

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

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

and similar for $x \in (1,\infty)$ comparing with β_0. The result now follows from Proposition A.18.

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

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

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 $\varphi\colon (0,\infty) \to \mathbb{C}$ be a function such that $\psi(u) \coloneqq e^{-\sigma u}\varphi\left(e^{-u}\right)$ 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 C.10 finishes. Following this outline, we compute

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

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 $\chi = \overline{\chi}$. We show

Proof. We combine two techniques called "positivity" and "smoothing." The main point is that $L(1,\chi) = 0$ implies that the zero of $L(s,\chi)$ at $s=1$ is able to cancel the pole of $\zeta(s)$ as $s=1$, implying that the function $\zeta(s)L(s,\chi)$ is holomorphic on $\{s : \operatorname{Re} s > 0\}$ by combining Propositions 1.33 and 1.36.

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

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

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

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

   Now, $\chi(p) = \overline{\chi(p)}$ by hypothesis on χ, so because $|\chi(p)| = 1$ by Remark 1.12, we conclude $\chi(p) \in \{\pm 1\}$. Thus, on one hand, if $\chi(p) = 1$, then $(1*\chi)\left(p^\nu\right) = \nu + 1 \ge 1$ always. On the other hand, if $\chi(p) = -1$, then $(1*\chi)\left(p^\nu\right)$ is 1 when ν is even and 0 if ν is odd. The claim follows.

   To finish, our positivity claim is that

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

   Thus, for x large enough, we see

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

2. We now apply smoothing Let $\varphi\colon (0,\infty) \to (0,\infty)$ 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

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

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

   We now use the Mellin transform $\mathcal{M}\varphi$. Indeed, note that φ is decaying at a rate of (α,β) for any $\alpha < \beta$ by Remark 1.58. Further, for any $\sigma > 0$, the function $\psi(u) := e^{-\sigma u}\varphi\left(e^{-u}\right)$ 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

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

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

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

by Remarks 1.34 and 1.37, where $C_0(q,\sigma)$ is some constant. Thus,

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

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

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

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

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

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

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

3. Anyway, we now know we can write

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

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

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

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

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

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

In total, we see

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

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

Remark 1.61. 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 $f\colon \mathbb{Z}^2 \to \mathbb{Z}$ where $f(x,y) \coloneqq ax^2+bxy+cy^2$ 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

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

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

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

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

Remark 1.66. For a binary quadratic form $f(x,y)\coloneqq ax^2+bxy+cy^2$, note that

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

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

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

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

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

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

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

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

Definition 1.68 (discriminant)**.** The *discriminant* of the binary quadratic form $f(x,y) \coloneqq ax^2 + bxy + cy^2$ is given by $\operatorname{disc} f \coloneqq b^2 - 4ac$. 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

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

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

$$f_d(x,y) \coloneqq dxy$$

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

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

Theorem 1.70. 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 $\mathrm{SL}_2(\mathbb{Z})$ on quadratic forms with the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H} \coloneqq \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ given by

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

Here are some checks on this action.

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

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

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

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

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

Proof. We show the parts one at a time.

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

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

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

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

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

We now run our checks to have a group action.

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

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

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

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

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

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

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

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

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

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

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

The above cases complete the proof. ■

Remark 1.73. 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
$$D \coloneqq \{z \in \mathbb{H} : |z| > 1, -1/2 \leq \operatorname{Re} z < 1/2\} \cup \{z \in \mathbb{H} : |z| = 1, -1/2 \leq \operatorname{Re} z \leq 0\}.$$
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
$$S \coloneqq \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \text{and} \qquad T \coloneqq \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}.$$
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 $f(x,y) \coloneqq ax^2+bxy+cz^2$ where $a, c > 0$ without loss of generality, we can study $f(x,1)$ to have a root

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

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 γf such that $z_{\gamma f} \in D$. The point here is that the number of quadratic forms up to equivalence is bounded above by the number of points in D with imaginary part $\sqrt{|d|}$. For example, the condition $|z_f| \geq 1$ 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 $d = -r$ and $w_d = 6$ if $d = -3$. (Namely, w_d is the number of roots of unity in $\mathbb{Q}(\sqrt{d})$.)

(b) If $d > 0$, then

$$h(d) \log \varepsilon_d = |d|^{1/2} L(1, \chi_d),$$

where ε_d is a fundamental unit for $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. (Namely, $\varepsilon_d = (t_0 + u_0\sqrt{d})/2$ yields the least positive solution to $t_0^2 - du_0^2 = 4$.)

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

Remark 1.77. The interested should now be able to do the first part of the first problem set.

Theme 2
The ζ-Function

Combinatorics is an honest subject. No adéles, no sigma-algebras. You count balls in a box, and you either have the right number or you haven't.

—Gian-Carlo Rota, [Rot85]

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 1.5, 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 1.36, 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.

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

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 $x \ge 2$, we have

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

Proof. Note

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

Now, note $k \ge \log_2 x$ implies that $p^k \ge 2^k \ge x$ 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

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

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

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

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 $x \to \infty$.

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 $f(n) \coloneqq 1/\log n$ if $n > 1$ and 0 at $n = 1$. Then Theorem 1.29 tells us

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

which is what we wanted. ∎

Proposition 2.7. The following are equivalent.

(a) $\pi(x) \sim x/\log x$ as $x \to \infty$.

(b) $\vartheta(x) \sim x$ as $x \to \infty$.

(c) $\psi(x) \sim x$ as $x \to \infty$.

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

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

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 $f(x) \coloneqq \log x$ for $x \ge 1$ and 0 otherwise. Thus, Theorem 1.29 implies

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $f\colon \mathbb{R} \to \mathbb{C}$ 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

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

The point is to compute the Fourier series of $F\colon \mathbb{R} \to \mathbb{C}$. 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 Nth partial sum, where $N \ge 1$. Thus, to show that F is continuous on some closed interval $[a,b]$, it suffices to show that $F_N \to F$ 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 $|x| \le m$ where $m \coloneqq \max\{|a|,|b|\}$, so we will take $N > 2m$ throughout. Now, the Schwartz condition on f lets us find a constant $C \in \mathbb{R}$ such that $\left|x^2 f(x)\right| \le C$, so

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

   The sum now splits into

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

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

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

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

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

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

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 C.20, but for this we must show that S_F converges absolutely and uniformly. Well, by Lemma C.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 C.5, so find M such that $|(\mathcal{F}f'')(s)| \le M$ for all s. Checking the absolute and uniform convergence, we see $N > 0$ lets us upper-bound

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

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

5. The previous step gives our absolute and uniform convergence, so Theorem C.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 $f_x(t) \coloneqq f(tx)$ 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 $x > 0$.

Here is the most common way we will use Theorem 2.8, which is in the form Example 2.9.

Corollary 2.10. Fix some $t > 0$ and $\alpha \in \mathbb{R}$. Then

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t - 2\pi i n\alpha} = \frac{1}{\sqrt{t}} \sum_{n\in\mathbb{Z}} e^{-\pi(n+\alpha)^2/t},$$

and both sums converge absolutely.

Proof. Set $f(x) \coloneqq e^{-\pi x^2 t - 2\pi i x\alpha}$. In particular, we note that the Gaussian $g(x) \coloneqq e^{-\pi x^2}$ is Schwarz with Fourier transform $(\mathcal{F}g)(s) = g(s)$ by Exercise C.7, so $f(x) = g(\sqrt{t}x)e^{-2\pi i x\alpha}$ is a Schwarz function with Fourier transform

$$(\mathcal{F}f)(s) = \frac{1}{\sqrt{t}}(\mathcal{F}g)\left(\frac{s+\alpha}{\sqrt{t}}\right) = \frac{1}{\sqrt{t}} e^{-\pi(s+\alpha)^2/t}.$$

Thus, by Theorem 2.8, we have

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t - 2\pi i n\alpha} = \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} (\mathcal{F}f)(n) = \sum_{n\in\mathbb{Z}} \frac{1}{\sqrt{t}} e^{-\pi(s+\alpha)^2/t} = \frac{1}{\sqrt{t}} \sum_{n\in\mathbb{Z}} e^{-\pi(s+\alpha)^2/t},$$

and all sums converge absolutely. ∎

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 2.11. Call a Schwarz function $f : \mathbb{R} \to \mathbb{R}$ "slow" if and only if the function

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

is defined on $(0,\infty)$ and decays at a rate of (α,β) for all $0 < \alpha < \beta$. If f is slow, then $I(f,s) \coloneqq (\mathcal{M}S_f)(s)$ 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 2.12. Continue in the context of Proposition 2.11, 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

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

Note at $\overset{*}{=}$ we have assumed that $f(0) = 0$, which holds because $S_f(x)$ converges absolutely. (Indeed, if $f|(0)| > 0$, then as $x \to 0^+$, 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 2.11. ∎

Remark 2.13. 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 2.14. For $\operatorname{Re} s > 0$, we define

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

Remark 2.15. 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 2.16. Define $f : [0, \infty) \to \mathbb{R}$ by $f(t) \coloneqq e^{-t}$ 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

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

(Explicitly, find N such that $|t^c f(t)| < 1$ for any $x > N$; for $x \le N$, 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 2.16 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 2.17. For any $\operatorname{Re} s > 0$, we have $\Gamma(s + 1) = s\Gamma(s)$.

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

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

which is what we wanted. ∎

Example 2.18. For any positive integer n, applying Lemma 2.17 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 2.19. We now describe how to (inductively) continue Γ using Lemma 2.17. Fix some $n \in \mathbb{N}$ and set $U_n \coloneqq \{s : \operatorname{Re} s > -n, -s \notin \mathbb{Z}_{\ge 0}\}$. Then we define $\Gamma_n \coloneqq U_n \to \mathbb{C}$ by

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

Because Γ is holomorphic on $\operatorname{Re} s > 0$, we see Γ_n is holomorphic on U_n. Further, Lemma 2.17 implies that $\Gamma_n(s) = \Gamma(s)$ for $\operatorname{Re} s > 0$, so we have indeed defined a continuation of Γ. Sending $n \to \infty$ provides our meromorphic continuation of Γ to all of $\mathbb{C}$.

Remark 2.19 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 1.38. However, just as with ζ, there is a "functional equation" for Γ which does not require the sort of inductive arguments of Remark 2.19. We begin by upgrading Lemma 2.17.

Lemma 2.20. 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 2.16 tells us that the integral defining Γ converges absolutely, so Fubini's theorem lets us write

$$\Gamma(s_1)\Gamma(s_2) = \int_0^\infty \int_0^\infty e^{-t_1-t_2}t_1^{s_1-1}t_2^{s_2-1}\,dt_1dt_2.$$

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

$$\det\left(\begin{bmatrix}\partial t_1/\partial u & \partial t_1/\partial t\\ \partial t_2/\partial u & \partial t_2/\partial t\end{bmatrix}\right) = \det\left(\begin{bmatrix}t & u\\ -t & 1-u\end{bmatrix}\right) = t.$$

Thus,

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

This still absolutely converges (indeed, we can just change coordinates back to dt_1dt_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 2.21. Because $\Gamma(1) = 1$ and $\int_0^1 u^s\,du = \frac{1}{s}$ for $\operatorname{Re} s > 0$, we see Lemma 2.20 implies

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

thus recovering Lemma 2.17.

Proposition 2.22 (Functional equation for Γ)**.** For any s with $0 < \operatorname{Re} s < 1$, we have

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

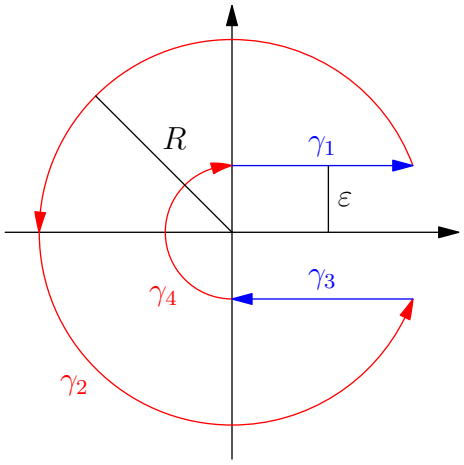
Proof. By Lemma 2.20, we see

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

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 $\mathbb{C} \setminus \mathbb{R}_{\ge 0}$ by $t \mapsto \exp((s-1)\log t)$, where $\log t$ has a branch cut at $\mathbb{R}_{\ge 0}$; 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 $f(z) \coloneqq z^{s-1}/(1+z)$ is meromorphic on $\mathbb{C} \setminus \mathbb{R}_{\ge 0}$ 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
$$\left| \frac{(t \pm \varepsilon i)^{s-1}}{1 + (t + \varepsilon i)} \right| \le \frac{(t+1)^{\operatorname{Re} s - 1}}{1+t},$$
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 $\varepsilon \to 0^+$ tells us that
$$\lim_{R\to\infty} \lim_{\varepsilon \to 0^+} \int_{\gamma_i} f(z)\,dz = \lim_{R\to\infty} \pm\lambda_i \int_0^R \frac{t^{s-1}}{1+t}\,dt = \pm\lambda_i \int_0^\infty \frac{t^{s-1}}{1+t}\,dt.$$
- On γ_2, we bound
$$\left| \int_{\gamma_2} f(z)\,dz \right| \le 2\pi R \cdot \max_{z \in \operatorname{im}\gamma_2} |f(z)|.$$
To compute this maximum, we use the fact that $|z| = R > 1$ to see
$$\left| \frac{z^{s-1}}{1+z} \right| \le \frac{R^{\operatorname{Re} s - 1}}{R-1},$$
so
$$\left| \int_{\gamma_2} f(z)\,dz \right| \le \frac{2\pi R^{\operatorname{Re} s}}{R-1} = \frac{2\pi R^{\operatorname{Re} s - 1}}{1 - 1/R}.$$
Sending $R \to \infty$ has this integral go to $0/1$ because $\operatorname{Re} s < 1$.

- On γ_4, we bound
$$\left|\int_{\gamma_4} f(z)\,dz\right| \le \pi\varepsilon \cdot \max_{z\in \operatorname{im}\gamma_t} |f(z)|.$$
To compute this maximum, we use the fact that $|z| = \varepsilon < 1$ to see
$$\left|\frac{z^{s-1}}{1+z}\right| \le \frac{\varepsilon^{\operatorname{Re} s-1}}{1-\varepsilon},$$
so
$$\left|\int_{\gamma_4} f(z)\,dz\right| \le \frac{\pi\varepsilon^{\operatorname{Re} s}}{1-\varepsilon}.$$
Sending $\varepsilon \to 0^+$ has this integral go to $0/1$ because $\operatorname{Re} s > 0$.

Combining the above integrals, we see
$$-2\pi i e^{\pi i s} = \oint_\gamma f(z)\,dz = \left(1-e^{2\pi i s}\right)\int_0^\infty \frac{t^{s-1}}{1+t}\,dt$$
upon sending $\varepsilon \to 0^+$ and then $R \to \infty$. Rearranging,
$$\Gamma(s)\Gamma(1-s) = \int_0^\infty \frac{t^{s-1}}{1+t}\,dt = \frac{-2\pi i e^{\pi i s}}{1-e^{2\pi i s}} = \frac{\pi}{\left(e^{-\pi i s}-e^{\pi i s}\right)/(2i)} = \frac{\pi}{\sin(\pi s)},$$
which is what we wanted. ∎

Example 2.23. Plugging in $s = 1/2$ into Proposition 2.22, 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 2.24. 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 $U \coloneqq \mathbb{C} \setminus (\mathbb{Z}_{\le 0} \cup \{s : 1-s \in Z\})$, and define a function $U \to \mathbb{C}$ 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 2.22 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 $\Gamma\colon U \to \mathbb{C}$.

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
$$\lim_{s\to 0} s\Gamma(s-n) = \lim_{s\to 0} \frac{s\Gamma(s-n+1)}{(s-n)} = \cdots = \lim_{s\to 0} \frac{s\Gamma(s+1)}{(s-n)(s-n+1)\cdots(s-1)(s)} = \frac{\Gamma(1)}{(-1)^n n!}.$$
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 2.18, 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 $\mathbb{C} \setminus \mathbb{Z}_{\le 0}$ by Remark 2.19. Thus, we see each $s \in \mathbb{C} \setminus \mathbb{Z}_{\le 0}$ has $1-s \in \mathbb{C} \setminus \mathbb{Z}_{\le 0}$, 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 2.25. Corollary 2.24 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! Notably, Corollary 2.24 tells us that $1/\Gamma(s)$ is entire with only simple zeroes at the nonpositive integers n.

While we're here, we give another application of Lemma 2.20.

Proposition 2.26. For any $s \in \mathbb{C} \setminus \mathbb{Z}_{\le 0}$, 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 2.20 lets us write

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

By Corollary 2.24, $\Gamma(s/2) \neq 0$ 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 2.23 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]. From Theorem B.22, we know that a lower bound on Γ will produce an upper bound on $1/\Gamma$ and thus a factorization of $1/\Gamma$. However, it will be convenient to actually provide this factorization first and then use it to produce bounds.

Proposition 2.27. For any $s \in \mathbb{C}$, we have

$$\frac{1}{\Gamma(s)} = se^{\gamma s}\prod_{n=-1}^{-\infty} E_1(s/n).$$

Here, γ is the Euler–Mascheroni constant, and $E_1(z) = (1-z)e^z$. In fact, this product converges absolutely and uniformly.

Proof. The infinite product converges absolutely and uniformly to an entire function by Lemma B.18. Indeed, we see that

$$\#\{k : -k < r\} = \lfloor r \rfloor + 1 < r + 1 \ll r^{1+\varepsilon}$$

for any $\varepsilon > 0$. (Formally, note $(r+1)r^{-1-\varepsilon} \to 0$ as $r \to \infty$, so this continuous function is bounded.) So indeed, we have all the correct convergence.

It follows from the uniqueness of analytic continuation that we can just check the identity for $s \in \mathbb{R}_{>0}$. Quickly, we remove the γ term by writing

$$\begin{aligned} se^{\gamma s} \prod_{n=-1}^{-\infty} E_1(s/n) &= \lim_{n\to\infty} se^{\sum_{k=1}^n s/k - s\log n} \prod_{k=1}^n (1+s/k)e^{-s/k} \\ &= \lim_{n\to\infty} sn^{-s} \prod_{k=1}^n (1+s/k) \\ &= \lim_{n\to\infty} \frac{s(s+1)\cdots(s+n)}{n^s n!}. \end{aligned}$$

Thus, it suffices to show that

$$\Gamma(s) \stackrel{?}{=} \lim_{n\to\infty} \frac{n^s n!}{s(s+1)\cdots(s+n)}.$$

Using the functional equation $\Gamma(s+1) = s\Gamma(s)$ from Lemma 2.17 inductively tells us that $\Gamma(n+1) = n!$ and $\Gamma(s+n+1) = (s+n)\cdots(s+1)s\Gamma(s)$, so we see

$$\lim_{n\to\infty} \frac{n^s n!}{s(s+1)\cdots(s+n)} = \lim_{n\to\infty} \left(n^s \cdot \frac{\Gamma(s)\Gamma(n+1)}{\Gamma(s+n+1)} \right).$$

Now using Lemma 2.20, this is

$$\begin{aligned} \lim_{n\to\infty} n^s \cdot \frac{\Gamma(s)\Gamma(n+1)}{\Gamma(s+n+1)} &= \lim_{n\to\infty} n^s \int_0^1 t^{s-1}(1-t)^n \, dt \\ &= \lim_{n\to\infty} \int_0^1 (nt)^{s-1}(1-t)^n \, n dt \\ &= \lim_{n\to\infty} \int_0^n t^{s-1} \left(1 - \frac{t}{n}\right)^n \, dt. \end{aligned}$$

We would like to use the Dominated convergence to compute this limit of integrals as $\Gamma(s)$. As such, we for each n, define

$$f_n(t) \coloneqq t^{s-1} \left(1 - \frac{t}{n}\right)^n 1_{\le n}(t).$$

We would like to use the Dominated convergence theorem on the f_n. Well, for $t \ge n$, we see $f_n(t) = 0$, and for $t < n$, we see

$$\log f_n(t) = (s-1)\log t + n\log\left(1 - \frac{t}{n}\right) \stackrel{*}{\le} (s-1)\log t + n\left(1 - \frac{t}{n}\right) = (s-1)\log t - t,$$

where $\stackrel{*}{\le}$ holds by using the power series $-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots$. Thus, $f_n(t) \le t^{s-1}e^{-t}$, which has a finite integral over $(0,\infty)$ bounded by $\Gamma(s)$. Thus, by the Dominated convergence theorem, we see

$$\lim_{n\to\infty} \int_0^\infty f_n(t)\, dt = \int_0^\infty \left(\lim_{n\to\infty} f_n(t)\right) \, dt = \int_0^\infty t^{s-1}e^{-t} \, dt = \Gamma(s),$$

where we have used the fact that $\left(1 - \frac{t}{n}\right)^n \to e^{-t}$ as $n \to \infty$. (This also can be seen by taking logs and bounding the error term.) This completes the proof. ∎

Corollary 2.28. For $s \in \mathbb{C} \setminus \mathbb{Z}_{\le 0}$, we have

$$\frac{\Gamma'(s)}{\Gamma(s)} = \lim_{n\to\infty} \left(\log n - \sum_{k=0}^{n} \frac{1}{s+k} \right).$$

Proof. Note that the product of Proposition 2.27 converges absolutely and uniformly. Thus, Corollary A.28 applies and tells us that

$$-\frac{\Gamma'(s)}{\Gamma(s)} = \frac{(1/\Gamma)'(s)}{(1/\Gamma)(s)} = \underbrace{\frac{1}{s}}_{s} + \underbrace{\gamma}_{e^{\gamma s}} + \sum_{k=-1}^{-\infty} \underbrace{\frac{1}{k} \cdot \frac{E_1'(s/k)}{E_1(s/k)}}_{E_1(s/k)}$$

wherever $1/\Gamma(s) \neq 0$, which is exactly $s \in \mathbb{C} \setminus \mathbb{Z}_{\le 0}$ by Remark 2.25. Now, we see

$$\frac{E_1'(z)}{E_1(z)} = \frac{1}{z-1} + 1,$$

so

$$\frac{\Gamma'(s)}{\Gamma'(s)} = -\frac{1}{s} - \gamma + \sum_{k=-1}^{-\infty} \left(\frac{1}{-k} - \frac{1}{s-k} \right) = -\frac{1}{s} - \gamma + \sum_{k=1}^{\infty} \left(\frac{1}{k} - \frac{1}{s+k} \right),$$

where we must be very careful about signs. To finish, we use the definition of γ to write

$$\frac{\Gamma'(s)}{\Gamma(s)} = \lim_{n\to\infty} \left(-\frac{1}{s} + \log n - \sum_{k=1}^{n} \frac{1}{k} + \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{s+k} \right) \right) = \lim_{n\to\infty} \left(\log n - \sum_{k=0}^{n} \frac{1}{s+k} \right),$$

which is what we wanted. ∎

Thus, to estimate Γ'/Γ, we want to know about the rate of growth of harmonic numbers. It turns out that Abel summation is not quite good enough for our purposes, so we will have to integrate by parts one more time.

Lemma 2.29 (Trapezoid rule)**.** Fix a continuously twice-differentiable function $f\colon [m,n] \to \mathbb{C}$, where $m < n$ are integers. Then

$$\sum_{k=m}^{n} f(k) = \int_m^n f(t)\,dt + \frac{f(m)+f(n)}{2} + O\left(\int_m^n |f''(t)|\,dt \right).$$

Proof. This is integration by parts twice. Indeed, we see

$$\begin{aligned}
\int_m^n f(t)\,dt &= \sum_{k=m}^{n-1} \int_k^{k+1} f(t)\,dt \\
&= \sum_{k=m}^{n-1} \left(\frac{1}{2} f(k+1) - -\frac{1}{2} f(k) - \int_k^{k+1} \left(t - n - \frac{1}{2}\right) f'(t)\,dt \right) \\
&= \sum_{k=m}^{n-1} \left(\frac{f(k+1)+f(k)}{2} - \int_k^{k+1} \left(t - n - \frac{1}{2}\right) f'(t)\,dt \right) \\
&= \sum_{k=m}^{n-1} \left(\frac{f(k+1)+f(k)}{2} - \left(\frac{1}{2}\left(n+1-n-\frac{1}{2}\right)^2 - \frac{1}{8} \right) f'(n+1) \right. \\
&\quad \left. + \left(\frac{1}{2}\left(n-n-\frac{1}{2}\right)^2 - \frac{1}{8} \right) f'(n) + \int_k^{k+1} \left(\frac{1}{2}\left(t-n-\frac{1}{2}\right)^2 - \frac{1}{8} \right) f''(t)\,dt \right) \\
&= \sum_{k=m}^{n-1} \left(\frac{f(k+1)+f(k)}{2} + \frac{1}{2} \int_k^{k+1} \left(\{t\}^2 - \{t\} \right) f''(t)\,dt \right) \\
&= \sum_{k=m}^{n} f(k) - \frac{f(m)+f(n)}{2} + \frac{1}{2} \int_m^n \left(\{t\}^2 - \{t\} \right) f''(t)\,dt.
\end{aligned}$$

Rearranging the above equality finishes upon noting that the function $\frac{\{t\}^2 - \{t\}}{2}$ has a maximum (for example, it is bounded in magnitude by $\frac{1+1}{2} = 1$). ∎

And here is our estimate.

Proposition 2.30. Fix $\varepsilon \in (0, \pi)$. For $s \in \{z \in \mathbb{C} : |\arg z| < \pi - \varepsilon\}$, we have

$$\frac{\Gamma'(s)}{\Gamma(s)} = \log s - \frac{1}{2s} + O_\varepsilon\left(1/|s|^2\right).$$

Proof. We use Corollary 2.28. Using Lemma 2.29, we set $f(t) \coloneqq 1/(s+t)$ so that

$$\begin{aligned}
\sum_{k=0}^{n} \frac{1}{s+k} &= \int_0^n \frac{1}{s+t}\,dt + \frac{f(0)+f(n)}{2} + O\left(\int_0^n \frac{2}{|s+t|^3}\,dt \right) \\
&= \log(n+s) - \log s + \frac{1}{2s} + \frac{1}{2(n+s)} + O\left(\int_0^n \frac{2}{|s+t|^3}\,dt \right).
\end{aligned}$$

We would like for the integral to be $O_\varepsilon\left(1/|s|^2\right)$ as $n \to \infty$. We have two cases.

- If $\operatorname{Re} s \geq 0$, then $|s+t| \geq \operatorname{Re}(s+t) \geq t$ and $|s+t| \geq |s|$ for each $t \geq 0$, so we can easily upper-bound

$$\begin{aligned}
\int_0^n \frac{2}{|s+t|^3}\,dt &\leq \int_0^1 \frac{2}{|s+t|^3}\,dt + \int_1^\infty \frac{2}{|s+t|^3}\,dt \\
&\leq \int_0^1 \frac{2}{|s|^3}\,dt + \int_1^\infty \frac{2}{|t|^3}\,dt \\
&= \frac{2}{|s|^3} + \left(-\frac{1}{t^2}\Big|_1^\infty \right) \\
&= \frac{2}{|s|^3} - 1,
\end{aligned}$$

  which is in fact $O\left(1/|s|^2\right)$.

- If $\operatorname{Re} s < 0$, then we note $\operatorname{Im} s > 0$ because $\arg z \neq \pi$. Here the bounding is harder; take $n > 2|s|$ for convenience. For large values of t, we note $t \geq 2|s|$ will make $|s+t| \geq t - |s|$ fairly large, so

$$\int_{2|s|}^{n} \frac{2}{|s+t|^3}\,dt \leq \int_{2|s|}^{\infty} \frac{2}{(t-|s|)^3}\,dt = -\frac{1}{(t-|s|)^2}\bigg|_{2|s|}^{\infty} = \frac{1}{|s|^2},$$

which is $O\left(1/|s|^2\right)$.

Now, the interval $t \in [0, 2|s|]$ is more difficult to handle. Because t is real, we note that $|s+t| = \sqrt{(t+\operatorname{Re} s)^2 + (\operatorname{Im} s)^2} \geq |\operatorname{Im} s|$, which is perhaps the best we can do because $s+t$ can have arbitrarily small real part in this interval. However, letting $\theta \coloneqq \arg z$, we note that

$$\frac{\operatorname{Im} s}{|s|} = |\sin\theta| \geq \sin(\pi - \varepsilon)$$

by assumption on $\arg s$. Thus,

$$\int_0^{2|s|} \frac{2}{|s+t|^3}\,dt \leq \int_0^{2|s|} \frac{2}{|\operatorname{Im} s|^3}\,dt = 2|s| \cdot \frac{2}{|\operatorname{Im} s|^3} \leq 4|\sin(\pi-\varepsilon)|^3 \cdot \frac{1}{|s|^2},$$

which is still $O_\varepsilon\left(1/|s|^2\right)$, so we are safe. Totaling our integrals finishes.

In total, we see that

$$\sum_{k=0}^{n} \frac{1}{s+k} = \log(n+s) - \log s + \frac{1}{2s} + \frac{1}{2(n+s)} + O_\varepsilon\left(1/|s|^2\right).$$

Thus, by Corollary 2.28, we see

$$\begin{aligned}
\frac{\Gamma'(s)}{\Gamma(s)} &= \lim_{n\to\infty} \left(\log n - \sum_{k=0}^{n} \frac{1}{s+k}\right) \\
&= \lim_{n\to\infty} \left(\log n - \log(n+s) + \log s - \frac{1}{2s} - \frac{1}{2(n+s)} + O_\varepsilon\left(1/|s|^2\right)\right) \\
&= \log s - \frac{1}{2s} + \lim_{n\to\infty} \left(\log\left(1 - \frac{s}{n+s}\right) - \frac{1}{2(n+s)}\right) + O_\varepsilon\left(1/|s|^2\right) \\
&= \log s - \frac{1}{2s} + O_\varepsilon\left(1/|s|^2\right),
\end{aligned}$$

which is what we wanted. ∎

Taking the integral of this allows us to recover a version of Stirling's approximation.

Proposition 2.31 (Stirling's approximation)**.** Fix $\varepsilon \in (0, \pi/2)$. For $s \in \{z \in \mathbb{C} : |\arg z| < \pi - \varepsilon\}$, we have

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

Proof. Set $\Omega_\varepsilon \coloneqq \{z \in \mathbb{C} : |\arg z| < \pi - \varepsilon\}$; note that Ω_ε is convex because (roughly speaking) any complex nonzero complex number on the line segment connecting two nonzero complex numbers α, β will have argument between the two arguments of α and β. Anyway, we proceed in steps.

1. The function Γ is holomorphic on Ω_ε and does not vanish there by Remark 2.25, so Lemma A.16 grants us a logarithm. In fact, using Remark A.17 to get our explicit logarithm, we see

$$\log\Gamma(s) = \underbrace{\log\Gamma(1)}_{0} + \int_1^s \frac{\Gamma'(z)}{\Gamma(z)}\,dz,$$

where the integral here is along the straight line from 1 to s (which does live in Ω_ε because Ω_ε is convex). Thus, we see we do in fact want to integrate the bound given by Proposition 2.30.

2. Being a little careful, we set
$$E_\varepsilon(s) \coloneqq \frac{\Gamma'(s)}{\Gamma(s)} - \log s + \frac{1}{2s}.$$
Notably, E_ε is holomorphic on Ω_ε because the right-hand side here is holomorphic on Ω_ε (for suitably chosen $\log$), so E_ε is in particular integrable. Additionally, we note that $|E_\varepsilon(s)| \le C_\varepsilon/|s|^2$ for some constant C_ε and $|s|$ large enough. Thus, fixing s and some large $N > |s|$, we compute for $|s|$ large enough that
$$\int_1^s E_\varepsilon(z)\,dz = \int_1^N E_\varepsilon(z)\,dz - \int_s^N E_\varepsilon(z)\,dz.$$
The left integral here converges absolutely as $N \to \infty$ because
$$\int_1^\infty |E_\varepsilon(z)|\,dz \le C_\varepsilon \int_1^\infty \frac{1}{z^2}\,dz = C_\varepsilon.$$
We would like to show that the right integral is $O_\varepsilon(1/|s|)$. However, if s is close to the negative real axis, there are potentially large contributions of the integral when z is roughly 0, so we change our path.

Instead of using the straight line from s to N, we follow the arc of a circle with center at $z = 0$ and radius $|s|$ until we hit the positive real axis (moving clockwise if $\operatorname{Re} s > 0$ and counterclockwise otherwise); then we move along the positive real axis from $|s|$ to N. Letting γ denote this arc, we see
$$\begin{aligned}
\left|\int_s^N E_\varepsilon(z)\,dz\right| &\le \left|\int_\gamma E_\varepsilon(z)\,dz\right| + \left|\int_{|s|}^N E_\varepsilon(z)\,dz\right| \\
&\le \ell(\gamma) \cdot \max_{z \in \operatorname{im}\gamma}\{|E_\varepsilon(z)|\} + \int_{|s|}^N |E_\varepsilon(z)|\,dz \\
&\le \pi|s| \cdot \frac{C_\varepsilon}{|s|^2} + C_\varepsilon \int_{|s|}^N \frac{1}{z^2}\,dz \\
&= \frac{C_\varepsilon \pi}{|s|} + \frac{C_\varepsilon}{|s|} - \frac{C_\varepsilon}{N}.
\end{aligned}$$
In total, we see
$$\int_1^s E_\varepsilon(z)\,dz = \int_1^N E_\varepsilon(z)\,dz + O\left(\frac{C_\varepsilon\pi}{|s|} + \frac{C_\varepsilon}{|s|} - \frac{C_\varepsilon}{N}\right).$$
Sending $N \to \infty$ shows that this is
$$\int_1^s E_\varepsilon(z)\,dz = \underbrace{\int_1^\infty E_\varepsilon(z)\,dz}_{C\coloneqq} + O_\varepsilon(1/|s|),$$
which is good enough for our purposes.

3. Integrating over E_ε, we see
$$\begin{aligned}
\log\Gamma(s) &= \int_1^s \frac{\Gamma'(z)}{\Gamma(z)}\,dz \\
&= \int_1^s \left(\log z - \frac{1}{2z}\right)\,dz + \int_1^s E_\varepsilon(z)\,dz \\
&= s\log s - s - \frac{1}{2}\log s + C + O_\varepsilon(1/|s|) \\
&= \left(s - \frac{1}{2}\right)\log s - s + C + O_\varepsilon(1/|s|)
\end{aligned}$$
for some constant C chosen above.

4. It remains to show $C = \frac{1}{2}\log 2\pi$. For this, we use Proposition 2.22. We restrict our attention to $\Omega'_\varepsilon := \{z \in \mathbb{C} : \varepsilon < |\arg z| < \pi - \varepsilon\}$. For $t > 0$, set $s := \frac{1}{2} + it$; notably, $s, 1-s \in \Omega_\varepsilon$ for $t > \frac{1}{2}$ because this gives $\arg s, \arg(1-s) \in (-\pi/2, \pi/2)$. Also, $|s| = |1-s| \geq t$. Thus, on one hand, we can use our bound above to show

$$\begin{aligned}\log\Gamma(s)\Gamma(1-s) &= \log\Gamma(s) + \log\Gamma(1-s)\\ &= it\log\left(\frac{1}{2}+it\right) - \left(\frac{1}{2}+it\right) + C - it\log\left(\frac{1}{2}-it\right) - \left(\frac{1}{2}-it\right) + C + O_\varepsilon(1/|t|)\\ &= 2C + it\log\left(\frac{1/(2t)+i}{1/(2t)-i}\right) - 1 + O_\varepsilon(1/|t|).\end{aligned}$$

We are going to need to understand the log term here more carefully. Choosing a suitable branch of $\log$ (say, now away from the positive reals), we write $x := 1/t$ so that we are interested in the behavior of the holomorphic function $f(x) := \log\left(\frac{x/2+i}{x/2-i}\right)$ at $x = 0$. Notably, $f(0) = \log(-1) = \pi i$ (for some choice of branch of $\log$). Additionally, we see

$$f'(x) = \frac{1/2}{x/2+i} - \frac{1/2}{x/2-i}$$

yields $f'(0) = -i$. Thus, our power series for f is given by $f(x) = \pi i - it + \cdots$, so

$$\lim_{t\to\infty}\left(\pi t + it\log\left(\frac{1/(2t)+it}{1/(2t)-i}\right)\right) = \lim_{x\to 0}\frac{if(x)+\pi}{x} = 1.$$

On the other hand, we see

$$\begin{aligned}\log\left(\frac{\pi}{\sin(\pi s)}\right) &= \log\pi - \log\sin\left(\frac{\pi}{2}+\pi it\right)\\ &= \log\pi - \log\left(\frac{e^{i\pi/2-\pi t} - e^{-i\pi/2+\pi t}}{2i}\right)\\ &= \log\pi - \log\left(\frac{e^{\pi t}+e^{-\pi t}}{2}\right)\\ &= -\pi t + \log 2\pi - \log\left(1+e^{-2\pi t}\right),\end{aligned}$$

up to multiples of $2\pi i$, so

$$2C + it\log\left(\frac{1/(2t)+i}{1/(2t)-i}\right) - 1 + O_\varepsilon(1/|t|) = -\pi t + \log 2\pi - \log\left(1+e^{-2\pi t}\right).$$

Quickly, we rearrange this to

$$2C + \left(\pi t + it\log\left(\frac{1/(2t)+i}{1/(2t)-i}\right) - 1\right) + O_\varepsilon(1/|t|) = \log 2\pi - \log\left(1+e^{-2\pi t}\right).$$

Thus, sending $t \to \infty$ makes almost all terms vanish, leaving us with $C = \frac{1}{2}\log 2\pi$ (up to a multiple of $2\pi i$). This completes the proof. ∎

Corollary 2.32. Fix real numbers $a < b$. For any $\sigma \in [a, b]$, we have

$$|\Gamma(\sigma+it)| \sim_{a,b} \sqrt{2\pi}e^{-\pi|t|/2}|t|^{\sigma-1/2}$$

as $|t| \to \infty$.

Proof. For psychological reasons, we quickly reduce to the case where $t > 0$. By definition of Γ, we see that $\Gamma(s) \in \mathbb{R}$ if $s \in \mathbb{R}_{>0}$, so $\Gamma(s) = \overline{\Gamma(\overline{s})}$. However, these are both holomorphic functions, so the uniqueness of analytic continuation enforces

$$|\Gamma(\sigma + it)| = |\overline{\Gamma(\sigma + it)}| = |\Gamma(\overline{\sigma + it})| = |\Gamma(\sigma - it)|.$$

Thus, adjusting for the sign appropriately, we may assume $t > 0$ in the argument which follows.

Now, this bound is an application of Proposition 2.31. Set $\varepsilon \coloneqq \pi/4$ and assume that $t > \max\{|a|, |b|\}$ throughout so that $\arg s \in (\pi/4, 3\pi/4)$. Thus, noting $|s| \geq t$, we get the estimate

$$\begin{aligned}
\log \Gamma(\sigma + it) &= \left(\sigma + it - \frac{1}{2}\right) \log(\sigma + it) - (\sigma + it) + \frac{1}{2} \log 2\pi + O(1/t) \\
&= \left(\sigma - \frac{1}{2}\right) \log t + it \log\left(\frac{\sigma}{t} + i\right) - \sigma + \frac{1}{2} \log 2\pi \\
&\quad + \left(\sigma - \frac{1}{2}\right) \log\left(\frac{\sigma}{t} + i\right) + it(\log t - 1) + O(1/t).
\end{aligned}$$

Because we want $|\Gamma(\sigma + it)| = \exp(\operatorname{Re} \log \Gamma(\sigma + it))$, we are primarily interested in the real part of the above expression. Notably, $\log\left(\frac{\sigma}{t} + i\right) \to \log i = \pi i/2$ as $t \to \infty$, so this term contributes no real part. Similarly, $it(\log t - 1)$ is purely imaginary and doesn't matter.

The hardest term left to understand is $it \log\left(\frac{\sigma}{t} + i\right)$. Well, set $x \coloneqq 1/t$ and $f(x) \coloneqq \log(\sigma x + i)$, and we want to understand the behavior of f around $x = 0$. Notably, for suitably chosen $\log$, we are holomorphic at $x = 0$ with $f(0) = \log i = i\pi/2$ and $f'(0) = \frac{\sigma}{\sigma \cdot 0 + i} = -\sigma i$. Thus,

$$\lim_{t \to \infty} \left(it \log\left(\frac{\sigma}{t} + i\right) - \sigma + \frac{\pi}{2} t\right) = \lim_{x \to 0} \frac{if(x) + \frac{\pi}{2} - \sigma x}{x} = 0,$$

so in total,

$$\lim_{t \to \infty} \log \left| \frac{\Gamma(\sigma + it)}{\sqrt{2\pi} e^{-\pi t/2} t^{\sigma - 1/2}} \right| = \lim_{t \to \infty} \left(\left(\sigma - \frac{1}{2}\right) \log t - \log t^{\sigma - 1/2} + it \log\left(\frac{\sigma}{t} + i\right) - \sigma + \frac{\pi}{2} t \right) = 0.$$

Taking $\exp$ of both sides completes the proof. ∎

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 $f \colon \mathbb{R} \to \mathbb{R}$. Staring at Corollary 2.12, we see that it will be helpful to have control over both f and $\mathcal{F}f$, so we will take $f(x) \coloneqq e^{-\pi x^2}$, even this of course does not satisfy all the hypotheses. The associated function S_f has a name.

Definition 2.33 (Γ)**.** For complex numbers $s \in \mathbb{C}$ such that $\operatorname{Re} s > 0$, define the function Θ by

$$\Theta(s) \coloneqq \sum_{n \in \mathbb{Z}} e^{-\pi n s^2}.$$

Remark 2.34. Note that series defining Θ converges absolutely and uniformly on any region $\{s : \operatorname{Re} s > \varepsilon\}$ for any $\varepsilon > 0$ by the Weierstrass M-test: indeed, we may upper-bound

$$\sum_{n \in \mathbb{Z}} \left| e^{-\pi n^2 s} \right| = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 (\operatorname{Re} s)} \leq 1 + 2 \sum_{n=1}^{\infty} e^{-\pi \varepsilon n^2} \leq 1 + 2 \sum_{n=1}^{\infty} e^{-\pi \varepsilon n} = 1 + 2 \cdot \frac{e^{-\pi\varepsilon}}{1 - e^{-\pi\varepsilon}} < \infty.$$

In particular, the uniform convergence confirms that Θ defines a holomorphic function on $\{s : \operatorname{Re} s \geq \varepsilon\}$ for any $\varepsilon > 0$ by Lemma A.15; taking the union over all $\varepsilon > 0$ confirms that Θ is holomorphic on $\{s : \operatorname{Re} s > 0\}$.

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

Proposition 2.35. For any s such that $\operatorname{Re} s > 0$, we have

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

Proof. Note that Θ is holomorphic on the region $\{s : \operatorname{Re} s > 0\}$ by Remark 2.34. On the other side, we note that $\operatorname{Re} s > 0$ implies that $\operatorname{Re}(1/s) > 0$ as well: writing $s = a + bi$ for $a > 0$, we have

$$\frac{1}{s} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i,$$

which does have positive real part. Thus, we see that $\Theta(1/s)$ is the composite of holomorphic functions and is therefore holomorphic, as is $s^{-1/2}\Theta(1/s)$.

In total, by the uniqueness of analytic continuation, it therefore suffices to show that our holomorphic functions are equal on $\mathbb{R}_{>0}$. Well, for fixed $t > 0$, we note Corollary 2.10 grants

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

which is what we wanted. ∎

As an application, we note that we get some asymptotics for Θ.

Corollary 2.36. As $\varepsilon \to 0^+$, we have $\Theta(\varepsilon) \sim 1/\sqrt{\varepsilon}$.

Proof. Note that

$$\lim_{t\to\infty} \Theta(t) \overset{*}{=} \lim_{t\to\infty} \sum_{n\in\mathbb{Z}} e^{-\pi n t^2} = \sum_{n\in\mathbb{Z}} \left(\lim_{t\to\infty} e^{-\pi n t^2}\right) = 1 + 2\sum_{n=1}^{\infty}\left(\lim_{t\to\infty} e^{-\pi n t^2}\right) = 1,$$

where the interchange of the sum and limit in $\overset{*}{=}$ is justified by the Dominated convergence theorem. For example, take the limit over functions with $t > 1$; because the functions are decreasing with respect to t, it's enough to note $\Theta(1)$ converges by Remark 2.34.

