These are notes for an ongoing Fall 2023 course on the Riemann zeta function and its generalizations, L-functions, taught with Sergey Arkhipov. These notes will be filled in as we go.

1. References thus far

- Generating functions and asymptotics: [6, §5.2]
- Mellin transform and asymptotics: [7]
- Zeros of zeta and the prime number theorem: [1], [3], Tao's notes

2. Outlines thus far

(Some links here refer to external files; I'll have to think of a good way to notate that.)

- Tuesday, 29 Aug: parts of §5; §1, §2
- Thursday, 31 Aug: §3, §4
- Friday, 1 Sep: §5 and §6
- Tuesday, 5 Sep: §6
- Thursday, 7 Sep: §6.2, §2.1
- Tuesday, 12 Sep and Thursday, 14 Sep: Fourier transform, Pontryagin duality, Poisson summation (see these notes and the book [2])
- Tuesday, 19 Sep: Euler products, relevance of zeta zeros to asymptotics §6.3
- Thursday, 21 Sep: harmonic functions (external §5), approximate factorizations of holomorphic functions (external §6), crude control over zeta zeros (§6.5)
- Tuesday, Thursday and Friday, 26–29 Sep: Sergey's lectures concerning zeroes of zeta on or near the 1-line. References:
  - [5, Chapter III], up through 3.6,
  - [1, Chapter 13], and
  - part 3 of https://terrytao.wordpress.com/2014/12/09/254a-notes-2-complex-analytic-multiplicative-number-theory/.
- Tuesday, 3 October: contour shifting, especially Proposition 6.13
- Thursday, 5 October: deduction of the prime number theorem, §6.8
- Tuesday, 10 October: Dirichlet characters (start of §7)
- Thursday, 12 October: basics on Dirichlet L-functions (more of §7)

3. Possible exam topics

(1) Beurling primes. [**?**].
(2) Infinite product formula for the zeta function. [1, §12]. Can also learn more general factorization theorem of holomorphic functions, see for instance [**?**].
(3) Quantitative form of the prime number theorem. [1, §18, 20–22].
(4) Asymptotics for the number of zeros in a given region. [1, §15–16].
(5) Pontryagin duality and related aspects of the Fourier transform, even in the setting of groups related to $\mathbb{R}$, or discrete groups. See for instance [4, §3].
(6) Exponential sums over primes: [1, §24–25].
(7) Sums of three primes: [1, §26]
(8) Bombieri–Vinogradov theorem: [1, §27–28].

(9) Class number formula and related topics, e.g., class number one problem of Gauss.
(10) Function field analogues of L-functions.
(11) Dedekind zeta functions and their factorizations.
(12) More on the functional equation for zeta and L. Stirling asymptotics for Γ.
(13) The perspective of Tate's thesis and Weil's interpretation, with local and global functional equations (optionally, with adeles).
(14) p-adic interpolation of L-functions.

4. Course notes that I've since split off into separate files

- Complex-analytic preliminaries
- Generating functions and asymptotics
- Fourier and Mellin transforms
- Bernoulli numbers and Euler–Maclaurin summation

5. Background

5.1. **General notation.** $\mathbb{R}^+ := (0, \infty)$.

5.2. **Asymptotic notation.** We use the equivalent notations

$$A = \mathrm{O}(B), \qquad A \ll B, \qquad B \gg A$$

to denote that

$$|A| \leq C|B|$$

for some "constant" C. The precise meaning of "constant" will either be specified or clear from context.

5.3. **Definition and basic properties of ζ: overview.** The Riemann zeta function is defined for a complex number s by the series

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$

Lemma 5.1. *The series converges absolutely for $\Re(s) > 1$, uniformly for $\Re(s) \geq 1+\varepsilon$ for each $\varepsilon > 0$.*

Proof. Using the identity

$$\left| \frac{1}{n^s} \right| = \frac{1}{n^{\Re(s)}},$$

we reduce to the case that s is real, in which this is a familiar consequence of the integral test. □

Our first main goal in the course is to explain the following basic facts.