Anyway, Proposition 2.35 now implies

$$\lim_{\varepsilon\to 0^+} \sqrt{\varepsilon}\Theta(\varepsilon) = \lim_{t\to\infty} \sqrt{1/t}\Theta(1/t) = \lim_{t\to\infty} \Theta(t) = 1.$$

Rearranging completes the proof. ∎

Remark 2.37. For $z \in \mathbb{H}$, set $q \coloneqq e^{2\pi i z}$ so that $|q| < 1$. Then

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

converges absolutely and satisfies $f(z) = \Theta(-iz)$. (Notably, $z \in \mathbb{H}$ implies that $-iz \in \{s : \operatorname{Re} s > 0\}$.) Now, f is a modular form: note that $f(z+2) = f(z)$. Further, Proposition 2.35 grants $f(-1/z) = (z/i)^{1/2} f(z)$ 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 2.38 (ξ)**.** For $\operatorname{Re} s > 0$, we define

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

Similarly, we define $\Xi(s) \coloneqq s(1-s)\xi(s)$.

Remark 2.39. Note ξ is meromorphic on $\{s : \operatorname{Re} s > 0\}$ with only a simple pole at $s = 1$ because $s \mapsto \pi^{-s/2}\Gamma(s/2)$ is holomorphic here (see Remark 2.16), and ζ is meromorphic with only a simple pole at $s = 1$ (see Proposition 1.36).

Remark 2.40. 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 2.41. For $\operatorname{Re} s > 1$, 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 2.12. 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 2.42 (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 2.35 with Lemma 2.41. We proceed in steps.

1. The integral in Lemma 2.41 is poorly behaved for $\operatorname{Re} s < 1$ because of the integral over $t \in (0, 1)$, so we define
$$I(s) \coloneqq \int_1^\infty \left(\frac{\Theta(t) - 1}{2}\right) t^{s/2} \frac{dt}{t}.$$
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 A.18. For one, the function $t \mapsto \left(\frac{\Theta(t)-1}{2}\right) t^{s/2}$ is continuous (recall Θ is continuous by Remark 2.34) and hence measurable. Lastly, we must upper-bound
$$\begin{aligned}
\int_1^\infty \left|\left(\frac{\Theta(t) - 1}{2}\right) t^{s/2}\right| \frac{dt}{t} &= \frac{1}{2}\int_1^\infty \left(\sum_{n=1}^\infty e^{-\pi n^2 t}\right) t^{\sigma/2} \frac{dt}{t} \\
&\le \frac{1}{2}\int_1^\infty \left(\sum_{n=1}^\infty e^{-\pi n t}\right) t^{\sigma/2} \frac{dt}{t} \\
&= \frac{1}{2}\int_1^\infty \frac{e^{-\pi t} t^{\sigma/2}}{1 - e^{-\pi t}} \frac{dt}{t} \\
&\le \frac{1}{2\left(1 - e^{-\pi}\right)} \int_1^\infty e^{-\pi t} t^{\sigma/2} \frac{dt}{t}.
\end{aligned}$$
   Thus, we take $g \colon (1, \infty) \to \mathbb{C}$ by $g(t) \coloneqq e^{-\pi t} t^{\sigma/2 - 1} / \left(2\left(1 - e^{-\pi}\right)\right)$. Using Proposition A.18, it remains to show that $\int_1^\infty g(t)\, dt < \infty$. Well, $e^{-\pi t} t^{\sigma/2+1} \to 0$ as $t \to \infty$, so this function achieves a maximum on $[1, \infty)$,[1] which we will call M. It follows
$$\int_1^\infty g(t)\, dt \le \frac{1}{2\left(1 - e^{-\pi}\right)} \int_1^\infty \frac{M}{t} \frac{dt}{t} < \infty.$$

2. Having controlled the $(1, \infty)$ part of the integral in Lemma 2.41, we turn to the $(0, 1)$ part. The idea here is to use Proposition 2.35 to transform the $(0, 1)$ part back into a well-behaved $(1, \infty)$ part. Indeed, for $\operatorname{Re} s > 1$, we may evaluate
$$\begin{aligned}
\int_0^1 \left(\frac{\Theta(t) - 1}{2}\right) t^{s/2} \frac{dt}{t} &= \int_1^\infty \left(\frac{\Theta(1/t) - 1}{2}\right) t^{-s/2} \frac{dt}{t} \\
&= \int_1^\infty \left(\frac{\sqrt{t}\Theta(t) - 1}{2}\right) t^{-s/2} \frac{dt}{t} \\
&= \int_1^\infty \left(\frac{\sqrt{t}\Theta(t) - \sqrt{t}}{2}\right) t^{-s/2} \frac{dt}{t} - \frac{1}{2}\int_1^\infty t^{-s/2} \frac{dt}{t} + \frac{1}{2}\int_1^\infty t^{(1-s)/2} \frac{dt}{t} \\
&= \int_1^\infty \left(\frac{\Theta(t) - 1}{2}\right) t^{(1-s)/2} \frac{dt}{t} - \int_1^\infty t^{-s} \frac{dt}{t} + \int_1^\infty t^{1-s} \frac{dt}{t} \\
&= I(1 - s) - \frac{1}{s} - \frac{1}{1 - s}.
\end{aligned}$$

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

3. Synthesizing the previous steps, Lemma 2.41 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. ∎

Remark 2.43. Directly from Theorem 2.42, we see that $\Xi(s) = s(1-s)\xi(s)$ is an entire function and satisfies the functional equation

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

2.2.5 Corollaries of the Functional Equation

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

Corollary 2.44 (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 $s \in \mathbb{C} \setminus \mathbb{Z}_{\le 0}$, 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 2.42 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 through $\Gamma(s/2)$ has a simple pole at nonpositive even integers $-2n$ by Corollary 2.24 at these points $\xi(s)$ will have at worst simple pole by Theorem 2.42 as well, so we can just multiply the numerator and denominator by $(s-2n)$ until the denominator is nonzero.

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 2.24.) However, at $s = 1$, we already know that ζ has a simple pole of residue 1 by Proposition 1.36.

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 2.42 grants

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

Multiplying both sides by $\Gamma\left(\frac{1+s}{2}\right)$, we see Proposition 2.22 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 2.26 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 2.45. Note

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

Using L'Hôpital's rule, we see $\cos(\pi s/2)/(s-1)\to -\pi/2$ as $s\to 1$. By Proposition 1.36, we see $(s-1)\zeta(s)\to 1$ as $s\to 1$. 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 2.46. We have the following.

(a) Conjugate symmetry: if $\zeta(s) = 0$, then $\zeta(\overline{s}) = 0$.

(b) Trivial zeroes: the function ζ has a simple zero at $-2n$ for each positive integer n.

(c) Critical strip: if $\zeta(s) = 0$ and $-s/2\notin\mathbb{N}$, then $0\le\operatorname{Re}s\le 1$.

(d) Horizontal symmetry: if $\zeta(s) = 0$ and $0\le\operatorname{Re}s\le 1$, then $\zeta(1-s) = 0$.

Proof. Here we go.

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

Because ζ is holomorphic in this region, we see that $s\mapsto\overline{\zeta(\overline{s})}$ 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

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

(b) For any positive integer n, write

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

As $s\to -2n$, the numerator vanishes because ξ is holomorphic at $s=-2n$ by Theorem 2.42. 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 2.24 which is cancelled by the factor of $(s+2n)$. In total, we conclude

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

To compute the order of the zero at $-2n$, the argument above implies that the order of vanishing of ζ is one more than the order of vanishing of ξ. However,

$$\xi(-2n) = \xi(1+2n) = \pi^{-(1+2n)}\Gamma((1+2n)/2)\zeta(1+2n)$$

does not vanish. In particular, Γ does not vanish by Remark 2.25, and ζ does not vanish by Corollary 1.41.

(c) If $\operatorname{Re} s > 1$, then $\zeta(s) \neq 0$ by Corollary 1.41 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 2.24, 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 2.45, 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 2.24.) Thus, $\zeta(s) = 0$ implies $\zeta(1-s) = 0$. ∎

Remark 2.47. The negative even integers are called the "trivial" zeroes of $\zeta(s)$. The remaining ones, which all lie in the "critical strip" $\{s \in \mathbb{C} : 0 \leq \operatorname{Re} s \leq 1\}$ by Corollary 2.46, are called the "nontrivial" zeroes.

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 Counting Zeroes of ζ

We would like to understand the (nontrivial) 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 $\mathbb{C}$.

It will be convenient to work with the more symmetric (and entire) function Ξ instead of ζ. Let's justify this.

Lemma 2.48. We have an equality of multisets

$$\{s \in \mathbb{C} : \Xi(s) = 0\} = \{s \in \mathbb{C} : \zeta(s) = 0 \text{ and } 0 \leq \operatorname{Re} s \leq 1\}.$$

Proof. Recall that $\Xi(s) = s(1-s)\pi^{-s/2}\Gamma(s/2)\zeta(s)$. We now show our two inclusions.

- If $\zeta(s) = 0$ and $0 \leq \operatorname{Re} s \leq 1$, then we $s \neq 1$ (because $\zeta(s)$ has a pole there by Proposition 1.36) and $s \neq 0$ by Example 2.45, and we note $\pi^{-s/2} \neq 0$. Thus, $s \neq 0$, so $\Gamma(s/2) \neq 0$ by Corollary 2.24 as well, so the order of vanishing of ζ at s equals the order of vanishing of Ξ at s.
- If $\Xi(s) = 0$, then one of the factors must vanish. For $s = 0$, we see $\Gamma(s/2)$ has a simple pole by Corollary 2.24 cancelling out the zero. For $s = 1$, we see $\zeta(s)$ has a simple pole by Proposition 1.36 cancelling out the zero. Further, $\Gamma(s/2)$ has no zeroes at all by Remark 2.25. Thus, we see we must have $\zeta(s) = 0$, and in fact s cannot be a trivial zero because $\Gamma(s/2)$ has simple poles there to cancel out those zeroes by Corollary 2.24.

  So s must be in the critical strip, where we note that all the other terms fail to vanish (in particular, Γ fails to vanish by Remark 2.25), so the order of vanishing of Ξ at s is equal to the order of vanishing of ζ at s. ∎

Quickly, we give a pretty basic bound on the number of zeroes from Proposition B.12.

Lemma 2.49. The order of Ξ is less than or equal to 1.

Proof. Because $\Xi(s) = \Xi(1-s)$, we will focus on the region $\operatorname{Re} s \geq 1/2$. Recalling that $\Xi(s) = s(1-s)\pi^{-s/2}\Gamma(s/2)\zeta(s)$, we will simply compute the orders of these terms one at a time.

- The order of $s(1-s)$ is 0 by Example B.7.
- We note
$$\left|\pi^{-s/2}\right| = \left|e^{-s(\log\pi)/2}\right| = e^{-\operatorname{Re}(s)(\log\pi)/2}.$$
In particular, $\operatorname{Re} s > 0$ implies that this term is less than or equal to 1 and hence bounded by a polynomial and hence order 0 by Example B.7 again.
- For $\operatorname{Re} s > 1/2$, we note that $|\arg s| < \pi/2$, so we can apply Proposition 2.31. In particular, we note that
$$\begin{aligned}
\lim_{|s|\to\infty}\left|\frac{\Gamma(s)}{s^s}\right| &= \exp\left(\left|\lim_{|s|\to\infty}\frac{\log\Gamma(s)}{s\log s}\right|\right) \\
&= \exp\left(\lim_{|s|\to\infty}\frac{\left(s-\frac{1}{2}\right)\log s - s + \frac{1}{2}\log 2\pi + O(1/|s|)}{s\log s}\right) \\
&= \exp\left(\left|1 + \lim_{|s|\to\infty}\frac{\left(-\frac{1}{2}\right)\log s - s + \frac{1}{2}\log 2\pi + O(1/|s|)}{s\log s}\right|\right) \\
&= \exp(1).
\end{aligned}$$
Thus, $|\Gamma(s)/s^s|$, which is continuous in our region with $\operatorname{Re} s > 1/2$, is a bounded function.

■

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 2.50. Define
$$N(T) \coloneqq \#\{\rho : 0 \leq \operatorname{Re}\rho \leq 1, \operatorname{Im}\rho \geq 0 \zeta(\rho) = 0\}.$$
Then
$$N(T) = \frac{T}{2\pi}\log\left(\frac{T}{2\pi}\right) - \frac{T}{2\pi} + O(\log T)$$
as $T \to \infty$.

We will first show the following lemma.

Lemma 2.51. 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

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

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 2.52. 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 2.51.

Corollary 2.53. 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 2.51 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 2.54. For $t > 3$, we have

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

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 2.51 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 2.55. One can give more accurate bounding than the above, but we will not need it.

We now return to the proof of Theorem 2.50.

Proof of Theorem 2.50. 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 2.54 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 2.53, 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 2.56. When x is not a prime-power, we have

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

Remark 2.57. Ignoring convergence issues, we may compute

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

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

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

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

Here is a lemma.

Lemma 2.58. We have

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

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

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

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

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

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

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

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

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

Now, setting $c = 1 + 1/\log T$, we get an upper-bound of $O\left(x(\log x)^2/T\right)$. 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 $U \to \infty$ for fixed T. We will then send $T \to \infty$, always remembering to choose T avoiding zeroes of $\zeta(s)$. In particular, by Corollary 2.53, 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 $|x^s| \le x^{\operatorname{Re} s}$, 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

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

for, say, $-1 \le \sigma \le 2$. Thus, the contribution of the integral over $-1 \le \sigma \le c$ 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 $T \to \infty$.

> **Remark 2.59.** 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 $\{s : \operatorname{Re} s \le -1\}$ 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 $\operatorname{Re} s \le -1$ 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

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

where x is not a prime power. Note the contributions of $-\frac{1}{2}\log\left(1-x^{-s}\right)$ 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 2.60. Fix some $t_0 \in \mathbb{R}$ and $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$. Defining $\sigma_z(n) \coloneqq \sum_{d|n} d^z$, 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 2.61 (Landau)**.** Let $\{a_n\}_{n\in\mathbb{N}}$ be a sequence of nonnegative real numbers, and define

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

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 2.61, but we cannot vanish at $s = 1/2$ by just staring at it. Thus, we could not actually have continued it any further.

Remark 2.62. 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 2.63. 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 $M := (D+1)\prod_{i=1}^{L}(|\alpha_i|+1)$ is the "analytic conductor," and $c(\ell, m)$ is a constant computable from ℓ and m.

Remark 2.64. 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 2.63 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 2.65. 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 2.63 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 2.66. The magical $D(s)$ from Example 2.65 does come from a larger structure, but it is somewhat advanced to explain.

Remark 2.67. It might look upsetting that Example 2.65 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 2.63, let's prove it.

Proof of Lemma 2.63. 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

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

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

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

where C_1 is some constant depending on ℓ and m. In particular, if we send $s \to 1^+$ 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

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

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

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

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

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

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 $x \to \infty$.

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

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

However, we can upper-bound

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

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

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

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

Theme 3
Dirichlet L-Functions

Come on, baby
Let's do the twist

—Chubby Checker, [Che60]

3.1 February 8

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

Warning 3.1. In the class, the professor spread discussion of things about characters throughout this chapter. In order to isolate the elementary parts of the discussion from the analytic ones, I have attempted to collect all the character theory in today's lecture.

3.1.1 Quadratic Residues

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

Proof. We proceed in steps.

1. Given $a, b \in \mathbb{F}_p^\times$ of orders k and ℓ, we claim that there is an element $x \in \mathbb{F}_p^\times$ of order $\operatorname{lcm}(k, \ell)$. Roughly speaking, the idea is that $\gcd(k, \ell) = 1$ will imply that ab has order $k\ell$: of course, $(ab)^{k\ell} = 1$, and to see that $k\ell$ is the smallest exponent, note $(ab)^n = 1$ implies $(ab)^{nk} = 1$, so $b^{nk} = 1$, so $\ell \mid nk$, so $\ell \mid n$ because $\gcd(k, \ell) = 1$. Analogously, $k \mid n$, so $k\ell \mid n$.

   To extend the above proof to the case of $\gcd(k, \ell) > 1$, we use unique prime factorization. Set

$$k' \coloneqq \prod_{\nu_p(k) \geq \nu_p(\ell)} p^{\nu_p(k)} \qquad \text{and} \qquad \ell' \coloneqq \prod_{\nu_p(k) < \nu_p(\ell)} p^{\nu_p(\ell)}.$$

In particular, we see that $\nu_p(k') > 0$ if and only if $\nu_p(k) \geq \nu_p(\ell)$, and $\nu_p(\ell') > 0$ if and only if $\nu_p(k) < \nu_p(\ell)$. Thus, no prime p divides both k' and ℓ', so $\gcd(k', \ell') = 1$. Further, by construction, we see $k' \mid k$ and $\ell' \mid \ell$ and

$$k'\ell' = \prod_{\nu_p(k) \geq \nu_p(\ell)} p^{\nu_p(k)} \cdot \prod_{\nu_p(k) < \nu_p(\ell)} p^{\nu_p(\ell)} = \prod_p p^{\max\{\nu_p(k), \nu_p(\ell)\}} = \operatorname{lcm}(k, \ell).$$

Thus, we see that $a^{k/k'}$ has order k', and $b^{\ell/\ell'}$ has order ℓ', so their product $x \coloneqq a^{k/k'} b^{\ell/\ell'}$ has order $k'\ell' = \gcd(k, \ell)$.

2. Inductively applying the previous step to every $a \in \mathbb{F}_p^\times$, we produce an element $g \in \mathbb{F}_p^\times$ with order n which is the least common multiple of the orders of all $a \in \mathbb{F}_p^\times$. In particular, the order of $a \in \mathbb{F}_p^\times$ divides into n, so we see that

$$a^n \equiv 1 \pmod{p}.$$

In particular, the equation $x^n - 1 = 0$ has $p - 1$ roots in $\mathbb{F}_p$ given by the elements of $\mathbb{F}_p^\times$. However, for a field, the number of roots of a polynomial is bounded by the degree, so $x^n - 1 = 0$ has at most n solutions, so we conclude $n \geq p - 1$. Because the order of g must divide $\#\mathbb{F}_p^\times = p - 1$, we conclude that $n \leq p - 1$ as well, so $n = p - 1$ is forced. So g is a generator of $\mathbb{F}_p^\times$. ∎

We can extend this result as follows.

Proposition 3.3. Fix an odd prime p. For any $\nu > 0$, the group $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ is cyclic.

Proof. We induct in steps.

- The case of $\nu = 1$ is from Proposition 3.2.
- The case of $\nu = 2$ requires some care. Let $g \in \mathbb{F}_p^\times$ be a generator from the $\nu = 1$ case. If $g \pmod{p^2}$ already has order $p(p-1)$, then we are done. Otherwise, $g \pmod{p^2}$ has order n strictly less than $p(p-1)$. However, note that $g^n \equiv 1 \pmod{p^2}$ implies

$$g^n \equiv 1 \pmod{p},$$

so $p - 1 \mid n$ because the order of $g \pmod{p}$ is $p - 1$. Thus, $p - 1 \mid n$ and $k \mid p(p-1)$ but $n < p(p-1)$ forces $n = p - 1$, so $g^{p-1} \equiv 1 \pmod{p^2}$.

Now, the trick is to consider $g + p$. Note $g + p$ is still a generator of $\mathbb{F}_p^\times$, so its order is divisible by $(p-1)$ but divides $p(p-1)$ and so equals $p(p-1)$ or $(p-1)$. To see that the order is not $(p-1)$, we note

$$\begin{aligned}(g+p)^{p-1} &= \sum_{k=0}^{p-1} \binom{p-1}{k} g^{(p-1)-k} p^k \\ &\equiv g^{p-1} + (p-1)g^{p-2}p \\ &\equiv 1 - g^{p-2}p \pmod{p^2}.\end{aligned}$$

However, $g^{p-2} \not\equiv 0 \pmod{p}$, so $(g+p)^{p-1} \not\equiv 1 \pmod{p-1}$. We conclude that the order of $g + p$ must be $p(p-1)$.

- To help the following induction, we note that some $g \in \mathbb{Z}$ which is a generator of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ will have $g^{p-1} \equiv 1 \pmod{p}$ but $g^{p-1} \not\equiv 1 \pmod{p^2}$, so we can write

$$g^{p-1} = 1 + pa$$

for some integer a not divisible by p. Thus, we see

$$\begin{aligned} g^{p(p-1)} &= (1+pa)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} (pa)^k \\ &\equiv 1 + p \cdot pa + \frac{p(p-1)}{2} \cdot (pa)^2 \\ &\equiv 1 + p^2 a \pmod{p^3}. \end{aligned}$$

Thus, we actually see $g^{p(p-1)} \not\equiv 1 \pmod{p^3}$. Note that we have used $p \neq 2$ in the above computation.

- The induction in the remaining cases $\nu \geq 2$ is easier. Suppose that we have $g \in \mathbb{Z}$ which is a generator $g \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times$ with $g^{p^{\nu-1}(p-1)} \not\equiv 1 \pmod{p^{\nu+1}}$. Then we claim that g is also a generator of $(\mathbb{Z}/p^{\nu+1}\mathbb{Z})^\times$ with $g^{p^\nu(p-1)} \not\equiv 1 \pmod{p^{\nu+2}}$. This will complete the proof by induction, where the base case was shown in the previous two steps.

  Well, we note that the order of $g \pmod{p^{\nu+1}}$ must certainly divide $p^\nu(p+1)$, and we want to show equality. For this, we see $g^n \equiv 1 \pmod{p^{\nu+1}}$ will imply $g^n \equiv 1 \pmod{p^\nu}$, so n is divisible by $p^{\nu-1}(p-1)$. Thus, the order of $g \pmod{p^{\nu+1}}$ is divisible by $p^{\nu-1}(p-1)$, but the order is not actually equal to $p^{\nu-1}(p-1)$ because

  $$g^{p^{\nu-1}(p-1)} \not\equiv 1 \pmod{p^{\nu+1}}.$$

  So the order is a divisor of $p^\nu(p+1)$ divisible by but strictly greater than $p^{\nu-1}(p-1)$, so the order must actually be $p^\nu(p+1)$. We conclude that $g \pmod{p^{\nu+1}}$ is a generator.

  To complete the induction, we must show $g^{p^\nu(p-1)} \not\equiv 1 \pmod{p^{\nu+2}}$. Well, by hypothesis, we may write $g^{p^\nu(p-1)} = 1 + p^{\nu+1}a$ for some a not divisible by p. Then

  $$\begin{aligned} g^{p^{\nu+1}(p-1)} &= \left(1 + p^{\nu+1}a\right)^p \\ &= \sum_{k=0}^{p} \binom{k}{p} \left(p^{\nu+1}a\right)^k \\ &\equiv 1 + p^{\nu+1}a \pmod{p^{\nu+2}}, \end{aligned}$$

  where we don't care about the other terms because $p^{(\nu+1)k} \equiv 0 \pmod{p^{\nu+2}}$ for $k \geq 2$. Because $p \nmid a$, the conclusion follows. ∎

Proposition 3.4. For any $\nu \geq 2$, we have $(\mathbb{Z}/2^\nu\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{\nu-2}\mathbb{Z}$.

Proof. We proceed in steps.

1. For any $\nu \geq 0$, we claim that

   $$5^{2^\nu} \equiv 1 + 2^{\nu+2} \pmod{2^{\nu+3}}.$$

   We proceed by induction. For $\nu = 0$, the statement reads $5 \equiv 1 + 4 \pmod 8$, which is true. Then for the induction, we are given that $5^{2^\nu} = 1 + (1+2a)2^{\nu+2}$ for some integer a and compute

   $$\begin{aligned} 5^{2^{\nu+1}} &= \left(1 + (1+2a)2^{\nu+2}\right)^2 \\ &= 1 + (1+2a)2^{\nu+3} + (1+2a)^2 2^{2\nu+4} \\ &\equiv 1 + 2^{\nu+3} \pmod{2^{\nu+4}}. \end{aligned}$$

   Notably, $2\nu+4 \geq \nu+4$, so the rightmost term vanishes in the last equivalence. Anyway, this completes the induction.

2. For any $\nu \geq 0$, we claim that the order of $5 \pmod{2^{\nu+2}}$ is 2^ν. Certainly the order divides 2^ν because
$$5^{2^\nu} \equiv 1 \pmod{2^{\nu+2}}$$
from the previous step. If $\nu = 0$, there is nothing else to say. Otherwise, we see the order must exceed $2^{\nu-1}$ because
$$5^{2^{\nu-1}} \equiv 1 + 2^{\nu+1} \pmod{2^{\nu+2}}$$
by the previous step again, so we conclude the order actually equals 2^ν.

3. For any $\nu \geq 2$, we claim that
$$\mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2^{\nu-2}\mathbb{Z}) \cong \langle \pm 1 \rangle \oplus \langle 5 \rangle \to (\mathbb{Z}/2^\nu\mathbb{Z})^\times$$
is an isomorphism, which will complete the proof. Note that the left map is an isomorphism because -1 has order 2, and $5 \pmod{2^\nu}$ has order $2^{\nu-2}$ by the previous step. As such, it remains to show that the right map given by $(a, b) \mapsto ab$ is an isomorphism.

   To begin, note that the map is a group homomorphism because it is the product map induced by the inclusions $\langle \pm 1 \rangle \subseteq (\mathbb{Z}/2^\nu\mathbb{Z})^\times$ and $\langle 5 \rangle \subseteq (\mathbb{Z}/2^\nu\mathbb{Z})^\times$. Further, we note that our two groups both have size $2 \cdot 2^{\nu-2} = 2^{\nu-1} = \varphi(2^\nu)$, so it is enough to show that our map is injective to show that we have a bijection. Well, suppose that
$$(-1)^a \cdot 5^b \equiv 1 \pmod{2^\nu}$$
for some (a, b); we must show that $(a, b) = (0, 0)$. Well, $\nu \geq 2$, so we may reduce $\pmod 4$ to give us that $(-1)^a \equiv 1 \pmod 4$, so $a \equiv 0 \pmod 2$. We then see $5^b \equiv 1 \pmod{2^\nu}$, so $b \equiv 0 \pmod{2^{\nu-2}}$. This completes the proof. ■

Anyway, let's start talking about quadratic residues.

Corollary 3.5. Fix a prime p and some $d \in \mathbb{Z}^+$.

(a) The function $\mu_d \colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ given by $\mu_d \colon x \mapsto x^d$ is a homomorphism.

(b) If $\gcd(d, p-1) = 1$, then μ_d is an isomorphism.

(c) If $d \mid p-1$, then each $a \in \mathbb{F}_p^\times$ makes $x^d \equiv a \pmod p$ have either 0 or d solutions.

Proof. Here we go.

(a) This holds because $\mathbb{F}_p^\times$ is abelian: note $\mu_d(xy) = (xy)^d = x^d y^d = \mu_d(x)\mu_d(y)$.

(b) Because $\gcd(d, p-1) = 1$, we can find $k \pmod{p-1}$ such that $dk \equiv 1 \pmod{p-1}$. It follows that
$$\mu_k(\mu_d(x)) = x^{dk} = x \qquad \text{and} \qquad \mu_d(\mu_k(x)) = x^{kd} = x$$
for each $x \in \mathbb{F}_p^\times$, where we are using the fact that the order of x divides $p-1$. Thus, μ_k provides the inverse homomorphism for μ_d, which shows that μ_d is an isomorphism.

(c) If $x^d \equiv a \pmod p$ has no solutions, then there is nothing to say.

   Otherwise, fix a generator $g \in \mathbb{F}_p^\times$ by Proposition 3.2, and suppose that $g^\ell \in \mathbb{F}_p^\times$ is a solution to $x^d \equiv a \pmod p$ so that $a = g^{d\ell}$. Then we note some $x = g^k$ is a solution to $x^d = a$ if and only if
$$g^{dk} = x^d = a = g^{d\ell},$$
which is equivalent to $p-1 \mid (dk - d\ell)$. Because $d \mid p-1$, this is equivalent to $\frac{p-1}{d} \mid (k - \ell)$, or $\ell \equiv k \pmod{\frac{p-1}{d}}$. As ℓ varies through $\mathbb{Z}/(p-1)\mathbb{Z}$, we see that there are exactly $(p-1)/d$ total options present for ℓ. ■

This motivates the Legendre symbol.

Definition 3.6 (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 $p \mid a$.

Remark 3.7. Suppose p is an odd prime. Given $a \in \mathbb{F}_p^\times$, write $a = g^k$, where $g \in \mathbb{F}_p^\times$ is a generator.

- If k is even, then note a is a quadratic residue because $a \equiv \left(g^{k/2}\right)^2 \pmod{p}$.
- Conversely, if a is a quadratic residue, then k is even. Indeed, if we can write $a \equiv x^2 \pmod{p}$, then we see $p \nmid a$ enforces $p \nmid x$, so writing $x = g^\ell$ for some integer ℓ, we must have
$$g^k = a = x^2 = g^{2\ell}.$$
Rearranging, we have $k - 2\ell \equiv 0 \pmod{p-1}$, but $p-1$ is even, so this forces k to be even.

Definition 3.8 (Legendre symbol)**.** Fix an odd prime p and some $a \in \mathbb{Z}$. Then we define the *Legendre symbol* by
$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue}, \\ -1 & \text{if } a \text{ is a nonquadratic residue}. \end{cases}$$

Here is a quick way to evaluate Legendre symbols.

Proposition 3.9 (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. We proceed in cases.

- If $p \mid a$, then we see $0 \equiv 0^{(p-1)/2} \pmod{p}$.
- If $a \pmod{p}$ is a quadratic residue, then we can write $a \equiv b^2 \pmod{p}$ for some $b \pmod{p}$. Note $p \nmid a$ forces $p \nmid b$, so we can compute
$$a^{(p-1)/2} = b^{p-1} \equiv 1 = \left(\frac{a}{p}\right) \pmod{p},$$
as desired.
- If $a \pmod{p}$ is a nonquadratic residue, then we pick up a generator $g \in \mathbb{F}_p^\times$ from Proposition 3.2. As such, we can write $a = g^k$ for some integer k; note that k is odd by Remark 3.7. As such, we compute
$$a^{(p-1)/2} \equiv g^{k(p-1)/2} = \left(g^{(p-1)/2}\right)^k \equiv (-1)^k = -1 \pmod{p}.$$
Notably, $g^{(p-1)/2} \equiv -1 \pmod{p}$ because $g^{(p-1)/2}$ cannot be $1 \pmod{p}$ (because the order of g is $p-1$), but $g^{(p-1)/2}$ must square to $1 \pmod{p}$, which forces $g^{(p-1)/2} \equiv -1 \pmod{p}$. ∎

Remark 3.10. Requiring $p \neq 2$ might look concerning, but every residue in $\mathbb{F}_2^\times = \{1\}$ is a square anyway, so the analysis here is somewhat trivial.

Corollary 3.11. 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. If $p \equiv 1 \pmod 4$, we write $p = 1 + 4k$ and note

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} = (-1)^{2k} = 1 \pmod p,$$

so $p > 2$ forces $\left(\frac{-1}{p}\right) = 1$. Similarly, if $p \equiv -1 \pmod 4$, we write $p = -1 + 4k$ and note

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} = (-1)^{-1+2k} = -1 \pmod p,$$

so $p > 2$ forces $\left(\frac{-1}{p}\right) = -1$. This is what we wanted. ∎

In our discussion of L-functions, the following result explains why we care about Legendre symbols.

Proposition 3.12. Fix a prime p. Then the Legendre symbol $\left(\frac{\bullet}{p}\right)$ is the unique non-principal real Dirichlet character $\pmod p$.

Proof. Fix a real Dirichlet character $\chi \pmod p$. In particular, χ arises from a character $\chi\colon \mathbb{F}_p^\times \to \mathbb{R}^\times$, but by Remark 1.12, we see that χ must output to $S^1 \cap \mathbb{R}^\times = \{\pm 1\}$. Fixing a generator $g \in \mathbb{F}_p^\times$ by Proposition 3.2, we have two cases.

- Suppose $\chi(g) = 1$. Then for any $g^k \in \mathbb{F}_p^\times$, we see $\chi\left(g^k\right) = \chi(g)^k = 1$. Thus, $\chi \pmod p$ is the principal character.
- Suppose $\chi(g) = -1$. Then for any $g^k \in \mathbb{F}_p^\times$, we see

  $$\chi\left(g^k\right) = \chi(g) = (-1)^k.$$

  Now, comparing Remark 3.7 with the definition of the Legendre symbol, we see that $\chi(a) = \left(\frac{a}{p}\right)$ for each $a \in \mathbb{F}_p^\times$ because, upon writing $g = a^k$ for some integer k, both are 1 when k is even, and both are -1 when k is odd. Lastly, both χ and $\left(\frac{\bullet}{p}\right)$ vanish on multiples of p, so we conclude that $\chi = \left(\frac{\bullet}{p}\right)$.

The above classification of real Dirichlet characters $\pmod p$ completes the proof. ∎

Remark 3.13. 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.

3.1.2 Primitive Characters

Motivated by Proposition 3.12, we introduce primitive Dirichlet characters. This requires discussing conductors.

Definition 3.14 (conductor). Fix a Dirichlet character $\chi \pmod q$. The *conductor* $f(\chi)$ of χ is the smallest positive integer f such that

$$\chi(a) = \chi(b)$$

for any $a \equiv b \pmod f$ such that $\gcd(a,q) = \gcd(b,q) = 1$.

Here is a basic check.

Lemma 3.15. Fix a Dirichlet character $\chi \pmod q$. Then $f(\chi) \mid q$.

Proof. Set $f \coloneqq \gcd(f(\chi), q)$. We claim any $a \equiv b \pmod f$ with $\gcd(a,q) = \gcd(b,q) = 1$ will have $\chi(a) = \chi(b)$. This will finish the proof because it will force $f \geq f(\chi)$, but $f \mid f(\chi)$ enforces $f = f(\chi)$.

To show the claim, write $f = xf(\chi) + yq$ for some integers $x, y \in \mathbb{Z}$. Then note $a = b + fk$ for some integer k, which implies

$$\chi(a) = \chi(b + fk) = \chi(b + xf(\chi)k + yqk) = \chi(b + xf(\chi)).$$

Now, $\chi(a) \neq 0$, so $\chi(b + xf(\chi)) \neq 0$, so $b + xf(\chi)$ must be coprime with q. Thus, by definition of $f(\chi)$, we conclude that $\chi(a) = \chi(b + xf(\chi)) = \chi(b)$, which is what we wanted. ∎

Definition 3.16 (primitive). A Dirichlet character $\chi \pmod q$ is *primitive* if and only if $f(\chi) = q$. In other words, q is the smallest integer f such that $a \equiv b \pmod f$ implies $\chi(a) = \chi(b)$ for $\gcd(a,q) = \gcd(b,q) = 1$.

We are going to work almost exclusively with primitive characters in the sequel; let's justify why.

Proposition 3.17. Fix a Dirichlet character $\chi \pmod q$ of conductor f. Then there is a unique Dirichlet character $\chi_f \pmod f$ such that

$$\chi(n) = \begin{cases} \chi_f(n) & \text{if } \gcd(n,q) = 1, \\ 0 & \text{if } \gcd(n,q) > 1. \end{cases}$$

In fact, χ_f is primitive.

Proof. We show uniqueness, existence, and primitivity separately.

- We show that χ_f is unique. For each $n \in \mathbb{Z}$ such that $\gcd(n,f) = 1$, we claim that there is some n' such that $\gcd(n',q) = 1$ but $n \equiv n' \pmod f$. This is surprisingly technical and arises from the fact $f \mid q$ from Lemma 3.15. Well, the Chinese remainder theorem allows us to find some $n' \pmod q$ such that

$$n' \equiv \begin{cases} n \pmod{p^{\nu_p(q)}} & \text{if } p \mid f, \\ 1 \pmod{p^{\nu_p(q)}} & \text{if } p \mid q \text{ and } p \mid f. \end{cases}$$

  Notably, the moduli are coprime, and their product is q. Further, for each $p \mid q$, we claim $p \nmid n'$: if $p \mid f$, then $p \mid n' - n$, so $p \nmid n$ implies $p \nmid n'$; otherwise if $p \nmid f$, so $p \mid n' - 1$, so $p \nmid n'$. However, for each $p \mid f$, we see that

$$n' \equiv n \pmod{p^{\nu_p(f)}}$$

  because $\nu_p(f) \leq \nu_p(q)$, so we conclude that $n' \equiv n \pmod f$.

To complete the proof, we note that each $n \in \mathbb{Z}$ such that $\gcd(n,f) = 1$ has some n' such that $\gcd(n',q) = 1$ while $n \equiv n' \pmod f$, so

$$\chi_f(n) = \chi_f(n') = \chi(n').$$

Otherwise, for $n \in \mathbb{Z}$ such that $\gcd(n,f) > 1$, we must have $\chi_f(n) = 0$ because $\chi_f \pmod f$ is a Dirichlet character. So χ_f is uniquely determined by χ.

- We show that χ_f exists. Well, for each $n \in \mathbb{Z}$ such that $\gcd(n,f) = 1$, we note from the previous step that there is some n' such that $\gcd(n',q) = 1$ and $n \equiv n' \pmod f$. But by the definition of f, we note that the value of $\chi(n')$ is uniquely determined, so we may define

$$\chi_f(n) \coloneqq \begin{cases} \chi(n) & \text{if } \gcd(n,q) = \gcd(n',f) = 1 \text{ and } n \equiv n' \pmod f, \\ 0 & \text{if } \gcd(n,f) > 1. \end{cases}$$

Quickly, note that $\chi_f \pmod f$ is a Dirichlet character: certainly χ_f vanishes on n such that $\gcd(n,f) > 1$. Further, given $a, b \in \mathbb{Z}$ such that $\gcd(a,f) = \gcd(b,f) = 1$, we find a' and b' such that $a' \equiv a \pmod f$ and $b' \equiv b \pmod f$ and $\gcd(a',q) = \gcd(b',q) = 1$. Thus, we see

$$\chi_f(a)\chi_f(b) = \chi(a')\chi(b') = \chi(a'b') = \chi_f(ab),$$

where the last equality is valid because $a'b' \equiv ab \pmod f$ and $\gcd(a'b',q) = 1$ because $\gcd(a',q) = \gcd(b',q) = 1$.

Lastly, we check that χ is built from χ_f as claimed. Well, for $n \in \mathbb{Z}$, if $\gcd(n,q) > 1$, then of course $\chi(n) = 0$. Alternatively, if $\gcd(n,q) = 1$, then $\gcd(n,f) = 1$ as well, so the construction of χ_f grants $\chi(n) = \chi_f(n)$.

- We show that $\chi_f \pmod f$ is a primitive Dirichlet character, using the construction of the previous step. Indeed, let f' be the conductor of χ_f; we want to show $f = f'$. Certainly $f' \mid f$ by Lemma 3.15, so $f' \le f$. On the other hand, if $a \equiv b \pmod{f'}$ and $\gcd(a,q) = \gcd(b,q) = 1$, then we see

$$\chi(a) = \chi_f(a) \overset{*}{=} \chi_f(b) = \chi(b),$$

where $\overset{*}{=}$ holds because $\gcd(a,f) = \gcd(b,f) = 1$ as well by Lemma 3.15. Thus, because f is the conductor of χ, we see $f' \ge f$, so we conclude $f = f'$. ∎

3.1.3 Gauss Sums

We mentioned in Remark 2.15 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 3.18 (Gauss sum)**.** Fix a Dirichlet character $\chi \pmod q$. Then the *Gauss sum* is

$$\tau(\chi, m) \coloneqq \sum_{n=0}^{q-1} e\left(\frac{nm}{q}\right) \chi(n).$$

For brevity, we set $\tau(\chi) \coloneqq \tau(\chi, 1)$.

Namely, $\psi_m \colon n \mapsto e\left(\frac{nm}{p}\right)$ 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. To set up our discussion, we emphasize that primitive characters are better-behaved.

Lemma 3.19. Fix a Dirichlet character $\chi \pmod q$. The following are equivalent.

(a) χ is primitive.

(b) For each proper divisor $q' \mid q$, there exists $k \equiv 1 \pmod{q'}$ such that $\chi(k) \notin \{0,1\}$.

(c) For each proper divisor $q' \mid q$ and integer r, we have

$$\sum_{k=0}^{q/q'-1} \chi(kq'+r) = 0.$$

Proof. We show our implications in sequence.

(a) We show (a) implies (b). Because χ is primitive, we know that the nonzero values of χ are not periodic $\pmod{q'}$. In particular, we may find $r \equiv s \pmod{q'}$ such that $\chi(r)$ and $\chi(s)$ are distinct and nonzero. In particular, we must have $r, s \in (\mathbb{Z}/q\mathbb{Z})^\times$, so we let $s' \in \mathbb{Z}$ denote a multiplicative inverse of $s \pmod q$ so that $rs' \equiv ss' \equiv 1 \pmod{q'}$, but

$$\chi(rs') = \chi(r)\chi(s') = \chi(r)/\chi(s) = 1.$$

This is what we wanted.

(b) We show (b) implies (c). Well, fix an integer $\ell \equiv 1 \pmod{q'}$ such that $\chi(\ell) \notin \{0,1\}$. Writing $\ell = 1 + q'\ell'$ and $d \coloneqq q/q'$, we see that

$$\begin{aligned}\chi(\ell) \sum_{k=0}^{q/q'-1} \chi(kq'+r) &= \sum_{k=0}^{d-1} \chi(\ell kq' + \ell r) \\ &= \sum_{k=0}^{d-1} \chi(\ell kq' + (1+q'\ell')r) \\ &= \sum_{k=0}^{d-1} \chi((\ell k + \ell')q' + r).\end{aligned}$$

Now, we claim that $k \mapsto \ell k + \ell'$ is a bijection $\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$. Indeed, it is enough to show injectivity because this is a map from a finite set to itself, so we see that $\ell k_1 + \ell' \equiv \ell k_2 + \ell' \pmod d$ implies

$$\ell k_1 \equiv \ell k_2 \pmod d,$$

which implies $k_1 \equiv k_2 \pmod d$ because $\gcd(\ell, d) = \gcd(\ell, q) = 1$. This completes the proof of the claim, so we can re-index our sum as

$$\chi(\ell) \sum_{k=0}^{q/q'-1} \chi(kq'+r) = \sum_{k=0}^{q/q'-1} \chi(kq'+r)$$

because the value of k in the sum only matters $\pmod d$. (Recall $d = q/q'$, and χ is periodic $\pmod q$.) Because $\chi(\ell) \neq 1$, we conclude that the value of the sum must be 0.

(c) We show (c) implies (a) by contraposition. Indeed, if χ is not primitive, then Proposition 3.17 grants us a Dirichlet character $\chi_f \pmod f$ where $f \coloneqq f(\chi)$ such that

$$\chi(n) = \begin{cases} \chi_f(n) & \text{if } \gcd(n,q) = 1, \\ 0 & \text{if } \gcd(n,q) > 1. \end{cases}$$

Now, by Lemma 3.15, we see $f \mid q$, and because χ fails to be primitive, we have $f < q$, so f is a proper divisor. As such, we see that

$$\sum_{k=0}^{q/f-1} \chi(kf+1) = \sum_{k=0}^{q/f-1} 1_{\gcd(kf+1,q)=1}.$$

This sum has nonnegative terms and at least one positive term at $k = 0$, so the total sum is at least 1 and hence is nonzero. ■

We can now relate our Gauss sums together.

Lemma 3.20. Fix a primitive Dirichlet character $\chi \pmod q$. Then for any integer m, we have

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

Proof. We have the following cases.

- Suppose that $\gcd(m, q) = 1$. Here, the argument is a change of variables. Indeed, we note $\chi(m) \neq 0$, so we may write

$$\begin{aligned}\tau(\chi, m) &= \sum_{n=0}^{q-1} e\left(\frac{nm}{q}\right)\chi(n) \\ &= \frac{1}{\chi(m)}\sum_{n=0}^{q-1} e\left(\frac{nm}{q}\right)\chi(nm) \\ &= \frac{1}{\chi(m)}\sum_{n=0}^{q-1} e\left(\frac{n}{q}\right)\chi(n),\end{aligned}$$

  where we have re-indexed our sum in the last step; in particular, we see that multiplication by $m \in (\mathbb{Z}/q\mathbb{Z})^\times$ is a bijection $(\mathbb{Z}/q\mathbb{Z})^\times \to (\mathbb{Z}/q\mathbb{Z})^\times$. In total, we note $\chi(m)^{-1} = \overline{\chi(m)}$ because $|\chi(m)| = 1$ by Remark 1.12, so we conclude that $\tau(\chi, m) = \overline{\chi(m)}\tau(\chi)$, as desired.

- Suppose that $\gcd(m, q) > 1$. This is harder and requires using that $\chi \pmod q$ is primitive. Quickly, note that $\overline{\chi}(m)\tau(\chi) = 0$ because $\gcd(m, q) > 1$, so we must show that $\tau(\chi, m) = 0$.

  Well, take $d \coloneqq \gcd(m, q)$ and $m' \coloneqq m/d$ and $q' \coloneqq q/d$ so that $\gcd(m', q') = 1$. As such, we write each $n \in \mathbb{Z}/q\mathbb{Z}$ as $kq' + r$ by the division algorithm, which gives

$$\begin{aligned}\tau(\chi, m) &= \sum_{n=0}^{q-1} e\left(\frac{nm}{q}\right)\chi(n) \\ &= \sum_{k=0}^{d-1}\left(\sum_{r=0}^{q'-1} e\left(\frac{(kq'+r)m'}{q'}\right)\chi(kq'+r)\right) \\ &= \sum_{r=0}^{q'-1}\left(e\left(\frac{rm'}{q'}\right)\sum_{k=0}^{d-1}\chi(kq'+r)\right).\end{aligned}$$

  We now note that the inner sums vanish by Lemma 3.19 because q' is a proper divisor of q. Note that we have used the fact that χ is primitive here. ■

Proposition 3.21. Fix a primitive Dirichlet character $\chi \pmod q$. Then $|\tau(\chi)|^2 = q$.

Proof. This is essentially the Plancherel formula. Using Lemma 3.20, we note $|\chi(m)| = 1$ if $\gcd(m,q) = 1$ (by Remark 1.12) and $|\chi(m)| = 0$ otherwise, so

$$\begin{aligned}
\varphi(q)|\tau(\chi)|^2 &= \sum_{m=0}^{q-1} |\overline{\chi}(m)\tau(\chi)|^2 \\
&= \sum_{m=0}^{q-1} |\tau(\chi,m)|^2 \\
&= \sum_{m=0}^{q-1} \tau(\chi,m)\overline{\tau(\chi,m)} \\
&= \sum_{m=0}^{q-1} \left(\sum_{k,\ell=0}^{q-1} e\left(\frac{km}{q}\right)\chi(k)\overline{e\left(\frac{\ell m}{q}\right)\chi(\ell)} \right) \\
&= \sum_{k,\ell=0}^{q-1} \left(\chi(k)\overline{\chi}(\ell) \sum_{m=0}^{q-1} e\left(\frac{(k-\ell)m}{q}\right) \right).
\end{aligned}$$

Now, if $k \neq \ell$, then the inner sum is

$$\sum_{m=0}^{q-1} e\left(\frac{(k-\ell)m}{q}\right) = \frac{e\left(\frac{(k-\ell)q}{q}\right) - 1}{e\left(\frac{k-\ell}{q}\right) - 1} = 0,$$

so we only care about the terms with $k = \ell$, where the inner sum is q. Thus,

$$\varphi(q)|\tau(\chi)|^2 = \sum_{k=0}^{q-1} \underbrace{\chi(k)\overline{\chi(k)}}_{|\chi(k)|^2} q = \varphi(q)q,$$

which yields $|\tau(\chi)|^2 = q$. This is what we wanted. ∎

3.2 February 10

We continue discussing applications of the Gauss sum.

3.2.1 The Pólya–Vinogradov Inequality

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

Theorem 3.22 (Pólya–Vinogradov inequality)**.** Fix a prime p and a nontrivial character $\chi \pmod p$. Then for any a, b, we have

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

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 $a, b \le p$. (If shifting yields $a \le p \le b \le p + a$, then we can flip the entire sum to make it $b - p \le p - a \le p$.)

Now, the main point is to take the Fourier transform

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

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 1.24 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 Proposition 3.21, 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 3.23. The least nonquadratic residue is $O(\sqrt{x}\log x)$.

Proof. This is direct from Theorem 3.22. ∎

Remark 3.24. For "short" intervals, one can do better, which is the point of the Burgess bound.

Remark 3.25 (Nir). Here is another nice corollary: fix real numbers $0 \le \alpha < \beta \le 1$. For a prime $p \equiv 1 \pmod 3$, define the character $\chi \pmod p$ by $\chi(g) \coloneqq \zeta_3$ where $g \in \mathbb{F}_p^\times$ is a generator. Then the function $f \coloneqq \frac{1}{3}\left(1 + \chi + \chi^2\right)$ has $f(a)$ indicating if $a \pmod p$ is a cube. Thus, the proportion of cubic residues $\pmod p$ in the interval $[\alpha p, \beta p]$ is

$$\frac{\#\{a \pmod p \text{ is a square} : \alpha p \le a \le \beta p\}}{(\beta-\alpha)p} = \frac{1}{(\beta-\alpha)p}\cdot\frac{1}{3}((\beta-\alpha)p + O(\sqrt{p}\log p)) = \frac{1}{3} + O\left(p^{-1/2}\log p\right).$$

In other words, cubic residues are equidistributed $\pmod p$. A similar argument works for higher powers.

3.2.2 The Functional Equation for $L(s,\chi)$

Given a primitive Dirichlet character $\chi \pmod q$, we would like to provide a functional equation akin to Theorem 2.42. It will be convenient to divide our analysis in the cases $\chi(-1) = 1$ and $\chi(-1) = -1$. Notably, $\chi(-1)^2 = \chi(1) = 1$, so $\chi(-1) \in \{\pm 1\}$ is indeed forced.

Remark 3.26. Roughly speaking, the case of $\chi(-1) = 1$ makes $L(s,\chi)$ a factor of the Dedekind ζ-function of a real quadratic field, but the case of $\chi(-1) = -1$ makes $L(s,\chi)$ a factor of the Dedekind ζ-function of an imaginary quadratic field. Because the infinite place of $\mathbb{Q}$ splits differently in these cases, the Γ-factors used to complete our L-function will be different, which is why we must separate our analysis into cases.

Despite the philosophical remark of Remark 3.26, our entire discussion will avoid discussing number fields. As in the proof of Theorem 2.42, our functional equation will follow from the functional equation of a suitably defined Θ-function.

Definition 3.27. Fix a Dirichlet character $\chi \pmod q$.

- If $\chi(-1) = 1$, we define, for $\operatorname{Re} s > 0$,
$$\Theta(s, \chi) \coloneqq \sum_{n \in \mathbb{Z}} \chi(n) e^{-\pi n^2 s/q}.$$
- If $\chi(-1) = -1$, we define, for $\operatorname{Re} s > 0$,
$$\Theta(s, \chi) \coloneqq \sum_{n \in \mathbb{Z}} n\chi(n) e^{-\pi n^2 s/q}.$$

Note that $\chi(-1) = -1$ would imply that

$$\sum_{n \in \mathbb{Z}} \chi(n) e^{-\pi n^2 s} = 0,$$

which explains why we should add the factor of n here.

Lemma 3.28. For any Dirichlet character $\chi \pmod q$ and $\varepsilon > 0$, the sum defining $\Theta(s, \chi)$ converges absolutely and uniformly on $\{s : \operatorname{Re} s \geq \varepsilon\}$. Thus, $\Theta(s, \chi)$ defines a holomorphic function on $\{s : \operatorname{Re} s > 0\}$.

Proof. Note that the second sentence follows from the first: by Lemma A.15, we see that $\Theta(s, \chi)$ is holomorphic on $\{s : \operatorname{Re} s \geq \varepsilon\}$ for any $\varepsilon > 0$, so taking the union over all $\varepsilon > 0$ achieves the result. We now show our convergences by the Weierstrass M-test.

- For $\chi(-1) = 1$, we see
$$\sum_{n \in \mathbb{Z}} \left| \chi(n) e^{-\pi n^2 s/q} \right| \leq \sum_{n \in \mathbb{Z}} e^{-\pi n^2 \operatorname{Re} s/q} \leq \sum_{n \in \mathbb{Z}} e^{-\pi n^2 \varepsilon/q} = \Theta(\varepsilon/q),$$
which already converges by Remark 2.34. Note that the bound $e^{-\pi n^2 \varepsilon}$ is independent of s, which gives our uniformity.
- For $\chi(-1) = -1$, we see
$$\sum_{n \in \mathbb{Z}} \left| n\chi(n) e^{-\pi n^2 s/q} \right| \leq \sum_{n \in \mathbb{Z}} |n| e^{-\pi n^2 \operatorname{Re} s/q} \leq 1 + 2 \sum_{n=1}^{\infty} n e^{-\pi n \varepsilon/q}.$$
Because $ne^{-\pi n\varepsilon/q}$ is independent of s, it remains to show that the rightmost sum converges. Well, note that $n^3/e^{\pi n\varepsilon/q} \to 0$ as $n \to \infty$, so because this is a continuous function, we actually see that it is bounded by some constant $C > 0$, so we see
$$\sum_{n=1}^{\infty} n e^{-\pi n\varepsilon/q} \leq \sum_{n=1}^{\infty} n \cdot \frac{M}{n^3} = M \sum_{n=1}^{\infty} \frac{1}{n^2},$$
which converges. For example, this is $\zeta(2)$, which converges by Proposition 1.2, say. ∎

And here is our functional equation for $\Theta(s, \chi)$.

Proposition 3.29. Fix a primitive Dirichlet character $\chi \pmod q$.

- If $\chi(-1) = 1$, then for any $\operatorname{Re} s > 0$,
$$\Theta(s, \chi) = \frac{\sqrt{q}}{\tau(\overline{\chi})} \cdot s^{-1/2} \Theta\left(\frac{1}{s}, \overline{\chi}\right).$$
- If $\chi(-1) = -1$, then for any $\operatorname{Re} s > 0$,
$$\Theta(s, \chi) = \frac{i\sqrt{q}}{\tau(\overline{\chi})} \cdot s^{-3/2} \Theta\left(\frac{1}{s}, \overline{\chi}\right).$$

Proof. The argument is similar to Proposition 2.35. Note that $\Theta(s, \chi)$ is holomorphic on the region $\{s : \operatorname{Re} s > 0\}$ by Remark 2.34. On the other side, we note that $\operatorname{Re} s > 0$ implies that $\operatorname{Re}(1/s) > 0$ as well: writing $s = a + bi$ for $a > 0$, we have $\frac{1}{s} = \frac{a-bi}{|s|^2}$, which also has positive real part. Thus, we see that $\Theta(1/s, \overline{\chi})$ is the composite of holomorphic functions and is therefore holomorphic, as are $\frac{\sqrt{q}}{\tau(\overline{\chi})} \cdot s^{-1/2} \Theta\left(\frac{1}{s}, \overline{\chi}\right)$ and $\frac{i\sqrt{q}}{\tau(\overline{\chi})} \cdot s^{-3/2} \Theta\left(\frac{1}{s}, \overline{\chi}\right)$.

In total, by the uniqueness of analytic continuation, it therefore suffices to show that our holomorphic functions are equal on $\mathbb{R}_{>0}$. As such, fix some $t > 0$, and we use Poisson summation, roughly in the form of Corollary 2.10.

- Suppose $\chi(-1) = 1$. Then we note Lemma 3.37 implies
$$\begin{aligned}
\tau(\overline{\chi})\Theta(t, \chi) &= \sum_{n \in \mathbb{Z}} \chi(n) \tau(\overline{\chi}) e^{-\pi n^2 t/q} \\
&= \sum_{n \in \mathbb{Z}} \tau(\overline{\chi}, n) e^{-\pi n^2 t/q} \\
&= \sum_{r=0}^{q-1} \left(\overline{\chi}(r) \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t/q + 2\pi i n r/q} \right).
\end{aligned}$$
Now, taking the conjugate of Corollary 2.10, the inner sum becomes
$$\sum_{n \in \mathbb{Z}} e^{-\pi n^2 (t/q) + 2\pi i n (r/q)} = \frac{1}{\sqrt{t/q}} \sum_{n \in \mathbb{Z}} e^{-\pi (n + r/q)^2/(t/q)},$$
so
$$\begin{aligned}
\tau(\overline{\chi})\Theta(t, \chi) &= \sum_{r=0}^{q-1} \left(\overline{\chi}(r) \cdot \frac{1}{\sqrt{t/q}} \sum_{n \in \mathbb{Z}} e^{-\pi (n + r/q)^2/(t/q)} \right) \\
&= \frac{\sqrt{q}}{\sqrt{t}} \sum_{r=0}^{q-1} \left(\sum_{n \in \mathbb{Z}} \overline{\chi}(r) e^{-\pi (qn + r)^2 (1/t)} \right) \\
&= \frac{\sqrt{q}}{\sqrt{t}} \underbrace{\sum_{n \in \mathbb{Z}} \overline{\chi}(n) e^{-\pi n^2 (1/t)}}_{\Theta(1/t, \overline{\chi})},
\end{aligned}$$
where in the last equality we have used the absolute convergence of $\Theta(1/t, \overline{\chi})$ to rearrange the sum. Rearranging our equality, we see
$$\Theta(t, \chi) = \frac{\sqrt{q}}{\tau(\overline{\chi})} \cdot t^{-1/2} \Theta\left(\frac{1}{t}, \overline{\chi}\right).$$

- Suppose $\chi(-1) = -1$. Again, we note that Lemma 3.37 implies

$$\begin{aligned}\tau(\overline{\chi})\Theta(t,\chi) &= \sum_{n\in\mathbb{Z}} \chi(n)\tau(\overline{\chi})ne^{-\pi n^2 t/q} \\ &= \sum_{n\in\mathbb{Z}} \tau(\overline{\chi},n)ne^{-\pi n^2 t/q} \\ &= \sum_{r=0}^{q-1}\left(\overline{\chi}(r)\sum_{n\in\mathbb{Z}} ne^{-\pi n^2 t/q+2\pi inr/q}\right).\end{aligned}$$

This time around, Poisson summation in the form of Corollary 2.10 is not good enough for our purposes, but Poisson summation still suffices. Set $f\colon \mathbb{R}\to\mathbb{C}$ by $f(x) \coloneqq xe^{-\pi x^2(t/q)+2\pi ix(r/q)}$. Setting $g(x) \coloneqq e^{-\pi x^2}$, we note that $g'(x) = -2\pi xe^{-\pi x^2}$, so

$$f(x) = -\frac{1}{2\pi\sqrt{t/q}}g'(\sqrt{t/q}x)e^{2\pi ix(r/q)}.$$

Thus, Lemma C.6 and Exercise C.7 tell us that f is Schwarz with Fourier transform given by

$$\begin{aligned}(\mathcal{F}f)(s) &= -\frac{1}{2\pi\sqrt{t/q}}\cdot\frac{1}{\sqrt{t/q}}(\mathcal{F}g')\left(\frac{s-r/q}{\sqrt{t/q}}\right) \\ &= -\frac{1}{2\pi(t/q)}\cdot 2\pi i\left(\frac{s-r/q}{\sqrt{t/q}}\right)e^{-\pi(s-r/q)^2/(t/q)} \\ &= -i\sqrt{q}t^{-3/2}(qs-r)e^{-\pi(qs-r)^2/t}.\end{aligned}$$

Now applying Theorem 2.8, we get

$$\sum_{n\in\mathbb{Z}} ne^{-\pi n^2 t/q+2\pi inr/q} = \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}}(\mathcal{F}f)(n) = \sum_{n\in\mathbb{Z}} -i\sqrt{q}t^{-3/2}(qn-r)e^{-\pi(qn-r)^2/t}.$$

As such, we get rid of the sign here by noting $\overline{\chi}(-r) = -\overline{\chi}(r)$, so

$$\begin{aligned}\tau(\overline{\chi})\Theta(t,\chi) &= \sum_{r=0}^{q-1}\left(\overline{\chi}(r)\sum_{n\in\mathbb{Z}} -i\sqrt{q}t^{-3/2}(qn-r)e^{-\pi(qn-r)^2/t}\right) \\ &= i\sqrt{q}t^{-3/2}\sum_{r=0}^{q-1}\left(\sum_{n\in\mathbb{Z}}\overline{\chi}(qn-r)(qn-r)e^{-\pi(qn-r)^2/t}\right) \\ &= i\sqrt{q}t^{-3/2}\underbrace{\sum_{n\in\mathbb{Z}}\overline{\chi}(n)ne^{-\pi n^2(1/t)}}_{\Theta(1/t,\overline{\chi})}.\end{aligned}$$

Rearranging our equality, we see

$$\Theta(t,\chi) = \frac{\sqrt{q}}{\tau(\overline{\chi})}\cdot t^{-3/2}\Theta\left(\frac{1}{t},\overline{\chi}\right),$$

which is what we wanted. ∎

We will focus on the case of $\chi\neq\chi_0$. Now, for $\alpha\in\mathbb{R}$, an argument similar to Corollary 2.10 yields

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

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 $\chi(-1) = 1$.[1] Here, we set

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

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 1.24, we see

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

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

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

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

Now, to find our functional equation, we write

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

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 3.30 (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

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

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

Proof. We follow the proof of Theorem 2.42. One can compute the integral

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

[1] This is called the "unramified at ∞ case" because the place here at infinity is totally real.

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

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

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

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

This completes the proof. ∎

Remark 3.31. 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 3.32. We omit the case of $\chi(-1) = -1$.

3.3 February 13

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

3.3.1 All Functional Equations

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

Definition 3.33 (primitive)**.** A Dirichlet character $\chi \pmod q$ is *primitive* if and only if $\chi\colon (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ has no smaller period than q.

Remark 3.34. In more general contexts, q is called the "conductor" of χ.

Here is our statement.

Theorem 3.35. Fix a primitive Dirichlet character $\chi \pmod q$ for $q > 1$. Then set $a_\chi \coloneqq \frac{1}{2}(1-\chi(-1)) \in \{0,1\}$, and define

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

Then Ξ_χ is entire and satisfies the functional equation

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

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

Proof. Omitted. ■

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

Lemma 3.36. Fix a primitive Dirichlet character $\chi \pmod q$. Then $|\tau(\chi)|^2 = \sqrt{q}$.

Proof. Again sum over the $\tau(\chi, m)$ as in Proposition 3.21. ■

The rest of the proof of Theorem 3.35 now follows exactly as we proceeded last class.

3.3.2 The Sign of the Gauss Sum

Proposition 3.21 tells us the magnitude of $\tau(\chi)$, but we might be interested in its exact value, for example because these determine our functional equations. This is referred to as the "sign" of the Gauss sum. While we're here, we will examine a special case.

Lemma 3.37. Fix a prime p, and set $\chi_p \coloneqq \left(\frac{\bullet}{p}\right)$. Then

$$\tau(\chi_p) = \sum_{k=0}^{p-1} e\left(\frac{k^2}{p}\right).$$

Proof. Quickly, note that $\sum_{k=0}^{p-1} e(k/p) = \frac{e(p/p)-1}{e(1/p)} = 0$, so we can add this to our original sum to see

$$\tau(\chi_p) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) e\left(\frac{k}{p}\right) + \sum_{k=0}^{p-1} e\left(\frac{k}{p}\right) = \sum_{k=0}^{p-1} \left(1 + \left(\frac{k}{p}\right)\right) e\left(\frac{k}{p}\right).$$

In particular, if $k \pmod p$ is a quadratic residue, then the coefficient of $e(k/p)$ in the sum is 2; if $k \equiv 0 \pmod p$, then the coefficient of $e(k/p)$ is 1; and lastly, if k is a nonquadratic residue, then the coefficient of $e(k/p)$ is 0.

However, by staring at these cases, we see that the coefficient of $e(k/p)$ here is the number of solutions x to $x^2 \equiv k \pmod p$: there are two solutions if k is a quadratic residue, only $x \equiv 0$ if $k \equiv 0$ and none if k is a nonquadratic residue. Thus,

$$\tau(\chi_p) = \sum_{k=0}^{p-1} \#\left\{x \in \mathbb{Z}/p\mathbb{Z} : x^2 \equiv k \pmod p\right\} e\left(\frac{k}{p}\right) = \sum_{x=0}^{p-1} e\left(\frac{x^2}{p}\right),$$

which is what we wanted. ■

The benefit of Lemma 3.37 is that this expression is more amenable to Poisson summation.

Proposition 3.38. 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. To set us up, define $f(z) \coloneqq \Theta(z/\sqrt{\pi}) = \sum_{n\in\mathbb{Z}} e^{-ns^2}$, which is holomorphic by Remark 2.34, and by Proposition 2.35, we see that

$$f(z) = \left(\frac{\pi}{z}\right)^{1/2} f\left(\frac{\pi^2}{z}\right) \tag{3.1}$$

for z such that $\operatorname{Re} z > 0$. Notably, $\operatorname{Re} z > 0$ implies $\operatorname{Re} z/\sqrt{\pi} > 0$ as well.

Now, the series defining Θ absolutely converges, so for any $\varepsilon > 0$, we may rearrange

$$\begin{aligned} f\left(\varepsilon + \frac{2\pi i}{q}\right) &= 1 + 2\sum_{n=1}^{\infty} e^{-(\varepsilon + 2\pi i/q)n^2} \\ &= 1 + 2\sum_{n=1}^{\infty} e^{-\varepsilon n^2} e^{-2\pi i n^2/q} \\ &\overset{*}{=} 1 + 2\sum_{r=0}^{q-1}\left(e^{-2\pi i r^2/q}\sum_{m=0}^{\infty} e^{-(r+mq)^2\varepsilon}\right), \end{aligned}$$

where in the last equality we have written $n = mq + r$ for $r \in [0, q)$ and rearranged.

Use theta chi.

Now, one can check that $\varepsilon \to 0^+$ 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 $\varepsilon \to 0^+$. As such, using the functional equation (3.1) for f, as well as the computation

$$\frac{\pi^2}{\varepsilon + 2\pi i/q} = -\frac{\pi i q}{2} + \frac{q^2}{4}\varepsilon + O\left(\varepsilon^2\right)$$

to take the asymptotics on the other side. This will complete the proof. ∎

Remark 3.39. One can use Proposition 3.38 to prove the law of quadratic reciprocity, essentially by comparing Gauss sums $\pmod p$ and $\pmod q$ for distinct odd primes p and q. One can also use these techniques to prove the supplement $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

3.3.3 A Zero-Free Region for Complex Characters

We continue to let $\chi \pmod q$ be a primitive character.

Remark 3.40. 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 3.41. Fix

$$D(s) \coloneqq \zeta(s)^3 L(s,\chi)^2 L(s,\overline{\chi})^2 L(s,\chi^2) L(s,\overline{\chi}^2).$$

When χ is a complex character, one can check that this has nonnegative real coefficients, so Lemma 2.63 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.

3.4 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 3.42. 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

$$\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + \zeta^{-2} + 2 = 2.$$

Now, we see $\left(\frac{2}{p}\right) = 1$ is equivalent to having $\zeta + \zeta^{-1} \in \mathbb{F}_p$, which because $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is topologically generated by the Frobenius, is equivalent to

$$\zeta^p + \zeta^{-p} = \left(\zeta + \zeta^{-1}\right)^p \stackrel{?}{=} \zeta + \zeta^{-1}.$$

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. ∎

3.4.1 Counting Zeroes of $L(s, \chi)$

We would like to generalize Theorem 2.50. For this, we have the following definition.

Notation 3.43. Fix a primitive character $\chi \pmod q$. Then we define

$$N_\chi(T) \coloneqq \#\{|\rho| \le T : \Xi_\chi(\rho) = 0\}.$$

Remark 3.44. Note that the functional Theorem 3.35 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 2.51 that

$$\sum_{\Xi_\chi(\rho)=0} \frac{1}{1 + |\operatorname{Im}\rho - T|^2} \ll \log(|T|+2) + \log q,$$

where the implied constant is absolute. Following the rest of the proof of Theorem 2.50 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.

3.4.2 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 3.45. Can one determine if an integer n is prime in $\mathrm{Poly}(\log n)$ 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 3.46 (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 3.47 (Miller–Rabin)**.** Assume GRH. Then we can test if an integer n is prime in $\mathrm{Poly}(\log n)$ time.

For this, we describe the Miller–Rabin primality test, which is one of the more efficient probabilistic primality tests.

Lemma 3.48 (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 $\left|\mathbb{F}_p^\times\right| = p-1$. ∎

Remark 3.49. 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 3.48 to test for primality.

Instead, we will want to use Proposition 3.9, 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 3.50 (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 3.51. 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 3.52. Remark 3.51 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 3.53. 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 $\pmod{p}$ statements; if n is not squarefree, then one can look $\pmod{p^2}$ 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 $O\left((\log n)^2\right)$ time.
3. Compute $a^{(n-1)/2} \pmod{n}$ using exponentiation by repeated squaring. This will run in $O\left((\log n)^3\right)$ 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 $O\left((\log n)^5\right)$.

3.5 February 17

The next two classes (Wednesday and Friday) will be recorded and posted online.

3.5.1 Deterministic Solovay–Strassen

Here is our main theorem, which tells us that the Solovay–Strassen primality test can be made deterministic.

Theorem 3.54. 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 3.55. 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

$$\left\{[k] \in (\mathbb{Z}/n\mathbb{Z})^\times : k \leq c(\log q)^2\right\} \subseteq A$$

implies $A = (\mathbb{Z}/q\mathbb{Z})^\times$.

One can quickly prove Theorem 3.54 from Proposition 3.55.

Proof of Theorem 3.54. Indeed, the set

$$A \coloneqq \left\{a \in (\mathbb{Z}/q\mathbb{Z})^\times : \left(\frac{a}{q}\right) \not\equiv a^{(n-1)/2} \pmod{q}\right\}$$

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 3.55 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 3.55.

Proof of Proposition 3.55. 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 $0 \le k \le c(\log q)^2$ coprime to n.

As in the proof of the Prime number theorem, we want to consider the infinite sum

$$\sum_{n \le x} \Lambda(n)\chi(n) = \frac{1}{2\pi i}\int_{\operatorname{Re} s = c} \left(-\frac{L'(s,\chi)}{L(s,\chi)}\right) x^s \frac{ds}{s}$$

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

$$\sum_{n \ge 0} \Lambda(n)\chi(n)\psi\left(\frac{n}{x}\right) = \frac{1}{2\pi i}\int_{\operatorname{Re} s = 2} \left(-\frac{L'(s,\chi)}{L(s,\chi)}\right) (\mathcal{M}\psi)(s) x^s \, ds.$$

Shifting the contour is somewhat delicate, but it can be done similarly as in our proof of the Prime number theorem. This gives

$$\sum_{n \ge 0} \Lambda(n)\chi(n)\psi\left(\frac{n}{x}\right) = -\sum_{L(\rho,\chi)=0} (\mathcal{M}\psi)(\rho_\chi) x^{\rho_\chi}$$

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

$$x \ll \left|\sum_{n \ge 0} \Lambda(n)\chi(n)\psi\left(\frac{n}{x}\right)\right| \ll \sqrt{x}\log q,$$

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. ∎

3.5.2 Imprimitive Characters

Let's talk a little more about our characters.

Definition 3.56 (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 3.57 (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 3.58. The principal Dirichlet characters are induced by the constantly 1 character.

Remark 3.59. The point is that a Dirichlet character $\chi \pmod q$ induced by a primitive Dirichlet character $\chi' \pmod f$ has L-function given by

$$L(s,\chi') = L(s,\chi) \prod_{\substack{p \nmid f \\ p \mid q}} \frac{1}{1-\chi'(p)p^{-s}}.$$

Note that these finitely many Euler factors do not add any zeroes or poles or similar.

Remark 3.60. 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 $\left(\frac{\bullet}{p}\right)$ 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.

3.6 February 22

This lecture was recorded.

3.6.1 Real Primitive Characters

We continue discussing primitive characters χ modulo prime powers p^ν. Recall that these are controlled for p odd because $(\mathbb{Z}/p^\nu)^\times$ is still cyclic. In particular, there is exactly one real primitive Dirichlet character $\pmod p$ and none for p^ν for $\nu > 1$.

For $p = 2$, one must be a little more careful.

- There is a unique primitive real character $\pmod 2$ which is the trivial one.
- There is a real primitive character $\chi_4 \pmod 4$ given by $\left(\frac{-1}{\bullet}\right)$.
- Further, there are two real primitive characters $\pmod 8$ given by $\left(\frac{2}{\bullet}\right)$ and $\left(\frac{-2}{\bullet}\right)$.
- There are no more real primitive characters $\pmod{2^\nu}$.

Roughly speaking, these characters can give all primitive characters by the Chinese remainder theorem. We can be a little more explicit about this.

Remark 3.61. Using the Kronecker symbol, one can write all real primitive Dirichlet characters as $\left(\frac{d}{\bullet}\right)$. The values d yielding primitive characters are the ones which are fundamental discriminants; namely,

$$d \equiv \begin{cases} N & \text{if } N \equiv 1 \pmod 4 \text{ and is squarefree,} \\ 4N & \text{if } N \equiv 2,3 \pmod 4 \text{ and is squarefree.} \end{cases}$$

Note that we permit $N < 0$.

Remark 3.62. Fix a real primitive character $\chi = \left(\frac{d}{\bullet}\right)$. Then $\zeta(s)L(s,\chi)$ is the Dedekind ζ-function for the quadratic field $\mathbb{Q}(\sqrt{d})$. Roughly speaking, this explains why $\zeta(s)L(s,\chi)$ should have positive coefficients. See [Dav80, Chapter 6] for details.

3.6.2 Zero-Free Regions for $L(s,\chi)$

We now establish some zero-free regions for $L(s,\chi)$. For complex primitive Dirichlet characters χ, one can use the product

$$\zeta(s)^3 L(s+it_0,\chi)^2 L(s-it_0,\overline{\chi})^2 L(s+2it_0,\chi^2)L(s-2it_0,\overline{\chi}^2)$$

combined with Lemma 2.63 to see that $L(s,\chi)$ has no zeroes in the region

$$\left\{ s \in \mathbb{C} : \operatorname{Re} s > 1 - \frac{c}{\log(q(|t|+2))} \right\}.$$

Note that any imprimitive character χ can be reduced to a primitive one by adjusting finitely many Euler factors of $L(s,\chi)$, which do not change a vanishing region.

In the case of real primitive Dirichlet characters χ, one does not do as well. Notably, $\chi^2 = \overline{\chi}^2$ is the principal character, so $L(s+2it_0,\chi^2)$ is lacking a pole at $s=1$. Nonetheless, an argument will still work except at $t_0 = 0$, where we see that we have at most one zero in the real numbers in the region

$$\left\{ s \in \mathbb{C} : \operatorname{Re} s > 1 - \frac{c}{\log(q(|t|+2))} \right\}.$$

However, at most one zero is still not good enough for our purposes. Well, to deal with a possibly real zero, we can apply Lemma 2.63 to

$$\zeta(s)L(s,\chi),$$

and we can produce a lower bound (using the proof of $L(1,\chi) \neq 0$) to produce the lower bound

$$|L(1,\chi)| > cq^{-1/2}.$$

In particular, from the summation, our Dirichlet series is 1 on squares, which is where the square root comes from.

Remark 3.63. In contrast, we can upper-bound $L(s,\chi)$ relatively easily as

$$|L'(\sigma,\chi)| \ll (\log q)^2 \qquad \text{for} \qquad 1 - \frac{1}{\log q} \le \sigma \le 1,$$

and

$$|L(\sigma,\chi) \ll \log q, \qquad \text{for} \qquad 1 - \frac{1}{\log q} \le \sigma \le 1.$$

For details, see [Dav80, Chapter 14]. Roughly speaking, one can just use the Dirichlet series for $L(s,\chi)$. In particular, early terms rotate quickly and can be bounded as sines and cosines, and the later terms are small.

The idea above is that we can use the above derivative combined with our lower bound for $L(1,\chi)$ in order to get some very small interval in the real numbers where we are nonzero. This is indeed technically a zero-free region; in the next lecture, we will cover Siegel's theorem, which is ineffective but will do a little better.

In total, we get that any problematic real zero β of $L(s,\chi)$ must satisfy

$$\beta < 1 - \frac{c}{(\log q)^2 \sqrt{q}}.$$

Of course, this is much worse when compared to $c/\log q$, but it does give us a zero-free region to work with.

Remark 3.64 (Landau). Fix $\chi_d \coloneqq \left(\frac{d}{\bullet}\right)$. Then one can use

$$\zeta(s)L(s,\chi_{d_1})L(s,\chi_{d_2})L(s,\chi_{d_1}\chi_{d_2}),$$

for $d_1 \neq d_2$, which is the ζ function of a biquadratic field. Now, because each of these L-functions have at most one real zero in the desired region $\left(1 - \frac{c}{\log|d_1 d_2|}, 1\right]$, we note that a zero for $L(s,\chi_{d_1})$ will force the other L-functions to not have zeroes! An idea like this is able to produce a zero-free region, and it is the key input to Siegel's theorem.

3.7 February 24

Again, this lecture was recorded. Our goal here is to state and prove Siegel's theorem. This will be our first "ineffective" theorem.

3.7.1 Siegel's Theorem

Fix a primitive Dirichlet character $\chi \pmod q$. Recall that there is an effective constant $c > 0$ such that $L(s,\chi)$ has no zeroes in the region

$$\left\{ s : \operatorname{Re} s > 1 - \frac{c}{\log(q|t|+2)} \right\}$$

except possibly a real zero in the case where χ is a real character.

We also recall from Landau that distinct primitive Dirichlet characters χ_1 and χ_2 with coprime moduli will make

$$\zeta_K(s) \coloneqq \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2)$$

have nonnegative coefficients.

Remark 3.65. If we set $\chi_1 = \left(\frac{d_1}{\bullet}\right)$ and $\chi_2 = \left(\frac{d_2}{\bullet}\right)$, then the above Dirichlet series is the Dedekind ζ-function associated to the biquadratic field $K \coloneqq \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. In particular, the fact that ζ_K has nonnegative coefficients is direct from this definition.

Now, one can repeat the argument from Lemma 2.63 to get that there is at most one zero of ζ_K in the desired region, that it must be real, and that it must live in $(1 - c/\log(q_1 q_2), 1]$. As an aside, we do note that $L(1,\chi) \gg 1/\sqrt{q}$, so we get somewhat automatically (from also bounding $L'(s,\chi)$) that $L(s,\chi)$ does not vanish on $\left(1 - c/(\sqrt{q}(\log q)^2), 1\right)$ for some constant $c > 0$.

Remark 3.66. As an example, one can estimate the first prime p which is $p \equiv a \pmod q$ for some (a,q) with $\gcd(a,q) = 1$. From the above considerations, one gets about e^q, but we expect $q^{1+\varepsilon}$ for any $\varepsilon > 0$.

With these preliminaries, we are ready to state Siegel's theorem.

Theorem 3.67 (Siegel). Fix a primitive Dirichlet character $\chi \pmod q$. For any $\varepsilon > 0$ with $\varepsilon \leq 1/2$, there is a(n ineffective) constant $c(\varepsilon) > 0$ such that

$$L(1,\chi) \geq c(\varepsilon) q^{-\varepsilon}.$$

Remark 3.68. From this lower bound, one sees that $L(s,\chi)$ has no zeroes in the region $(1 - c(\varepsilon)/q^{\varepsilon}, 1]$. Namely, we also have a bound on $L'(s,\chi)$.

Remark 3.69. One can use this result, combined with the class number formula, to show that there are only finitely many imaginary quadratic fields with class number equal to 1.

We now turn to the proof of Theorem 3.67.

Proof of Theorem 3.67. We follow Goldfeld's proof of this result. Recall

$$\zeta_K(s) \coloneqq \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2)$$

has nonnegative coefficients. Choose $\beta \in [3/4, 1)$, which is a surprise tool which will help us later. The trick is to look at

$$I(\beta) \coloneqq \frac{1}{2\pi i}\int_{\operatorname{Re} s=2} \zeta_K(s+\beta)\Gamma(s)x^s\,ds.$$

Notably, as $|t| \to \infty$, we have $|\Gamma(\sigma+it)| \sim e^{-\pi|t|/2}|t|^{\sigma-1/2}$ for bounded $|\sigma|$, so everything is going to converge absolutely. Now, absolute convergence everywhere allows us to exchange the sum and integral to give

$$I(\beta) = \sum_{n=1}^{\infty} \frac{a_n}{n^\beta} e^{-n/x},$$

where a_n are the coefficients of $\zeta_K(s)$. Notably, by positivity, we have the lower bound $I(\beta) \geq 1$.

We now shift the contour of I to $\operatorname{Re} s = 1/2 - \beta$. ∎

3.8 February 27

Last class we showed Siegel's theorem. In particular, for real primitive characters χ with conductor q, we have $|L(1,\chi)| \gg q^{-\varepsilon}$ for any $\varepsilon > 0$, where the implied constant is ineffective.

Remark 3.70. As a correction, Mordell's conjecture that curves of genus at least 2 have at most finitely many rational solutions. For example, for any $n \geq 4$, the equation $x^n + y^n = 1$ has finitely many rational solutions. We mention this because computing the number of points exactly (though finite) is ineffective; this is an active area of research in arithmetic geometry.

In this second half of the semester, we are going to cover quite a few disparate topics. In particular, after doing a few more applications (the Burgess bound and elementary counting over finite fields), we will turn to sieve theory (e.g., the weak Goldbach conjecture).

3.8.1 The Burgess Bound

We are going to do the analytic part of the argument here. Roughly speaking, we are interested in bounding sums which look like

$$\left|\sum_{n=1}^{N} \chi(n)\right|.$$

From Theorem 3.22, we do have a bound of $\sqrt{q}\log q$, but we would like to do better for smaller N.

Remark 3.71. Under the Generalized Riemann Hypothesis, one can achieve

$$\left|\sum_{n=1}^{N} \chi(n)\right| \ll \sqrt{q}\log\log q.$$

This is due to Montgomery–Vaughan. However, one expects to have $\ll_\varepsilon \sqrt{N}q^\varepsilon$ for any $\varepsilon > 0$.

For applications, we are primarily interested in the smallest q for which $\chi(q) \neq 1$, for which these sums help, up to some constants. (For example, this implies an upper bound on the least nonquadratic residue.) We are going to achieve some cancellation for N bigger than $q^{1/4}$, which is better than what is given by Theorem 3.22.

Theorem 3.72 (Burgess)**.** Fix $\delta, \varepsilon > 0$. There exists some $p_0(\delta, \varepsilon) > 0$ such that, for primes $p > p_0(\delta, \varepsilon)$ and $N > p^{1/4+\delta}$, we have

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < \varepsilon N$$

for nontrivial characters $\chi \pmod p$.

Remark 3.73. One can even allow the conductor p to be cube-free, where $\chi \pmod p$ is now forced to be primitive.

3.8.2 A Little on Curves

We are going to show Theorem 3.72 in the real character case, where $\chi = \left(\frac{\bullet}{p}\right)$. For this, we are going to want the following ingredient.

Definition 3.74 (hyperelliptic curve)**.** Fix a polynomial $P(x) \in \mathbb{Z}[x]$ of degree $r \geq 3$. Given a prime p, we may consider *the hyperelliptic curve*

$$C_p \coloneqq \left\{(x, y) \in \mathbb{F}_p^2 : y^2 = P(x)\right\}.$$

Further, we say that C_p is *irreducible* if and only if $P(x) \pmod p$ is not a square.

Theorem 3.75 (Riemann hypothesis for curves)**.** Fix an irreducible projective curve $C/\mathbb{F}_p$, and define $N_p \coloneqq \#C(\mathbb{F}_p)$. Then

$$|N_p - (p+1)| < 8(\deg C)\sqrt{p}$$

for p large enough.

Remark 3.76. Our definition of N_p is including points at infinity, so one must be careful about just counting $\mathbb{F}_p$-points on a curve. Our following argument

We are not going to prove Theorem 3.75 in full generality (e.g., this should hold for arbitrary projective varieties), but we will be able to show a somewhat weaker statement in our case, which will be good enough for our purposes.

Quickly, let's explain why we are looking at these hyperelliptic curves at all.

Lemma 3.77. Fix a polynomial $P(x) \in \mathbb{Z}[x]$ of degree r. Further, fix a prime p.

(a) There are most r points $(x, y) \in \mathbb{F}_p^2$ such that $y^2 = f(x)$ such that $P(x) \equiv 0 \pmod{p}$.

(b) There are either zero or two points $(x, y) \in \mathbb{F}_p^2$ such that $y^2 = f(x)$ if $P(x) \not\equiv 0 \pmod{p}$; we have zero if $\left(\frac{P(x)}{p}\right) = 1$ and 0 if $\left(\frac{P(x)}{p}\right) = -1$.

(c) In total, the number of points $(x, y) \in \mathbb{F}_p^2$ is

$$p + \sum_{x \pmod{p}} \left(\frac{P(x)}{p}\right).$$

Proof. This is somewhat direct. The first statement (a) holds because $P(x)$ has at most r roots $\pmod{p}$, and then $y = 0$ is forced. The second statement (b) holds by tracking if $P(x)$ is a quadratic residue or not. Then the third statement (c) holds by the above casework on $x \pmod{p}$. ■

Comparing Lemma 3.77 with Theorem 3.75 produces the bound

$$\left| \sum_{x \pmod{p}} \left(\frac{P(x)}{p}\right) \right| \le 2 + r\sqrt{p}.$$

One can improve the constant here with some effort. With elementary methods, one can actually achieve

$$\left| \sum_{x \pmod{p}} \left(\frac{P(x)}{p}\right) \right| \le 9r\sqrt{p}.$$

3.9 March 1

We continue discussing the Burgess bound.

3.9.1 Proving the Burgess Bound

For the Burgess bound, we want the following moment result.

Notation 3.78. We set $\chi_p := \left(\frac{\bullet}{p}\right)$ to be the non-principal real Dirichlet character $\pmod{p}$.

Lemma 3.79. Fix a prime p. Given some B, we have

$$\sum_{x=0}^{p-1} \left| \sum_{1 \le b \le B} \chi(x+b) \right|^{2r} \le (2rB)^r p + 2rB^{2r}\sqrt{p}.$$

Roughly speaking, it will turn out that understanding moments as above will be enough to control sums of polynomials.

Proof. By Weil's bound above, we see that

$$\left| \sum_{x=0}^{p-1} \chi_p(x+b_1) \cdots \chi(x+b_{2r}) \right| \le r\sqrt{p},$$

provided that the b_i are not just r pairs. As such, we note that

$$\#\left\{(b_1,\dots,b_{2r})\in[1,B]^{2r}:\text{they are not } r \text{ pairs}\right\}\le\binom{2r}{r}B^r r!\le(2r)^rB^r.$$

The left inequality is combinatorial: there are $\binom{2r}{r}$ elements to choose to be the left element of a pair, each has B options, and then there are $r!$ ways to rearrange these pairs. To finish the proof, one fully expands out

$$\left|\sum_{1\le b\le B}\chi(x+b)\right|^{2r}$$

by using some kind of multinomial theorem. Most of the terms can be bounded as above, but some terms (namely, the ones which are r pairs) must be bounded more crudely. Summing these as such completes the proof. ■

Now here is our result.

Theorem 3.80 (Burgess)**.** Set

$$S_M(N):=\sum_{M<n\le M+N}\chi_p(n).$$

Then

$$|S_M(N)|\ll_r N^{1-1/r}p^{(r+1)/\left(4r^2\right)}(\log p)^{1/r}$$

for all positive integers r.

Proof. This is by the moment method. Roughly speaking, this is stated so precisely in order to be able to induct on N. Comparing with the needed exponents, we are done except in the case where

$$Cp^{1/r+1/4r}\le N\le p^{1/2+1/4r}\log p,$$

where C is some large absolute constant. Namely, the left is because $|S_M(N)\le N$, and the right is because $|S_M(N)|\le 6\sqrt{p}\log p$ by Theorem 3.22. For example, we may assume that $N<p$.

Now, the idea is to shift the sum $S_M(N)$ by some $0\le h<N$. This yields

$$S_M(N)=\sum_{M\le n\le M+N}\chi_p(n+h)+2\theta E(h),$$

where $|\theta|\le 1$ and $E(h)=Ch^{1-1/r}p^{(r+1)/\left(4r^2\right)}(\log p)^{1/r}$. In particular, the $E(h)$ is covering the small overlaps from $M+1$ to $M+h$ and from $M+N+1$ to $M+N+h$.

To optimize our shifting, we will take $h=ab$ for $a\in[1,A]$ and $b\in[1,B]$, where $H:=AB$ is less than N. As such, doing all shifts at once, we see

$$S_M(N)=\frac{1}{H}\sum_{\substack{1\le a\le A\\1\le b\le B}}\sum_{M<n\le M+N}\chi(n+ab)+2\theta E(H).$$

To force this to behave (arithmetic progressions are hard!), we see

$$\left|\sum_{b=1}^{B}\chi_p(n+ab)\right|=\left|\sum_{1\le b\le B}\chi_p\left(a^{-1}n+b\right)\right|,$$

where the point is that we have turned this sum into a sum of some consecutive χ_ps. As such, we may re-index everything as follows: we see

$$|S_M(N)|\le\frac{1}{H}\cdot V+2E(H),$$

where

$$V = \sum_{x=0}^{p-1} \left(v(x) \left| \sum_{b=1}^{B} \chi(x+b) \right| \right),$$

where $v(x)$ is the number of ordered pairs (a,n) such that $a \in [1,A]$ and $n \in (M, M+N]$ and $a^{-1}n \equiv x \pmod p$. Note that $a^{-1} \pmod p$ makes sense because $A \leq H \leq N < p$. Roughly speaking, we are doing better now because $v(x)$ has somewhat controlled moments. For example, we see

$$V_1 \coloneqq \sum_{x=0}^{p-1} v(x) \leq AN,$$

and

$$V_2 \coloneqq \sum_{x=0}^{p-1} v(x)^2$$

is also relatively small, as we will shortly see. In particular, we have the following upper bound.