Theorem 5.2. *The Riemann zeta function admits a meromorphic continuation to the entire complex plane. It is holomorphic away from a simple pole at $s = 1$, where it has residue 1. It admits a functional equation relating $\zeta(s)$ to $\zeta(1 - s)$.*

One historical motivation for considering the zeta function at complex arguments comes from the prime number theorem.

Theorem 5.3 (Prime number theorem)**.** *Let $\pi(x) := \#\{\text{primes } p \leq x\}$ denote the prime counting function. Then*

$$\frac{\pi(x)}{x/\log x} \to 1 \text{ as } x \to \infty.$$

This is related to the following analytic fact concerning the zeros of the zeta function.

Theorem 5.4 (Prime number theorem, formulated in terms of ζ)**.** *We have $\zeta(s) = 0$ only if $\Re(s) < 1$.*

Remark 5.5. Even the statement of Theorem 5.4 is not clear without knowing the meromorphic continuation of ζ. This may offer some motivation for understanding the latter.

We expect stronger nonvanishing properties:

Conjecture 1 (Riemann Hypothesis)**.** *We have $\zeta(s) = 0$ only if $\Re(s) < 1/2$.*

This corresponds to a conjectural stronger form of the prime number theorem, namely that

$$\pi(x) = \int_2^x \frac{t}{\log t}\, dt + \mathrm{O}(x^{1/2} \log x).$$

6. Basic analytic properties of ζ

6.1. **Meromorphic continuation and evaluation at negative integers.** Take

$$h(y) = \frac{1}{e^y - 1}.$$

The function $yh(y)$ extends to a holomorphic function of y on the disc $\{y \in \mathbb{C} : |y| < 2\pi\}$, so h is represented for small $y > 0$ by an absolutely convergent Laurent series of the following form:

$$h(y) = \frac{1}{y} + \sum_{n=1}^{\infty} \frac{B_n}{n!} y^{n-1}.$$

Here the B_n are complex coefficients, called the *Bernoulli numbers* (see this note). On the other hand, h decays rapidly (like $\mathrm{O}(y^N)$ for any fixed N) as $y \to \infty$. By the analysis we've now seen many times, we deduce that the Mellin transform $H(s)$ of $h(y)$ converges absolutely for $\Re(s) > 1$, where it defines a holomorphic function, and extends to a meromorphic function on the complex plane whose only poles are simple poles at $s = 1$ (corresponding to the $1/y$ term in the asymptotic expansion as $y \to 0$) and at $s = -n$ for each $n \in \mathbb{Z}_{\geq 0}$, with residue given by 1 in the former case and by $B_{n+1}/(n+!)!$ in the latter.

On the other hand, we can rewrite

$$h(y) = \frac{e^{-y}}{1 - e^{-y}} = e^{-y} + e^{-2y} + e^{-3y} + \cdots,$$

giving

$$H(s) = \int_{\mathbb{R}^+} y^s \sum_{n=1}^{\infty} e^{-ny}\, d^\times y.$$

The following calculations will show that the doubly integral/sum converges absolutely for $\Re(s) > 1$, so we may rearrange it as

$$\sum_{n=1}^{\infty} \int_{\mathbb{R}^+} y^s e^{-ny}\, d^\times y.$$

The inner integral may be simplified by the substitution $y \mapsto y/n$. This has no effect on the measure $d^\times y$, but replaces y^s by $n^{-s} y^s$, giving

$$\sum_{n=1}^{\infty} n^{-s} \int_{\mathbb{R}^+} y^s e^{-y}\, d^\times y = \zeta(s)\Gamma(s).$$

We see in this way that the ζ function admits a meromorphic continuation. Since the Γ-function does not vanish, we deduce that the only pole of ζ is the simple one at $s = 1$, with residue $s = 0$. Also, since we have computed the residues of both $\Gamma(s)$ and $\zeta(s)\Gamma(s)$ at the nonpositive integers, we may calculate in this way the values of $\zeta(-n)$ for each $n \in \mathbb{Z}_{\geq 0}$:

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}.$$

6.2. **Another perspective on the meromorphic continuation.** (TODO: think of better section titles)

Given $f : \mathbb{R} \to \mathbb{C}$ of sufficient decay at infinity, we define $g : \mathbb{R}^+ \to \mathbb{C}$ by

$$g(y) := \sum_{n \in \mathbb{Z}} f(ny).$$

We assume henceforth that f lies in the Schwartz space $\mathcal{S}(\mathbb{R})$.

The asymptotics of $g(y)$ are described as follows.

Lemma 6.1. *Let $f \in \mathcal{S}(R)$.*

(1) As $y \to \infty$, we have

$$g(y) = f(0) + \mathrm{O}(y^{-N}) \tag{6.1}$$

for each fixed N.

(2) As $y \to 0$, we have

$$g(y) = y^{-1} \int_{\mathbb{R}} f(x)\, dx + \mathrm{O}(y^N) \tag{6.2}$$

for each fixed N.

Proof. The first estimate (6.1) is an easy exercise using the definition of the Schwartz space. The second estimate (6.2) may be proved either via Euler–Maclaurin summation (see external §2.1) or Poisson summation (see external §**??**). □

Assuming that $f(0)$ and $\int f$ are nonzero, it follows that the Mellin transform of g does not converge absolutely at any point. We can still define a regularized Mellin transform

$$G(s) = \int_{\mathbb{R}^+}^{\mathrm{reg}} y^s g(y)\, d^\times y,$$

like in §4, by splitting the integral into two pieces (e.g, the contributions of $(0, 1)$ and $(1, \infty)$), meromorphically continuing each piece, and then summing the results on their domain of overlap (if any).

Lemma 6.2. *$G(s)$ defines a meromorphic function on the complex plane whose only poles at simple ones:*

- *at $s = 0$, with residue $-f(0)$, and*
- *at $s = 1$, with residue $\int_{\mathbb{R}} f(x)\, dx$.*

Proof. Let's carry this out in detail, applying the recipe of external §2.

- We see from (6.1) that the integral

$$G_+(s) := \int_1^\infty y^s g(y)\, d^\times y$$

converges absolutely for $\Re(s) < 0$ and extends to a meromorphic function of s, whose only pole is a simple pole at $s = 0$ of residue $-f(0)$. Indeed,

$$G_+(s) = \int_1^\infty y^s \left(g(y) - f(0)\right)\, d^\times y + f(0) \underbrace{\int_1^\infty y^s\, d^\times y}_{-1/s},$$

where the first integral on the right hand side converges absolutely for all s.

- We see from (6.2) that the integral
$$G_-(s) := \int_0^1 y^s g(y)\, d^\times y$$
converges absolutely for $\Re(s) > 1$ and extends to a meromorphic function of s, whose only pole is a simple pole at $s = 1$ of residue I_f, where $I_f := \int_{\mathbb{R}} f(x)\, dx$. Indeed,
$$G_-(s) = \int_0^1 y^s \left(g(y) - y^{-1} I_f\right)\, d^\times y + I_f \underbrace{\int_0^1 y^{s-1}\, d^\times y}_{1/(s-1)}.$$

□

We denote henceforth by $\mathcal{F}f$ the (normalized) Fourier transform
$$\mathcal{F}f(\xi) := \int_{x\in\mathbb{R}} f(x) e^{-2\pi i x\xi}\, dx.$$

Lemma 6.3. *Write $G(s) = G_f(s)$ to indicate the dependence upon f. Then we have the following functional equation:*
$$G_f(s) = G_{\mathcal{F}f}(1-s).$$