Lemma 3.81. Fix everything as above. Then $V_2 \leq 8AN(AN/p + \log(3A))$.

Proof. We count. Note that we can write

$$V_2 = \#\{(a_1,a_2,n_1,n_2) : 1 \leq a_1,a_2 \leq A, M \leq n_1,n_2 \leq M+N, a_1n_2 \equiv a_2n_1 \pmod p\},$$

where the x has disappeared because V_2 is a sum over all possible values of x. We now fix a few parameters to determine the other ones. For example, we will fix a_1 and a_2 and $k \coloneqq (a_1n_2 - a_2n_1)/p$ and then determine how many possible n_1 and n_2 fit these constraints; i.e., we want the number of ordered pairs (n_1,n_2) such that

$$a_1n_2 - a_2n_1 = kp.$$

Notably, this is bounded above by $2N \gcd(a_1,a_2)/\max\{a_1,a_2\}$: namely, n_1 lives in an interval of length N (without loss of generality, take $a_1 \geq a_2$), and two solutions n_2 for the single n_1 must be the same modulo $\gcd(a_1,a_2)$. Thus, we see

$$V_2 \leq 2N \sum_{1 \leq a_1,a_2 \leq A} \frac{\gcd(a_1,a_2)}{\max\{a_1,a_2\}} \left(\frac{2AN}{\gcd(a_1,a_2)p} + 1 \right).$$

Namely, we are counting the number of possible k here: certainly this difference is less than AN in magnitude, but if $\gcd(a_1,a_2) > 1$, then the differences will have this divisibility condition as well. So we are counting the number of k in some interval of length $2AN$ with modularity conditions modulo $p\gcd(a_1,a_2)$, which provides the bound.

The remaining computation is relatively straightforward. The left term is

$$\frac{2(AN)^2}{p} \sum_{1 \leq a_1,a_2 \leq A} \frac{1}{\max\{a_1,a_2\}},$$

and the sum here is a constant. The right term here is

$$2N \sum_{1 \leq a_1,a_2 \leq A} \frac{\gcd(a_1,a_2)}{\max\{a_1,a_2\}},$$

so one can sum over divisors to finish. In particular, with $\gcd(a_1,a_2) = d$, then we achieve at most $4NA/d$ from this sum, but summing over all possible d grants a $\log A$ term. The bounding is annoying, but apparently it can be done. ∎

Further, we may set

$$W_r \coloneqq \sum_{x=0}^{p-1} \left| \sum_{b=1}^{B} \chi_p(x+b) \right|^{2r} \leq (2rB)^r p + 2rB^{2r}\sqrt{p}$$

by Lemma 3.79, so Hölder's inequality yields

$$V \leq V_1^{1-1/r} V_2^{1/2r} W^{1/2r}.$$

As a technical choice, we assume that p is sufficiently large, which we may do by adjusting the constant C appropriately. Now, we set $B \coloneqq \lfloor rp^{1/(2r)} \rfloor$ so that $W < (4r)^{2r} p^{3/2}$ for p large enough; this allows us to set $A \coloneqq \lfloor N/\left(9rp^{1/(2r)}\right) \rfloor$ so that $AB < N$ (but is only off by some constant factor). From here, one computes

$$AN \leq \frac{N^2}{9rp^{1/(2r)}} \leq p(\log p)^2.$$

From the previous lemma, one sees $V_2 \leq AN(4\log p)^2$, and in total we see

$$\begin{aligned} V &\leq V_1^{1-1/r} V_2^{1/(2r)} W^{1/(2r)} \\ &\leq (AN)^{1-1/r} \left(AN \cdot (4\log p)^2\right)^{1/(2r)} \cdot \left((4r)^{2r} p^{3/2}\right)^{1/(2r)} \\ &\leq (AN)^{1-1/(2r)} \cdot 4r \cdot \left(4\log p \cdot p^{3/4}\right)^{1/r} \\ &\leq 2N^{2-1/r} \left(p^{(r+1)/(2r)} \log p\right)^{1/r}. \end{aligned}$$

Now, we note $H = AB \leq 2N/9$ by construction of A and B, and we can also see that $H \geq N/10$ by some computation, so the result follows. ∎

Remark 3.82. To see how this implies Theorem 3.72, the point is that $N > p^{1/4+\delta}$ will give $N^{1-1/r} \cdot p^{(r+1)/\left(4r^2\right)}$ relatively small. In particular, $p^{(r+1)/\left(4r^2\right)}$ is about $p^{1/(4r)}$, so we want N to be at least $p^{1/4}$ plus perhaps some small thing.

3.10 March 3

We began class by finishing the proof of Siegel's theorem. I have edited directly into those notes for completeness.

3.10.1 The Prime Number Theorem in Arithmetic Progressions

We are now ready to prove the Prime number theorem in arithmetic progressions. The point here is to input our zero-free region (improved by Siegel's theorem) into our Prime number theorem machine to get out a prime number theorem for arithmetic progressions.

Definition 3.83. Fix coprime integers a and q. Then we define

$$\psi(x; q, a) \coloneqq \sum_{\substack{n<x \\ n \equiv a \pmod q}} \Lambda(n).$$

Let's be more explicit about our zero-free regions. Fix a primitive Dirichlet character $\chi \pmod q$.

- For some constant $c > 0$, we know that $L(s, \chi)$ has no zeroes in the region

$$\left\{ s : \operatorname{Re} s > 1 - \frac{c}{\log(q(|t| + 2))} \right\}$$

  except for possibly a real zero if χ is a real character.
- In the event that χ is a real character, then each $\varepsilon > 0$ provides an ineffective constant $c(\varepsilon)$ such that $L(s, \chi)$ does not have a zero in the interval $(1 - c(\varepsilon)/q^{\varepsilon}, 1]$ for any $\varepsilon > 0$.

These inputs give the following result.

Theorem 3.84 (Siegel–Walfisz)**.** Fix coprime integers a and q, and fix some $\varepsilon > 0$. Then we see

$$\psi(x; q, a) = \frac{x}{\varphi(q)} + O_{\varepsilon}\left(\frac{x}{(\log x)^{1+\varepsilon}} \right),$$

where the implied constant is ineffective.

Remark 3.85. One can improve this result in various ways. For example, averaging over $a \pmod q$ is the Bombieri–Vinogradov theorem. Under the assumption of the generalized Riemann hypothesis, we have

$$\psi(x; q, a) = \frac{x}{\varphi(q)} + O_{\varepsilon}\left(x^{1/2+\varepsilon} \right),$$

where the implied constant is effective.

For the remainder of the class, we are going to turn towards sieve theory.

Theme 4
Introduction to Sieve Theory

4.1 March 6

Let's begin sieve theory.

4.1.1 Elementary Sieve Theory

Roughly speaking, the idea here is that we have some sequence $\{a_n\}_{n\in\mathbb{N}}$ of nonnegative real numbers, and we want to compute the asymptotics of the sum

$$\sum_{p\le N} a_p$$

for N large. The reason we call this "sieve theory" is that we are going to remove terms by inclusion–exclusion. In particular, we are going to assume that we have understanding of the sum in arithmetic progressions (say, with small arithmetic progressions) and then compute some our sum with some error terms.

Example 4.1. If we let a_n denote the condition that $n-2$ is prime, then

$$\sum_{p\le N} a_p$$

counts the number of twin prime pairs less than or equal to N.

To set up our sieving, we set the following notation.

Notation 4.2. For real number z, we define

$$P_z \coloneqq \prod_{p\le z} p.$$

The point is that we might instead sieve for

$$\sum_{\substack{n\le N\\ \gcd(n,P_z)=1}} a_n$$

for N large. In other words, we are asking for n to not have small prime factors.

Let's state a basic sieve, which is the Selberg sieve. Roughly speaking, the idea is to use Möbius inversion to sieve out entries in our sum which have small prime factors. Here is the definition of the Möbius function.

Definition 4.3 (μ)**.** We define the *Möbius* function $\mu\colon \mathbb{N} \to \mathbb{C}$ as

$$\mu(n) \coloneqq \begin{cases} (-1)^k & \text{if } n = p_1 \cdots p_k \text{ where } n \text{ is squarefree,} \\ 0 & \text{if } n \text{ is not squarefree.} \end{cases}$$

Note that $\mu(1) = (-1)^0 = 1$.

Remark 4.4. Observe that μ is multiplicative. This is a direct computation.

Remark 4.5. By the Euler product, we see that

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^{-s}}\right) = \prod_p \left(\sum_{k=0}^{\infty} \frac{\mu\left(p^k\right)}{p^{ks}}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

As such, using the Dirichlet convolution, we see that

$$\sum_{d \mid n, d \mid P_z} \mu(d) = \begin{cases} 1 & \text{if } \gcd(n, P_z) = 1, \\ 0 & \text{if } \gcd(n, P_z) > 1. \end{cases}$$

This is the Möbius inversion formula.

Proposition 4.6 (Selberg sieve)**.** Fix a sequence $\mathcal{A} = \{a_n\}_{n=1}^N$ of nonnegative real numbers in $[0, 1]$. Further, suppose that we have (large) integers X and D such that we may write

$$\sum_{n \le N} a_n = X \qquad \text{and} \qquad \sum_{n \equiv 0 \pmod d} g(d)X + r(d, \mathcal{A}),$$

for each squarefree d, where we satisfy the following conditions.

(i) d is squarefree.

(ii) g is multiplicative and $0 \le g(p) < 1$ for all p.

(iii) The sum $\sum_{d \le D} |r(d)|$ is relatively small.

Then we define $S(\mathcal{A}, P_z) \coloneqq \sum_{n \le N, \gcd(n, P_z) = 1} a_n$. Then

$$S(\mathcal{A}, P_z) \le \frac{X}{J} + \sum_{d \le D} \tau_3(d) |r(d, \mathcal{A})|,$$

where J is some effective constant, and $\tau_3(d) = \#\{(a, b, c) : abc = d\}$.

Remark 4.7. It is true that $\tau_3(d) \ll_\varepsilon d^\varepsilon$ for any $\varepsilon > 0$. This is a combinatorial result, which we will not show explicitly here.

Remark 4.8. One expects that $J \approx V(z) \coloneqq \prod_{p\le z}(1-g(p))$. Roughly speaking, this is what we expect to occur if the primes behave randomly, meaning that there is absolutely no error in our inclusion–exclusion arguments.

Remark 4.9. In the event that $g(p) = 1/p$ always, one is able to bound (using the proof of the Selberg sieve)

Remark 4.10. One can use the Brun sieve, which we have not introduced here, to "truncate" the above sums to produce a lower bound.

Remark 4.11. If we can achieve $z > \sqrt{N}$, then our sum is actually

$$\sum_{z<p\le N} a_p \le S(\mathcal{A}, P_z).$$

Thus, we have the basic upper bound of

$$\sum_{p\le N} a_p \le S(\mathcal{A}, P_z) + z$$

because $a_n \le 1$ always. In fact, if we can achieve $z = N^\alpha$ for small $\alpha > 0$, then we achieve our upper bound as needed. However, we do not get good lower bounds from our sieving. Roughly speaking, $z = N^\alpha$ keeps values of n which have at most $1/\alpha$ prime factors because the smallest prime permitted is 2.

Let's move towards a proof of Proposition 4.6 over time. By Möbius inversion in the form of Remark 4.5, we may write

$$\begin{aligned} S &\coloneqq \sum_{\substack{n\le N\\ \gcd(n,P_z)=1}} a_n \\ &= \sum_{n\le N} a_n \left(\sum_{d\mid n, d\mid P_z} \mu(d) \right) \\ &= \sum_{d\mid P_z} \mu(d) \left(\sum_{n\equiv 0 \pmod d} a_n \right). \end{aligned}$$

Now, the idea is that only the terms with $d \le z$ should matter, which is why we defined $V(z)$ in that way.

Roughly speaking, the idea is to define real parameters $\rho_1, \dots, \rho_d$, where $d \le \sqrt{D}$ and $\rho_1 = 1$, and we examine the sums

$$\sum_{n\le N} \left(\sum_{\substack{d\le\sqrt{D}\\ d\mid \gcd(n,P_z)}} \rho_d \right)^2 a_n,$$

which we know must be an upper bound for $S = S(\mathcal{A}, P_z)$ because $\rho_1^2 = 1$ is our term in the event of $\gcd(n, P_z) = 1$. The internal sum is a quadratic form in our parameters $\rho_\bullet$, so we will minimize its value by diagonalizing. For example, we can write

$$S \le \sum_{d_1,d_2\mid P_z} \rho_{d_1}\rho_{d_2} \sum_{\substack{d_1,d_2\mid n\\ n\le N}} a_n = \sum_{d_1,d_2\mid P_z} \rho_{d_1}\rho_{d_2} \left(g(\operatorname{lcm}(d_1,d_2))X + r(\operatorname{lcm}(d_1,d_2),\mathcal{A}) \right),$$

which we hope gives us something to work with. As such, we define

$$G \coloneqq \sum_{d_1,d_2 \mid P_z} \rho_{d_1}\rho_{d_2} g(\operatorname{lcm}(d_1,d_2)) \qquad \text{and} \qquad R \coloneqq \sum_{d_1,d_2 \mid P_z} r(\operatorname{lcm}(d_1,d_2),\mathcal{A})\rho_{d_1}\rho_{d_2}.$$

Here, our main term is G, and our remainder term is R. Notably, if we can achieve $\rho_\bullet \in [0,1]$ for all $\rho_\bullet$, then we can immediately bound

$$R \le \sum_{d_1,d_2 \mid P_z} |r(\operatorname{lcm}(d_1,d_2),\mathcal{A})| = \sum_{d \le D} \tau_3(d)|r(d,\mathcal{A})|,$$

where the last inequality simply counts the number of times some $r(d,\mathcal{A})$ might appear in the sum. As such, the difficulty will arise in bounding the main term G.

4.2 March 8

We continue discussing the Selberg sieve. I'm just going to edit into the previous day's lecture notes for continuity.

4.2.1 Bounding the Main Term

Roughly speaking, we are going to work through some Cauchy–Schwarz argument in order to achieve our lower bound on G. The idea is to view G as a quadratic form in the $\rho_{d_\bullet}$, for which we have tools to optimize. In particular, we see that pairs (d_1,d_2) each dividing P_z is equivalent to coprime triples (a,b,c) with product dividing P_z by setting $c \coloneqq \gcd(d_1,d_2)$ and $a \coloneqq d_1/c$ and $b \coloneqq d_2/c$. As such, we see

$$G = \sum_{\text{coprime } abc \mid P_z} g(abc)\rho_{ac}\rho_{bc} = \sum_{c \mid P} \left(g(c) \sum_{\text{coprime } ab \mid (P_z/c)} g(a)g(b)\rho_{ac}\rho_{bc} \right).$$

We would like to relax the condition that a and b are coprime. For this, we use Möbius inversion to get

$$G = \sum_{c \mid P_z} \left(g(c) \sum_{a,b \mid P_z/c} \left(\sum_{d \mid \gcd(a,b)} \mu(d) \right) g(a)g(b)\rho_{ac}\rho_{bc} \right).$$

Exchanging the order of summation to pull d to the front, we get

$$G = \sum_{c \mid P} \left(g(c) \sum_{d \mid P_z/c} \mu(d)g(d)^2 \left(\sum_{m \mid P_z/(cd)} g(m)\rho_{cdm} \right)^2 \right)$$

by factoring out our square. To make our sum easier to optimize (namely, we would like the coefficient $g(m)$ to $g(cdm)$), we write this as

$$G = \sum_{c \mid P_z} \left(\frac{1}{g(c)} \sum_{d \mid P_z/c} \mu(d) \left(\sum_{m \mid P_z/(cd)} g(cdm)\rho_{cdm} \right)^2 \right).$$

The internal sum only depends on cd, so we set $k \coloneqq cd$ and exchange the order of summation to see

$$G = \sum_{k \mid P_z} \left(\sum_{c \mid k} \frac{\mu(k/c)}{g(c)} \right) \left(\sum_{m \mid P_z/k} g(km)\rho_{km} \right)^2.$$

Now, the function $k \mapsto \sum_{c \mid k} \frac{\mu(k/c)}{g(c)}$ is just $\frac{1}{h} \coloneqq \frac{1}{g} * \mu$ and is therefore multiplicative, so we can factor appropriately to see

$$\frac{1}{h(k)} = \sum_{c \mid k} \frac{\mu(k/c)}{g(c)} = \prod_{p \mid k} \left(\sum_{c \mid p} \mu(p/c) \cdot \frac{1}{g(c)} \right) = \prod_{p \mid k} \left(\frac{1}{g(p)} - 1 \right).$$

Anyway, we go ahead and write

$$G = \sum_{k \mid P_z} \frac{1}{h(d)} \left(\sum_{k \mid m, m \mid P_z} g(m) \rho_m \right)^2.$$

We now apply a chance of variables to finish the diagonalization. For $d \le \sqrt{D}$, we set

$$y_d \coloneqq \frac{\mu(d)}{h(d)} \sum_{\substack{d \mid m \\ m \text{ squarefree} \\ m \le \sqrt{D}}} g(m) \rho_m$$

so that

$$G = \sum_{d \le \sqrt{D}} h(d) y_d^2,$$

where our constraint is given by $\rho_1 = 1$. Notably, we can invert our definition of $y_\bullet$ to see

$$\rho_\ell = \frac{\mu(\ell)}{g(\ell)} \sum_{\substack{\ell \mid d \\ d \le \sqrt{D}}} h(d) y_d,$$

which we leave as an exercise. Thus, we are optimizing the quadratic form

$$G = \sum_{d \le \sqrt{D}} h(d) y_d^2$$

under the constraint that $1 = \rho_1 = \sum_{d \le \sqrt{D}} h(d) y_d$. In particular, by Cauchy–Schwarz, we can minimize G as $1/J$, where

$$J \coloneqq \sum_{d \le \sqrt{D}} h(d).$$

However, we see

$$\begin{aligned} J &= \sum_{k \mid \ell} \sum_{d \le \sqrt{D}, \gcd(d, \ell) = k} h(d) \\ &= \sum_{k \mid \ell} h(k) \sum_{m \le \sqrt{D}/k, \gcd(m, \ell) = 1} h(m) \\ &\ge \left(\sum_{k \mid \ell} h(k) \right) \left(\sum_{m \le \sqrt{D}/\ell, \gcd(m, \ell) = 1} h(m) \right) \\ &= \mu(\ell) \rho_\ell J. \end{aligned}$$

As such, we are able to bound $|\rho_\ell| \le 1$. Notably, our bound on G has now completed the proof of the Selberg sieve.

4.3 March 10

Today we apply the Selberg sieve in order to count twin primes.

4.3.1 The Sieve Dimension

We work in the context of the Selberg sieve. Suppose now that $\beta_p \coloneqq pg(p)$ is actually bounded. Then we may compute

$$\begin{aligned} -\log V(z) &= \sum_{p<z} -\log(1-g(p)) \\ &= \sum_{p<z} g(p) + O(1) \\ &= \sum_{p<z} \frac{\beta_p}{p} + O(1). \end{aligned}$$

In general, we hope that

$$\sum_{p<z} \frac{\beta_p}{p} \sim \kappa \log\log z,$$

roughly because β_p ought to be bounded.

Remark 4.12. Let's justify the above intuition. We claim that

$$\sum_{p\le z} \frac{1}{p} = \log\log z + O(1),$$

which will be enough by expanding out $\log V(z)$, expanding out the Taylor series, and only paying attention to the degree-one terms. Indeed, to see the above equality, one notes that

$$\sum_{d\le x} \Lambda(d) \left\lfloor \frac{x}{d} \right\rfloor = \sum_{n\le x} \log n = x\log x - x + O(\log x),$$

but this left-hand side is about $\sum_{d\le x} \frac{\log p}{p}$, so the original equality follows by partial summation.

This κ is called the "sieve dimension." Anyway, we see thus see that $V(z) \sim (\log z)^{-\kappa}$.

Example 4.13. Suppose the sequence a_n is constant. Then we have $g(d) = 1/d$ always because

$$\sum_{n\equiv 0 \pmod d} a_n = \frac{x}{d} + O(1),$$

so we note that $\kappa = 1$ because $\sum_{p\le x} \frac{1}{p} = \log\log x + O(1)$.

Example 4.14. Fix some b. Define a_n to be 1 if $n = m^2 + b$ for some m and 0 otherwise. Then for any $p > 2$ such that $p \nmid b$, we have

$$\beta_p = \#\left\{x \pmod p : p \mid x^2 + b\right\} = \begin{cases} 2 & \text{if } \left(\frac{-b}{p}\right) = 1, \\ 0 & \text{otherwise.} \end{cases} = \left(\frac{-b}{p}\right) + 1$$

Now, by summation by parts, we see that $\sum_{p\le x} \left(\frac{-b}{p}\right) = o(x/\log x)$, so $\kappa = 1$ follows by adding in the needed 1 to our summing. Algebraic number theory is able to relate this situation to some counting of prime ideals with specified splitting behavior, which provides some context.

Remark 4.15. More generally, we might ask for the number of roots of $f(x) \pmod p$ for a fixed irreducible $f \in \mathbb{Z}[x]$. One can show that the sieve dimension is still 1 here, but the proof requires the Chebotarev density theorem.

Example 4.16. We might ask how frequently the function x^2+y^2+1 is prime. Then one gets

$$\sum_{x,y \le T, d \mid f(x,y)} = g(d)X + r,$$

where one sets $X = 4T^2$. Now, we define $g(p)$ to be the number of solutions to $x^2+y^2+1 \equiv 0 \pmod p$. By summing appropriately over the Legendre symbol, we see that $g(p) = (1+O(1/\sqrt{p}))/p$, so the sieve dimension is $\kappa = 1$ again.

4.3.2 Twin Primes

Here is our goal.

Theorem 4.17. We show

$$\sum_{\substack{p \le x \\ p+2 \text{ is prime}}} 1 \ll \frac{x}{(\log x)^2}.$$

Proof. Fix some x. Define a_n to be 1 if n takes the form $m(m+2)$ for some $m \le x$ and zero otherwise. Then for any d, we want that

$$\sum_{n \equiv 0 \pmod d} a_n = \beta_d \left(\frac{x}{d} + O(1) \right),$$

so we set $g(d) \coloneqq \beta_d/d$, and we note that we can make g multiplicative by the Chinese remainder theorem (we are asking how frequently $m(m+2)$ is divisible by some fixed d), so we can evaluate at primes to find $g(2) = 1/2$ and $g(p) = 2/p$ for p odd by counting the outputs.

Now, we set $z \coloneqq \sqrt{x}$. As in the Selberg sieve, we expect for

$$V(z) = \prod_{p<z} (1-g(p)) = \frac{1}{2} \prod_{2<p<z} \left(1 - \frac{2}{p}\right).$$

We expect $V(z) \ll 1/(\log x)^2$, which we get from taking the exponential of the estimate $\sum_{p \le z} \frac{1}{p} = \log\log p$ as in our discussion above.

For our proof, take $D \approx X^{1-\varepsilon}$. One can see without too much pain that $|r(d,\mathcal{A})| \ll_\varepsilon X^{3/2}$, so our remainder is

$$|R| \ll_\varepsilon X^{1-3/4}.$$

It remains to bound our main term, which we will out next class. ∎

4.4 March 13

Let's briefly introduce the Brun sieve.

4.4.1 The Brun Sieve

In contrast to the Selberg sieve, the Brun sieve provides a lower bound.

Theorem 4.18 (Brun sieve)**.** Fix a sequence $\mathcal{A} = \{a_n\}_{n=1}^N$ of nonnegative real numbers in $[0,1]$. Further, suppose that we have (large) integers X and D such that we may write

$$\sum_{n\le N} a_n = X \qquad \text{and} \qquad \sum_{n\equiv 0 \pmod d} g(d)X + r(d,\mathcal{A}),$$

for each squarefree d, where we satisfy the following conditions.

(i) d is squarefree.

(ii) g is multiplicative and $0 \le g(p) < 1$ for all p.

Then we can lower-bound $\mathcal{S}(\mathcal{A}, P_z) \coloneqq \sum_{n\le N, \gcd(n,P_z)=1} a_n$.

Idea. We will not prove this rigorously. As before, we note

$$S(\mathcal{A}, P_z) = \sum_{n=1}^N a_n \left(\sum_{d \mid \gcd(n,P_z)} \mu(d) \right),$$

where the internal sum is an indicator for $\gcd(n, P_z) = 1$. For the Brun sieve, we will optimize real numbers λ_d^+ and λ_d^- for $1 \le d \le D$ such that $\lambda_1^+ = \lambda_1^- = 1$ and

$$\sum_{d\mid n} \lambda_d^- \le 0 \le \sum_{d\mid n} \lambda_d^+$$

for each n. The point is that the $\lambda_\bullet^\pm$ behave as a truncated Möbius function.

Assuming the existence of these real numbers, we get some error terms R^+ and R^- such that

$$X \sum_{\substack{d\mid P_z \\ d\le D}} \lambda_d^- g(d) - R^- \le S(\mathcal{A}, P_z) \le X \sum_{\substack{d\mid P_z \\ d\le D}} \lambda_d^+ g(d) + R^+,$$

where

$$R^\pm \coloneqq \sum_{\substack{d\mid P_z \\ d\le D}} \left| \lambda_d^\pm r(d,\mathcal{A}) \right|.$$

We would like these remainder terms to be relatively small.

The point is that the magic goes into choosing the $\lambda_\bullet^\pm$. Roughly speaking, we will want to choose them to approximately agree with μ on small values. As such, we choose real parameters $y_m > 0$, and let D^+ denote the set of squarefree positive integers $d = q_1 \cdots q_r$ (with $q_i < q_{i+1}$) such that $q_m < y_m$ for each odd m, and we define D^- analogously as the set of squarefree positive integers $d = q_1 \cdots q_r$ (with $q_i < q_{i+1}$) such that $q_m < q_m$ for m even. We now want to define

$$\lambda_d^\pm \coloneqq \mu(d)|_{D^\pm}$$

for each d. To ensure that this is nonzero for enough d, we set our parameters y_m by

$$y_m \coloneqq \left(\frac{D}{p_1 \cdots p_m} \right)^{1/\beta}$$

where $\beta \ge 1$. ∎

4.4.2 Twin Primes

We now bound the main term of our Selberg sieve.

Theorem 4.19. Fix everything as in the Selberg sieve. Suppose we have an explicit constant $\kappa \in \mathbb{N}$ such that $g(p) \geq \kappa/p$ for all but finitely many primes p. Then, letting q denote the product of these finitely many primes, we have

$$J \geq \frac{(\frac{1}{2}\log D)^\kappa}{k! H_q}\left(1 - \frac{\kappa \ell(q)}{\frac{1}{2}\log D}\right),$$

where H_q and $\ell(q)$ are effective constants depending on q.

Proof. Explicitly, we will show that we may set

$$H_q = \prod_{p \mid q}(1-g(p))\left(1-\frac{1}{p}\right)^{-\kappa} \qquad \text{and} \qquad \ell(q) = \sum_{p \mid q} g(p)\log p.$$

Define $\tau_\kappa(n)$ denote the number of κ-tuples of positive integers $(a_1, \dots, a_k)$ such that $a_1 \cdots a_\kappa = n$. (The point is to be able to rearrange summations with some ease.) Recall that

$$h(b) \coloneqq \prod_{p \mid b}\left(\sum_{k=1}^{\infty} g(p)^k\right)$$

for squarefree b. As an aside, a direct computation with sticks-and-stones tells us that

$$\sum_{n \geq 0} \frac{\tau_\kappa(p^n)}{p^n} = \sum_{n \geq 0} \frac{\binom{\kappa+n-1}{n-1}}{p^n} = \left(1-\frac{1}{p}\right)^{-\kappa} = \left(\frac{\varphi(p)}{p}\right)^{-\kappa}. \tag{4.1}$$

Now, again by definition, we see

$$J = \sum_{\substack{\text{squarefree } a,b \\ ab < \sqrt{D} \\ a \mid q \\ \gcd(b,q)=1}} h(a)h(b)$$

by unwinding the Selberg sieve. As such, we see that we want to find a lower bound for

$$F(x) \coloneqq \sum_{\substack{\text{squarefre } b < x \\ \gcd(b,q)=1}} h(b).$$

Extending g to be completely multiplicative for technical reasons, we can define $h(b)$ in the same way, and we note that we still have $g(b) \geq \tau_\kappa(b)/b$ by checking locally at prime-powers and then multiplying. Notably, by expanding out the products in $h(b)$, we see

$$F(x) \geq \sum_{\substack{b < x \\ \gcd(b,q)=1}} g(b),$$

but our inequality $g(b) \geq \tau_\kappa(b)/b$ now grants

$$F(x) \geq \sum_{\substack{b < x \\ \gcd(b,q)=1}} \frac{\tau_\kappa(b)}{b}.$$

Adding in the remainder terms by multiplying through with (4.1), we see that actually

$$F(x) \geq \left(\frac{\varphi(q)}{q}\right)^\kappa \sum_{b<x} \frac{\tau_\kappa(b)}{b},$$

so upon expanding out τ_κ and using the integral bound for a sum, we see that

$$F(x) \geq \left(\frac{\varphi(q)}{q}\right)^\kappa \int_{\substack{x_1\cdots x_k<x\\ x_1,\dots,x_k\geq 1}} \frac{dx_1\cdots dx_\kappa}{x_1\cdots x_\kappa} = \left(\frac{\varphi(q)}{q}\right)^\kappa \cdot \frac{1}{\kappa!}(\log x)^\kappa,$$

where we have omitted the computation of the integral. In total, we conclude

$$J \geq \frac{1}{k!} \sum_{\substack{\text{squarefree } a<\sqrt{D}\\ a\mid q}} h(a) \left(\frac{\varphi(q)}{q}\log\left(\frac{\sqrt{D}}{a}\right)\right)^\kappa.$$

However, we can lower-bound $(1-y)^\kappa \geq 1-\kappa y$, which turns this bound into

$$J \geq \frac{1}{k!}\left(\frac{\varphi(q)}{q}\log\sqrt{D}\right)^\kappa \sum_{\text{squarefree } a\mid q} h(a)\left(1-\kappa\cdot\frac{\log a}{\log\sqrt{D}}\right).$$

We are essentially done at this point, but we will massage this a little to make it prettier. For example, observe

$$j(q) \coloneqq \sum_{a\mid q} h(a) = \prod_{p\mid q}(1+h(p)) = \prod_{p\mid q}\frac{1}{1-g(p)}.$$

As such, we see

$$\begin{aligned}
\sum_{a\mid q} h(a)\log a &= \sum_{a\mid q}\left(h(a)\sum_{p\mid a}\log p\right)\\
&= \sum_{p\mid q}\left(\log p\sum_{b\mid q/p} h(bp)\right)\\
&= \sum_{p\mid q}\left(\log p\cdot\frac{g(p)}{1-g(p)}\prod_{p'\mid q/p}\frac{1}{1-g(p)}\right)\\
&= j(q)\ell(q).
\end{aligned}$$

■

Remark 4.20. For twin primes, we take $k=q=2$ in Theorem 4.19, which shows that our J has a suitable upper bound for our result. In particular, we get $J \gg (\log X)^2$, which is essentially what we want.

4.5 March 15

We began class by finishing the proof from last class. I have directly edited into those notes for continuity reasons.

4.5.1 More Counting by Geometry

As usual, fix a polynomial $F\in\mathbb{Z}[x,y]$. Roughly speaking, we are interested in the number of solutions to $F(x,y) \pmod p$ as a prime p varies. For analytic number theory, we care because these sorts of local factors appear when sieving or applying the circle method.

Example 4.21. Take $F(x,y) \coloneqq x^n+y^n-a$. Then one can show that $N_F(p) = p + O\left(n^2\sqrt{p}\right)$. The corresponding character sums here as x varies turns into a Gauss sum computation, which we do know how to bound already.

Remark 4.22. If F is irreducible, then the Weil conjecture grants

$$N_F(p) = p + O(g\sqrt{p}),$$

where g is the genus of the corresponding Riemann surface cut out by F. However, this is quite difficult to prove.

Here is the result that we will show.

Theorem 4.23. Fix an irreducible polynomial $f \in \mathbb{Z}[x]$ of degree 3 or 4, and define $F(x,y) \coloneqq y^2 - f(x)$. Then

$$N_F(p) - p \ll p^{2/3}.$$

Here, the implied constant is independent of f.

Proof in degree 4. Set $N \coloneqq N_F(p)$ for brevity. The idea is to average over a lot of fs and compute some moments. By looping over all x and y, we see that

$$\sum_{t\in\mathbb{F}_p} \sum_{x,y\in\mathbb{F}_p} e\left(\frac{tF(x,y)}{p}\right) = pN_F(p),$$

where the point is that the summation over t cause the sums to vanish whenever $F(x,y) = 0$. Now, removing the contribution at $t = 0$, we see

$$\sum_{t=1}^{p-1} \sum_{x,y\in\mathbb{F}_p} e\left(\frac{tF(x,y)}{p}\right) = p(N-p).$$

Now, going to the moment at $r \coloneqq 6$, so we note we can fully expand everything out as

$$p^r(N-p)^r = \sum_{t_1,\dots,t_r=1}^{p-1} \sum_{\substack{x_1,\dots,x_r=0\\ y_1,\dots,y_r=0}}^{p-1} e\left(\frac{1}{p}\sum_{k=1}^{r} t_k F(x_k,y_k)\right).$$

In order to smooth over some issues, we will work over a family of fs given by

$$F_a(x,y) = y^2 - a_1x^4 - a_2x^3 - a_3x^2 - a_4x - a_5$$

where the coefficients fully vary over $\mathbb{F}_p^5$. As such, summing over all $a \in \mathbb{F}_p^5$, we will see that we cancel everything out (namely, fix x and y and t, letting a vary) unless $t_1x^d + \cdots + t_6x^d = 0$ for $d \in \{0,1,2,3,4\}$ already. Call the set of (x,t) satisfying this system to be S.

Now, summing over y where $(x,t) \in S$, we see our contribution over y is

$$\left| p^5 \prod_{s=1}^{6} \sum_{y_s=0}^{p-1} e\left(\frac{t_s y_s^2}{p}\right)\right| \le p^8$$

by factoring everything appropriately. Thus, we see that

$$\sum_{a\in\mathbb{F}_p^5} p^6(N_{F_a} - p)^6 \le Mp^8,$$

where M is the number of solutions $(x,t) \in S$.

The game, now, is to bound M. For example, if the $x_\bullet$ are all distinct, then a computation of the Vandermonde determinant tells us that the only possible solution is $t_1 = \cdots = t_6 = 0$; this gives about p^7 total

solutions. If some of $x_\bullet$ are the same, then one can compute what happens in our degenerate cases, but they only contribute $O\left(p^6\right)$ solutions total,[1] so this term does not matter. In total, we get

$$\sum_{a\in\mathbb{F}_p^5}(N_a-p)^6\le p^9+O\left(p^8\right)$$

in total.

We now examine the $a\in\mathbb{F}_p^5$ more closely. Notably, we don't actually care about all $a\in\mathbb{F}_p^5$ because we require F_a to be irreducible for our argument. Let $B\subseteq\mathbb{F}_p^5$ be the set of the "worst" $a\in\mathbb{F}_p^5$ where F_a fails to be irreducible. In particular, we take the following cases for $f_a:=a_1x^4+\cdots+a_5x^0$.

- We might have $f_a=r\left(x^2+ex+f\right)^2$ for r a quadratic residue and $E,F\in\mathbb{F}_p$. Here, $N_{F_a}-p=p+O(1)$ by taking the square root directly. The number of solutions a here is given by $p^3/2+O\left(p^2\right)$.
- We might have $f_a=n\left(x^2+ex+f\right)^2$, where n is a non-quadratic residue, and $E,F\in\mathbb{F}_p$. Here, $N_{F_a}-p=-p+O(1)$, and the total number of a is the same.

Totaling the above contributions, we see that these "worst" as in fact total to p^9 in contribution, so we see

$$\sum_{a\notin B}(N_a-p)^6=O\left(p^8\right).$$

To complete the argument, we require one more idea: some $a\notin B$ are essentially the same curve F_a, up to a fractional linear transformation, which will in particular not change the number of our points. Explicitly, our fractional linear transformation is given by

$$\begin{bmatrix}a&b\\c&d\end{bmatrix}x=\frac{ax+b}{cx+d}\qquad\text{and}\qquad\begin{bmatrix}a&b\\c&d\end{bmatrix}y=\frac{y}{(cx+d)^2}.$$

Notably, hitting a curve with such a transformation by an element $\gamma\in\mathrm{GL}_2(\mathbb{F}_p)$, the number of points on the projective plane curve will not change, so the number of points in N_a will only change by $O(1)$. One can also compute directly that each $a\in\mathbb{F}_p^5$ gets transformed to at least $\gg p^4$ different $a'\in\mathbb{F}_p^5$.[2] Looking at a particular class of p^4 different $a\in\mathbb{F}_p^5$, we see that particular $a\in\mathbb{F}_p^5$ cannot have N_a-p exceeding $O\left(p^{2/3}\right)$. This completes the proof. ∎

4.6 March 17

We began class discussing Theorem 4.23.

4.6.1 Introducing the Circle Method

Roughly speaking, the idea is that

$$\int_{[0,1]^k}\sum_{j=1}^n e\left(n_j\cdot\alpha\right)\,d\alpha=\#\{j:n_j=0\}$$

by a direct integration. As an example, if we want to count the number of ways to write some N as the sum of ten cubes, we can use the function

$$e(-N\alpha)\left(\sum_{n=1}^p e\left(n^3\alpha\right)\right)^{10}.$$

[1] Roughly speaking, if some $x_\bullet$ are equal, then the "Lagrange interpolation problem" we are solving for the $t_\bullet$ has more degrees of freedom, in particular p more degrees of freedom. Nonetheless, we will dominate the main term.

[2] Rigorously, one can see that the action of $\mathrm{GL}_2(\mathbb{F}_p)$ on the space of degree-4 polynomials provides a symmetric action on the roots most of the time. The fact that our action is symmetric and hence essentially transitive will do the trick.

Now, these exponential sums can be studied separately, which allows us to bound the integral. In particular, the sum is large essentially only when we are close to rational numbers with reasonably small denominator; these are the major arcs. Then we call everything else a minor arc. Analyzing our integral on the major and minor arcs separately is occasionally able to produce novel bounds. This is the circle method.

Remark 4.24. The above function suggests that the circle method will have applications in additive number theory, which is indeed the case. By trying harder, one can achieve results in multiplicative number theory as well. (Our main application will be Vinogradov's three primes theorem.)

Historically, the circle method was introduced to study partitions.

Definition 4.25 (partition)**.** Given a positive integer n, we let $p(n)$ denote the number of *partitions* of n, where a partition is a summation

$$n = \lambda_1 + \cdots + \lambda_k$$

where the order here does not matter.

From the definition, an analysis of the generating function tells us that

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \left(1 + x^k + x^{2k} + x^{3k} + \cdots\right) = \prod_{k=1}^{\infty} \frac{1}{1-x^k},$$

where the choice of factor in the kth summation factor communicates the number of terms in our partition equal to k. Indeed, Hardy and Littlewood showed

$$p(n) \sim \frac{1}{4^n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

4.7 March 20

Either today or tomorrow we will receive an email with our preference for a project.

4.7.1 Partitions via the Circle Method

Let's sketch the following results.

Theorem 4.26 (Hardy–Ramanujan)**.** Let $p(n)$ be the number of partitions of n. Then

$$p(n) \sim \frac{1}{4^n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

Sketch. Let $\eta\colon \mathbb{H} \to \mathbb{C}$ denote the function

$$\eta(z) \coloneqq e^{2\pi i z/24} \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n z}\right).$$

Notably, we see

$$\eta(z)^{24} = \Delta(z) \coloneqq q \prod_{n=1}^{\infty} (1-q^n)^{24},$$

where $q \coloneqq e^{2\pi i z}$, and Δ is a modular form. In particular, we can compute

$$\eta(z+1) = e^{2\pi i/24}\eta(z) \qquad \text{and} \qquad \eta(-1/z) = \sqrt{-iz}\eta(z),$$

so η is a modular form of weight $1/2$ and some level. (This second equality is a bit nontrivial.) Roughly speaking, we would like to integrate the contour from $-\infty$ to $-1/2-iy$ to $1/2+iy$ to ∞. By integrating over our product, we see

$$p(n) = \int_{iy}^{i(y+1)} \frac{e^{2\pi iz}}{\eta(z)} \cdot e^{-2\pi inz}\, dz.$$

The idea is to send $y \to 0^+$. Namely, by the modularity condition, one sees that $|\eta(z)|^2(\operatorname{Im} z)$ is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, so $\eta(z)$ is forced to explode as $y \to 0^+$. Being explicit, we set $y \coloneqq 1/n$ for $n \to \infty$, and one can track through the action by $\mathrm{SL}_2(\mathbb{Z})$ to see that the "main" contribution into the integral over the aforementioned contour arises from rational a/q with small denominators; this is due to the pole of $1/\eta$. ■

Remark 4.27. One does not really need modularity to track through the circle method, even though it is fairly important in the above discussion. This is called the Hardy–Littlewood circle method.

4.7.2 Overview of the Circle Method

For the Hardy–Littlewood circle method, we are interested in nontrivial solutions to a Diophantine equation

$$f(x_1, \dots, x_n) = 0$$

where f is homogeneous of degree t. Roughly speaking, as long as n is large enough, the circle method will provide us with nontrivial solutions; in fact, when the circle method works, it is also able to track "local obstructions" to solutions: if (for example) it is difficult to obtain nontrivial solutions $\pmod p$ for some prime p, then this will be visible in the result.

Now, set

$$N_f(T) \coloneqq \#\left\{(x_1, \dots, x_n) \in (\mathbb{Z} \cap [-T, T])^n : f(x_1, \dots, x_n) = 0\right\},$$

and we can exchange the sum and the integral to see that

$$N_f(T) = \int_0^1 S_T(\alpha)\, d\alpha \qquad \text{where} \qquad S_T(\alpha) \coloneqq \sum_{-T \le x_1, \dots, x_n \le T} e(\alpha f(x_1, \dots, x_n)).$$

To be more rigorous about our previous remark, the circle method (if it succeeds) will be able to show that $N_f(T) \sim cT^{n-t}$, where c is some constant sensitive to local obstructions. For example, one can upper-bound $|S_T(\alpha)| \le S_T(0)$ absolutely, and $S_T(0) \sim (2T)^n$. To see local obstructions, we track $\alpha = a/q$ where $\gcd(a, q) = 1$ to see

$$S_T(a/q) = \sum_{-T \le x_1, \dots, x_n \le T} e\left(\frac{a}{q} f(x_1, \dots, x_n)\right) = \sum_{y \in (\mathbb{Z}/q\mathbb{Z})^n} \left(e\left(\frac{a}{q} f(y)\right) \sum_{\substack{-T \le x_1, \dots, x_n \le T \\ x \equiv y \pmod q}} 1 \right).$$

The rightmost sum is approximately $(2T/q)^n$, and then the left sum approximately picks up on some local density of solving $f \pmod q$. Thus, we hope we can integrate $S_T(\alpha)$ in two phases.

- Major arcs: for $\alpha = a/q$ with small denominators, we compute some local densities. Tracking through error terms also lets us estimate $S_T(\alpha)$ close by these rationals.
- Minor arcs: elsewhere (away from these rationals), we expect large cancellation to occur. Hopefully, we are able to run some computation to bound these terms.

Let's be more explicit. Fix some large T, and we will work with $q \le T^\beta$ for small β. For some $\gamma \approx 1$, we work with $Q \coloneqq T^\gamma$. We now define the "major arc"

$$\mathfrak{M}(a, q) \coloneqq \left\{\alpha \in [0, 1] : \left|\alpha - \frac{a}{q}\right| < \frac{1}{Q}\right\},$$

and we let $\mathfrak{M}$ denote the union of the major arcs. Then the complement $\mathfrak{m} \coloneqq [0,1] \setminus \mathfrak{M}$ consists of the minor arcs. In total, we see

$$N_f(T) = \int_{\mathfrak{M}} S_T(\alpha)\, d\alpha + \int_{\mathfrak{m}} S_T(\alpha)\, d\alpha,$$

and if the circle method works, then we have

$$N_f(T) \sim \int_{\mathfrak{M}} S_T(\alpha)\, d\alpha$$

as $T \to \infty$; a little work can show that this should evaluate as

$$N_f(T) \sim \mu_\infty(T) \prod_{p \text{ prime}} \delta_p,$$

where μ_∞ is the archimedean volume cut out by $f(x_1, \dots, x_n) = 0$ in the box $[-T, T]^n$, and δ_p arises as a density of solutions $f(x_1, \dots, x_n)$ in $\mathbb{Z}_p$. For example, if there is a local obstruction (i.e., no solutions in some $\mathbb{Z}_p$ or $\mathbb{R}$), then we will of course expect no solutions to appear.

Here is an example of the power present here.

Theorem 4.28 (Heath–Brown)**.** Fix a homogeneous nonsingular cubic polynomial $f(x_1, \dots, x_{10})$. Then $f(x) = 0$ has infinitely many solutions $(x_1, \dots, x_{10})$ where $\gcd(x_1, \dots, x_{10})$.

Remark 4.29. In nine variables, it is possible to have local obstructions making the above theorem false.

4.7.3 Beginning Vinogradov's Theorem

The idea here is to use the circle method and apply "diagonality." In particular, we define

$$S(\alpha) = \sum_{x \le N} \Lambda(x) e(\alpha x)$$

where $\alpha \in [0,1]$. One can now show that

$$\int_0^1 S(\alpha)^3 e(-N\alpha)\, d\alpha = \sum_{x_1+x_2+x_3=N} \Lambda(x_1)\Lambda(x_2)\Lambda(x_3),$$

so we see that the name of the game here is to show that the integral will be nonzero.

4.8 March 22

We continue discussing Vinogradov's theorem. We hope to make good progress discussing the main term.

4.8.1 Major Arcs

Our end goal of is to show that

$$\int_0^1 S(\alpha) e(-N\alpha)\, d\alpha \sim c(N) N^2,$$

where $c(N)$ is some collection of local densities; in particular, we will be able to bound it from above and below (by positive constants) for N odd.

Now, to define our major arcs, we choose some large $B > 0$ and set $P \coloneqq (\log N)^B$ (to upper-bound our denominators) and $Q \coloneqq N/(\log N)^B$ (to quantify the allowed error). In particular, for $q \le P$ and a with $\gcd(a,q) = 1$, we define

$$\mathfrak{M}(a,q) \coloneqq \left\{ \alpha : \left| \alpha - \frac{a}{q} \right| < \frac{1}{Q} \right\}.$$

Notably, for N large enough, all these majors are disjoint. Indeed, the point P is quite small in comparison to our error Q, so noting that the distance between two rationals $\frac{a}{q}$ and $\frac{a'}{q'}$ is bounded above by $\frac{1}{qq'} > \frac{1}{P^2} \gg \frac{1}{N}$ does the trick. As such, we may write

$$\mathfrak{M} \coloneqq \bigsqcup_{\substack{1 \le a < q \le P \\ \gcd(a,q)=1}} \mathfrak{M}(a,q) \qquad \text{and} \qquad \mathfrak{m} \coloneqq [0,1] \setminus \mathfrak{M}.$$

For now, the goal is to bound $\int_{\mathfrak{M}} S(\alpha)^3 e(-N\alpha)\,d\alpha$ and $\int_{\mathfrak{m}} S(\alpha)^3 e(-N\alpha)\,d\alpha$. Note that, for N large enough, $\mathfrak{M}(a,q) \subseteq [0,1]$ for $1 \le a < q$ because $q \le P \ll Q$.

Remark 4.30. For minor arcs, we will have

$$\left| \int_{\mathfrak{m}} S(\alpha) e(-N\alpha)\,d\alpha \right| \le \int_{\mathfrak{m}} |S(\alpha)|^3\,d\alpha \le \sup_{\alpha \in \mathfrak{m}} |S(\alpha)| \cdot \int_0^1 |S(\alpha)|^2\,d\alpha.$$

Now, one can use some moment methods in order to bound the rightmost integral. Vinogradov's main contribution was to figure out how to bound the L^∞-norm term $\sup_{\alpha \in \mathfrak{m}} |S(\alpha)|$. (In particular, Vinogradov obtained a $\log$ saving here, which was good enough.)

Let's focus on the major arcs for now. Here, living in some $\mathfrak{M}(a,q)$, any $\alpha \in \mathfrak{M}(a,q)$ can set $\beta \coloneqq \alpha - a/q$ so that $|\beta| < 1/Q$. Writing this out, we have

$$S(\alpha) = \sum_{x \le N} \Lambda(x) e\left(\frac{a}{q}x\right) e(\beta x).$$

The plan is to study $\sum_{x \le y} \Lambda(x) e\left(\frac{a}{q}x\right)$ via the Prime number theorem for arithmetic progressions and then apply summation by parts to appropriately bound $S(\alpha)$. In particular, we are going to use Siegel's theorem to select our B in our bounding.

Well, we recall that, for any q and b, we have

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \tau(\overline{\chi})\chi(b) = \begin{cases} e(b/q) & \text{if } \gcd(b,q) = 1, \\ 0 & \text{else,} \end{cases}$$

by the orthogonality relations. Thus,

$$\sum_{\substack{\gcd(x,q) \\ x \le N}} e(\alpha x)\Lambda(x) = \frac{1}{\varphi(q)} \sum_{\substack{\gcd(x,q) \\ x \le N}} \sum_{\chi \pmod q} \tau(\overline{\chi})\chi(x)\chi(a)\Lambda(x)e(\beta x).$$

Now, we do have a good understanding of

$$\psi(y,\chi) = \sum_{x \le y} \chi(x)\Lambda(x)$$

by Siegel's theorem. By adding in values of x with $\gcd(x,q) > 1$, we see

$$S(\alpha) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \left(\tau(\overline{\chi})\chi(a) \underbrace{\sum_{k \le N} \chi(k)\Lambda(k)e(\beta k)}_{\Sigma(\chi) \coloneqq} \right) + O\left((\log N)^2\right).$$

By summation by parts, this inner sum is

$$\Sigma(\chi) = e(N\beta)\psi(N,\chi) - 2\pi i\beta \int_1^N e(u\beta)\psi(u,\chi)\,du,$$

where the point is that β being small allows us to treat the right term as an error term. Now, if $\chi \neq \chi_0$, we can thus bound

$$|\Sigma(\chi)| \ll_B (1 + |\beta|N) Ne^{-c\sqrt{\log N}},$$

where c is some constant. Otherwise, in the case where $\chi = \chi_0$, one has to deal with $\psi(u, \chi)$ as no longer being negligible, so we need to deal with it when summing for our main contribution. As such, this is a little tricky. Set

$$T(\beta) \coloneqq \sum_{k=1}^{n} e(k\beta).$$

Then summation by parts yields

$$T(\beta) = e(N\beta)N - 2\pi i\beta \int_1^N e(u\beta) \lfloor u \rfloor \, du,$$

which is comparable to $\Sigma(\chi_0)$ by Siegel's theorem. To be explicit, we set $R(u) \coloneqq \psi(u, \chi_0) - \lfloor u \rfloor$, so we see

$$\Sigma(\chi) = T(\beta) + e(N\beta)R(N) - 2\pi i\beta \int_1^N e(u\beta)R(u) \, du = T(\beta) + O_B\left(1 + |\beta|Ne^{-c\sqrt{\log N}}\right).$$

We now note that $\tau(\chi_0) = \mu(q)$ by direct expansion, so we achieve

$$S(\alpha) = \frac{\mu(q)}{\varphi(q)} T(\beta) + O_B\left(Ne^{-c\sqrt{\log N}}\right),$$

where the point is that all the non-principal characters have gone into the error term. Cubing, we find

$$S(\alpha)^3 e(-N\alpha) = \frac{\mu(q)^3}{\varphi(q)^3} e\left(-N \cdot \frac{a}{q}\right) \cdot T(\beta)^3 e(-N\beta) + O\left(N^3 e^{-c\sqrt{\log N}}\right),$$

where the point is that $|T(\beta)| \ll N$, allowing us to move cross terms into the error term. As such, we may integrate

$$\int_{\mathfrak{M}(a,q)} S(\alpha)^3 e(-N\alpha) \, d\alpha = \left(\int_{-1/a}^{1/a} T(\beta)^3 e(-N\beta) \, d\beta\right) \left(\sum_{\substack{q \leq P \\ \gcd(a,q)=1}} \frac{\mu(q)^3}{\varphi(q)^3} e\left(-N \cdot \frac{a}{q}\right)\right) + O_B\left(N^2 e^{-c\sqrt{\log N}}\right).$$

Notably, it remains to discuss how to bound $T(\beta)$, which we will focus on next class.

4.9 March 24

We continue discussing the Hardy–Littlewood circle method.

4.9.1 Singular Things

Last class we showed that we have the contribution

$$\int_{\mathfrak{M}(a,q)} S(\alpha)^3 e(-N\alpha) \, d\alpha = \left(\int_{-1/Q}^{1/Q} T(\beta)^3 e(-N\beta) \, d\beta\right) \left(\sum_{\substack{1 \leq a < q \leq p \\ \gcd(a,q)=1}} \left(\frac{\mu(q)}{\varphi(q)^3}\right) e\left(-N\frac{a}{q}\right)\right).$$

Our goal for now is to compute the "singular integral"

$$\int_{-1/Q}^{1/Q} T(\beta)^3 e(-N\beta) \, d\beta.$$

Roughly speaking, the intuition is that these singular integrals are supposed to give rise to the archimedean factor in our major-arc contribution, which is a bit surprising because we are only looking at such a small interval. Well, we note that

$$\int_0^1 T(\beta)^3 e(-N\beta)\,d\beta = \frac{1}{2}(N-1)(N-2) = \frac{1}{2}N^2 + O(N)$$

by the definition of T as some geometric series which mostly vanishes. As such, we go compute

$$\int_{1/Q}^{1-1/Q} T(\beta)^3 e(-N\beta)\,d\beta \ll \int_{x>1/Q} x^{-3}\,dx \ll Q^2 = N^2(\log N)^{-2\beta},$$

where we have again used the definition of T in the second inequality. Thus, our singular integral is approximately

$$\int_{-1/Q}^{1/Q} T(\beta)^3 e(-N\beta)\,d\beta = \frac{1}{2}N^2 + O\left(N^2(\log N)^{-2\beta}\right) \sim \frac{1}{2}N^2,$$

which is indeed our archimedean density.

It remains to sum over the other major arcs to get the rest of our density contribution. This is our "singular series"

$$\sum_{\substack{1\le a<q\le p\\ \gcd(a,q)=1}} \left(\frac{\mu(q)}{\varphi(q)^3}\right) e\left(-N\frac{a}{q}\right).$$

To agree with the literature, we will be interested in evaluating

$$C_q(n) \coloneqq \sum_{\gcd(a,q)=1} e\left(-\frac{a}{q}n\right).$$

Notably, without the constraint $\gcd(a,q) = 1$, we can just use the Chinese remainder theorem to easily compute this sum; to add in this condition, we must sieve via Möbius inversion. As such, we observe

$$\sum_{n=1}^{q} e\left(-\frac{a}{q}n\right) = \sum_{d\mid q} \sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q} e\left(-\frac{a}{q}n\right) = \sum_{d\mid q} c_d(n).$$

However, the left-hand side vanishes when $q \nmid n$ and is q when $q \mid n$, so Möbius inversion yields

$$c_q(n) = \sum_{d\mid q,n} d\mu(q/d).$$

Namely, we morally should have $d \mid q$ over all divisors d here, but when $d \nmid n$, the contribution in the sum vanishes by our previous computation of the Möbius inversion; thus, we only pay attention to the terms with $d \mid n$ which yield d in the summation. We can check by hand that $C_q(n)$ is multiplicative in q (with n fixed), which now lets us fully compute $C_q(n)$. We can now compute

$$C_{p^\beta}(n) = \begin{cases} \varphi\left(p^\beta\right) & \text{if } \beta \le \nu_p(n),\\ -p^\alpha & \text{if } \beta = \alpha+1,\\ 0 & \text{else.}\end{cases}$$

Now, in our application, we really only care about the cases where q is semiprime (because we have a $\mu(q)$ term in our summation). Anyway, one can show that

$$c_q(n) = \frac{\mu(q/(n,q))\varphi(q)}{\varphi(q/(n,q))}$$

by checking on prime powers and extending multiplicatively. Thus, we bound $\varphi(q) \gg_\varepsilon q^{1-\varepsilon}$ for any $\varepsilon > 0$, so our summation is small enough in the sense

$$\left|\sum_{a>p} \frac{\mu(q)}{\varphi(q)^3} C_q(N)\right| \le \sum_{q>p} \varphi(q)^{-2} \ll (\log N)^{-B/2}$$

by using the bound that we just achieved. Thus, our summation converges.

We are now ready to compute our infinite sum as

$$\mathfrak{S}(N) := \sum_{q-1}^{\infty} \frac{\mu(q)}{\varphi(q)^2} C_q(N) = \prod_p \left(1 - \frac{C_p(N)}{(p-1)^3}\right) = \prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right)$$

by factoring the infinite geometric series in the usual way. As such, we morally expect $\mathfrak{S}(N)$

4.10 April 3

Today we bound the minor arcs. We are dealing with powers of $\log$s, so it's going to be a little technical today.

4.10.1 How to Bound Minor Arcs

We are going to apply Vinogradov's bilinear form method. Roughly speaking, we have

$$S(\alpha) \approx \sum_{p\le N} (\log p) e(\alpha p),$$

and we want cancellations to occur for α away from rationals with small denominator. More generally, we might be interested in bounding a summation of the form

$$\sum_{p\le N} f(p) \log p.$$

This will be done in two steps.

- Type I sums: for fixed$d$, we bound sums which look like

$$\sum_{\substack{n\le N \\ d|n}} f(n).$$

- Type II sums: for $d_1, d_2 \approx N^\beta$, we bound the bilinear sums

$$\sum_{n\le N} f(nd_1)\overline{f(nd_2)}.$$

These then combine to yield the desired summation. Here is the result we will build towards.

Theorem 4.31 (Vinogradov)**.** Suppose $\alpha \in \mathbb{R}$ has $|\alpha - a/q| < 1/q^2$ with $\gcd(a,q) = 1$. Then

$$|S(\alpha)| \ll \left(Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2}\right)(\log N)^4.$$

(The implied constant is absolute.)

Remark 4.32. This is our "pointwise bound" in our minor arcs. Momentarily, we will show that this pointwise bound manages to glue together to show the minor arcs give small contribution.

Roughly speaking, this will provide a good bound on our minor arcs. For example, for $\alpha = 1/4$, we don't get very much (it turns out to be worse than the trivial bound on S). However, for α irrational or rational with large denominator, we will get something more substantial. For example, $\alpha = \sqrt{2}$ is able to achieve

$$|S(\alpha)| \ll N^{4/5}(\log N)^4.$$

The point is that each N has some $q \approx N^{1/2}$ such that $|\alpha - a/q| < 1/q^2$ for some integer a. Explicitly, one should use the continued fraction expansion of $\sqrt{2}$ in order to achieve this bound.

Thus, we see that we are moving towards a Diophantine approximation problem to apply Theorem 4.31. Notably, we are interested in α which are not in the major arcs; namely, $\alpha \in \mathfrak{M}(a,q)$ means that

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{Q}$$

with $q \le P = (\log N)^B$ and $Q = N/(\log N)^B$. However, by Dirichlet's approximation theorem (in Diophantine approximation), we can still find some a/q such that

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

(This is essentially a Pigeonhole principle argument: consider integer multiples $0, \alpha, \dots, Q\alpha$ and choose the smallest distance once considered $\pmod 1$.) Notably, we have $q > P$ because α is not in a major arc, so we achieve

$$|S(\alpha)| \ll \left(NP^{-1/2} + N^{4/5} + N^{1/2}Q^{1/2}\right)(\log N)^4 \ll N(\log N)^{4-B/2},$$

so we have successfully saved our $\log$ terms. Thus, we see that

$$\left|\int_{\mathfrak{m}} S(\alpha)^3 e(-N\alpha)\,d\alpha\right| \le \sup_{\alpha\in\mathfrak{m}} |S(\alpha)| \int_{[0,1]} |S(\alpha)|^2\,d\alpha \ll N(\log N)^{4-B/2} \sum_{k\le N} \Lambda(k)^2 \le N^2(\log N)^{5-B/2}.$$

Taking $B = 2A + 10$ achieves $\le N^2(\log N)^{-A}$, so we achieve

$$\int_0^1 S(\alpha)^3 e(-N\alpha)\,d\alpha = \frac{1}{2}\mathfrak{S}(N)N^2 + O\left(N^2(\log N)^{-A}\right),$$

which will finish the proof.

4.10.2 Sieving in Minor Arcs: Type I

We now move towards proving Theorem 4.31. This is going to be done via sieving; here is the relevant result.

Theorem 4.33 (Vinogradov's sieve)**.** Fix $U, V, N \ge 2$ with $UV \le N$. Then

$$\left|\sum_{n\le N} f(n)\Lambda(n)\right| \ll 1 + (\log N)\sum_{t\le UV} \max_w \left|\sum_{w\le r\le N/t} f(rt)\right| + N^{1/2}(\log N)^3 \max_{\substack{U\le M\le N/V\\ V\le j\le N/M}} \sum_{V\le k\le N/M} \left|\sum_{\substack{M\le m\le 2M\\ m\le N/k, N/j}} f(mk)\overline{f(mj)}\right|^{1/2}.$$

Here, $\operatorname{im} f \subseteq [-1,1]$.

Roughly speaking, the point is that we are turning a summation on primes into sums on arithmetic progressions in the form of Type I and Type II described above. We will prove Theorem 4.33 later; for now, we will explain how to apply it.

The point is that the sums of the form Type I and Type II are just geometric series, so we can somewhat easily bound them. Explicitly, we have $f(x) \coloneqq e(\alpha x)$, so we have the following result.

Lemma 4.34. Fix $N_1 < N_2$. Then

$$\left| \sum_{N_1 \le n \le N_2} e(\alpha n) \right| \ll \min\{N_2 - N_1, 1/\lfloor x \rceil\},$$

where $\lfloor \alpha \rceil$ is the distance between α and the nearest integer.

Proof. The $N_2 - N_1$ bound arises from the triangle inequality. The other bound arises from bounding this by summing the geometric series; we get something like $\ll e(-\alpha) - 1$ which produces the bound after noting $e(-\alpha) - 1 \approx -\alpha - 1$. ∎

Thus, for the Type I sums, we see that

$$\sum_{t \le UV} \max_w \left| \sum_{w \le r \le N/t} f(rt) \right| \le \sum_{t \le UV} \min\left\{ \frac{N}{t}, \frac{1}{\lfloor \alpha t \rceil} \right\},$$

which we now work towards upper-bounding. One could just take the N/t only, but this will be a little problematic. The trick is to take some string of consecutive integers $t \in \{hq+1, hq+2, \dots, hq+q\}$ as h varies.

We now bound our right-hand side. Find a rational approximation a/q of α so that $|\alpha - a/q| < 1/q^2$. Then set $t \coloneqq hq + r$ for $0 \le r < q-1$; this yields

$$\alpha t = \alpha hq + \frac{a}{q} r + \beta r,$$

where $\beta \coloneqq |\alpha - a/q| < 1/q^2$. The point is that $\frac{a}{q} r$ cycles through $\{0/q, 1/q, \dots, (q-1)/q\}$, so αt will cycle around the circle by this αhq as h varies. Thus, for $h \ge 1$, we can upper-bound

$$\sum_{1 \le r \le q} \min\left\{ \frac{N}{hq+r}, \frac{1}{\lfloor \alpha(hq+r) \rceil} \right\} \ll \frac{N}{hq} + 2\left(q + \frac{q}{2} + \cdots + \frac{q}{q/2} \right).$$

Namely, there is only value of r where $\frac{a}{q} r$ is too close to 0 (where we choose to use $N/(hq)$ as our bound), and for the other values of r we have $\frac{a}{q} r$ close to one of the other rationals in $\{0/q, \dots, (q-1)/q\}$, which gives the other terms. Anyway, we can upper-bound this as

$$\sum_{1 \le r \le q} \min\left\{ \frac{N}{hq+r}, \frac{1}{\lfloor \alpha(hq+r) \rceil} \right\} \ll \frac{N}{hq} + q \log q,$$

which is small enough for our purposes. (For $h = 0$, essentially the same argument works, but one has to pay a little more attention to the $N/(hq+r)$ term, though one still does achieve $O(N/q + q \log q)$.) Summing over all $h \ge 0$, we achieve

$$\sum_{t \le UV} \min\left\{ \frac{N}{t}, \frac{1}{\lfloor \alpha t \rceil} \right\} \ll \left(\frac{N}{q} + UV + q \right) \log(2qUV).$$

Namely, roughly speaking we are summing over $h \le T/q$. The extra $+q$ in the summation is occurring just in case our summation is "too short." In total, we can estimate our Type I contribution is given by

$$(\log N) \sum_{t \le UV} \max_w \left| \sum_{w \le r \le N/t} e(\alpha r t) \right| \ll \left(\frac{N}{q} + UV + q \right) (\log 2qN)^2.$$

4.11 April 5

We began class in the middle of an argument; I have edited directly into those notes for continuity.

4.11.1 Sieving in Minor Arcs: Type II

One can argue as we did in the Type I sums to see that the contribution here is

$$\ll N^{1/2}(\log N)^3 \max_{U\le M\le N/V}\left(M+\sum_{1\le m\le N/M}\min\left\{\frac{N}{m},\frac{1}{\lfloor m\alpha\rceil}\right\}\right)^{1/2},$$

where the point is that we have managed to sum our geometric series using the same bound as before. Anyway, we can use the bound achieved in the previous argument to achieve

$$\ll \left(NV^{-1/2}+NU^{-1/2}+Nq^{-1/2}+N^{1/2}q^{1/2}\right)(\log qN)^4,$$

so in total we achieve

$$|S(\alpha)|\ll \left(UV+q+NU^{-1/2}+NV^{-1/2}+Nq^{-1/2}+N^{1/2}q^{1/2}\right)(\log qN)^4$$

by combining with the Type I contribution. Taking $U=V=N^{2/5}$ completes the proof of Theorem 4.31.

4.11.2 Vinogradov's Sieve

Putting everything together, we see that it remains to prove Theorem 4.33. The main idea is that we can "sieve" via Möbius inversion as

$$f(1)+\sum_{\sqrt{N}<p\le N}f(p)=\sum_{\substack{n\le N\\ \gcd(n,P_{\sqrt{N}})=1}}f(n)=\sum_{\substack{t\mid P_{\sqrt{N}}\\ t\le N}}\left(\mu(t)\sum_{r\le N/t}f(rt)\right).$$

Here $P_{\sqrt{N}}$ is the product of all the primes less than $\sqrt{N}$. This explains why we might expect we want bounds on Type I sums. However, when t is relatively close to N, the inner sum will have essentially no cancellation—it's too short!

This is where Type II sums come in.

Proposition 4.35 (Vaughan's identity)**.** Fix $F(s):=\sum_{n\le U}\Lambda(n)n^{-s}$ and $G(s):=\sum_{n\le V}\mu(n)n^{-s}$. Then

$$-\frac{\zeta'(s)}{\zeta(s)}=F(s)-\zeta(s)F(s)G(s)-\zeta'(s)G(s)+\left(-\frac{\zeta'(s)}{\zeta(s)}-F(s)\right)(1-\zeta(s)G(s)).$$

Proof. Fully expand our the product on the right-hand side and cancel. ∎

The fourth term here turns out to be Type II sums. Namely, we use the "TT^*" method to estimate the operator norm of

$$(f(mn))_{M\le m\le 2M,N\le n\le 2N}.$$

4.12 April 7

We continue.

4.12.1 Using Vaughan's Identity

We compare coefficients in Proposition 4.35 to write $\Lambda(n) = a_1(n) + a_2(n) + a_3(n) + a_4(n)$ where

$$a_1(n) \coloneqq \begin{cases} \Lambda(n) & \text{if } n \le U, \\ 0 & \text{else}, \end{cases}$$

and

$$a_2(n) \coloneqq -\sum_{\substack{mdr=n \\ m\le U, d\le V}} \Lambda(m)\mu(d),$$

and

$$a_3(n) \coloneqq \sum_{hd=n, d\le V} \mu(d)\log h,$$

and

$$a_4(n) \coloneqq -\sum_{\substack{mk=n \\ m>U, k>1}} \Lambda(m)\left(\sum_{\substack{d\mid k \\ d\le V}} \mu(d)\right).$$

(Notably, $\zeta'(s)/\zeta(s) = \sum_{n=1}^{\infty}(\log n)n^{-s}$.) The Type I and Type II sums will arise from these. Roughly speaking, the point is that we can estimate a_2 and a_3 via Type I sums because our values tend to be away from n. Further, a_1 can be estimated via the Prime number theorem, and a_4 can be estimated because the inner sum tends to vanish frequently. Namely, if $k \le V$, then the inner sum goes over all divisors of d, so it vanishes, so we might as well assume that $k > V$. So we are looking at some kind of Dirichlet convolution with longish arithmetic progressions, so we will be able to use Type II sums in our estimation.

Now, we define

$$S_j(N) \coloneqq \sum_{n\le N} f(n)a_j(n)$$

for each $j \in \{1, 2, 3, 4\}$, so we see

$$\sum_{n\le N} f(n)\Lambda(n) = S_1(N) + S_2(N) + S_3(N) + S_4(N).$$

We are now equipped to begin our bounding. By the Prime number theorem, we have $|S_1(N)| \le U$, so it's under control. For $S_2(N)$, we are computing

$$S_2(N) = \sum_{t\le UV}\left(\sum_{\substack{md=t \\ m\le U, d\le V}} \mu(d)\Lambda(m)\right)\sum_{r\le N/t} f(rt)$$

after sufficient rearranging. (The point is that the new variable t roughly amounts to the n we had earlier, where we choose to sum over rt as needed.) The inner sum in parentheses has cancellation by

$$\left|\sum_{\substack{md=t \\ m\le U, d\le V}} \mu(d)\Lambda(m)\right| \le \sum_{md=t} \Lambda(m) = \log t \le \log UV,$$

where we are saying that we're okay losing various $\log$ factors. Thus, we see

$$|S_2(N)| \ll (\log UV)\sum_{t\le UV}\left|\sum_{r\le N/t} f(rt)\right|,$$

which does fit into the Type I sum contribution in Theorem 4.33.

Now we move on to bounding $S_3(N)$. We use summation by parts here. Indeed, rearranging a sum and integral, we find

$$\begin{aligned} S_3(N) &= \sum_{d\le V}\mu(d)\sum_{h\le N/d}(\log h)f(dh) \\ &= \sum_{d\le V}\mu(d)\sum_{h\le N/d}f(dh)\int_1^h\frac{dw}{w} \\ &= \int_1^N\sum_{d\le V}\mu(d)\sum_{w<h\le N/d}f(dh)\frac{dw}{w} \\ &\ll (\log N)\sum_{d\le V}\max_w\left|\sum_{w<h\le N/d}f(dh)\right|, \end{aligned}$$

which again fits into the Type I sum contribution in Theorem 4.33.

Lastly, we need to bound S_4. Unsurprisingly, this is somewhat more involved. As discussed above, we can take $k > V$ in our expression for a_4 as

$$a_4(n) = -\sum_{\substack{mk=n\\ m>U,k>V}}\Lambda(m)\left(\sum_{\substack{d|k\\ d\le V}}\mu(d)\right).$$

Thus, we see

$$S_4(N) = -\sum_{U<m\le N/V}\Lambda(m)\sum_{V\le k\le N/m}\left(\sum_{\substack{d|k\\ d\le V}}\mu(d)\right)f(mk).$$

We will now get bounds on this sum by the "TT^* method" because $f(mk)$ as a matrix has a pretty small operator norm. In particular, we are going to give up trying to cancel Λ and μ and instead focus solely on trying to estimate f. Explicitly, we claim that

$$\left|\sum_{M\le m\le 2M}b_m\sum_{V<k\le N/m}c_kf(mk)\right| \ll_f \sqrt{\sum_{M\le m\le 2M}|b_m|^2}\cdot\sqrt{\sum_{V<k\le N/m}|c_k|^2}. \tag{4.2}$$

Here, the implied constant is Δ, defined as the operator norm of the matrix $(f(mk))_{m,k}$. The point is that we are using some dyadic intervals in order to suitably bound. To see that it is enough to show (4.2), we see

$$S_4(N) \ll (\log N)\max_{U\le M\le N/V}\Delta\sqrt{\sum_{m=M}^{2M}|\Lambda(m)|^2}\cdot\sqrt{\sum_{V<k\le N/M}|d(k)|^2},$$

which we claim is $\ll (\log N)^3N^{1/2}\max_{U\le M\le N/V}\Delta$. Namely, to bound the sum of the $|\Lambda(m)|$, one can just bound this as $(\log m)$ and not lose too much. To bound the $d(k)^2$ sum, we note that Möbius inversion lets us write

$$d(k)^2 = \sum_{d|k}h(d),$$

where $h(d)$ is a multiplicative function (namely, $h = d^2 * \mu$), and we can compute that we need defined by $h(p^\alpha) = 2\alpha+1$ for each prime-power p^α. Thus, we see

$$\sum_{k\le z}d(k)^2 = \sum_{k\le z}\sum_{d|k}h(d) \le \sum_{d\le z}h(d)\cdot\frac{z}{d}.$$

We now bound this as an Euler product

$$z\sum_{d\le z}\frac{h(d)}{d} \le z\prod_{p\le z}\sum_{\alpha=0}^{\infty}\frac{h(p^\alpha)}{p^\alpha} \le z\prod_{p\le z}\left(1-\frac{1}{p}\right)^{-3} \ll z(\log z)^3,$$

where the last bound is by bounding the corresponding Harmonic series. In total, we get the claimed bound.

Anyway, it remains to see what Δ is. Well, this requires a closer analysis of (4.2), so we note Cauchy–Schwarz yields

$$\leq \sqrt{\sum_{M\leq m\leq 2M} |b_m|^2} \cdot \sqrt{\sum_{M\leq m\leq 2M} \left| \sum_{V<k\leq N/m} c_k f(mk) \right|^2}.$$

Expanding, we may upper-bound this as

$$\sqrt{\sum_{M\leq m\leq 2M} |b_m|^2} \sqrt{\sum_{\substack{V\leq j\leq N/M \\ V\leq k\leq N/M}} c_j \overline{c_k} \sum_{\substack{M\leq m\leq 2M \\ m\leq N/j, m\leq N/k}} f(mj)\overline{f(mk)}}.$$

Upon noting $|c_j\overline{c_k}| \leq \frac{1}{2}\left(c_j^2 + c_k^2\right)$, we can achieve an upper-bound of

$$\max_{V<j\leq N/M} \left(\sum_{V<k\leq N/m} \left| \sum_{\substack{M\leq m\leq 2M \\ m\leq N/j, m\leq N/k}} f(mj)\overline{f(mk)} \right| \right)^{1/2}.$$

4.13 April 10

We began class by proving some small technicality, so I have edited last class's notes for continuity.

Remark 4.36. For $\sqrt{x} \leq n \leq x$, one can use the bilinear method to show

$$\Lambda(n) = \sum_{\substack{m\leq \sqrt{x} \\ m|n}} \mu(x)\log(n/m) - \sum_{m\leq\sqrt{x}} \mu(m) \sum_{\substack{k\leq\sqrt{x} \\ km|n}} \Lambda(k).$$

4.13.1 A Duality Theorem

We are going to talk about the large sieve. To give a flavor for what we will achieve, here is an application of the large sieve. Recall that

$$\psi(x;q,a) \coloneqq \sum_{\substack{m\leq x \\ n\equiv a \pmod q}} \Lambda(n).$$

Theorem 4.37 (Bombieri–Vinogradov)**.** For given A, there is a constant B such that we have

$$\psi(x;q,a) = \frac{x}{\varphi(q)}\left(1 + O\left((\log x)^{-A}\right)\right)$$

for almost every $q \leq x^{1/2}(\log x)^{-B}$.

Remark 4.38. As another example, one can use the large sieve to show that there is a finite set of integers which contains a primitive root $\pmod p$ for any prime p. This is a weaker version of Artin's conjecture. In general, one is able to achieve reasonably strong results with the large sieve if one is willing to allow a few exceptions.

Our approach to the large sieve will be to take some hard analysis techniques and combine with stuff like Vaughan's identity to turn our results into number theory.

Anyway, here is our duality theorem.

Theorem 4.39. Fix some countable sets A and B. Additionally, fix some sequence $\{x_{mn}\}_{(m,n)\in A\times B}$ such that $\|x\|_2 < \infty$ and $X > 0$. The following are equivalent.

(a) For each sequence $\{a_m\}_{m\in A}$ of complex numbers such that $\|a\|_2 < \infty$, we have

$$\sum_{n\in B}\left|\sum_{m\in A} x_{mn}a_m\right|^2 \le X\|a\|_2^2.$$

(b) For each sequence $\{b_m\}_{m\in A}$ of complex numbers such that $\|b\|_2 < \infty$, we have

$$\sum_{m\in A}\left|\sum_{n\in B} x_{mn}b_m\right|^2 \le X\|b\|_2^2.$$

Here, $\|\cdot\|$ refers to the L^2-norm.

Proof. By symmetry, it is enough to show that (a) implies (b). The idea is to introduce an auxiliary vector defined by

$$c_m \coloneqq \sum_{n\in A} x_{mn}b_n.$$

Note that this sum is finite because (by Cauchy–Schwarz) we have $\|c\|_2^2 \le \|x\|_2^2 \cdot \|b\|_2^2$; in particular, each coordinate in c must be finite. We now compute

$$\|c\|_2^2 = \sum_{m\in A}\overline{c_m}\sum_{n\in B} b_n x_{mn} = \sum_{n\in B} b_n \sum_{m\in A}\overline{c_m}x_{mn},$$

where the exchange of summation is fine by Fubini's theorem. Now, using Cauchy–Schwarz, we see that the above is an inner product (indexed over n) which can be bounded as

$$\|c\|_2^2 \le \|b\|_2^2\sqrt{\sum_{n\in B}\left|\sum_{m\in A} x_{mn}\overline{c_m}\right|^2}.$$

Then by (a), we achieve the bound $\|c\|_2^2 \le \sqrt{X}\cdot\|c\|_2\cdot\|b\|_2$, which rearranges into $\|c\|_2 \le \sqrt{X}\cdot\|b\|_2$. Upon squaring, this is what we wanted. ∎

4.14 April 12

We won't meet on Friday.

4.14.1 The Large Sieve Inequality

Let's show the following nice result.

Theorem 4.40. Fix $\delta \in (0, 1/2)$ and some δ-separated real numbers $x_1, \dots, x_R$ on $\mathbb{R}/\mathbb{Z}$. Then

$$\sum_{r=1}^{R}\left|\sum_{n=M}^{M+N-1} a_n e(nx_r)\right|^2 \ll \left(N + \delta^{-1}\right)\|a\|_2^2$$

for any vector $(a_1, \dots, a_R)$.

Here, δ-separated means that $\|x_i - x_j\| \geq \delta$ for each distinct i and j where $\|x\|$ is the distance from x to the closest integer. The idea is to use duality and then the TT^* method, followed by some smoothing to optimize. As a model, we will first show the following result.

Proposition 4.41. Fix $\delta \in (0, 1/2)$ and some δ-separated real numbers $x_1, \dots, x_R$ on $\mathbb{R}/\mathbb{Z}$. Then

$$\sum_{r=1}^{R} \left| \sum_{n=M}^{M+N-1} a_n e(nx_r) \right|^2 \ll \left(N + \delta^{-1} \log(1/\delta)\right) \|a\|_2^2$$

for any vector $(a_1, \dots, a_R)$.

Proof. Set $X \coloneqq N + \delta^{-1} \log(1/\delta)$. By duality, it suffices to show

$$\sum_{n=M}^{M+N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 \ll X \|a\|_2^2 .$$

However, we can compute

$$\begin{aligned} \sum_{n=M}^{M+N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 &= \sum_{r,s \leq R} c_r \overline{c_s} \sum_{n=M}^{M+N-1} e(n(x_r - x_s)) \\ &\ll \sum_{r \neq s} |c_r| \cdot |c_s| \cdot \frac{1}{\|x_r - x_s\|} + N \sum_{r \leq R} |c_r|^2 \\ &\leq \sum_{r \leq R} |c_r|^2 \left(N + \sum_{s \neq r} \frac{1}{\|x_r - x_s\|} \right). \end{aligned}$$

Now, to estimate this, the point is that the x_i are δ-separated, so we can estimate distances between the entire sum $\sum_{s \neq r} \frac{1}{\|x_r - x_s\|}$ as looking at worst like $\frac{2}{\delta} + \frac{4}{\delta} + \cdots + 2$, which is harmonic. So the internal sum is $\ll \left(N + \delta^{-1} \log(1/\delta)\right) \|c\|_2^2$, which is what we wanted. ∎

And now let's prove Theorem 4.40.

Proof of Theorem 4.40. For psychological reasons, we note that we can shift everything by $n \mapsto n - M$ so that we may assume $M = 0$. Again, we set $X \coloneqq N + \delta^{-1}$ and observe that by duality it is enough to show

$$\sum_{n=M}^{M+N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 \ll X \|a\|_2^2 .$$

Motivated by Poisson summation, we write

$$\sum_{n=0}^{N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 \leq e^{\pi} \sum_{n \in \mathbb{Z}} e^{-\pi (n/N)^2} \sum_{n=0}^{N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 .$$

Roughly speaking, we are adding weights to the summation in order to smooth ourselves a little more. Intuitively, the previous proof was trying to compute a Fourier transform of the indicator function on $[N, M+N)$, but this is poorly behaved, so the weights above will help us be closer to the truth. Anyway, we see

$$\begin{aligned} \sum_{n=0}^{N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 &\leq \sum_{n=0}^{N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 \\ &= e^{\pi} \sum_{r,s} c_r \overline{c_s} \sum_{n \in \mathbb{Z}} e^{-\pi (n/N)^2} e(n(x_r - x_s)). \end{aligned}$$

Now, by Poisson summation, one sees

$$\sum_{n\in\mathbb{Z}} e^{-\pi(n/N)^2} e(n(x_r - x_s)) = N \sum_{n\in\mathbb{Z}} e^{-\pi N^2(n+x_r-x_s)} = Ne^{-\pi N^2\|x_r-x_s\|^2} + O(1).$$

Here, the $O(1)$ includes all the terms which are away from $n = \lfloor x_r - x_s \rceil$, which we can upper-bound pretty explicitly via some kind of geometric series.

In total, we achieve

$$\sum_{n=0}^{N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 \ll \sum_r |c_r|^2 \cdot N \sum_s e^{-\pi N^2 \|x_r - x_s\|^2}$$

by expanding out the summation as before. We now use the fact that our terms are δ-separated, to bound our distances as having $1/\delta$ at most twice, having $2/\delta$ at most twice, so on and so forth. As such,

$$\sum_{n=0}^{N-1} \left| \sum_{r=1}^{R} c_r e(nx_r) \right|^2 \ll \|c\|_2^2 N \sum_{k\geq 0} e^{-\pi(j\delta N)^2}.$$

It remains to bound the right factor on the right-hand side, which we evaluate as

$$N \sum_{k\geq 0} e^{-\pi(j\delta N)^2} \ll N\left(1 + \int_0^\infty e^{-\pi(t\delta N)^2}\,dt\right) \ll N\left(1 + \frac{1}{\delta N}\int_0^\infty e^{-\pi t^2}\,dt\right) \ll N + \frac{1}{\delta},$$

which is what we wanted. ∎

4.14.2 Quick Applications

Here's a fun application to Farey fractions. Namely, for $Q \geq 1$, consider the sequence of rational numbers

$$\mathcal{F}_Q \coloneqq \{a/q : a, q \geq 0 \text{ and } \gcd(a,q) = 1 \text{ and } q \leq Q\}.$$

The point is that two distinct $x, x' \in \mathcal{F}_q$ will have $\|x - x'\| \geq \frac{1}{Q^2}$ by writing $x = \frac{a}{q}$ and $x' = \frac{a'}{q'}$. Explicitly,

$$\|x - x'\| = \frac{|aq' - a'q|}{qq'} \geq \frac{1}{Q^2}.$$

As such, we are seeing that $\mathcal{F}_Q$ is separated by $1/Q^2$. Here is our application.

Corollary 4.42. Fix $N, Q \geq 1$. Then

$$\sum_{q\leq Q} \sum_{\substack{1\leq a\leq q \\ \gcd(a,q)=1}} \left| \sum_{M\leq n<M+N} b_n e\left(\frac{a}{q}n\right) \right| \ll \left(N + Q^2\right) \|b\|_2^2$$

for any vector b of complex numbers.

Proof. This follows directly from Theorem 4.40. ∎

4.15 April 17

We continue discussing the Bombieri–Vinogradov theorem.

4.15.1 The Bombieri–Vinogradov Theorem

Recall the following statement.

Theorem 4.43. For all $A > 0$ and $Q \in \left[\sqrt{x}(\log x)^{-A}, x^{1/2}\right]$, we have

$$\sum_{q\le Q} \max_{y\le x} \max_{\substack{1\le a\le q\\ \gcd(a,q)=1}} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \ll \sqrt{x}Q(\log x)^5.$$

Proof. During the Friday lecture, we found

$$\max_{\substack{1\le a\le q\\ \gcd(a,q)=1}} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \le \frac{1}{\varphi(q)} \sum_{\chi} |\psi'(y,\chi)|,$$

for some function ψ'. We would like to only use primitive characters, so observe that if χ is an imprimitive character induced by $\overline{\chi}$, then we can upper-bound the difference as

$$|\psi'(y,\chi) - \psi'(y,\overline{\chi})| \ll (\log qy)^2,$$

so we achieve

$$S \coloneqq \max_{\substack{1\le a\le q\\ \gcd(a,q)=1}} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \ll (\log qy)^2 + \frac{1}{\varphi(q)} \sum_{\chi} |\psi'(y,\overline{\chi})|.$$

Summing gives

$$\sum_{q\le Q} \max_{y\le x} \max_{\substack{1\le a\le q\\ \gcd(a,q)=1}} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \ll \sum_{q\le Q} Q(\log qx)^2 + \sum_{\chi \pmod q}^{*} \max_{y\le x} |\psi'(y,\chi)| \sum_{kq\le Q} \frac{1}{\varphi(kq)}.$$

We now note that $\varphi(kq) \ge \varphi(k)\varphi(q)$, so the last summation can be controlled like a harmonic series. Namely, we observe

$$\sum_{k\le z} \frac{1}{\varphi(k)} \le \prod_{p\le z} \sum_{\nu=0}^{\infty} \frac{1}{\varphi(p^\nu)} = \prod_{p\le z} \left(1 + \frac{1}{p-1} \sum_{\nu=0}^{\infty} \frac{1}{p^\nu}\right) = \prod_{p\le z} \frac{1}{1-\frac{1}{p}} \left(1 + \frac{1}{p(p-1)}\right) \ll \log z.$$

Notably, the second term here converges absolutely, and the $\frac{1}{1-\frac{1}{p}}$ term produces the $\log z$. Inputting this inequality grants

$$S \ll Q(\log Qx)^2 + \log x \sum_{q\le Q} \sum_{\chi}^{*} \max_{y\le x} |\psi'(y,\chi)|^2.$$

Thus, it remains to show

$$\sum_{q\le Q} \frac{1}{\varphi(q)} \sum_{\chi}^{*} \max_{y\le x} |\psi'(y,\chi)| \ll \sqrt{x}Q(\log x)^4.$$

Instead, we will prove the "dyadic" inequality

$$\sum_{U\le q\le 2U} \frac{1}{\varphi(q)} \sum_{\chi}^{*} \max_{y\le x} |\psi'(y,\chi)| \ll \left(\frac{x}{U} + x^{5/6} + x^{1/2}U\right)(\log x)^4.$$

To see how this implies the desired inequality, we sum over our dyadic intervals: note that the sum of the $x^{5/6}$ terms do not matter (they are strictly less than $x^{1/2}Q$). Similarly, the $x^{1/2}U$ term will sum to $\ll x^{1/2}Q$ and also does not matter. The last term is harder. To write it out, for $U \in [Q_1, Q]$ for some Q_1, we have

$$\sum_{Q_1\le q\le Q} \frac{1}{\varphi(q)} \sum_{\chi}^{*} \max_{y\le x} |\psi'(y,\chi)| \ll (\log x)^4 \left(\frac{x}{Q_1} + x^{5/6}\log x + x^{1/2}Q\right).$$

For example, taking $Q_1 = (\log x)^A$, we note that Siegel's theorem lets us bound

$$|\psi'(y,\chi)| \ll x(\log x)^{-2A-4},$$

so we can deal with the small values of q as

$$\sum_{q \le (\log x)^A} \frac{1}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{y \le x} |\psi'(y,\chi)| \ll x(\log x)^{-A-4},$$

which is good enough for our purposes.