Proof. This is a consequence of the Poisson summation formula (see external (**??**))
$$\sum_{n\in\mathbb{Z}} f(ny) = y^{-1} \sum_{n\in\mathbb{Z}} \mathcal{F}f(n/y).$$
Writing g_f to indicate the dependence of g upon f, the above identity reads
$$g_f(y) = y^{-1} g_{\mathcal{F}f}(1/y).$$
Taking the (regularized) Mellin transform of both sides yields
$$G_f(s) = \int_{\mathbb{R}^+}^{\mathrm{reg}} y^{s-1} g_{\mathcal{F}f}(1/y)\, d^\times y.$$
To evaluate this last integral, we substitute $y \mapsto 1/y$, which leaves the measure $d^\times y$ invariant (and is unaffected by the regularization). This gives
$$G_f(s) = \int_{\mathbb{R}^+}^{\mathrm{reg}} y^{1-s} g_{\mathcal{F}f}(y)\, d^\times y = G_{\mathcal{F}f}(1-s),$$
as required. □

We suppose henceforth that f is even. This is without much loss of generality – any function can be written as a sum of even and odd functions, and if f is odd, then g vanishes identically.

Exercise 1. Let $f \in \mathcal{S}(\mathbb{R})$ be even. Show that the Mellin transform
$$F(s) := \int y^s f(y)\, d^\times y$$
converges initially for $\Re(s) > 0$ and extends to a meromorphic function on the complex plane, whose only poles are simple ones at $s = -2n$ for $n \in \mathbb{Z}_{\geq 0}$ with residue
$$\mathrm{res}_{s=-2n} F(s) = \frac{1}{(2n)!} f^{(2n)}(0).$$

[Use Taylor's theorem with remainder, and note that the odd Taylor coefficients vanish in view of the evenness assumption on f.]

Example 6.4. Take $f(x) := e^{-\pi x^2}$. Then

$$F(s) = \pi^{-s/2}\Gamma(s/2), \tag{6.3}$$

as one sees by substituting $y \mapsto \sqrt{y}$ and then $y \mapsto y/\pi$ in the defining integral. This has poles in the expected places.

For f even, we have

$$g(y) = f(0) + 2\sum_{n=1}^{\infty} f(ny).$$

Using that the constant function 1 has vanishing regularized Mellin transform (for reasons similar to external Exercise 3), we see that $G(s)$ admits the following absolutely convergent integral representation for $\Re(s) > 1$:

$$G(s) = 2\int_{\mathbb{R}^+} y^s \sum_{n=1}^{\infty} f(ny)\, d^\times y.$$

By substituting $y \mapsto y/n$, we see that

$$G(s) = 2\zeta(s)F(s), \qquad F(s) := \int y^s f(y)\, d^\times y.$$

This gives another proof of the meromorphic behavior of ζ. TODO: say more.

We can also deduce the functional equation:

Theorem 6.5. *We have*

$$\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \xi(1-s).$$

Proof. Take $f(x) := e^{-\pi x^2}$. By (6.3), we then have $G_f(s) = \xi(s)$. On the other hand, by the well-known formula for the Fourier transform of a Gaussian, we have $\mathcal{F}f = f$. By Lemma 6.3, it follows that $G_f(s) = G_f(1-s)$. The claimed formula follows. □

6.3. **Euler product.** The link between the zeta function and the prime numbers is given by the following alternative formula:

Lemma 6.6. *For $\Re(s) > 1$, we have*

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}},$$

where the product ranges over the primes p and converges absolutely. In particular,

$$\zeta(s) \neq 0 \text{ for } \Re(s) > 1.$$

Quantitatively, for $\sigma > 1$, we have

$$|\zeta(\sigma + it)| \geq \zeta(1+\sigma)^{-1}. \tag{6.4}$$

Here we say that an infinite product *converges absolutely* if it converges to the same nonzero value for any rearrangement of the factors.

Proof. We first observe that for S any finite set of primes, we have

$$\prod_{p\in S}\frac{1}{1-p^{-s}}=\prod_{p\in S}\sum_{k\geq 0}\frac{1}{p^{ks}}=\sum_{n\in\mathbb{N}(S)}\frac{1}{n^s},$$

where $\mathbb{N}(S)$ denotes the set of natural numbers each of whose prime factors lie in S. This identity follows from the fundamental theorem of arithmetic, which implies that every element of $\mathbb{N}(S)$ may be written uniquely as a product of powers of elements of S. We now take the limit as $S\to\mathbb{N}$.