It remains to prove our dyadic bound. We split this into two parts. To begin, we use the large sieve. We claim that

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{U} \left| \max_{\substack{1 \le m \le M \\ 1 \le n \le N \\ mn \le U}} a_m b_n \chi(mn) \right| \ll$$
$$\left(M + Q^2\right)^{1/2} \left(N + Q^2\right)^{1/2} \log(2MN) \left(\sum_{1 \le m \le M} |a_m|^2 \right)^{1/2} \left(\sum_{1 \le n \le N} |b_n|^2 \right)^{1/2}.$$

The main difficulty is dealing with the $mn \le U$ constraint. Indeed, without this requirement, we could use Cauchy–Schwarz by writing

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \left| \sum_{1 \le m \le M} \sum_{1 \le n \le N} a_m b_n \chi(mn) \right| \le \left(\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \left| \sum_{1 \le m \le M} a_m \chi(m) \right| \right)^{1/2} \cdot$$
$$\left(\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \left| \sum_{1 \le n \le N} b_n \chi(n) \right| \right)^{1/2}.$$

Then the large sieve grants us

$$\ll \left(M + Q^2\right)^{1/2} \left(N + Q^2\right)^{1/2} \left(\sum_{1 \le m \le M} |a_m|^2 \right)^{1/2} \left(\sum_{1 \le n \le N} |b_n|^2 \right)^{1/2}.$$

To achieve the desired inequality, the point is to "complete the sum." Intuitively, we are essentially adding in a term of $1_{mn \le U}$ to our sum in order to bound via Fourier analysis. Namely, the Mellin transform of $1_{[0,1]}(t)$ is $\frac{1}{s}$. We will continue this next class. ■

4.16 April 19

We continue the proof of the Bombieri–Vinogradov theorem.

4.16.1 Using the Large Sieve

We are now interested in proving the following inequality.

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{U} \left| \max_{\substack{1 \le m \le M \\ 1 \le n \le N \\ mn \le U}} a_m b_n \chi(mn) \right| \overset{?}{\ll}$$
$$\left(M + Q^2\right)^{1/2} \left(N + Q^2\right)^{1/2} \log(2MN) \left(\sum_{1 \le m \le M} |a_m|^2 \right)^{1/2} \left(\sum_{1 \le n \le N} |b_n|^2 \right)^{1/2}. \tag{4.3}$$

For this, we use a little Fourier analysis. As discussed before, the issue with our bounding is dealing with $mn \leq U$. To give us more to work with, we will try to indicate with functions like $(mn)^{it}$. To set us up, for $T, \beta > 0$, we note

$$\int_{-T}^{T} e^{-it\alpha} \frac{\sin t\beta}{\pi t}\, dt = \begin{cases} \pi + O\left(T^{-1}(\beta - |\alpha|)^{-1}\right) & \text{if } |\alpha| < \beta, \\ O\left(T^{-1}(|\alpha - \beta)^{-1}\right) & \text{if } |\alpha > \beta. \end{cases}$$

Thus, we set $A(t,\chi) \coloneqq \sum_{m=1}^{M} a_m \chi(m) m^{it}$ and $B(t,\chi) \coloneqq \sum_{n=1}^{N} b_m \chi(n) n^{it}$ so that multiplying $A(t,\chi)$ and $B(t,\chi)$ will detect values of mn by some kind of Fourier analysis. Explicitly,

$$\int_{-T}^{T} A(t,\chi)B(t,\chi)\frac{\sin(t\log u)}{\pi t}\, dt = \sum_{\substack{1\leq m\leq M \\ 1\leq n\leq N \\ mn\leq U}} a_m b_n \chi(mn) + O\left(T^{-1} \sum_{\substack{1\leq m\leq M \\ 1\leq n\leq N}} |a_m b_n \log(mn/u)|^{-1}\right),$$

where we take u to be (say) a half-integer. For the error term, we see we may as well assume that $u \leq MN$, so we note $\log(mn/u) \gg \frac{1}{MN}$ and $\sin(t\log u) \ll \min\{1, |t|\log 2MN\}$ (by staring at the graph of $\sin x$ either close to 0 or away from 0). Rearranging, we achieve

$$\left| \sum_{\substack{1\leq m\leq M \\ 1\leq n\leq N \\ mn\leq u}} a_m b_n \chi(mn) \right| \ll \int_{-T}^{T} |A(t,\chi)| \cdot |B(t,\chi)| \cdot \min\{1/|t|, \log 2MN\}\, dt + \frac{MN}{T} \sum_{\substack{1\leq m\leq M \\ 1\leq n\leq N}} |a_m b_n|.$$

At this point, we set $T \coloneqq (MN)^{3/2}$. We now use the large sieve inequality to bound

$$\sum_{q\leq Q} \frac{q}{\varphi(q)} \sum_{\chi}^{*} |A(t,\chi)B(t,\chi)|$$

as we did last class when we did not have to deal with the χs; we omit the details. Further, we see that

$$\int_{-T}^{T} \min\left\{\frac{1}{|t|}, \log 2MN\right\} dt \ll \log 2MN$$

by first integrating over the region $[-1,1]$ to achieve $\ll \log 2MN$ and then recalling $T = (MN)^{3/2}$ to integrate outside $[-1,1]$ to be sure that we do not overcome $\ll \log 2MN$. Additionally, summing over all q and χ, our term is bounded by

$$\begin{aligned} \frac{MN}{T} \sum_{\substack{1\leq m\leq M \\ 1\leq n\leq N}} |a_m b_n| Q^2 &\leq \frac{Q^2 MN}{T} \left(\sum_{1\leq m\leq M} |a_m|^2\right)^{1/2} \left(\sum_{1\leq n\leq N} |b_n|^2\right)^{1/2} M^{1/2} N^{1/2} \\ &\leq \left(Q^2 + M\right)^{1/2} \left(Q^2 + N\right)^{1/2} \left(\sum_{1\leq m\leq M} |a_m|^2\right)^{1/2} \left(\sum_{1\leq n\leq N} |b_n|^2\right)^{1/2}. \end{aligned}$$

Combining the previous bounds on $|A(t,\chi)B(t,\chi)|$ is able to complete the proof of the inequality.

4.16.2 Using the Bilinear Method

We use Vaughan's identity to continue. Arguing as before, we may write $\psi(y,\chi) = S_1 + S_2 + S_3 + S_4$ where

$$\begin{aligned}
S_1 &= \sum_{n\le U} \Lambda(n)\chi(n) \\
S_2 &= -\sum_{t\le UV} \left(\sum_{\substack{t=md \\ m\le U, d\le V}} \mu(d)\Lambda(m) \right) \sum_{r\le y/t} \chi(rt) \\
S_3 &= \sum_{\substack{d\le V \\ dh\le y}} \mu(d)\log h\chi(dh) \\
S_4 &= -\sum_{U\le m\le y/V} \Lambda(m) \sum_{V\le k\le y/m} \left(\sum_{d\mid k, d\le V} \mu(d) \right) \chi(mk).
\end{aligned}$$

Quickly, we see that $|S_1| \ll U$ by the Prime number theorem. Also, as in the proof of Vinogradov's theorem, summation by parts produces

$$|S_3| \ll \log y \sum_{d\le V} \max_w \left| \sum_{w\le h\le y/d} \chi(h) \right|.$$

Next up, we bound S_4. We'll do this next class.

4.17 April 21

We continue.

4.17.1 Continuing the Bilinear Method

The theme of today is to use our large sieve inequality to bound as many of the $S_\bullet$ terms with bilinear sums because the large sieve inequality is quite efficient. From last time, our next task is to bound

$$S_4 = -\sum_{U\le m\le y/V} \Lambda(m) \sum_{V\le k\le y/m} \left(\sum_{d\mid k, d\le V} \mu(d) \right) \chi(mk).$$

We use a dyadic decomposition. For each $M \in [U, y/V]$, we see

$$\sum_{q\le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{y\le x} \left| \sum_{\substack{U\le m\le y/V \\ M\le m\le 2M}} \Lambda(m) \sum_{V\le k\le y/M} \left(\sum_{\substack{d\mid k \\ d\le V}} \mu(d) \right) \chi(mk) \right|^2,$$

which is our averaged version of S_4. Now, by (4.3), this is

$$\ll \left(Q^2+M\right)^{1/2} \left(Q^2 + x/M\right)^{1/2} \left(\sum_{M\le m\le 2M} \Lambda(m)^2 \right) \left(\sum_{k\le x/M} d(k)^2 \right)^{1/2} \log 2x,$$

which we can now upper-bound as in the proof of Vinogradov's theorem. After doing so, we achieve

$$\ll \left(Q^2+M\right)^{1/2} \left(Q^2 + x/M\right)^{1/2} x^{1/2} (\log 2x)^3.$$

"Expanding" the square root using something like Hölder, up to a constant term we get

$$\ll \left(Q^2 x^{1/2} + QxM^{-1/2} + Qx^{1/2}M^{1/2} + x \right) (\log 2x)^3.$$

We now sum over all $U/2 \leq M \leq x/V$ via our dyadic intervals to compute

$$\sum_{q\leq Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{y\leq x} |S_4(y,\chi)| \ll \left(Q^2 x^{1/2} Q x U^{-1/2} + Q x^{-1/2} + x\right) (\log 2x)^4,$$

where the extra $\log$ factor comes from summing over $\log$ many dyadic intervals.

Continuing, we bound

$$S_2 = -\sum_{t\leq UV} \left(\sum_{\substack{t=md \\ m\leq U, d\leq V}} \mu(d)\Lambda(m) \right) \sum_{r\leq y/t} \chi(rt).$$

For this, we split the sum into the two pieces

$$S_2' \coloneqq -\sum_{t\leq U} \left(\sum_{\substack{t=md \\ m\leq U, d\leq V}} \mu(d)\Lambda(m) \right) \sum_{r\leq y/t} \chi(rt),$$

$$S_2'' \coloneqq -\sum_{U\leq t\leq UV} \left(\sum_{\substack{t=md \\ m\leq U, d\leq V}} \mu(d)\Lambda(m) \right) \sum_{r\leq y/t} \chi(rt).$$

The same technique that we used for S_4 also works for S_2''. Namely, repeating the above argument with some M lets us estimate the averaged version of S_2''

$$\sum_{q\leq Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{y\leq x} \left| -\sum_{U\leq t\leq UV} \left(\sum_{\substack{t=md \\ m\leq U, d\leq V \\ M\leq m\leq 2M}} \mu(d)\Lambda(m) \right) \sum_{r\leq y/t} \chi(rt) \right|^2.$$

Summing over the dyadic ranges appropriately, keeping track of the number of $\log$s, we produce

$$\ll \left(Q^2 + QxU^{-1}2 + Qx^{1/2}U^{1/2}V^{1/2} + x\right) (\log 2x)^3$$

as the bound for averaged version of S_2''. For S_2', our averaged version can be bounded as

$$\begin{aligned} &\sum_{1<q\leq Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{y\leq x} |S_2'(y,\chi)| \\ &\ll Q^2 \max_{\text{prim. } \chi \pmod q} \max_{y\leq x} |S_2'(y,\chi)|. \end{aligned}$$

Staring at $S_2'(y,\chi)$, we are able to bound via the Pólya–Vinogradov inequality to produce

$$\ll Q^{5/2} U (\log xU)^2.$$

Adding in $q=1$ with the trivial character, we see that the maximum of $|S_2'(y,\chi_0)|$ is bounded by $x(\log xU)^2$ by simply evaluating the inner sum via the Prime number theorem. In total, we achieve

$$\sum_{q\leq Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{y\leq x} |S_2'(y,\chi)| \ll \left(Q^{5/2}U + x\right) (\log xU)^2.$$

For S_3, we use the same techniques of S_2' (combining with the upper bound we achieved last class) in order to achieve

$$\sum_{q\leq Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{y\leq x} |S_3(y,\chi)| \ll \left(Q^{5/2}V + x\right) (\log xV)^2.$$

Combining all of our bounds, we may upper-bound

$$\sum_{q\leq Q} \frac{1}{\varphi(q)} \sideset{}{^*}\sum_{\chi} \max_{y\leq x} |\psi'(y,\chi)|$$

by

$$\ll \left(Q^2x^{1/2} + QxU^{-1/2} + QxV^{-1/2} + Qx^{1/2}U^{1/2}V^{1/2} + Q^{5/2}U + Q^{5/2}V\right)(\log xUV)^4.$$

To optimize, over $x^{1/3} \le Q \le x^{1/2}$, we take $U = V := x^{2/3}Q^{-1}$ to achieve $\ll \left(Q^2x^{1/2} + x\right)(\log x)^4$. Then for $Q \le x^{1/3}$, we take $U = V := x^{1/3}$ to achieve $\ll \left(x + x^{5/6}Q\right)(\log x)^4$. Summing, we produce the desired inequality.

Remark 4.44. There is an Elliott–Halberstam conjecture which asserts that any $0 < \theta < 1$ has

$$\sum_{q<x^\theta} \max_{\gcd(a,q)=1} \left|\psi(x;q,a) - \frac{x}{\varphi(q)}\right| \ll_A x(\log x)^{-A}.$$

The Bombieri–Vinogradov theorem achieves the result for $\theta < 1/2$. Any progress for larger θ would mark extreme progress. For example, this conjecture has connections to bounded gaps between primes.

Remark 4.45. Goldston–Pintz–Yildirim were able to show that the Elliott–Halberstam conjecture for any $\theta > 1/2$ is able to achieve bounded gaps between primes. Zhang was able to achieve a variant for $\theta > 1/2$ which gave bounded gaps unconditionally. In a different direction, Maynard uses a "multidimensional" version of the Selberg sieve to achieve bounded gaps, whereupon the machinery merely requires $\theta > 0$.

4.18 April 24

It is the last week of instruction.

4.18.1 Least Nonquadratic Residues

Here is the conjecture.

Conjecture 4.46 (Vinogradov)**.** For each prime $p > 2$, let $n(p)$ be the least positive integer which is not a quadratic residue $\pmod p$. Then $n(p) \ll_\varepsilon p^\varepsilon$ for all $\varepsilon > 0$.

Remark 4.47. Continuing our discussion of the Elliott–Halberstam conjecture, Tao was able to conditionally show Conjecture 4.46. Also, the grand Riemann hypothesis implies Conjecture 4.46. The argument is akin to our discussion of primality testing.

Remark 4.48. Quickly, note that $n(p)$ is prime. Indeed, suppose we have a prime factorization

$$n(p) = \prod_{q \text{ prime}} q^{\nu_q(n(p))}.$$

Then $\left(\frac{n(p)}{p}\right) = -1$ implies that $\left(\frac{q}{p}\right) = -1$ for some prime $q \mid n(p)$. Thus, $q \le n(p)$, so minimality enforces $q = n(p)$, so $n(p)$ is prime.

Remark 4.49. The Burgess bound is able to achieve $n(p) \ll_\varepsilon p^{1/4+\varepsilon}$.

Vinogradov's sieving trick is able to achieve $n(p) \ll_\varepsilon p^{1/(4\sqrt{e})+\varepsilon}$, which is the current record. Let's see this.

Theorem 4.50. For any $\varepsilon > 0$, we have $n(p) \ll_\varepsilon p^{1/(4\sqrt{e})+\varepsilon}$.

Proof. Intuitively, the point is to compute the character sum

$$\sum_{k=1}^{n} \left(\frac{k}{p}\right),$$

and as soon as we can show that this is less than n, we get a nonquadratic residue. Some extra structure about primality of $n(p)$ is able to sharpen the bound.

Let's be more explicit. Set $\chi := \left(\frac{\cdot}{p}\right)$. The Burgess bound is able to achieve

$$\sum_{1 \le n \le y} \chi(n) = o_\varepsilon(y)$$

for $y = \lfloor p^{1/4+\varepsilon} \rfloor$. To see our nonquadratic residues, we write

$$\sum_{1 \le n \le y} \chi(n) = y - 2 \sum_{\substack{1 \le n \le y \\ \chi(n)}} 1 \ge y - 2 \sum_{\substack{1 \le q \le y \\ q \text{ prime} \\ \chi(q)=-1}} \frac{y}{q} = y\left(1 - 2 \sum_{\substack{1 \le q \le y \\ q \text{ prime} \\ \chi(q)=-1}} \frac{y}{q}\right).$$

The point is that if we get too many qs in the sum which are too big, then we're not going to achieve $o_\varepsilon(y)$. With this in mind, we use the definition of $n(p)$ to write

$$o_\varepsilon(y) = \sum_{1 \le n \le y} \chi(n) \ge y\left(1 - 2 \sum_{\substack{n(p) \le q \le y \\ q \text{ prime} \\ \chi(q)=-1}} \frac{y}{q}\right).$$

Thus, we achieve

$$\frac{1}{2} \le \sum_{\substack{n(p) \le q \le y \\ q \text{ prime}}} \frac{1}{q} + o_\varepsilon(1).$$

Because $\sum_{p \le n} \frac{1}{p} = \log\log n$, we see

$$\frac{1}{2} \le \log(\log_{n(p)} y) + o_\varepsilon(1),$$

so $\log_{n(p)} y \ge e^{1/2+o_\varepsilon(1)} \gg_\varepsilon e^{1/2}$. Rearranging, we see $n(p) \ll_\varepsilon y^{1/\sqrt{e}+\varepsilon} = y^{1/(4\sqrt{e})+\varepsilon}$, which is what we wanted. ∎

4.19 April 26

We continue our discussion of Linnik's theorem.

4.19.1 Reyni's Theorem

In a different direction, Linnik was able to show the following weakening of Conjecture 4.46.

Theorem 4.51. For any $\varepsilon > 0$, we have

$$|\{p \le N : n(p) > p^\varepsilon\}| = O_\varepsilon\left(N^\varepsilon\right).$$

In fact, we will show that there are $O_\varepsilon(1)$ exceptions with $p \gg N^\varepsilon$. This will come from the large sieve, not using Bombieri–Vinogradov directly. From our discussion of the large sieve, we showed in Corollary 4.42 that

$$\sum_{q \le Q} \sum_{\gcd(a,q)=1} \left| \underbrace{\sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q} n\right)}_{S(a/q) :=} \right|^2 \ll \left(N + Q^2\right) \sum_{n=M+1}^{M+N} |a_n|^2.$$

For this, we require the following result, which comes from the large sieve.

Theorem 4.52 (Reyni)**.** Let S be a set of integers in $[M+1, M+N]$, and let $\mathcal{P}$ be the set of primes less than or equal to some Q. For some $\tau \in (0,1)$, if S does not contain any integer x such that $x \equiv h \pmod p$ for at least τp values of $h \pmod p$ for each $p \in \mathcal{P}$, then

$$|S| \ll \frac{N + Q^2}{\tau |\mathcal{P}|}.$$

Proof. We use the large sieve. Let $Z(q,h)$ be the number of elements $z \in S$ with $z \equiv h \pmod q$; set $Z := |S|$. To detect deviation from the expected, we are interested in

$$V(q) := \sum_{h=0}^{q-1} \left| Z(q,h) - \frac{Z}{q} \right|^2.$$

Now, we claim that

$$\sum_{p \le Q} pV(p) \overset{?}{\ll} \left(N + Q^2\right) Z, \tag{4.4}$$

which will finish the proof after plugging into the hypotheses. This claim will follow from the large sieve: set $a_n := 1_S(n)$. Now, rearranging, we see

$$\sum_{a=1}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 = \sum_{m,n \in S} \left(\sum_{a=1}^{q} e\left(\frac{a}{q}(m-n)\right) \right) = q \sum_{h=1}^{q} Z(q,h)^2,$$

where the last equality holds because we only care about pairs $(m,n) \in S^2$ such that $m \equiv n \pmod q$, whereupon we get a contribution of q. Thus, we see

$$qV(q) \overset{*}{=} q\left(\sum_{h=1}^{q} Z(q,h)^2 - \frac{Z^2}{q} \right) = \sum_{a=1}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 - Z^2 = \sum_{a=1}^{q-1} \left| S\left(\frac{a}{q}\right) \right|^2.$$

Here, $\overset{*}{=}$ holds by expanding out the definition of $V(q)$, using the fact that the expected value of $Z(q,h)$ is Z/q when averaged over all possible values of h. As such, we see

$$\sum_{p \le Q} pV(p) = \sum_{p \le Q} \sum_{\gcd(a,p)=1} \left| S\left(\frac{a}{p}\right) \right|^2,$$

so the large sieve grants

$$\sum_{p \le Q} pV(p) \ll \left(N + Q^2\right) Z,$$

which was the desired claim.

To finish, we need to discuss $\mathcal{P}$. Namely, for each $p \in \mathcal{P}$, we see that

$$V(p) \ge \tau p \cdot \frac{Z^2}{p^2} = \frac{\tau Z^2}{p}.$$

Plugging this into (4.4), we see that $\tau Z^2 |\mathcal{P}| \ll \left(N + Q^2\right) Z$, which rearranges into the desired inequality. ∎

4.19.2 Smooth Numbers

To continue our discussion, we need the following definition.

Definition 4.53 (smooth)**.** Fix a real number $N > 0$. An N-smooth positive integer is one whose prime factors are less than N.

We will show the following result later.

Lemma 4.54. Fix some $\varepsilon > 0$. There is a constant $c_\varepsilon > 0$ such that the number of x^ε-smooth numbers less than x is at least $c_\varepsilon x$.

Proof. This proof is elementary and constructive. Without loss of generality, we may take $\varepsilon < 1/10$; set $k \coloneqq \lfloor 1/\varepsilon \rfloor$. The point is to construct enough numbers of the form

$$n = mp_1 \cdots p_k$$

where the p_i are primes between $x^{\varepsilon - \varepsilon^2/2}$ and x^ε. Here, any m achieve $n \le x$ must have

$$m \le np_1 \cdots p_k \le \frac{x}{x^{\varepsilon k - k\varepsilon^2/2}} \le x^\varepsilon,$$

so m is x^ε-smooth and thus can be ignored. Now, the number of such n is bounded below by

$$\frac{1}{k!} \sum_{\substack{p_1,\dots,p_k \\ x^{\varepsilon-\varepsilon^2/2} \le p_i \le x^\varepsilon}} \left\lfloor \frac{x}{p_1 \cdots p_k} \right\rfloor \gg \sum_{\substack{p_1,\dots,p_k \\ x^{\varepsilon-\varepsilon^2/2} \le p_i \le x^\varepsilon}} \frac{x}{p_1 \cdots p_k} = x \left(\sum_{x^{\varepsilon-\varepsilon^2/2} \le p \le x^\varepsilon} \frac{1}{p} \right)^k.$$

Lower-bounding each term via Mertens's theorem, we achieve

$$\gg_\varepsilon x \left(\log \frac{\log x^\varepsilon}{\log x^{\varepsilon-\varepsilon^2}} + o(1) \right)^k.$$

The right-hand side is bounded below by a constant times x, so we are done. ∎

Now, let's explain why Lemma 4.54 proves Theorem 4.51.

Theorem 4.51. For any $\varepsilon > 0$, we have

$$|\{p \le N : n(p) > p^\varepsilon\}| = O_\varepsilon\left(N^\varepsilon\right).$$

Proof. In Theorem 4.52, we work in the interval $\left[1, T^2\right]$; let $\mathcal{P}$ be the set of primes $p \in [T^\varepsilon, T]$ such that $n(p) > p^\varepsilon$. Now, S is defined as the set of integers in our interval, where we remove integers y such that $\left(\frac{y}{p}\right) = -1$ for some $p \in \mathcal{P}$. In other words, S should be quadratic residues for $\mathcal{P}$.

In particular, for each $p \in \mathcal{P}$, we see that S fails to contain about half of all residues $\pmod p$, so we may take $\tau = 1/3$, whereupon Theorem 4.52 grants

$$|S| \ll \frac{T^2}{|\mathcal{P}|}.$$

On the other hand, we claim that all T^{ε^2}-smooth numbers live in S. Indeed, the prime factor of any T^{ε^2}-smooth number must be less than T^{ε^2}, so it suffices to show the result for primes $p' \le T^{\varepsilon^2}$. Now, for any prime $p \in \mathcal{P}$, we see that

$$p' \le T^\varepsilon \le p^\varepsilon,$$

so the construction of $\mathcal{P}$ ensures $\left(\frac{p'}{p}\right) = 1$.

In total, Lemma 4.54 tells us that $T^2 \ll_\varepsilon |S|$, so we see that $|\mathcal{P}| \ll_\varepsilon 1$. In other words,

$$\mathcal{P} = \{p \geq T^\varepsilon : n(p) > p^\varepsilon\}$$

is finite, from which Theorem 4.51 follows. ∎

4.20 April 28

Today we discuss Hua's inequality for Waring's problem.

4.20.1 Hua's Inequality

Here is the problem we want to solve: for fixed positive integer k, compute the smallest positive integer s such that every natural number is the sum of $\leq s$ powers of k; we call this positive integer $g(k)$; it is a result of Waring–Hilbert that $g(k) < \infty$. A more interesting question to ask is to find $G(k)$ so that every sufficiently large integer is the sum of $\leq G(k)$ powers of k; this is more interesting because it turns out that small values will dominate so that $g(k)$ is more easily understood but less representative of the underlying structure.

We will be using the circle method, which will even get us an asymptotic formula. To be explicit, we want to study powers of the function

$$g_k(\alpha, X)) = \sum_{1 \leq x \leq X} e\left(\alpha x^k\right).$$

The main difficulty, as expected, is bounding the minor arcs. For example, consider the integral of the moment

$$\int_0^1 |g_k(\alpha, X)|^{2s} \, d\alpha = \#\left\{((x_i), (y_i)) \in [1, X]^s \times [1, X]^s : x_1^k + \cdots + x_s^k : y_1^k + \cdots + y_s^k\right\}$$

by expanding out $|g_k(\alpha, X)|^{2s} = g_k(\alpha, X)^s \overline{g_k(\alpha, X)}^s$ and integrating. These combinatorial objects are quite difficult to understand; for example, not much is even known at $k = 3$. Our result for today is Hua's inequality, as follows.

Theorem 4.55 (Hua's inequality)**.** For any $k \geq 0$, we have

$$\int_0^1 |g_k(\alpha, X)|^{2^k} \, d\alpha \ll_\varepsilon X^{2^k - k + \varepsilon}.$$

Sketch. We will sketch the main ideas. The 2^k here is going to arise from squaring this inequality repeatedly. Explicitly, note

$$(x + y)^k - x^k = y \sum_{j=0}^{k-1} \binom{k}{j} y^{k-j-1} x^j. \tag{4.5}$$

The point here is that control over y has made our polynomial have less degree; this method is called "differencing." To apply this, we need two lemmas.

Lemma 4.56. Fix $f(x) \in \mathbb{Z}[x]$ of positive degree with nonnegative coefficients. For $y \in \mathbb{Z}$, define the polynomial $\Delta_y f$ by $\Delta_y f(x) := f(x + y) - f(x)$, and define $\Delta_{y_1, \ldots, y_n} := \Delta_{y_1} \cdots \Delta_{y_n}$. Given positive integers $y_1, \ldots, y_v$ where $v \leq \deg f$, then $\Delta_{y_1, \ldots, y_v}$ is a polynomial of degree $\deg f - v$, with nonnegative coefficients, and is divisible by $y_1 \cdots y_v$.

Proof. Induct on v, using (4.5). ∎

Lemma 4.57. For $1 \le v \le k-1$, we have

$$|g_k(\alpha, X)|^{2^v} \ll_v X^{2^v-1} + X^{2^v-v-1} \operatorname{Re}\left(\sum_{y_1,\dots,y_v \in [1,X]} \sum_x e\left(\alpha \Delta_{y_1,\cdots,y_v} x^k\right) \right),$$

where the summation of x is in some interval of $[1, X]$ depending on the y_i.

The inequality now follows from the previous lemmas. ■

Remark 4.58. Vinogradov was able to improve the 2^k in the inequality to $O\left(k^2 \log k\right)$ by considering solutions to systems

$$x_1^j + \cdots + x_s^j = y_1^j + \cdots + y_s^j$$

for $1 \le j \le k$. This system appears somewhat unmotivated, but it turns out to be helpful; for example, this system of equations turns out to satisfy some form of translation-invariance.

APPENDIX A
COMPLEX ANALYSIS

Our reality isn't about what's real, it's about what we pay attention to.

—Hank Green, [Gre20]

In this chapter, we review some basic facts of complex analysis. We do not provide proofs of all statements.

A.1 Holomorphic Functions

Complex analysis is the study of holomorphic functions, so we quickly provide a definition.

Definition A.1 (holomorphic)**.** Fix a complex function $f\colon \Omega \to \mathbb{C}$, where $\Omega \subseteq \mathbb{C}$ is some subset. We say that f is *differentiable* at $z \in \Omega$ if and only if the limit

$$f'(z) \coloneqq \lim_{w \to z} \frac{f(z) - f(w)}{z - w}$$

exists. If f is differentiable at all $z \in \Omega$, then we say f is *holomorphic* on Ω.

Here is the main test on holomorphic functions.

Theorem A.2 (Cauchy–Riemann equations)**.** Fix a complex function $f\colon \Omega \to \mathbb{C}$, where Ω is a nonempty open subset. Writing $f(x+yi) \coloneqq u(x,y) + iv(x,y)$, then f is differentiable at $z_0 = x_0 + iy_0$ implies that

$$\begin{cases} u_x(x_0, y_0) = v_y(x_0, y_0), \\ v_x(x_0, y_0) = -u_y(x_0, y_0). \end{cases}$$

Proof. See [Elb22, Theorem 3.19]. Intuitively, we are saying that f is locally a scaled rotation, which is what multiplication by a complex numbers. ∎

Remark A.3. Under suitably hypotheses, satisfying the Cauchy–Riemann equations implies that f is differentiable at the point z_0. See [Elb22, Theorem 3.26].

A.2 Path Integrals

To do calculus on complex functions, we also want to know how to integrate them.

Definition A.4 (path integral)**.** Fix a piecewise continuous function $f\colon \Omega \to \mathbb{C}$, where $\Omega \subseteq \mathbb{C}$ is some subset. Given a piecewise C^1 path $\gamma\colon [0,1] \to \Omega$, we define

$$\int_\gamma f(z)\,dz \coloneqq \int_0^1 \operatorname{Re}\left(f(\gamma(t))\gamma'(t)\right)dt + i\int_0^1 \operatorname{Im}\left(f(\gamma(t))\gamma'(t)\right)dt.$$

If γ is closed (i.e., $\gamma(0)=\gamma(1)$), then we might write $\oint_\gamma f(z)\,dz$.

As usual, limits commute with integrals under suitably uniformity hypotheses.

Lemma A.5. Fix an open subset $\Omega \subseteq \mathbb{C}$ and a sequence $\{f_n\}_{n\in\mathbb{N}}$ of piecewise continuous function $\Omega \to \mathbb{C}$. Given a piecewise C^1 path $\gamma\colon [0,1] \to \Omega$, if $f_n \to f$ uniformly for some $f\colon \Omega \to \mathbb{C}$, then

$$\lim_{n\to\infty} \oint_\gamma f_n(z)\,dz = \oint_\gamma f(z)\,dz.$$

Proof. See [Elb22, Lemma 4.62]. Roughly speaking, the point is that we can upper-bound

$$\left|\oint_\gamma f(z)\,dz - \oint_\gamma f_n(z)\,dz\right| \le \oint_\gamma |f(z)-f_n(z)|\,dz \le \sup_{z\in\operatorname{im}\gamma} |f(z)-f_n(z)|\cdot \ell(\gamma),$$

which goes to 0 as $n\to\infty$ by the uniformity. ∎

Proposition A.6. Fix an open, connected subset $\Omega \subseteq \mathbb{C}$. Fix a piecewise C^1 path $\gamma\colon [0,1] \to \Omega$ and a function $f\colon \Omega \to \mathbb{C}$ continuous on $\operatorname{im}\gamma$. For any $z_0 \in \Omega$, we have

$$\frac{1}{2\pi i}\oint_\gamma \frac{f(z)}{z-w}\,dz = \sum_{n=0}^{\infty}\left(\frac{1}{2\pi i}\oint_\gamma \frac{f(z)}{(z-w)^{n+1}}\,dz\right)(w-z_0)^n$$

for w in some open neighborhood of z_0.

Proof. See [Elb22, Proposition 4.61]. Roughly speaking, we begin by translating so that $z_0 = 0$; then for $|w|$ small enough (for example, avoiding $\operatorname{im}\gamma$ and $|w| < \frac{1}{2}|z|$), we can write

$$\frac{f(z)}{z-w} = \frac{f(z)}{z}\cdot\frac{1}{1-(w/z)} = \sum_{n=0}^{\infty}\frac{f(z)w^n}{z^{n+1}},$$

and this geometric series converges absolutely and uniformly because $|w| < \frac{1}{2}|z|$. Thus, the Weierstrass M-test grants uniform convergence, so we can integrate both sides over $\oint_\gamma$ and finish by switching the infinite sum and integral by Lemma A.5. ∎

A.3 The Cauchy Integral Formula

In this section, we provide various formulations of the Cauchy integral formula. The most basic formulation is as follows.

Theorem A.7 (Cauchy–Goursat)**.** Fix a simply connected open subset $\Omega \subseteq \mathbb{C}$. If $f : \mathbb{C} \to \mathbb{C}$ is holomorphic on Ω, then for any piecewise C^1 closed path $\gamma : [0,1] \to \Omega$, we have

$$\oint_\gamma f(z)\,dz = 0.$$

Proof. See [Elb22, Theorem 4.65, Theorem 4.70]. Intuitively, this result follows from Green's theorem combined with Theorem A.2. ∎

We can extend this result in a few ways. For one, we can evaluate the function using integrals.

Theorem A.8 (Cauchy integral formula)**.** Fix an open connected subset $\Omega \subseteq \mathbb{C}$ containing some $\overline{B(z_0,r)}$. If $f : \Omega \to \mathbb{C}$ is holomorphic, then

$$f(w) = \frac{1}{2\pi i} \oint_\gamma \frac{f(z)}{z-w}\,dz$$

for $w \in B(z_0,r)$, where γ is the counterclockwise path around $\partial B(z_0,r)$.

Proof. See [Elb22, Theorem 4.63]. Roughly speaking, one can use Theorem A.7 in order to allow us to send $r \to 0^+$ without changing the value of the integral. Then we note

$$\frac{1}{2\pi i} \oint_\gamma \frac{f(z)}{z-w}\,dz = \frac{1}{2\pi i} \oint_\gamma \frac{f(z)-f(w)}{z-w}\,dz + f(w) \cdot \frac{1}{2\pi i} \oint_\gamma \frac{1}{z-w}\,dz.$$

The integral on the right is just 1, so we want to show that the other integral goes to 0. Well, $\frac{f(z)-f(w)}{z-w}$ is roughly $f'(w)$ as $r \to 0^+$, so we can upper-bound this integral by (say) $2|f'(w)| \cdot 2\pi r$ for small r, which goes to 0 as $r \to 0^+$. ∎

Remark A.9. Roughly speaking, using Theorem A.7 again, the above proof more or less says that we can replace γ with any counterclockwise path around z_0 provided that Ω is simply connected.

Remark A.10. Combining Theorem A.8 with Proposition A.6 implies that holomorphic $f : \Omega \to \mathbb{C}$ are locally equal to a power series.

In fact, we can evaluate derivatives using integrals.

Corollary A.11. Fix an open connected subset $\Omega \subseteq \mathbb{C}$ containing some $\overline{B(z_0,r)}$. If $f : \Omega \to \mathbb{C}$ is holomorphic, then

$$f^{(n)}(w) = \frac{n!}{2\pi i} \oint_\gamma \frac{f(z)}{(z-w)^{n+1}}\,dz$$

for $w \in \Omega$ and $n \geq 0$, where γ is the counterclockwise path around $\partial B(z_0,r)$.

Proof. See [Elb22, Corollary 4.71]. By Theorem A.8 and Proposition A.6, we may write

$$f(w) = \sum_{n=0}^{\infty} \left(\frac{1}{2\pi i} \oint_\gamma \frac{f(z)}{(z-w)^{n+1}}\,dz \right) (w-z_0)^n$$

for w in some open neighborhood of z_0. (As usual, the deformation process with Theorem A.7 allows us to shrink γ as necessary.) But now we can, with some pain, take derivatives of this power series by hand (see [Elb22, Proposition 3.44]) to achieve the result. ∎

As an application, we discuss analytic continuation.

Theorem A.12. Fix an open connected subset $\Omega \subseteq \mathbb{C}$. Given holomorphic functions $f_1, f_2 \colon \Omega \to \mathbb{C}$, if

$$\{z \in \mathbb{C} : f_1(z) = f_2(z)\}$$

contains an accumulation point, then $f_1 = f_2$ on Ω.

Proof. See [Elb22, Theorem 5.1]. By working with $f_1 - f_2$, it suffices to show that, if $f^{-1}(\{0\})$ has an accumulation point, then $f = 0$. We show this by contraposition: suppose $f \neq 0$, and we will show that each $z_0 \in f^{-1}(\{0\})$ has some $r > 0$ such that $B(z_0, r) \cap f^{-1}(\{0\}) = \{z_0\}$. By shifting, we may assume that $z_0 = 0$. By Remark A.10, we see that f is locally a power series around $z = 0$. Because f is nonzero, this local power series cannot identically vanish. However, this implies that there is some m such that the power series for $f(z)/z^m$ has a nonzero constant term. However, $f(z)/z^m$ is then a continuous function which is nonzero at 0 and is thus nonzero in an open neighborhood of 0. ∎

A.4 Building Primitives

We would like to build a converse for Theorem A.7.

Proposition A.13. Fix an open, connected subset $\Omega \subseteq \mathbb{C}$ and a continuous function $f \colon \Omega \to \mathbb{C}$. Given that

$$\oint_\gamma f(z)\,dz = 0$$

for any closed piecewise C^1 path $\gamma \colon [0,1] \to \Omega$. Then there exists a holomorphic function $F \colon \Omega \to \mathbb{C}$ such that $F' = f$.

Proof. See [Elb22, Theorem 4.44]. By translating, we may assume $0 \in \Omega$, and the point is to define

$$F(s) = f(0) + \int_\gamma f(s)\,ds,$$

where γ is any closed piecewise C^1 path from 0 to z. The hypothesis on f implies that F is well-defined. To show that $F'(w) = f(w)$ for any $w \in \Omega$, work in some small open neighborhood of w so that we may assume Ω is convex. In particular, let γ_z denote the straight line from w to z so that

$$\left| \frac{F(z) - F(w)}{z - w} - f(w) \right| = \left| \frac{1}{z - w} \int_{\gamma_z} f(s)\,ds - f(w) \right| \leq \sup_{s \in \operatorname{im} \gamma_z} |f(s) - f(w)|.$$

However, f is continuous, so this supremum goes to 0 as $z \to w$. ∎

And here is our converse.

Theorem A.14 (Morera)**.** Fix an open, connected subset $\Omega \subseteq \mathbb{C}$ and a continuous function $f \colon \Omega \to \mathbb{C}$. Given that

$$\oint_\gamma f(z)\,dz = 0$$

for any closed piecewise C^1 path $\gamma \colon [0,1] \to \Omega$. Then f is holomorphic.

Proof. By Proposition A.13, there exists holomorphic $F \colon \Omega \to \mathbb{C}$ such that $F' = f$. However, F is locally given by a power series by Remark A.10, so we can differentiate-term-by-term to tell us that F is infinitely differentiable. In particular, f is holomorphic. ∎

Here is are a couple useful corollaries of Theorem A.14.

Lemma A.15. Fix some open, connected subset $\Omega \subseteq \mathbb{C}$ and some function $f\colon \Omega \to \mathbb{C}$. Given holomorphic functions $f_n\colon \Omega \to \mathbb{C}$ for each $n \in \mathbb{N}$, if $f_n \to f$ uniformly on all compact subsets $D \subseteq U$, then f is holomorphic. In fact, for each $w \in \Omega$, we have $f_n'(w) \to f'(w)$ as $n \to \infty$.

Proof. To show f is holomorphic, the point is to use Morera's theorem. Quickly, note that to show f is differentiable at some particular $z \in \Omega$, we may find $r > 0$ such that $B(z,r) \subseteq \Omega$ and then replace Ω with $B(z,r)$; in particular, we may assume that Ω is simply connected. Each f_n is continuous, so we see f is continuous as well by the uniform convergence. Thus, fixing any closed piecewise C^1 path $\gamma\colon [0,1] \to U$, we would like to show

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

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

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

for all $n > N$. Fixing any $n > N$, we use Theorem A.7 to see

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

where $\ell(\gamma)$ is the length of γ. (Note $\ell(\gamma)$ is finite because γ is piecewise C^1.) Sending $\varepsilon \to 0^+$ finishes the application of Theorem A.14.

It remains to show the last sentence. The point is to use Corollary A.11. Well, for any fixed $w \in \Omega$, we again find some $r > 0$ such that $B(w,r) \subseteq \Omega$. Then for some $\varepsilon \in (0,r)$, we let γ be the counterclockwise path around w with radius ε. Then Corollary A.11 grants

$$\begin{aligned}
|f'(w) - f_n'(w)| &= \left|\frac{1}{2\pi i}\oint_\gamma \frac{f(z)}{(z-w)^2}\,dz - \frac{1}{2\pi i}\oint_\gamma \frac{f_n(z)}{(z-w)^2}\,dz\right| \\
&\le \frac{1}{2\pi}\cdot \sup_{z\in\Omega}\{|f(z) - f_n(z)|\} \cdot \oint_\gamma \frac{1}{|z-w|^2}\,dz \\
&= \frac{1}{2\pi}\cdot \sup_{z\in\Omega}\{|f(z) - f_n(z)|\} \cdot \frac{2\pi\varepsilon}{\varepsilon^2}.
\end{aligned}$$

Now, as $n \to \infty$, we see that $|f(z) - f_n(z)| \to 0$ uniformly, so the final expression goes to 0. This completes the proof. ∎

Lemma A.16. Fix some simply connected open subset $\Omega \subseteq \mathbb{C}$. Given a holomorphic function $f\colon \Omega \to \mathbb{C}$ which vanishes nowhere, there exists a holomorphic function $g\colon \Omega \to \mathbb{C}$ such that $f = \exp \circ g$.

Proof. By shifting Ω, we may assume that $0 \in \Omega$. By scaling f (which is the same as shifting g), we may assume that $f(0) = 1$. Now, note that f is locally a power series by Remark A.10, so f' is holomorphic, so f'/f is holomorphic because f vanishes nowhere on Ω. Thus, by Theorem A.7, we see that

$$\oint_\gamma \frac{f'(z)}{f(z)}\,dz = 0$$

for any closed piecewise C^1 path $\gamma\colon [0,1] \to \Omega$, where here we are using the fact that Ω is simply connected. Thus, we let g be a primitive for f'/f; by shifting g, we may assume that $g(0) = 0$. Now let $h(z) \coloneqq \exp(g(z))/f(z)$ so that we want to show $h(z) = 1$ for each z; note that f is always nonzero, so h is in fact holomorphic. Well, we see that

$$h'(z) = \frac{f(z)\cdot \exp(g(z))g'(z) - \exp(g(z))f'(z)}{f(z)^2} = 0,$$

so h is constant. But $h(0) = 1$ by construction of f and g, so $h(z) = 1$ for each z. ∎

Remark A.17. Unwinding the proof of Proposition A.13 and Lemma A.16, we see that we can actually explicitly define g by

$$g(z) \coloneqq \log f(z_0) + \int_\gamma \frac{f'(z)}{f(z)}\,dz,$$

where $z_0 \in \Omega$ is any point, and γ is any path connecting z_0 to z.

A.5 Differentiation Under the Integral

While we're here, we pick up the following very useful technical result from [Mat01].

Proposition A.18 (Differentiation under the integral sign)**.** Let $(X, \mathcal{S}, \mu)$ be a measurable space, and let $U \subseteq \mathbb{C}$ be open, and let $f\colon U \times X \to \mathbb{C}$ and $g\colon X \to X$ 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 $|f(z,x)| \le g(x)$ for all s.
- For fixed z, the function $x \mapsto f(z,x)$ is measurable.

Then the function $F\colon U \to \mathbb{C}$ given by $F(z) \coloneqq \int_X f(z,x)\,dx$ 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 $\gamma\colon [0,1] \to U$ denote the straight line from w to w'. Thus, the Fundamental theorem of calculus and Cauchy's integral formula grants

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

   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

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

   where we have used the computation $\ell(\gamma_z) = 2\pi\left|r - \frac{1}{2}|w-w'|\right|$ for each z. Now, as $w' \to w$, 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 $\gamma\colon [0,1] \to U$ be some closed curve, and we want to show

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

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

$$\int_\gamma \int_X |f(z,x)|\,dxdz \le \int_\gamma \int_X g(x)\,dxdz \le \ell(\gamma) \int_X g(x)\,dx < \infty.$$

Thus, Fubini's theorem lets us write

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

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
$$F'(w) = \frac{1}{2\pi i} \int_\gamma \frac{F(z)}{(z-w)^2}\,dz = \frac{1}{2\pi i} \int_\gamma \int_X \frac{f(z,x)}{(z-w)^2}\,dxdz.$$
As usual, we would like to exchange the two integrals, so we note that we have absolute convergence because
$$\int_\gamma \int_X \left|\frac{f(z,x)}{(z-w)^2}\right|\,dxdz \le \int_\gamma \int_X \frac{g(x)}{(r/2)^2}\,dxdz \le \frac{\ell(\gamma)}{(r/2)^2} \int_X g(x)\,dx < \infty.$$
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 A.19. Proposition A.18 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.

A.6 Infinite Products

Throughout analytic number theory, it is useful to take infinite products for one reason or another. In this section, we follow [SS03a, Section 5.3]. We begin by discussing products of elements.

Definition A.20 (absolutely converges)**.** Given a sequence of complex numbers $\{a_k\}_{k\in\mathbb{N}}$, the infinite product
$$\prod_{k=1}^{\infty} (a_k + 1)$$
converges absolutely if and only if the product $\prod_{k=1}^{\infty}(|a_k|+1)$ converges.

Lemma A.21. Let $\{a_k\}_{k\in\mathbb{N}}$ be a sequence of complex numbers such that

$$\sum_{k=1}^{\infty} |a_k| < \infty.$$

Then the infinite product $\prod_{k=1}^{\infty}(1+a_k)$ converges and vanishes if and only if some factor vanishes.

Proof. If any factor vanishes, then the entire product converges to 0, so there is nothing to say. Otherwise, assume that $a_k \neq -1$ for all k, and we must show that the infinite product converges to a nonzero value. We have two cases.

1. Suppose that $|a_n| < 1/2$ for all n. Then we can use the power series to define $\log$. The main claim is that the infinite sum
$$\sum_{k=1}^{\infty} \log(1+a_k)$$
converges. In fact, it converges absolutely: we compute
$$\begin{aligned}\sum_{k=1}^{\infty} |\log(1+a_k)| &= \sum_{k=1}^{\infty} \left|\sum_{\ell=1}^{\infty} (-1)^{\ell} \frac{a_k^{\ell}}{\ell}\right| \\ &\leq \sum_{k=1}^{\infty} \left(\sum_{\ell=1}^{\infty} \frac{|a_k|^{\ell}}{\ell}\right) \\ &\leq \sum_{k=1}^{\infty} -\log(1-|a_k|).\end{aligned}$$
Now, $\log$ is concave down on $(0,\infty)$, so $-\log(1-x)$ is concave up on $[0,1/2]$, so comparing with a line segment, we see
$$-\log(1-|a_k|) \leq \frac{(1/2-|a_k|)(-\log(1-0)) + |a_k|(-\log(1-1/2))}{1/2} < |a_k| \cdot \frac{-\log(1-1/e)}{1/2} = 2|a_k|$$
for each $|a_k| \in [0,1/2)$. Thus,
$$\sum_{k=1}^{\infty} |\log(1+a_k)| \leq \sum_{k=1}^{\infty} -\log(1-|a_k|) \leq \sum_{k=1}^{\infty} 2|a_k| = 2\sum_{k=1}^{\infty} |a_k|,$$
completing the proof of the claim.
To complete the proof in this case, we use the fact that $\exp$ is continuous to write
$$\begin{aligned}\prod_{k=1}^{\infty}(1+a_k) &= \lim_{n\to\infty} \prod_{k=1}^{n}(1+a_k) \\ &= \lim_{n\to\infty} \exp\left(\sum_{k=1}^{n} \log(1+a_k)\right) \\ &= \exp\left(\lim_{n\to\infty} \sum_{k=1}^{n} \log(1+a_k)\right) \\ &= \exp\left(\sum_{k=1}^{\infty} \log(1+a_k)\right),\end{aligned}$$
which we already know converges (absolutely). Additionally, we converge to a nonzero value because $\exp(z) \neq 0$ for all $z \in \mathbb{C}$. This is what we wanted.

2. In the general case, note that the convergence of the sum $\sum_{k=1}^{\infty} |a_k|$ enforces $|a_k| \to 0$ as $k \to \infty$. Thus, there exists some n such that $|a_k| < 1/2$ for $k > N$, so we see

$$\prod_{k=1}^{\infty}(1+a_k) = \prod_{k=1}^{n}(1+a_k) \cdot \prod_{k=n+1}^{\infty}(1+a_k).$$

The left product is finite, and the right product converges by the previous step: note $\sum_{k=n+1}^{\infty} |a_k| < \infty$ because $\sum_{k=1}^{\infty} |a_k| < \infty$. Thus, the entire product converges, and it converges to a nonzero value because the left and right factors above are both nonzero. ■

Remark A.22. In fact, by replacing $\{a_k\}_{k\in\mathbb{N}}$ with $\{|a_k|\}_{k\in\mathbb{N}}$, the lemma tells us that

$$\prod_{k=1}^{\infty}(1+|a_k|)$$

also converges. In particular, the product converges absolutely.

We even have a converse to the above result.

Lemma A.23. Fix a sequence of complex numbers $\{a_k\}_{k\in\mathbb{N}}$ such that the infinite product

$$\prod_{k=1}^{\infty}(1+a_k)$$

converges absolutely. Then $\sum_{k=1}^{\infty} |a_k|$ converges.

Proof. We may replace $\{a_k\}_{k\in\mathbb{N}}$ with $\{|a_k|\}_{k\in\mathbb{N}}$ so that we can assume that the a_k are positive real numbers. Now, the convergence of the infinite product allows us to use the continuity of $\log$ to write

$$\log\left(\prod_{k=1}^{\infty}(1+a_k)\right) = \log\left(\lim_{n\to\infty}\prod_{k=1}^{n}(1+a_k)\right) = \lim_{n\to\infty}\sum_{k=1}^{n}\log(1+a_k) = \sum_{k=1}^{\infty}\log(1+a_k).$$

In particular, this infinite sum converges, so $\log(1+a_k) \to 0$ as $k \to \infty$, so we can find N large enough so that $\log(1+a_k) < \log(3/2)$ for each $k > N$, meaning that $1 + a_k < 3/2$ and so $a_k < 1/2$. But here we note that $\log$ is concave down, so

$$\log(1+a_k) \geq \frac{(1/2-a_k)\log(1+0) + a_k\log(1+1/2)}{1/2} = a_k \cdot 2\log(3/2).$$

For psychological reasons, we note that $3\log(3/2) = \log(27/8) > \log 3 > 1$, so we see $\log(1+a_k) > \frac{2}{3}a_k$ here. In total, we see

$$\sum_{k=1}^{\infty} a_k = \sum_{k=1}^{N} a_k + \frac{3}{2}\sum_{k>N}\frac{2}{3}a_k \leq \sum_{k=1}^{N} a_k + \frac{3}{2}\sum_{k>N}\log(1+a_k) < \infty,$$

so the sum converges. This completes the proof. ■

Remark A.24. Combining Lemmas A.21 and A.23 shows that an infinite product which converges absolutely will only vanish if any of the factors vanish.

Now that we know how to take infinite products of elements, we can also take infinite products of functions. Here is our analogue of the Weierstrass M-test.

Proposition A.25. Fix an open subset $\Omega \subseteq \mathbb{C}$ and a sequence $\{f_k\}_{k\in\mathbb{N}}$ of holomorphic functions $\Omega \to \mathbb{C}$. Suppose that we have constants $\{c_k\}_{k\in\mathbb{N}} \subseteq \mathbb{C}$ such that

$$\sum_{k=1}^{\infty} |c_k| < \infty \qquad \text{and} \qquad |f_k(z) - 1| < |c_k| \text{ for all } z.$$

Then the infinite product $f(z) \coloneqq \prod_{k=1}^{\infty} f_k(z)$ converges absolutely and uniformly on compacts to a holomorphic function $\Omega \to \mathbb{C}$.

Proof. Set $a_k(z) \coloneqq f_k(z) - 1$ for each k. Then we see

$$\sum_{k=1}^{\infty} |a_k(z)| \le \sum_{k=1}^{\infty} |c_k| < \infty,$$

so Remark A.22 implies that the infinite product $f(z)$ converges absolutely for all $z \in \mathbb{C}$.

Now, because each f_k is holomorphic, each partial product defining f is holomorphic, so it suffices by Lemma A.15 to show that the partial products converge uniformly to f. As in the previous proof, we have two cases.

1. Suppose that $|c_k| < 1/2$ for each k. The idea is to use $\exp$ to turn our product into a sum. For technical reasons, we start by noting that $m > n$ gives

$$\left|\sum_{k=m}^{n} \log f_k(z)\right| \le \sum_{k=m}^{n} |\log(1 + a_k(z))| \le \sum_{k=m}^{n} -\log(1 - |a_k(z)|) \le \sum_{k=m}^{n} -\log(1 - |c_k|) \le 2\sum_{k=m}^{n} |c_k|,$$

where we have bounded as in the previous proof. (Here, $\log$ is defined using the power series.) In particular, this partial sum and even the full series has magnitude bounded by $C \coloneqq 2\sum_{k=1}^{\infty} |c_k|$.

For psychological reasons, we note that $\exp$ has continuous and hence bounded derivative on the compact set $\overline{B(0,C)}$, so $\exp$ is Lipschitz continuous; let L be the Lipschitz constant for $\exp$. The main computation is that any $z \in D$ have

$$\begin{aligned}\left|f(z) - \prod_{k=1}^{n} f_k(z)\right| &= \left|\exp\left(\sum_{k=1}^{\infty} \log(1 + a_k(z))\right) - \exp\left(\sum_{k=1}^{n} \log(1 + a_k(z))\right)\right| \\ &\le L\left|\sum_{k=n+1}^{\infty} \log(1 + a_k(z))\right| \\ &\le 2L \sum_{k=n+1}^{\infty} |c_k|\end{aligned}$$

by the above bounding. However, as $n \to \infty$, this right-hand side goes to 0 because $\sum_{k=1}^{\infty} |c_k|$ converges. The uniform convergence follows.

2. We reduce to the above case. Because $\sum_{k=1}^{\infty} |c_k|$ converges, we see $|c_k| \to 0$ as $k \to \infty$, so there exists n such that $|c_k| < 1/2$ for $k > n$. Thus,

$$f(z) = \prod_{k=1}^{n} f_k(z) \cdot \prod_{k=n+1}^{\infty} f_k(z).$$

By the previous step, the convergence in the right (infinite) product is uniform, and the left term is a finite product, so the convergence in the original product is also uniform. ∎

Remark A.26. It might look concerning that we have full uniform convergence instead of the usual more mild uniform convergence on compacts. However, the hypothesis requires that the f_k are bounded, so Ω will have to be pretty small anyway if the f_k are nonconstant.

Remark A.27. Note that the above proof shows that, for any $z \in \mathbb{C}$, the sequence $\{a_n(z)\}_{n\in\mathbb{N}}$ satisfies the hypotheses of Lemma A.21. Thus, $f(z) = 0$ if and only if $f_k(z) = 0$ for some k. As such, if $f(z) \neq 0$, we note that the above proof tells us that the equality

$$\log f(z) = \sum_{k=1}^{\infty} \log f_k(z)$$

makes sense, and the sum converges absolutely.

Because we are doing analysis, it will also be beneficial to be able to compute derivatives.

Corollary A.28. Fix an open subset $\Omega \subseteq \mathbb{C}$ and a sequence $\{f_k\}_{k\in\mathbb{N}}$ of holomorphic functions $\Omega \to \mathbb{C}$. Suppose that the infinite product $f(z) \coloneqq \prod_{k=1}^{\infty} f_k(z)$ converges absolutely and uniformly on compacts. Then

$$\frac{f'(z)}{f(z)} = \sum_{k=1}^{\infty} \frac{f_k'(z)}{f_k(z)}$$

if $f(z) \neq 0$.

Proof. Let $p_n(z)$ denote the nth partial product. By Lemma A.15, we know that $p_n'(z) \to f'(z)$ as $n \to \infty$. Now, $f(z) \neq 0$ implies that $f_k(z) \neq 0$ for each k by Remark A.27, so $p_n(z) \neq 0$ for each n as well. Thus, we may add in the fact $p_n(z) \to f(z)$ as $n \to \infty$ to compute

$$\frac{f'(z)}{f(z)} = \lim_{n\to\infty} \frac{p_n'(z)}{p_n(z)} \overset{*}{=} \lim_{n\to\infty} \sum_{k=1}^{n} \frac{f_k'(z)}{f_k(z)} = \sum_{k=1}^{\infty} \frac{f_k'(z)}{f_k(z)}.$$

Note that $\overset{*}{=}$ holds because we can formally check that $\frac{(ab)'(z)}{(ab)(z)} = \frac{a'(z)}{a(z)} + \frac{b'(z)}{b(z)}$ for holomorphic functions a and b not vanishing at z. In particular, there is no need for a logarithm here. ∎

Appendix B
Entire Functions

In this chapter, we provide enough of the theory of entire functions in order to state and prove the Hadamard factorization theorem. Throughout this section, entire functions will be nonzero. We follow [SS03a, Chapter 5].

B.1 Counting Zeroes

It will be useful to bound the number of zeroes of a nonzero entire function, so we establish some notation.

Notation B.1. Fix a nonzero entire function $f\colon \mathbb{C} \to \mathbb{C}$. Then we let $Z_f(r)$ denote the multiset of complex numbers $z \in B(0,r)$ such that $f(z) = 0$, counted with multiplicity. Additionally, we set $n_f(r) \coloneqq \#Z_f(r)$.

Remark B.2. If $f\colon \mathbb{C} \to \mathbb{C}$ is a nonzero entire function, then $n_f(r)$ is indeed finite: indeed, if $n_f(r)$ is infinite, then we claim $f = 0$. To see this, we note f has infinitely many zeroes in the compact set $\overline{B(0,r)}$, which has two cases.

- If f has infinitely many distinct zeroes in $\overline{B(0,r)}$, then the zero-set of f must have a limit point because it is an infinite subset of a compact set. But this implies $f = 0$.
- If f has a zero w of order infinity, then the Taylor expansion of f around w vanishes identically. It follows that f vanishes in an open neighborhood of w, so f has infinitely many zeroes, reducing to the previous case.

We will shortly be able to roughly bound the number of zeroes of f by the growth rate of f, but for the purpose of this section, we will not place constraints on the growth rate of f. To begin this counting, we pick up the following lemma.

Lemma B.3. Fix a nonzero entire function $f\colon \mathbb{C} \to \mathbb{C}$ such that $f(0) \neq 0$. For any $R > 0$, we have

$$\int_0^R n_f(r)\,\frac{dr}{r} = \sum_{\substack{f(z)=0 \\ |z|<R}} \log\left|\frac{R}{z}\right|,$$

where the sum counts zeroes with multiplicity.

Proof. Note that the $f(0) \neq 0$ hypothesis is included to ensure that the sum is well-defined. For each $z \in Z_f(R)$, we will use the indicator $1_{>|z|}(r)$ to indicate $z \in B(0,r)$. In particular, we compute

$$\begin{aligned}\int_0^R n_f(r)\,\frac{dr}{r} &= \int_0^R \left(\sum_{z\in Z_f(R)} 1_{>|z|}(r)\right)\frac{dr}{r} \\ &\overset{*}{=} \sum_{z\in Z_f(r)} \left(\int_0^R 1_{>|z|}(r)\,\frac{dr}{r}\right) \\ &= \sum_{z\in Z_f(r)} \left(\int_{|z|}^R \frac{dr}{r}\right) \\ &= \sum_{z\in Z_f(r)} \log\left|\frac{R}{z}\right|,\end{aligned}$$

which is what we wanted. Notably, we are able to switch the sum and integral in $\overset{*}{=}$ because the sum is finite by Remark B.2. ■

As such, we are motivated to understand this summation of logarithms as a proxy to understand $n_f(r)$. This is the content of Jensen's theorem.

Theorem B.4 (Jensen)**.** Fix a nonzero entire function $f\colon \mathbb{C} \to \mathbb{C}$ such that $f(0) \neq 0$. Further, suppose f does not vanish on $\partial B(0,R)$ for some $R > 0$. Then

$$\log|f(0)| = \sum_{\substack{f(z)=0\\ |z|<R}} \log\left|\frac{z}{R}\right| + \frac{1}{2\pi}\int_0^{2\pi} \log\left|f\left(Re^{i\theta}\right)\right|\,d\theta.$$

Proof. This is essentially a consequence of the Cauchy integral formula. Again, note that $f(0) \neq 0$ is required for the sum to make sense. Anyway, we proceed in steps to build up to the general case.

1. Suppose that f does not vanish on $B(0,R)$ so that f does not vanish on $\overline{B(0,R)}$. Here, the sum is empty, so we would like to show

$$\log|f(0)| \overset{?}{=} \frac{1}{2\pi}\int_0^{2\pi} \log\left|f\left(Re^{i\theta}\right)\right|\,d\theta. \tag{B.1}$$

   The idea is to apply the Cauchy integral formula to a suitably defined logarithm of f. This logarithm will exist because f is nonzero in our region.

   Quickly, we claim that f does not vanish on $B(0,R+\varepsilon)$ for some $\varepsilon > 0$. Indeed, suppose not. Then for each n, we can find $r_n e^{i\theta_n} \in B(0,R+1/n)$ such that $f(z_n) = 0$. In particular, we see $R < r_n < R+1/n$ for each n, and $e^{i\theta_n} \in S^1$.

   Thus, $r_n \to R$ as $n \to \infty$, and having infinitely many elements $e^{i\theta_n}$ in the compact set S^1 forces the θ_n to have a subsequence $e^{i\theta_{n_k}}$ to converge to some $e^{i\theta}$. It follows that $r_{n_k}e^{i\theta_{n_k}} \to Re^{i\theta}$, so because $f^{-1}(\{0\})$ is closed, we see that $Re^{i\theta}$ lives in $f^{-1}(\{0\})$, so f vanishes on some point in $\partial B(0,R)$. This is a contradiction to the construction of R.

   We now continue the proof with our $\varepsilon > 0$ such that f does not vanish $B(0,R+\varepsilon)$. Because f does not vanish, and $B(0,R+\varepsilon)$ is simply connected, we can use Lemma A.16 to define g so that g is holomorphic and satisfies $f(z) = \exp(g(z))$.

We now apply the Cauchy integral formula to $g(z)$. Let γ_R be the path $\theta \mapsto Re^{i\theta}$ so that the Cauchy integral formula grants

$$\begin{aligned} g(0) &= \frac{1}{2\pi i} \oint_{\gamma_R} \frac{g(z)}{z}\, dz \\ &= \frac{1}{2\pi i} \int_0^{2\pi} \frac{g\left(Re^{i\theta}\right)}{Re^{i\theta}} \cdot iRe^{i\theta}\, d\theta \\ &= \frac{1}{2\pi} \int_0^{2\pi} g\left(Re^{i\theta}\right)\, d\theta. \end{aligned}$$

Now, we see $\log|f(z)| = \log|\exp(g(z))| = \log\exp(\operatorname{Re} g(z)) = \operatorname{Re} g(z)$, so taking real parts of the above equation yields (B.1), as desired.

2. Suppose $f(z) = z - w$ for some nonzero $w \in B(0,R)$. Notably, f has only the root w, so after some rearranging, we would like to show

$$0 \stackrel{?}{=} \frac{1}{2\pi} \int_0^{2\pi} \log\left|e^{i\theta} - w/R\right|\, d\theta.$$

(Notably, $\log|f(0)| = w$.) We now would like to reduce to the previous case; set $\alpha \coloneqq R/w$ so that $|\alpha| > 1$. Now, we send $\theta \mapsto -\theta$, so we see

$$\frac{1}{2\pi} \int_0^{2\pi} \log\left|e^{i\theta} - 1/\alpha\right|\, d\theta = \int_0^{2\pi} \log\left|e^{-i\theta} - 1/\alpha\right|\, d\theta = \frac{1}{2\pi} \int_0^{2\pi} \log\left|1 - e^{i\theta}/\alpha\right|\, d\theta,$$

where we have factored out $\log\left|e^{-i\theta}\right| = \log 1 = 0$.

Thus, we set $g(z) \coloneqq 1 - z/\alpha$ so that g is entire but does not vanish on $\overline{B(0,1)}$ so that the previous case implies

$$0 = \log 1 = \log|g(z)| = \frac{1}{2\pi} \int_0^{2\pi} \log\left|g\left(e^{i\theta}\right)\right|\, d\theta = \frac{1}{2\pi} \int_0^{2\pi} \log\left|1 - e^{i\theta}/\alpha\right|\, d\theta,$$

which is what we wanted.

3. To set up the finish of the proof, suppose that the theorem is true for the nonzero entire functions $f_1, f_2 \colon \mathbb{C} \to \mathbb{C}$. Then we claim that the theorem is true for $f_1 f_2$. Indeed, we see $(f_1 f_2)(0) \neq 0$ implies $f_1(0), f_2(0) \neq 0$. Further, for any $R > 0$, we see $f_1 f_2$ not vanishing on $\partial B(0,R)$ implies that $f_2 f_2$ does not vanish on $\partial B(0,R)$ also.

Thus, the theorem hypotheses hold for both f_1 and f_2 if they hold for $f_1 f_2$. Now, for $i \in \{1,2\}$, let $Z_i(R)$ denote the multiset zeroes of f_i in $B(0,R)$ counted with multiplicity. Then the multiset $Z_1(R) \cup Z_2(R)$ is the multiset of zeroes of $f_1 f_2$ counted with multiplicity. Now, applying the theorem statement to both f_1 and f_2, we compute

$$\begin{aligned} \log|(f_1 f_2)(0)| &= \log|f_1(0)| + \log|f_2(0)| \\ &= \sum_{z \in Z_1(R)} \log\left|\frac{z}{R}\right| + \frac{1}{2\pi} \int_0^{2\pi} \log\left|f_1\left(Re^{i\theta}\right)\right|\, d\theta \\ &\quad + \sum_{z \in Z_2(R)} \log\left|\frac{z}{R}\right| + \frac{1}{2\pi} \int_0^{2\pi} \log\left|f_2\left(Re^{i\theta}\right)\right|\, d\theta \\ &= \sum_{z \in Z_1(R) \cup Z_2(R)} \log\left|\frac{z}{R}\right| + \frac{1}{2\pi} \int_0^{2\pi} \log\left|(f_1 f_2)\left(Re^{i\theta}\right)\right|\, d\theta, \end{aligned}$$

so the theorem statement also holds for $f_1 f_2$. This is what we wanted.

4. We now finish the proof in the general case. We define $g\colon \mathbb{C} \setminus Z_f(R) \to \mathbb{C}$ by

$$g(z) \coloneqq \frac{f(z)}{\prod_{w \in Z_f(R)} (z-w)}.$$

Now, the right-hand side will only have removable singularities at each element of $Z_f(R)$, so in fact we may extend analytically g to all $\mathbb{C}$ so that

$$f(z) = g(z) \prod_{w \in Z_f(R)} (z-w).$$

By the first step, the theorem statement holds for g, and by the second step, the theorem statement holds for each $z-w$. (Note $w \neq 0$ because $0 \notin Z_f(R)$ because $f(0) \neq 0$.) Thus, by the previous step, we may inductively take the product to show that the theorem statement holds for f, which is what we wanted. ∎

Corollary B.5. Fix a nonzero entire function $f\colon \mathbb{C} \to \mathbb{C}$ such that $f(0) \neq 0$. For any $R > 0$ such that f does not vanish on $\partial B(0,R)$, we have

$$\int_0^R n_f(r) \frac{dr}{r} = -\log|f(0)| + \frac{1}{2\pi} \int_0^{2\pi} \log\left|f\left(Re^{i\theta}\right)\right| \, d\theta.$$

Proof. By Lemma B.3 and Theorem B.4, we see

$$\int_0^R n_f(r) \frac{dr}{r} = \sum_{\substack{f(z)=0 \\ |z|<R}} \log\left|\frac{R}{z}\right| = -\log|f(0)| + \frac{1}{2\pi} \int_0^{2\pi} \log\left|f\left(Re^{i\theta}\right)\right| \, d\theta,$$

which is what we wanted. ∎

B.2 Functions of Bounded Order

Here is the central definition of this section.

Definition B.6 (order)**.** A function $f\colon \mathbb{C} \to \mathbb{C}$ has *order bounded by* ρ for some $\rho > 0$ if and only if there are $A, B > 0$ such that

$$|f(z)| \leq Ae^{B|z|^\rho}.$$

Then we define the *order* $\rho(f)$ as the infimum of the real numbers $\rho \geq 0$ such that f has order bounded by ρ. Note that we are permitting $\rho(f) = +\infty$.

Here are some starting examples and remarks.

Example B.7. Any polynomial $f(z) \in \mathbb{C}[z]$ has order 0. Indeed, write $f(z) = \sum_{k=0}^n a_k z^k$ so that any $\rho > 0$ has

$$\lim_{|z|\to\infty} |f(z)|e^{-|z|^\rho} \leq \sum_{k=0}^n \lim_{r\to\infty} a_k r^k e^{-r^\rho} = \sum_{k=0}^n \lim_{r\to\infty} \frac{a_k r^{k/\rho}}{e^r} = 0,$$

where the last equality holds by, say, L'Hôpital's rule. Thus, $z \mapsto |f(z)|e^{-|z|^\rho}$ is a bounded function on $\mathbb{C}$ (there exists R such that it is bounded by 1 for $|z| > R$, and the continuous function is certainly bounded on the compact set $\overline{B(0,R)}$), so we can find $A > 0$ such that $|f(z)| \leq Ae^{-|z|^\rho}$ for any $z \in \mathbb{C}$. It follows that f has order bounded by ρ for any $\rho > 0$, so $\rho(f) = 0$.

Example B.8. For any $A, B, \rho > 0$, the function $f(z) \coloneqq Ae^{B|z|^\rho}$ has order ρ. We now claim that f has order bounded by ρ' if and only if $\rho' \geq \rho$, which will finish the proof. This has the following components.

- If $\rho' = \rho$, then the inequality $|f(z)| \leq Ae^{B|z|^\rho}$ tells us that f has order bounded by ρ'.
- For any $\rho' > \rho$, we claim that f has order bounded by ρ'. Indeed, we see that

$$\lim_{|z|\to\infty} |f(z)|e^{-|z|^{\rho'}} = A\exp\left(\lim_{|z|\to\infty} B|z|^\rho \cdot \lim_{|z|\to\infty}\left(1 - |z|^{\rho-\rho'}\right)\right) = 0$$

  because $|z|^\rho \to \infty$ as $|z| \to \infty$. Thus, $|f(z)|e^{-|z|^{\rho'}}$ is bounded, so we can find $M > 0$ such that $|f(z)| \leq Me^{|z|^{\rho'}}$ for any $z \in \mathbb{C}$.
- For any $0 < \rho' < \rho$, we claim that f does not have order bounded by ρ'. Indeed, suppose for the sake of contradiction that we have $A', B' > 0$ such that $|f(z)| \leq A'e^{B'|z|^{\rho'}}$. Then the function $e^{B|z|^\rho - B'|z|^{\rho'}}$ is bounded above by A'/A, but

$$\lim_{|z|\to\infty} e^{B|z|^\rho - B'|z|^{\rho'}} = \exp\left(\lim_{|z|\to\infty} B|z|^{\rho'} \cdot \lim_{|z|\to\infty}\left(1 - (B/B')|z|^{\rho'-\rho}\right)\right) = +\infty.$$

Remark B.9. For any function $f\colon \mathbb{C} \to \mathbb{C}$, if f has order bounded by ρ, then f has order bounded by ρ' for any $\rho' > \rho$. Indeed, we are granted $A, B > 0$ such that $|f(z)| \leq Ae^{B|z|^\rho}$, so it suffices to find constants $A', B' > 0$ such that $Ae^{B|z|^\rho} \leq A'e^{B'|z|^{\rho'}}$. But $Ae^{B|z|^\rho}$ has order bounded by ρ' by Example B.8, so we are done.

Remark B.10. If f has order bounded by α, and g has order bounded by β, then fg has order bounded by $\max\{\alpha, \beta\}$. Without loss of generality, take $\alpha \geq \beta$. Now, $|g(z)| \leq Ae^{B|z|^\beta}$ for some $A, B > 0$, so Example B.8 implies that there exist $A', B' > 0$ such that $|g(z)| \leq A'e^{B'|z|^\alpha}$ because $\alpha \geq \beta$. But f also has constants $A'', B'' > 0$ such that $|f(z)| \leq A''e^{B''|z|^\alpha}$, so

$$|(fg)(z)| \leq A'A''e^{(B'+B'')|z|^\alpha},$$

implying that fg has order bounded by α.

Remark B.11. If the entire function $f\colon \mathbb{C} \to \mathbb{C}$ of order bounded by ρ has a zero at $z = 0$, then $g(z) \coloneqq f(z)/z$ still has order bounded by ρ. Indeed, we do know that there are $A, B > 0$ such that $|f(z)| \leq Ae^{B|z|^\rho}$ for $z \in \mathbb{C}$. Now, $g(z)e^{-B|z|^\rho}$ is a continuous function and hence bounded by some constant $A' > 0$ on $\overline{B(0,1)}$. However, $|z| > 1$, we see

$$|g(z)|e^{-B|z|^\rho} \leq |f(z)|e^{-B|z|^\rho} \leq A.$$

Thus, we see $|g(z)| \leq \max\{A, A'\}e^{B|z|^\rho}$, so g has order bounded by ρ.

It is a key fact, now, that we can count the number of zeroes of a function of bounded order.

Proposition B.12. Fix a nonzero entire function $f\colon \mathbb{C} \to \mathbb{C}$ with order bounded by $\rho > 0$. Then there exists a constant $C, D > 0$ such that $n_f(R) \leq Cr^\rho$ for $R > D$.

Proof. We would like to use Corollary B.5. We handle two cases.

1. Suppose $f(0) \neq 0$ so that Corollary B.5 applies. In particular, the key observation is that $n_f(r)$ is an increasing function. As such, we compute

$$\begin{aligned}\int_R^{2R} n_f(r)\,\frac{dr}{r} &= -\log|f(0)| + \frac{1}{2\pi}\int_0^{2\pi} \log\left|f\left(2Re^{i\theta}\right)\right|\,d\theta \\ &\quad - \left(-\log|f(0)| + \frac{1}{2\pi}\int_0^{2\pi} \log\left|f\left(Re^{i\theta}\right)\right|\,d\theta\right) \\ &= \frac{1}{2\pi}\int_0^{2\pi} \log\left|f\left(2Re^{i\theta}\right)\right|\,d\theta - \int_0^{2\pi} \log\left|f\left(Re^{i\theta}\right)\right|\,d\theta.\end{aligned}$$

However, because $|f(z)| \leq Ae^{B|z|^\rho}$ for some $A, B > 0$, we can upper-bound

$$\frac{1}{2\pi}\int_0^{2\pi} \log\left|f\left(2Re^{i\theta}\right)\right|\,d\theta \leq \frac{1}{2\pi}\int_0^{2\pi} \log\left|Ae^{BR^\rho}\right|\,d\theta = \log A + \frac{BR^\rho}{2\pi},$$

so it follows that

$$\int_R^{2R} n_f(r)\,\frac{dr}{r} \leq \left|\frac{1}{2\pi}\int_0^{2\pi} \log\left|f\left(2Re^{i\theta}\right)\right|\,d\theta\right| + \left|\int_0^{2\pi} \log\left|f\left(Re^{i\theta}\right)\right|\,d\theta\right| \leq 2\log A + \frac{B\left(1+2^\rho\right)}{2\pi}R^\rho.$$

On the other hand, because n_f is increasing, we can lower-bound

$$\int_R^{2R} n_f(r)\,\frac{dr}{r} \geq n_f(R)\int_R^{2R}\frac{dr}{r} = n_f(R)\log 2.$$

In total, we see

$$n_f(R)R^{-\rho} \leq \frac{2\log A}{\log 2}\cdot R^{-\rho} + \frac{B\left(1+2^\rho\right)}{2\pi}.$$

As $R \to \infty$, the right-hand side approaches $B\left(1+2^\rho\right)/2\pi$, so we can find some D such that the right-hand side is less than or equal to $B\left(1+2^\rho\right)/\pi$ for $R > D$. Thus, $n_f(R) \leq \frac{B(1+2^\rho)}{\pi}R^\rho$ for $R > D$, which is what we wanted.

2. We now reduce to the case where $f(0) \neq 0$. Suppose f has a zero order of m at 0. If $m = 0$, then we are already done by the previous case. Otherwise, set $g(z) \coloneqq f(z)/z^m$, which has only a removable singularity at $z = 0$ and thus extends to an entire function $g\colon \mathbb{C} \to \mathbb{C}$ such that $g(0) \neq 0$ while $f(z) = z^m g(z)$. Note that $n_f(R) = m + n_g(R)$ for any $R > 0$, and g still has order bounded by ρ by Remark B.11.

   It follows from the previous step that there are $C, D > 0$ such that $R > D$ have

$$n_f(R)R^{-\rho} = mR^{-\rho} + n_g(R)R^{-\rho} = mR^{-\rho} + C.$$

   Again, as $R \to \infty$, the right-hand side approaches C, so we can select $D' > 0$ such that the right-hand side is less than or equal to $2C$. Thus, $n_f(R) \leq 2CR^\rho$ for $R > \max\{D, D'\}$, which finishes. ■

Having a polynomial bound on the number of zeroes lets us bound sums with these zeroes.

Corollary B.13. Fix a sequence of nonzero complex numbers $\{z_k\}_{k\in\mathbb{N}}$ such that

$$n_f(r) \coloneqq \#\{k : z_k < r\} \ll r^\rho$$

for some positive real number ρ. For any $\sigma > \rho$, the sum

$$\sum_{k=1}^{\infty}\frac{1}{|z_k|^\sigma}$$

converges. (Note that this sum may be finite.)

Proof. We use the dyadic decomposition. Because we are working with an infinite sum of positive numbers, it suffices to bound the sum from above. Now, from Proposition B.12, we see $n_f(R) \le CR^\rho$ for some $R > D$; by replacing D with $2^{\lceil \log D \rceil} > D$ to no ill effect, we may assume that $D = 2^d$ for some positive integer d. Thus, we write

$$\begin{aligned}
\sum_{k=1}^{\infty} \frac{1}{|z_k|^\sigma} &= \sum_{z \in Z_f(D) \setminus \{0\}} \frac{1}{|z|^\sigma} + \lim_{R \to \infty} \sum_{\substack{f(z)=0 \\ |z| \ge D}} \frac{1}{|z|^\sigma} \\
&\le \sum_{z \in Z_f(D) \setminus \{0\}} \frac{1}{|z|^\sigma} + \sum_{k=d}^{\infty} \left(\sum_{\substack{f(z)=0 \\ 2^k \le |z| < 2^{k+1}}} \frac{1}{|z|^\sigma} \right) \\
&\le \sum_{z \in Z_f(D) \setminus \{0\}} \frac{1}{|z|^\sigma} + \sum_{k=d}^{\infty} \frac{n_f\left(2^{k+1}\right)}{2^{k\sigma}} \\
&\le \sum_{z \in Z_f(D) \setminus \{0\}} \frac{1}{|z|^\sigma} + C \sum_{k=d}^{\infty} \frac{2^{(k+1)\rho}}{2^{k\sigma}} \\
&\le \sum_{z \in Z_f(D) \setminus \{0\}} \frac{1}{|z|^\sigma} + 2^\rho C \sum_{k=d}^{\infty} 2^{k(\rho-\sigma)} \\
&\le \sum_{z \in Z_f(D) \setminus \{0\}} \frac{1}{|z|^\sigma} + 2^\rho C \cdot \frac{2^{d(\rho-\sigma)}}{1 - 2^{\rho-\sigma}},
\end{aligned}$$

which is indeed finite. ∎

B.3 Elementary Factors

Hadamard's factorization theorem requires taking an infinite product of some special factors with prescribed zeroes. Here are those factors.

Definition B.14 (elementary factor)**.** Given a nonnegative integer n, the *elementary factor* $E_n(z)$ is given by

$$E_n(z) := (1-z)e^{z + z^2/2 + \cdots + z^n/n}.$$

In particular, $E_0(z) = 1 - z$.

The proof of Hadamard's factorization theorem will roughly amount to combining Lemma A.16 with various bounds on elementary factors. As such, we take the time to establish the needed bounds on our elementary factors.

Lemma B.15. Given a nonnegative integer n, we have $|1 - E_n(z)| \le 2e|z|^{n+1}$ if $|z| \le 1/2$.

Proof. Because $|z| \le 1/2$, we may use the power series to define $\log$. Thus, we see

$$E_n(z) = \exp\left(\log(1-z) + \sum_{k=1}^{n} \frac{z^k}{k} \right) = \exp\left(-\sum_{k=1}^{\infty} \frac{z^k}{k} + \sum_{k=1}^{n} \frac{z^k}{k} \right) = \exp\left(\sum_{k>n} \frac{z^k}{k} \right).$$

Now, for brevity, set $z' := \sum_{k>n} z^k/k$. The bound on z' we will need is

$$|z'| = \left| z^{n+1} \sum_{k=0}^{\infty} \frac{z^k}{k+n+1} \right| \le |z|^{n+1} \sum_{k=0}^{\infty} \frac{|z|^k}{k+n+1} \le |z|^{n+1} \sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^k = 2|z|^{n+1}.$$

On the other hand, we see

$$\begin{aligned}|1-E_n(z)| &= |1-\exp(z')| \\ &= \left|-\sum_{k=1}^{\infty}\frac{(z')^k}{k!}\right| \\ &\le \sum_{k=1}^{\infty}\frac{|z'|^k}{k!} \\ &= \exp(|z'|)-1.\end{aligned}$$

However, $n \ge 0$, so $|z'| \in [0,1]$. Thus, because $\exp$ is concave up, we see that

$$\exp(|z'|)-1 \le (1-|z'|)(\exp(0)-1)+|z'|(\exp(1)-1) < e|z'|.$$

In total, we conclude $|1-E_n(z)| \le e|z'| \le 2e|z|^{n+1}$. ∎

Lemma B.16. Given a nonnegative integer n, we have $|E_n(z)| \ge \exp\left(-2|z|^{n+1}\right)$ if $|z| \le 1/2$.

Proof. As in the previous proof, $|z| \le 1/2$ allows us to define $\log$ by power series so that

$$E_n(z) = \exp\left(\sum_{k>n}\frac{z^k}{k}\right).$$

Again, we set $z' \coloneqq \sum_{k>n}\frac{z^k}{k}$ for brevity and compute

$$\begin{aligned}|E_n(z)| &= |\exp(z')| \\ &= \exp(\operatorname{Re} z') \\ &\ge \exp(-|z'|) \\ &= \exp\left(-\sum_{k=n+1}^{\infty}\frac{|z|^k}{k}\right) \\ &= \exp\left(-|z|^{n+1}\sum_{k=0}\frac{|z|^k}{k+n+1}\right) \\ &\ge \exp\left(-|z|^{n+1}\sum_{k=0}(1/2)^k\right) \\ &= \exp\left(-2|z|^{n+1}\right),\end{aligned}$$

which is what we wanted. ∎

Lemma B.17. Given a nonnegative integer n, we have $|E_n(z)| \ge |1-z|\exp\left(-2|z|^n\right)$ for $|z| \ge 1/2$.

Proof. Similar to the previous proof, we see

$$\left|\exp\left(\sum_{k=1}^{n}\frac{z^k}{k}\right)\right| = \exp\left(\operatorname{Re}\sum_{k=1}^{n}\frac{z^k}{k}\right) = \exp\left(\sum_{k=1}^{n}\frac{(\operatorname{Re} z)^k}{k}\right) \ge \exp\left(-\sum_{k=1}^{n}\frac{|z|^k}{k}\right).$$

However, we see

$$\sum_{k=1}^{n}\frac{|z|^k}{k} \le |z|^n\sum_{k=1}^{n}\frac{|z|^{k-n}}{k} \le |z|^n\sum_{k=1}^{n}\frac{(1/2)^{k-n}}{1} < |z|^n\sum_{k=0}^{\infty}\left(\frac{1}{2}\right)^k = 2|z|^n.$$

Combining,

$$|E_n(z)| = |1-z|\left|\exp\left(\sum_{k=1}^{n}\frac{z^k}{k}\right)\right| \geq |1-z|\exp\left(-\sum_{k=1}^{n}\frac{|z|^k}{k}\right) \geq |1-z|\exp\left(-2|z|^n\right),$$

which is what we wanted. ∎

B.4 Hadamard Factorization

Throughout this section, $f\colon \mathbb{C}\to\mathbb{C}$ will be a nonzero entire function of (finite) order ρ_0; set $n \coloneqq \lfloor \rho_0 \rfloor$ for brevity. We will also let $\{z_k\}_{k\in\lambda}$ denote the nonzero zeroes of f (with multiplicity), where λ is either finite or $\mathbb{N}$, ordered by magnitude. Notably, Remark B.2 tells us that there are only finitely zeroes with fixed bounded magnitude, so such an ordering possible.

The key to the proof will be the following lower bound on a product of elementary factors.

Lemma B.18. Fix a nonnegative real number ρ_0, and set $n \coloneqq \rho_0$. Further, fix a sequence $\{z_k\}_{k\in\lambda}$ of countably many nonzero such that

$$n_f(r) \coloneqq \#\{k : z_k < r\} \ll r^{\rho_0+\varepsilon}$$

for any $\varepsilon > 0$. Then given a real number s such that $\rho_0 < s < n+1$, there is some $c > 0$ such that

$$\left|\prod_{k\in\lambda} E_n(z/z_k)\right| \geq \exp\left(-c|z|^s\right) \qquad \text{for} \qquad |z-z_k| \geq |z_k|^{-n-1}$$

for $|z|$ sufficiently large, and the infinite product converges absolutely and uniformly on compacts to an entire function for all $z\in\mathbb{C}$.

Proof. We begin by showing that the infinite product converges absolutely and uniformly on compacts to an entire function; we use Proposition A.25. Indeed, for any compact subset $D\subseteq\mathbb{C}$, we know D is bounded, so find R such that $D\subseteq B(0,R)$. Then we are able to divide the infinite product into

$$\prod_{k\in\lambda} E_n(z/z_k) = \underbrace{\left(\prod_{|z_k|\leq 2R} E_n(z/z_k)\right)}_{P_1(z)\coloneqq}\underbrace{\left(\prod_{|z_k|>2R} E_n(z/z_k)\right)}_{P_2(z)\coloneqq}$$

because the z_k have been ordered by magnitude. Now, the $P_1(z)$ factor is finite and will therefore not affect our convergence, so we focus on showing that P_2 converges absolutely and uniformly on D. Well, by Lemma B.15, we see that any z_k with $|z_k| > 2R$ gives $|z/z_k| < 1/2$, so

$$|1-E_n(z/z_k)| \leq 2e|z/z_k|^{n+1} \leq \frac{2R^{n+1}}{|z_k|^{n+1}},$$

but

$$\sum_{k\in\lambda}\frac{2R^{n+1}}{|z_k|^{n+1}} = 2R^{n+1}\sum_{k\in\lambda}\frac{1}{|z_k|^{n+1}}$$

converges by hypothesis. Thus, Proposition A.25 kicks in to tell us that our infinite product converges absolutely and uniformly on D.

It remains to show the lower bound. Quickly, note that no term of the product will ever vanish by definition of the elementary factors and the fact that $|z-z_k| \geq |z_k|^{-n-1}$ for each z_k. This is somewhat technical.

As above, we divide the product into factors depending on $|z|$, though here we write

$$\prod_{k\in\lambda} E_n(z/z_k) = \underbrace{\left(\prod_{|z_k|\le 2|z|} E_n(z/z_k)\right)}_{Q_1(z):=}\underbrace{\left(\prod_{|z_k|>2|z|} E_n(z/z_k)\right)}_{Q_2(z):=}.$$

We now bound these terms independently.

- We control Q_2 using Lemma B.16. Indeed, we see

$$\begin{aligned}|Q_2(z)| &= \prod_{|z_k|>2|z|} |E_n(z/z_k)| \\ &\ge \prod_{|z_k|>2|z|} \exp\left(-2|z/z_k|^{n+1}\right) \\ &\overset{*}{=} \exp\left(\sum_{|z_k|>2|z|} -2|z/z_k|^{n+1}\right) \\ &= \exp\left(-2|z|^{n+1}\sum_{|z_k|>2|z|}\frac{1}{|z_k|^{n+1}}\right),\end{aligned}$$

  and this last sum again converges by Corollary B.13; note $\overset{*}{=}$ is valid here by the continuity of $\exp$ and the fact that our infinite product already converges.