To see that the product converges to a nonzero limit, we can apply the following general fact: if $\sum_p |a_p|<\infty$, then the product $\prod_p(1+a_p)$ converges to a limit, and that limit is nonzero provided that each factor $1+a_p$ is nonzero. Applying this facts with $a_p=p^{-s}$ gives what was claimed.

For the quantitative estimate (6.4), we observe that

$$\left|\frac{1}{\zeta(\sigma+it)}\right|=\prod_p\left|1-p^{-s}\right|\leq\prod_p\left(1+p^{-\sigma}\right)\leq\sum_n n^{-\sigma}=\zeta(1+\sigma).$$

□

As a basic illustration of the resulting link between the zeta function and the primes, we verify the following:

Lemma 6.7. *Let $s>1$ be real, tending to* 1. *Then*

$$\sum_p\frac{1}{p^s}=\log\frac{1}{1-s}+\mathrm{O}(1).$$

Proof. Using the Taylor series for the logarithm, we compute

$$\log\zeta(s)=\sum_p\log\left(\frac{1}{1-p^{-s}}\right)=\sum_p\sum_{k\geq 1}\frac{p^{-ks}}{k}. \tag{6.5}$$

We leave it to the reader to check that

$$\sum_{k\geq 2}\frac{p^{-ks}}{k}=\mathrm{O}(1) \tag{6.6}$$

in the indicated range. □

Corollary 6.8. $\sum_p 1/p=\infty$.

6.4. **Logarithmic derivatives.** While the logarithm $\log\zeta(s)$ is multi-valued, the logarithmic derivative

$$(\log\zeta(s))'=\frac{\zeta'}{\zeta}(s)$$

is single-valued. It may be computed by differentiating (6.5):

$$-\frac{\zeta'}{\zeta}(s)=\sum_p(\log p)\sum_{k\geq 1}p^{-ks}=\sum_n\frac{\Lambda(n)}{n^s},$$

where the *von Mangoldt function* $\Lambda(n)$ is defined by

$$\Lambda(n):=\begin{cases}\log p & \text{if } n=p^k,\\ 0 & \text{otherwise.}\end{cases}$$

The general theme of this course suggests a relationship between the asymptotics of $\Lambda(n)$ and the meromorphic behavior of $-\zeta'/\zeta$. The poles of the latter may be described as follows. Suppose that $\rho \in \mathbb{C}$ is a point at which ζ has a zero of order $m \in \mathbb{Z}$, i.e., $\zeta(s) \sim c(s-\rho)^m$ for some $c \in \mathbb{C}^\times$ as $s \to \rho$. Then

$$-\frac{\zeta'}{\zeta}(s) \sim \frac{-m}{s-\rho}.$$

Therefore the poles of $-\zeta'/\zeta$ are all simple, and occur at

- the (unique simple) pole $\rho = 1$ of ζ, with residue 1, and
- at the zeros ρ of ζ, with residue $-m$, where $m \geq 1$ denotes the order of the zero.

Suppose, for instance, that we wish to understand the asymptotics of a sum like

$$S := \sum_n \Lambda(n) f\left(\frac{n}{x}\right).$$

Here $f \in C_c^\infty(\mathbb{R}^+)$ is fixed, while we think of $x > 1$ as a parameter tending off to infinity. To do this, we expand f using its Mellin transform, which gives

$$f\left(\frac{n}{x}\right) = \int_{(c)} F(s) \left(\frac{x}{n}\right)^s \frac{ds}{2\pi i}.$$

Here $c \in \mathbb{R}$ is any real number. The double sum/integral obtained by inserting this expansion into the definition of S converges absolutely for $c > 1$, where we may rearrange it to obtain

$$S = \int_{(c)} F(s) x^s \underbrace{\sum_n \frac{\Lambda(n)}{n^s}}_{-\frac{\zeta'}{\zeta}(s)} \frac{ds}{2\pi i}. \tag{6.7}$$

We would now like to shift the contour to the left.