  To finish our bounding here, we see

$$\frac{1}{|z_k|^{n+1}} \le \frac{1}{|z_k|^{n+1-s}}\cdot\frac{1}{|z_k|^s} \le \frac{1}{(2|z|)^{n+1-s}}\cdot\frac{1}{|z_k|^s},$$

  because $n+1-s>0$, so

$$|Q_2(z)| \ge \exp\left(-2^{s-n}|z|^s\sum_{|z_k|>2|z|}\frac{1}{|z_k|^s}\right) = \exp\left(-c_1|z|^s\right)$$

  for $c_2 := 2^{s-n}\sum_{|z_k|>2|z|} 1/|z_k|^s$. (The sum still converges by Corollary B.13.) Note $c_2>0$.

- We control Q_1 using Lemma B.17 and the fact that $|z-z_k| \ge |z_k|^{-n-1}$ for each z_k. Indeed, freely rearranging this finite product, we see

$$\begin{aligned}|Q_1(z)| &= \prod_{|z_k|\le 2|z|} |E_n(z/z_k)| \\ &\ge \prod_{|z_k|\le 2|z|}\left(\left|1-\frac{z}{z_k}\right|\exp\left(-2|z/z_k|^n\right)\right) \\ &= \prod_{|z_k|\le 2|z|}\left|1-\frac{z}{z_k}\right|\cdot\exp\left(-2|z|^n\sum_{|z_k|\le 2|z|}\frac{1}{|z_k|^n}\right).\end{aligned}$$

  The left term here will be difficult to bound, but we can control the right term here as we did with Q_2. Indeed, we see

$$\frac{1}{|z_k|^n} \le \frac{1}{|z_k|^{n-s}}\cdot\frac{1}{|z_k|^s} \le \frac{1}{(2|z|)^{n-s}}\cdot\frac{1}{|z_k|^s},$$

  because $n-s<0$, so

$$\exp\left(-2|z|^n\sum_{|z_k|\le 2|z|}\frac{1}{|z_k|^n}\right) \ge \exp\left(-2^{s-n+1}|z|^s\sum_{|z_k|>2|z|}\frac{1}{|z_k|^s}\right) = \exp\left(-c_2|z|^s\right)$$

for $c_2' \coloneqq 2^{s-n+1}|z|^s \sum_{|z_k|>2|z|} 1/|z_k|^s$. Note $c_1' > 0$.

We now focus on the left term. By hypothesis on z, we see

$$\begin{aligned}\prod_{|z_k|\le 2|z|} \left|1 - \frac{z}{z_k}\right| &= \prod_{|z_k|\le 2|z|} \left|\frac{z - z_k}{z_k}\right| \\ &\ge \prod_{|z_k|\le 2|z|} |z_k|^{-n-2} \\ &\ge \left((2|z|)^{-n-2}\right)^{n_f(2|z|)} \\ &= \exp\left(-(n+2)\log(2|z|) n_f(2|z|)\right).\end{aligned}$$

Now, f has order bounded by $s > \rho_0$ (formally, one must use Remark B.9 here), so hypothesis tells us that $n_f(2|z|) \le C|z|^s$ for $|z|$ sufficiently large. In total, we set $c_1'' \coloneqq -C(n+2)\log(2|z|)$ so that

$$\prod_{|z_k|\le 2|z|} \left|1 - \frac{z}{z_k}\right| \ge \exp\left(-c_1''|z|^s\right).$$

Thus, for $c_1 \coloneqq c_1' + c_1''$, we see $|Q_1(z)| \ge \exp\left(-c_1|z|^s\right)$ for $|z|$ sufficiently large.

In total, we see that

$$\left|\prod_{k\in\lambda} E_n(z/z_k)\right| = |Q_1(z)| \cdot |Q_2(z)| \ge \exp\left(-(c_1+c_2)|z|^s\right)$$

for $|z|$ sufficiently large. This is what we wanted. ∎

We will use Lemma B.18 in the following form.

Lemma B.19. Fix everything as above. Then there is an unbounded set of positive real numbers $R \subseteq \mathbb{R}$ and constant $c > 0$ such that

$$\left|\prod_{k\in\lambda} E_n(z/z_k)\right| \ge \exp\left(-c|z|^s\right) \qquad \text{for} \qquad |z| \in R.$$

Proof. The hypotheses on $\{z_k\}$ are satisfied by Proposition B.12 and Corollary B.13. Quickly, note that the infinite product makes sense by Lemma B.18. In order to use Lemma B.18, we let μ denote the Lebesgue measure and note

$$\mu\Bigg(\underbrace{\bigcup_{k\in\lambda} \left(|z_k| - |z_k|^{-n-1}, |z_k| + |z_k|^{-n-1}\right)}_{S\coloneqq}\Bigg) \le 2\sum_{k\in\lambda} \frac{1}{|z_k|^{n+1}}$$

converges by Corollary B.13, so $\mu(S)$ is finite. Now, we note that $|z - z_k| < |z_k|^{-n-1}$ for some z_k implies $|z| \in \left(|z_k| - |z_k|^{-n-1}, |z_k| + |z_k|^{-n-1}\right) \subseteq S$, so we are roughly looking for real numbers r not in S.

Now, the "sufficiently large" condition on $|z|$ in Lemma B.18 amounts to requiring $|z| > D$ for some $D > 0$. Thus, we set

$$R \coloneqq \{r > D : r \notin S\}.$$

If R were bounded above, then there would be some M such that any $r > M$ has either $r \le D$ or $r \in S$, meaning that $(\max\{M, D\}, \infty) \subseteq S$, which is a contradiction because S has finite measure. Thus, R is not bounded above.

Lastly, note that any $z \in \mathbb{C}$ with $|z| \in R$ has $|z|$ sufficiently large and $|z| \notin S$ and thus $|z - z_k| \ge |z_k|^{-n-1}$ for each z_k, giving

$$\left|\prod_{k\in\lambda} E_n(z/z_k)\right| \ge \exp\left(-c|z|^s\right) \qquad \text{for} \qquad |z| = r_m$$

by Lemma B.18. This is what we wanted. ∎

In particular, the above lemma will be plugged into the following proposition.

Proposition B.20. Fix an entire function $g\colon \mathbb{C} \to \mathbb{C}$ and positive real number $s > 0$. Suppose there is a constant $C > 0$ and an unbounded set of positive real numbers $R \subseteq \mathbb{R}$ such that $\operatorname{Re} g(z) \le C|z|^s$ if $|z| \in R$. Then g is a polynomial of degree less than or equal to s.

Proof. This proof does not use the notation of the rest of the section. Because g is analytic (by Remark A.10), there is $\varepsilon > 0$ such that we may write

$$g(z) = \sum_{k=0}^{\infty} g_k z^k$$

for $z \in B(0, \varepsilon)$. By differentiating the power series by hand, we see that $g_n = g^{(n)}(0)/n!$ for each $n \ge 0$. However, by Cauchy's integral formula in the form Corollary A.11, we let γ_r denote the counterclockwise circle around $z = 0$ with radius $r \in R$ and see

$$\begin{aligned} g_n &= \frac{g^{(n)}(0)}{n!} \\ &= \frac{1}{2\pi i} \oint_{\gamma_r} \frac{g(z)}{z^{n+1}}\, dz \\ &= \frac{1}{2\pi i} \int_0^{2\pi} \frac{g\left(re^{i\theta}\right)}{r^{n+1}e^{i\theta(n+1)}} \cdot rie^{i\theta}\, d\theta \\ &= r^{-n} \cdot \frac{1}{2\pi} \int_0^{2\pi} g\left(re^{i\theta}\right) e^{-in\theta}\, d\theta. \end{aligned}$$

To access $\operatorname{Re} g$, we will want to take the conjugate of this. Well, the function $g(z)z^{n-1}$ is holomorphic for $n > 0$, so

$$\begin{aligned} 0 &= \oint_{\gamma_r} g(z) z^{n-1}\, dz \\ &= \oint_{\gamma_r} g\left(re^{i\theta}\right) \cdot r^{n-1} e^{i(n-1)\theta} \cdot rie^{i\theta}\, d\theta \\ &= r^n \oint_{\gamma_r} g\left(re^{i\theta}\right) e^{in\theta}\, d\theta. \end{aligned}$$

Thus, our conjugate integral is

$$\int_0^{2\pi} \overline{g\left(re^{i\theta}\right)} e^{-in\theta}\, d\theta = \overline{\int_0^{2\pi} g\left(re^{i\theta}\right) e^{in\theta}\, d\theta} = 0$$

for $n > 0$. Summing, we see

$$r^n g_n = \frac{1}{2\pi} \int_0^{2\pi} \left(g\left(re^{i\theta}\right) + \overline{g\left(re^{i\theta}\right)}\right) e^{-in\theta}\, d\theta = \frac{1}{\pi} \int_0^{2\pi} \left(\operatorname{Re} g\right)\left(re^{i\theta}\right) e^{-in\theta}\, d\theta$$

for $n > 0$. Now, we would like to use this integral to bound $|g_n|$, but we only have an upper bound on $\operatorname{Re} g$, so some trickery is required. In particular, we note that $\int_0^{2\pi} Cr^s e^{-in\theta}\, d\theta = 0$ for any $n > 0$, so we actually have

$$r^n g_n = \frac{1}{\pi} \int_0^{2\pi} \left(\left(\operatorname{Re} g\right)\left(re^{i\theta}\right) - Cr^s\right) e^{-in\theta}\, d\theta.$$

But now the integrand is always negative, so we can upper-bound the magnitude as

$$\begin{aligned} r^n|g_n| &\le \frac{1}{\pi}\int_0^{2\pi} \left|(\operatorname{Re} g)\left(re^{i\theta}\right) - Cr^s\right| d\theta \\ &= \frac{1}{\pi}\int_0^{2\pi} Cr^s\, d\theta - \frac{1}{\pi}\int_0^{2\pi} (\operatorname{Re} g)\left(re^{i\theta}\right)\, d\theta \\ &= 2Cr^s - \frac{1}{\pi}\operatorname{Re} g_0. \end{aligned}$$

In particular, we see that $|g_n| \le 2Cr^{s-n} - r^{-n}\cdot\frac{1}{\pi}\operatorname{Re} g_0$, so for any $n > s$, sending $r \to \infty$ (possible because R is unbounded) enforces $g_n = 0$. It follows that g is a polynomial of degree at most $\lfloor s\rfloor$ on $B(0,\varepsilon)$ and therefore a polynomial everywhere by analytic continuation. ■

Remark B.21. Intuitively, we expect entire functions to have growth rate which is exponential if they are not polynomial. And indeed, this sort of statement will follow from Hadamard's factorization theorem, so it is not surprising that this is a necessary ingredient to the proof.

We are finally able to state and prove Hadamard's factorization theorem.

Theorem B.22 (Hadamard's factorization)**.** Fix a nonzero entire function $f\colon \mathbb{C}\to\mathbb{C}$ of (finite) order ρ_0; set $n := \lfloor \rho_0\rfloor$ for brevity. We also let $\{z_k\}_{k\in\lambda}$ denote the nonzero zeroes of f (with multiplicity), where λ is either finite or $\mathbb{N}$, ordered by magnitude. Further, let m denote the order of the zero of f at $z=0$. Then

$$f(z) = e^{g(z)}z^m \prod_{k\in\lambda} E_n(z/z_k)$$

for some polynomial $g(z)$ of degree at most n.

Proof. Set

$$G(z) := \frac{f(z)}{z^m\prod_{k\in\lambda} E_n(z/z_k)}.$$

Note that G has a removable singularity at $z=0$ because m is the order of the zero of f at $z=0$. Further, the infinite product in the denominator converges absolutely and uniformly on compacts to an entire function by Lemma B.18. As such, by Proposition A.25, it will vanish exactly on the z_k, so G has only removable singularities at the z_k.

In total, we can continue G to an entire function due to these removable singularities, and G will have no zeroes because all zeroes of the numerator $f(z)$ are correctly cancelled out by the denominator. Thus, Lemma A.16 promises us an entire function $g\colon\mathbb{C}\to\mathbb{C}$ such that $G = \exp\circ g$. Thus, we see

$$f(z) = e^{g(z)}z^m\prod_{k\in\lambda} E_n(z/z_k),$$

so it remains to show that g is a polynomial of degree at most n. We would like to use Proposition B.20 to finish, so we want to bound g.

Choose some $s\in(\rho_0, n+1)$ so that f has order bounded by s by Remark B.9. By Remark B.11, we see that $f(z)/z^m$ still has order bounded by s, so we can find constants $A,B>0$ such that

$$\left|\frac{f(z)}{z^m}\right| < Ae^{B|z|^s}.$$

Now, by Lemma B.19, there is an unbounded set $R\subseteq\mathbb{R}$ of positive real numbers and constant $c>0$ such that we can write

$$\left|\prod_{k\in\lambda} E_n(z/z_k)\right| \ge \exp\left(-c|z|^s\right)$$

if $|z| \in R$, so

$$|G(z)| = \left|\frac{f(z)}{z^m}\right| \cdot \left|\prod_{k\in\lambda} E_n(z/z_k)\right|^{-1} < Ae^{(B+c)|z|^s}.$$

However, $|G(z)| = |\exp(g(z))| = \exp(\operatorname{Re} g(z))$, so we see that

$$\operatorname{Re} g(z) \le \log A + (B+c)|z|^s$$

for $|z| \in R$. Replacing R with $R \cap (1,\infty)$ (which is an unbounded subset if R is unbounded), we may assume that $|z| > 1$, so actually

$$\operatorname{Re} g(z) \le (\log A)|z|^s + (B+c)|z|^s,$$

so Proposition B.20 now kicks in and tells us that $g(z)$ is a polynomial of degree less than or equal to s. Because $\lfloor s \rfloor = n$, this finishes. ■

APPENDIX C
FOURIER ANALYSIS

Ring around the rosie,
A pocket full of posies.
Ashes! Ashes!
We all fall down!

—"Ring Around the Rosie"

C.1 The Fourier Transform

It will pay off for us later to have established a little Fourier analysis right now. Our exposition follows [SS03b, Chapter 5].

Definition C.1 (Schwarz)**.** A function $f : \mathbb{R} \to \mathbb{C}$ is *Schwarz* if and only if f is infinitely differentiable and the nth derivative $f^{(n)}$ satisfies that the function $x^A \cdot f^{(n)}(x)$ is bounded for all nonnegative integers A.

Remark C.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 C.3. If $f : \mathbb{R} \to \mathbb{R}$ is Schwarz, we note that $\left|x^A f(x)\right|$ 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 $\left|x^k f(x)\right| \leq C$. Thus,

$$\int_{\mathbb{R}} \left|x^A f(x)\right| \, dx \leq \int_{[-1,1]} \left|x^A f(x)\right| \, dx + \int_{|x|\geq 1} \frac{C}{x^{A-k}} \, dx,$$

which is finite because $A - k < -2$.

Definition C.4 (Fourier transform)**.** Let $f : \mathbb{R} \to \mathbb{C}$ be a Schwarz function. Then we define the *Fourier transform* to be the function $\mathcal{F}f : \mathbb{R} \to \mathbb{C}$ given by

$$(\mathcal{F}f)(s) \coloneqq \int_{\mathbb{R}} f(x) e^{-2\pi i s x} \, dx.$$

Remark C.5. The integral converges because it absolutely converges: we note

$$\int_{\mathbb{R}} \left| f(x)e^{-2\pi isx} \right| \, dx = \int_{\mathbb{R}} |f(x)| \, dx$$

is finite by Remark C.3. In fact, this shows that $\mathcal{F}f$ is bounded.

We now run some quick checks on the Fourier transform.

Lemma C.6. Let $f : \mathbb{R} \to \mathbb{C}$ be a Schwartz function.

(a) For some $\lambda > 0$, define $f_\lambda(x) := f(\lambda x)$. Then $f_\lambda : \mathbb{R} \to \mathbb{C}$ is Schwartz, and $(\mathcal{F}f_\lambda)(s) = \frac{1}{\lambda}(\mathcal{F}f)\left(\frac{s}{\lambda}\right)$.

(b) For some $\alpha > 0$, define $f_\alpha(x) := f(x)e^{-2\pi i\alpha x}$. Then $(\mathcal{F}f_\alpha)(s) = (\mathcal{F}f)(s+\alpha)$.

(c) We have $(\mathcal{F}f')(s) = 2\pi is(\mathcal{F}f)(s)$.

(d) The function $\mathcal{F}f$ is differentiable, and $(\mathcal{F}f)'(s)$ is the Fourier transform of the function $g(x) := -2\pi ixf(x)$.

(e) 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) We quickly verify f_α is Schwarz; for brevity, define $e_\alpha : \mathbb{R} \to \mathbb{C}$ by $e_\alpha(x) := e^{-2\pi i\alpha x}$ so that $f_\alpha = fe_\alpha$. Note that induction on n yields $e_\alpha^{(n)}(x) = (-2\pi i\alpha)^n e^{-2\pi i\alpha x}$ so that

$$\left| e_\alpha^{(n)}(x) \right| = |2\pi\alpha|^n \left| e^{-2\pi i\alpha x} \right| = |2\pi\alpha|^n,$$

so these derivatives are suitably bounded, though e_α is not actually Schwarz. As such, because f is Schwarz, for any nonnegative integer A, we may find $M_{A,n}$ bounding $x^A \cdot f^{(n)}(x)$. Now, for any n, the product rule (used inductively) yields

$$\left| x^A \cdot (fe_\alpha)^{(n)}(x) \right| \leq \sum_{k=0}^{n} \left| x^A f^{(k)}(x) \right| \cdot \left| e_\alpha^{(n-k)}(x) \right| \leq \sum_{k=0}^{n} M_{A,k}|2\pi\alpha|^n,$$

so $x^A \cdot (fe_\alpha)^{(n)}(x)$ is in fact bounded, which is what we wanted.

It remains to compute the Fourier transform of f_α, which is a direct computation. Note

$$\begin{aligned}(\mathcal{F}f_\alpha)(s) &= \int_{\mathbb{R}} f_\alpha(x)e^{-2\pi isx}\,dx \\ &= \int_{\mathbb{R}} f(x)e^{-2\pi i\alpha x}e^{-2\pi sx}\,dx \\ &= \int_{\mathbb{R}} f(x)e^{-2\pi i(\alpha+s)x}\,dx \\ &= (\mathcal{F}f)(s+\alpha).\end{aligned}$$

(c) Note f' is Schwarz by Remark C.2, so the statement at least makes sense. Now, by integration by parts, we see

$$\begin{aligned}(\mathcal{F}f')(s) &= \int_{\mathbb{R}} f'(x)e^{-2\pi isx}\,dx \\ &= f(x)e^{-2\pi isx}\Big|_{-\infty}^{\infty} - \int_{\mathbb{R}} f(x)\left(2\pi ise^{-2\pi isx}\right)\,dx \\ &= 2\pi is(\mathcal{F}f)(s).\end{aligned}$$

To justify the last equality, we see that $f(x)e^{-2\pi isx} \to 0$ as $x \to \pm\infty$ because f is Schwarz: note $\left|f(x)e^{-2\pi isx}\right| = |f(x)|$, and $|xf(x)|$ is bounded, so there is a constant C such that $f(x) \le C/|x|$ for all $x \neq 0$, meaning that $|f(x)| \to 0$ as $x \to \pm\infty$.

(d) 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 $k, \ell \ge 0$, the function $|x|^k \left|g^{(k)}(x)\right|$ is a $\mathbb{C}$-linear combination of bounded functions because f is Schwarz, so it follows that $|x|^k \left|g^{(\ell)}(x)\right|$ is bounded, so g is Schwarz.

The rest of the proof is a direct computation. For $t, t' \in \mathbb{R}$, we see

$$\int_t^{t'} (\mathcal{F}g)(s)\,ds = \int_t^{t'} \left(\int_{\mathbb{R}} -2\pi ixf(x)e^{-2\pi isx}\,dx\right)\,ds.$$

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 C.3, so

$$\int_t^{t'} \left(\int_{\mathbb{R}} \left|-2\pi ixf(x)e^{-2\pi isx}\right|\,dx\right)\,ds \le 2\pi|t'-t|\int_{\mathbb{R}} |xf(x)|\,dx < \infty.$$

Thus, we may write

$$\begin{aligned}\int_t^{t'} (\mathcal{F}g)(s)\,ds &= \int_{\mathbb{R}} \left(\int_t^{t'} -2\pi ixf(x)e^{-2\pi isx}\,ds\right)\,dx \\ &= \int_{\mathbb{R}} f(x)\left(e^{-2\pi it'x} - e^{-2\pi itx}\right)\,dx \\ &= (\mathcal{F}f)(t') - (\mathcal{F}f)(t).\end{aligned}$$

Thus, by the Fundamental theorem of calculus, we see

$$(\mathcal{F}f)'(t) = \lim_{t'\to t} \frac{(\mathcal{F}f)(t') - (\mathcal{F}f)(t)}{t'-t} = \lim_{t'\to t}\left(\frac{1}{t'-t}\int_t^{t'} (\mathcal{F}g)(s)\,ds\right) = (\mathcal{F}g)(t).$$

(e) By Remark C.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

$$x \mapsto \frac{1}{(2\pi i)^k}\left(\frac{d}{dx'}\right)^{(k)}\left((-2\pi ix')^\ell f(x')\right)\Big|_{x'=x}$$

by combining (b) and (c). This completes the proof. ∎

As an application, we can compute the Fourier transform of the Gaussian.

Exercise C.7 (Gaussian). Define $g\colon \mathbb{R} \to \mathbb{R}$ by $g(x) \coloneqq e^{-\pi x^2}$. 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 C.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 $f(x) \coloneqq (\mathcal{F}g)(x)e^{\pi x^2}$ 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 $(\mathcal{F}g)(x) = ae^{-\pi x^2}$ 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

$$\begin{aligned}(\mathcal{F}g)(0)^2 &= \left(\int_{\mathbb{R}} e^{-\pi x^2}\,dx\right)^2 \\ &= \int_{\mathbb{R}}\int_{\mathbb{R}} e^{-\pi\left(x^2+y^2\right)}\,dx\,dy \\ &= \int_0^{2\pi}\int_0^{\infty} e^{-\pi r^2}\,r\,dr\,d\theta \\ &= \int_0^{2\pi} \frac{1}{2\pi}\,d\theta \\ &= 1.\end{aligned}$$

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 $x \in \mathbb{R}$. ∎

C.2 Fourier Inversion

The goal of this subsection is to prove the Fourier inversion theorem; we continue to roughly follow [SS03b, Chapter 5]. Roughly speaking, this will follow from understanding the Gaussian. Here are the necessary tools.

Lemma C.8. Define the Gaussian $g\colon \mathbb{R} \to \mathbb{R}$ by $g(x) \coloneqq e^{-\pi x^2}$. For any $\delta > 0$, we have

$$\lim_{\varepsilon \to 0^+} \frac{1}{\varepsilon}\int_{|t|\geq\delta} g(t/\varepsilon)\,dt = 0.$$

Proof. Changing variables, we see

$$\lim_{\varepsilon\to 0^+}\int_{|t|\geq\delta} g(t/\varepsilon) = \lim_{\varepsilon\to 0^+}\int_{|t|\geq\delta/\varepsilon} g(t)\,dt = \lim_{N\to\infty}\int_{|t|\geq N} g(t)\,dt,$$

where $N = \delta/\varepsilon$ in the last equality. However, g is Schwarz by Exercise C.7, so $\int_{\mathbb{R}} g(t)\,dt$ is finite by Remark C.3, so

$$\lim_{N\to\infty} \int_{|t|\le N} g(t)\,dt = \int_{\mathbb{R}} g(t)\,dt.$$

Rearranging, we see

$$\lim_{N\to\infty} \int_{|t|\ge N} g(t)\,dt = 0,$$

which is what we wanted. ∎

Lemma C.9. Define the Gaussian $g\colon \mathbb{R}\to\mathbb{R}$ by $g(x) \coloneqq e^{-\pi x^2}$. For any bounded and continuous function $f\colon \mathbb{R}\to\mathbb{R}$, we have

$$f(0) = \lim_{\varepsilon\to 0^+} \frac{1}{\varepsilon}\int_{\mathbb{R}} f(t)g(t/\varepsilon)\,dt.$$

Proof. The point here is that, for any $\varepsilon > 0$, we have

$$\frac{1}{\varepsilon}\int_{\mathbb{R}} g(t/\varepsilon)\,dt = \int_{\mathbb{R}} g(t)\,dt = (\mathcal{F}g)(0) = g(0) = 1 \tag{C.1}$$

by Exercise C.7. However, the functions $t\mapsto g(t/\varepsilon)$ concentrate at $t=0$ as $\varepsilon\to 0^+$, 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 $|f(x)|\le M_f$ for each $x\in\mathbb{R}$, which gives

$$\int_{\mathbb{R}} |f(t)g(t/\varepsilon)|\,dt \le M_f\int_{\mathbb{R}} g(t/\varepsilon)\,dt = \varepsilon M_f,$$

where we have used (C.1).

We now proceed with the proof, which is somewhat technical. For psychological reasons, we set $h(x) \coloneqq f(x) - f(0)$ 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 (C.1) in the last equality, so it suffices to show

$$\lim_{\varepsilon\to 0^+}\frac{1}{\varepsilon}\int_{\mathbb{R}} h(t)g(t/\varepsilon)\,dt \stackrel{?}{=} 0.$$

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 $M_h \ge 0$ such that $|h(t)| < M_h$ for all t. Thus, we upper-bound

$$\begin{aligned}
\left|\frac{1}{\varepsilon}\int_{\mathbb{R}} h(t)g(t/\varepsilon)\,dt\right| &\le \frac{1}{\varepsilon}\int_{|t|\le\delta_0} |h(t)g(t/\varepsilon)|\,dt + \frac{1}{\varepsilon}\int_{|t|\ge\delta_0} |h(t)g(t/\varepsilon)|\,dt \\
&\le \frac{\delta}{\varepsilon}\int_{|t|\le\delta_0} g(t/\varepsilon)\,dt + \frac{M_h}{\varepsilon}\int_{|t|\ge\delta_0} g(t/\varepsilon)\,dt \\
&\le \frac{\delta}{\varepsilon}\int_{\mathbb{R}} g(t/\varepsilon)\,dt + \frac{M_h}{\varepsilon}\int_{|t|\ge\delta_0} g(t/\varepsilon)\,dt \\
&= \delta + \frac{M_h}{\varepsilon}\int_{|t|\ge\delta_0} g(t/\varepsilon)\,dt.
\end{aligned}$$

(As usual, we have used (C.1) in the last equality.) Thus, using Lemma C.8, sending $\varepsilon \to 0^+$ shows that

$$\lim_{\varepsilon \to 0^+} \left| \frac{1}{\varepsilon} \int_{\mathbb{R}} h(t) g(t/\varepsilon)\, dt \right| \le \delta$$

for any $\delta > 0$, so sending $\delta \to 0^+$ completes the proof. ∎

And here is our main attraction.

Theorem C.10 (Fourier inversion)**.** Let $f : \mathbb{R} \to \mathbb{R}$ 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

$$f_\varepsilon(x) \coloneqq \int_{\mathbb{R}} \int_{\mathbb{R}} f(t) e^{2\pi i (x-t) s} e^{-\pi \varepsilon^2 s^2}\, dt ds.$$

Notably, we expect $f_\varepsilon(x) \to \int_{\mathbb{R}} (\mathcal{F}f)(s) e^{2\pi i x s}\, ds$ as $\varepsilon \to 0^+$. As such, we compute the behavior of $\varepsilon \to 0^+$ in two ways.

- We integrate over dt first. Namely, we would like to send $\varepsilon \to 0^+$, for which we use the Dominated convergence theorem. For each $\varepsilon > 0$, note that we have the bound

  $$\left| \int_{\mathbb{R}} f(t) e^{2\pi i (x-t) s} e^{-\pi \varepsilon^2 s^2}\, dt \right| \le e^{-\pi \varepsilon^2 s^2} \int_{\mathbb{R}} |f(t)|\, dt.$$

  Now, $s \mapsto e^{-\pi \varepsilon^2 s^2}$ is Schwarz by Exercise C.7 (combined with (a) of Lemma C.6), so we may integrate the right-hand function over all $s \in \mathbb{R}$ by Remark C.3.

  Thus, our integrand in $f_\varepsilon(x)$ is dominated by an integrable function, so the Dominated convergence theorem implies

  $$\lim_{\varepsilon \to 0^+} f_\varepsilon(x) = \int_{\mathbb{R}} \left(\lim_{\varepsilon \to 0^+} e^{-\pi \varepsilon^2 s^2} \int_{\mathbb{R}} f(x) e^{2\pi i (x-t)}\, dt \right) ds = \int_{\mathbb{R}} (\mathcal{F}f)(s) e^{2\pi i x s}\, ds.$$

- We integrate over ds first. As such, we begin by justifying our application of Fubini's theorem: checking for absolute convergence, we compute

  $$\int_{\mathbb{R}} \int_{\mathbb{R}} \left| f(t) e^{2\pi i (x-t) s} e^{-\pi \varepsilon^2 s^2} \right| dt ds = \left(\int_{\mathbb{R}} |f(t)|\, dt \right) \left(\int_{\mathbb{R}} e^{-\pi \varepsilon^2 s^2}\, ds \right).$$

  Now, f is Schwarz by hypothesis, as is $s \mapsto e^{-\pi \varepsilon^2 s^2}$ by Exercise C.7, so both of these integrals are finite by Remark C.3.

Thus, we may switch the order of our integration. Setting up notation, we let $g(x) \coloneqq e^{-\pi x^2}$ denote the Gaussian (so that $(\mathcal{F}g)(s) = g(s)$ for all $s \in \mathbb{R}$) and $g_\varepsilon(x) \coloneqq g(\varepsilon x)$. Then we see

$$\begin{aligned} f_\varepsilon(x) &= \int_{\mathbb{R}} \int_{\mathbb{R}} f(t) e^{2\pi i(x-t)s} e^{-\pi \varepsilon^2 s^2} \, ds dt \\ &= \int_{\mathbb{R}} f(t) \left(\int_{\mathbb{R}} e^{-\pi(\varepsilon s)^2} e^{-2\pi i(t-x)} \, ds \right) dt \\ &= \int_{\mathbb{R}} f(t) (\mathcal{F} g_\varepsilon)(t-x) dt \\ &\overset{*}{=} \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t) g\left(\frac{t-x}{\varepsilon} \right) dt \\ &= \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t+x) g\left(t/\varepsilon\right) dt, \end{aligned}$$

where we have used part (a) of Lemma C.6 at $\overset{*}{=}$. Sending $\varepsilon \to 0^+$, Lemma C.9 tells us that

$$f(x) = \lim_{\varepsilon \to 0^+} \frac{1}{\varepsilon} \int_{\mathbb{R}} f(t+x) g(t/\varepsilon) \, dt = \lim_{\varepsilon \to 0^+} f_\varepsilon(x).$$

Combining the above two computations completes the proof. ∎

C.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 [SS03b, Chapter 2].

The idea here is that the functions $e_n \colon x \mapsto e^{2\pi i n x}$ for $n \in \mathbb{Z}$ form an orthonormal set of continuous functions $\mathbb{R} \to \mathbb{C}$, where our (Hermitian) inner product is given by

$$\langle f, g \rangle \coloneqq \frac{1}{2\pi i} \int_0^1 f(x) \overline{g(x)} \, dx.$$

Indeed, for any $n, m \in \mathbb{Z}$, we see

$$\langle e_n, e_m \rangle = \int_0^1 e^{2\pi i n x} \overline{e^{2\pi i m x}} \, dx = \int_0^1 e^{2\pi i (m-n) x} \, dx = \begin{cases} 1 & \text{if } m = n, \\ 0 & \text{if } m \neq n. \end{cases} \tag{C.2}$$

Now, the functions e_n are varied enough that we might hope that all sufficiently smooth 1-periodic functions $f \colon \mathbb{R} \to \mathbb{C}$ 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 $a_n \in \mathbb{Z}$. Thus, we might hope we can extract out the nth 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 C.11 (Fourier coefficient)**.** Fix a continuous 1-periodic function $f \colon \mathbb{R} \to \mathbb{C}$. Then we define the *$n$th Fourier coefficient* as

$$a_n(f) \coloneqq \int_0^1 f(x) e^{-2\pi i n x} \, dx.$$

Remark C.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 $|f(x)| \le M$ for $x \in [0,1]$, which implies

$$|a_n(f)| \le \int_0^1 \left|f(x)e^{-2\pi inx}\right| \, dx \le M \int_0^1 dx = M.$$

Of course, one can weaken the requirement that f be continuous, but we will have no need for these levels of generality.

Remark C.13. In fact, we note

$$a_n(f) = \int_t^{t+1} f(x)e^{2\pi inx} \, dx$$

for any $t \in \mathbb{R}$. Because $x \mapsto f(x)e^{2\pi inx}$ is 1-periodic, it suffices to show this for $t \in [0,1)$. Then the integral over $[t, t+1) = [t,1) \sqcup [1, 1+t)$ 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 C.14. Fix continuous 1-periodic functions $f, g \colon \mathbb{R} \to \mathbb{C}$.

(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 $a_n(\overline{f}) = \overline{a_{-n}(f)}$.

(c) Given $x_0 \in \mathbb{R}$, define $g(x) \coloneqq f(x + x_0)$. Then $a_n(g) = e^{-2\pi inx_0} a_n(f)$.

Proof. Here we go.

(a) This follows from the fact that $\langle \cdot, \cdot \rangle$ is an inner product. Indeed,

$$a_n(zf + wg) = z \int_0^1 f(x)e^{-2\pi inx} \, dx + w \int_0^1 g(x)e^{-2\pi inx} \, dx = za_n(f) + wa_n(g).$$

(b) We compute

$$a_n(\overline{f}) = \int_0^1 \overline{f(x)}e^{-2\pi inx} \, dx = \overline{\int_0^1 f(x)e^{2\pi inx} \, dx} = \overline{a_{-n}(f)}.$$

(c) We compute

$$a_n(g) = \int_0^1 f(x + x_0)e^{2\pi inx} \, dx = e^{-2\pi inx_0} \int_0^1 f(x + x_0)e^{2\pi in(x+x_0)} \, dx = e^{-2\pi inx_0} a_n(f),$$

where the last inequality used Remark C.13. ∎

Here is a slightly harder computation, still akin to Lemma C.6.

Lemma C.15. Fix a continuously differentiable 1-periodic function $f \colon \mathbb{R} \to \mathbb{C}$. For $n \neq 0$, we have

$$a_n(f') = -2\pi ina_n(f).$$

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

$$\begin{aligned} a_n(f') &= \int_0^1 f'(x)e^{-2\pi inx}\,dx \\ &= \frac{f(x)e^{-2\pi inx}}{-2\pi in}\bigg|_0^1 - \frac{1}{-2\pi in}\int_0^1 f(x)e^{-2\pi inx}\,dx \\ &= 0 + \frac{1}{2\pi in}\cdot a_n(f), \end{aligned}$$

which is what we wanted. ∎

The following is our key result.

Lemma C.16. Fix a continuous 1-periodic function $f\colon \mathbb{R}\to\mathbb{R}$ such that $f(0)\neq 0$. Then $a_n(f)\neq 0$ for some $n\in\mathbb{Z}$.

Proof. Define the function $p\colon \mathbb{R}\to\mathbb{C}$ by $p(x) \coloneqq e^{-2\pi inx}$. Roughly speaking, the idea is that $a_n(f)=0$ for all $n\in\mathbb{Z}$ implies that any "polynomial in p" named $q\in\mathbb{C}\left[p,p^{-1}\right]$ written as

$$q \coloneqq \sum_{n\in\mathbb{Z}} q_n p^n,$$

where all but finitely many of the q_n vanish, will have

$$\int_{-1/2}^{1/2} f(x)q(x)\,dx = \sum_{n\in\mathbb{Z}}\left(q_n\int_{-1/2}^{1/2} f(x)e^{2\pi inx}\,dx\right) = \sum_{n\in\mathbb{Z}} q_n a_n(f) = 0$$

by Remark C.13. Indeed, we will be able to build a function $q\in\mathbb{C}\left[p,p^{-1}\right]$ 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 $|f(x)|\le M_f$ for all $x\in[-1/2,1/2]$.

2. Because f is continuous, we may find $\delta_f>0$ such that $|f(x)-1|\le 1/2$ for $|x|<\delta_f$. In particular, we see $f(x)\ge 1/2$ for $|x|<\delta_f$. By making δ_f smaller if necessary, we will enforce $\delta_f\le 1/4$.

3. Now, define $q_1(x)\coloneqq 2\varepsilon + p(x) + p(x)^{-1} = 2\varepsilon+\cos(2\pi x)$, for $\varepsilon\coloneqq\frac{2}{3}(1-\cos(2\pi\delta_f))$. Note $\cos(2\pi x)$ is decreasing in the region in $[\delta_f,1/2]$, so in fact

   $$\varepsilon \le \frac{1}{3}(1-\cos(2\pi x))$$

   for $x\in[\delta_f,1/2]$. Rearranging, we see

   $$q_1(x) = 2\varepsilon+\cos(2\pi x)\le 1-\varepsilon$$

   for $x\in[\delta_f,1/2]$. In fact, because $q_1(x)\ge -1+2\varepsilon$, we see that $|q_1(x)|\le 1-\varepsilon$ 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 $|q_1(x)-q_1(0)|\le\varepsilon$ for $|x|<\delta_q$. In particular, $q_1(x)\ge 1-\varepsilon$ 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 $q_N \coloneqq q_1^N$ for $N \in \mathbb{N}$. (Notably, $q_1 = q_1^1$.) The point is that $k \to \infty$ 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 C.13, we compute

$$\begin{aligned}\int_{-1/2}^{1/2} f(x)q_N(x)\,dx &= \int_{|x|\le\delta_q} f(x)q_N(x)\,dx + \int_{\delta_q\le|x|\le\delta_f} f(x)q_N(x)\,dx + \int_{\delta_f\le|x|\le 1/2} f(x)q_N(x)\,dx \\ &\ge 2\delta_q\cdot\frac{1}{2}(1+\varepsilon)^N + 2(\delta_f-\delta_q)\cdot\frac{1}{2}\cdot 0 - 2\left(\frac{1}{2}-\delta_f\right)B(1-\varepsilon)^N \\ &\ge \delta_q(1+\varepsilon)^N - \delta_f B(1-\varepsilon)^N.\end{aligned}$$

Thus, as $N\to\infty$, 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

$$q_N = \left(2\varepsilon + p + p^{-1}\right)^N = \sum_{n=-N}^{N} q_{N,n}p^n$$

for some coefficients $q_{N,n}\in\mathbb{R}$. Thus,

$$0 < \int_{-1/2}^{1/2} f(x)q_N(x)\,dx = \sum_{n=-N}^{N}\left(q_{N,n}\int_{-1/2}^{1/2} f(x)e^{-2\pi inx}\,dx\right) = \sum_{n=-N}^{N} q_{N,n}a_n(f),$$

where we have used Remark C.13. Thus, there exists n with $|n|\le N$ such that $a_n(f)\neq 0$. ∎

Proposition C.17. Fix a continuous 1-periodic function $f\colon\mathbb{R}\to\mathbb{C}$ 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 C.16 and the following reductions.

- It suffices to show the result for real-valued functions f. Indeed, we may write $f(x)\coloneqq u(x)+iv(x)$ for some real-valued, continuous, and 1-periodic functions $u,v\colon\mathbb{R}\to\mathbb{R}$. (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 C.14 to see

  $$a_n(u) = a_n\left(\frac{f+\overline{f}}{2}\right) = \frac{1}{2}\left(a_n(f) + \overline{a_{-n}(f)}\right) = 0,$$

  and

  $$a_n(v) = a_n\left(\frac{f-\overline{f}}{2i}\right) = \frac{1}{2i}\left(a_n(f) - \overline{a_{-n}(f)}\right) = 0.$$

  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 C.16. Indeed, for some fixed $x_0\in\mathbb{R}$, we define $g(x)\coloneqq f(x+x_0)$. Note g is still continuous and 1-periodic. Further, Lemma C.14 tells us that $a_n(g) = e^{2\pi inx_0}a_n(f) = 0$ for each $n\in\mathbb{Z}$. Thus, Lemma C.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.

C.4 Fourier Series

Now that we have our coefficients, we can define our Fourier series. We continue to follow [SS03b, Chapter 2].

Definition C.18 (Fourier series)**.** Fix a continuous 1-periodic function $f\colon \mathbb{R} \to \mathbb{C}$. Then we define the Nth partial sum of the *Fourier series* of f as

$$S_{f,N}(x) \coloneqq \sum_{n=-N}^{N} a_n(f) e^{2\pi i n x}.$$

The *Fourier series* is defined as $S_f(x) \coloneqq \lim_{N\to\infty} S_{f,N}(x)$, 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 C.19. Fix a twice continuously differentiable 1-periodic function $f\colon \mathbb{R} \to \mathbb{C}$. Then the series $S_f(x)$ converges absolutely and uniformly.

Proof. This follows from Lemma C.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 C.12 grants $M \in \mathbb{R}$ such that $|a_n(f'')| \leq M$, so it follows that $|a_n(f)| \leq M/\left(4\pi^2 n^2\right)$ for $n \neq 0$. Thus, we see the series S_f converges absolutely because

$$\sum_{n\in\mathbb{Z}} \left|a_n(f) e^{2\pi i n x}\right| \leq a_0(f) + \frac{2M}{4\pi^2} \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty$$

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 $N \to \infty$. ∎

And in this situation, we can show that our Fourier series is well-behaved.

Theorem C.20. Fix a continuous 1-periodic function $f\colon \mathbb{R} \to \mathbb{C}$. 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 C.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

$$S_f(x+1) = \lim_{N\to\infty} \sum_{n=-N}^{N} a_n(f) e^{2\pi i n(x+1)} = \lim_{N\to\infty} \sum_{n=-N}^{N} a_n(f) e^{2\pi i n x} = S_f(x).$$

Thus, we are allowed to compute the Fourier coefficients

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

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

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

which converges because $S_f(0)$ converges absolutely by hypothesis. Thus, Fubini's theorem lets us write

$$a_n(S_f) = \sum_{m \in \mathbb{Z}} \left(\int_0^1 a_n(f) e^{2\pi i (m-n)x} \, dx \right) = a_n(f),$$

where we have used (C.2) in the last equality. To finish the proof, we note $a_n(S_f - f) = 0$ by Lemma C.14. As such, $S_f - f = 0$ by Proposition C.17, which finishes the proof. ■

BIBLIOGRAPHY

[Che60] Chubby Checker. *The Twist*. 1960. URL: https://www.youtube.com/watch?v=HLrxaNOuHyw.

[Dav80] Harold Davenport. *Multiplicative number theory*. eng. Second Edition. Vol. 74. Graduate Texts in Mathematics. New York, NY: Springer, 1980. ISBN: 9781475759297.

[Rot85] Gian-Carlo Rota. "Mathematics, Philosophy and Artificial Intelligence". In: *Los Alamos Science* 12 (1985).

[Mat01] Lutz Mattner. "Complex differentiation under the integral". In: *Nieuw Archief voor Wiskunde* 2.1 (2001), pp. 32–35.

[SS03a] Elias M. Stein and Rami Shakarchi. *Complex Analysis*. Vol. 2. Princeton University Press, 2003.

[SS03b] 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.

[Gre20] Hank Green. *A Beautifully Foolish Endeavour*. Dutton Books, 2020.

[Elb22] Nir Elber. *Introduction to Complex Analysis*. 2022. URL: https://dfoiler.github.io/notes/185/notes.pdf.

[Mer23] Merriam-Webster. *Hop, Skip, and Jump*. 2023. URL: https://www.merriam-webster.com/dictionary/hop%2C%20skip%2C%20and%20jump.

List of Definitions

absolutely converges, 147

binary quadratic form, 30

character, 10
conductor, 75, 91

decaying, 25
Dirichlet L-function, 15
Dirichlet character, 15
Dirichlet convolution, 23
discriminant, 31
dual group, 10

elementary factor, 158
equivalent, 30
Euler–Mascheroni constant, 17

Fourier coefficient, 172
Fourier series, 176
Fourier transform, 166

Γ, 53
Gauss sum, 76

holomorphic, 141

hyperelliptic curve, 96

imprimitive, 91
induces, 91

Jacobi, 89

Legendre symbol, 73

Mellin transform, 25
μ, 103
multiplicative, 7

order, 155

partition, 114
path integral, 142
primitive, 75, 85

quadratic residue, 73

Schwarz, 166
smooth, 138

ξ, 55