Working formally for the moment, we pick up contributiones from the poles of ζ at 1 and its zeros ρ, giving

$$S = F(1)x - \sum_\rho F(\rho) x^\rho + \cdots,$$

where $\cdots$ denotes the "remainder" term given by an integral like S, but with c large and negative, while ρ ranges over the zeros of ζ with $\Re(\rho) > c$. To implement such an argument rigorously requires some control over the growth of zeta and its number of zeros in vertical directions, which we will address shortly. Ignoring such details for the moment, one can see from such expansions why the zeros of ζ play such a large role in describing the asymptotics of sums over primes such as S. For instance, if we know that each ρ has real part strictly less than 1, then the corresponding term $F(\rho)x^\rho$ has lesser magnitude than x as $x \to \infty$.

To make arguments like the above precise, we need some control over the growth of ζ'/ζ in vertical strips, and also over the number of zeros.

6.5. **Crude control over zeros.** For the following, we closely follow the presentation of part 2 of https://terrytao.wordpress.com/2014/12/09/254a-notes-2-complex-analytic-multiplicative-number-theory/. In particular, the following results can all be sharpened a bit using the functional equation, but we won't pause to do so here.

We begin by giving a simple formula for ζ valid in the critical strip $0 < \Re(s) < 1$.

Lemma 6.9. *For $\Re(s) > 0$, we have*

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{y^s} \right) dy. \tag{6.8}$$

Proof. We have

$$\int_1^{\infty} \frac{1}{y^s}\, dy = \frac{1}{s-1},$$

thus

$$\begin{aligned} \zeta(s) - \frac{1}{s-1} &= \sum_{n=1}^{\infty} \frac{1}{n^s} - \int_1^{\infty} \frac{1}{y^s}\, dy \\ &= \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} \frac{1}{y^s}\, dy \right) \\ &= \sum_{n=1}^{\infty} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{y^s} \right) dy. \end{aligned}$$

□

From this, we conclude a basic but useful upper bound for ζ in the critical strip. (Much sharper forms are available, but we won't need them immediately.)

Lemma 6.10. *For $s = \sigma + it$ with $\sigma \geq \varepsilon > 0$ and $|t| \geq 2$, we have*

$$\log|\zeta(s)| \leq \log(|t|) + \mathrm{O}_{\varepsilon}(1). \tag{6.9}$$

Proof. We use the mean value theorem to estimate the integrand in (6.8):

$$\frac{1}{n^s} - \frac{1}{y^s} = -s \int_{t=n}^{y} t^{-s-1}\, dt \ll s n^{-s-1}.$$

It follows that for $\Re(s) \geq \varepsilon > 0$, we have

$$\zeta(s) - \frac{1}{s-1} \ll s \sum_{n=1}^{\infty} n^{-\varepsilon-1} \ll_{\varepsilon} s.$$

We conclude by taking the logarithm of this estimate. We can discard the contribution of the pole because we have assumed that $|t| \geq 2$. □

With these results in hand, we can appeal to general properties of holomorphic functions to deduce the following pair of propositions:

Proposition 6.11. *Fix $\varepsilon > 0$.*

(i) For $t_0 \in \mathbb{R}$, the number of zeros of ζ in the rectangle $\{\sigma + it : \varepsilon \leq \sigma \leq 1, |t - T| \leq 1\}$ is $\mathrm{O}_{\varepsilon}(\log(3 + |t_0|))$.

(ii) For $s \in \mathbb{C}$ with $\Re(s) \geq \varepsilon$, we have

$$\frac{\zeta'}{\zeta}(s) = \frac{1}{s-1} - \sum_{|\rho - s| \leq \varepsilon/2} \frac{1}{s-\rho} + \mathrm{O}_{\varepsilon}\left(\log(3 + |t|)\right). \tag{6.10}$$

Proof. We apply Lemma 15 of these notes to the function $f(s) := (s-1)\zeta(s)$, the basepoint $s_0 := 2 + it_0$, the radius $r := 2 - \varepsilon/4$ and the disc $D = \{s : |s - s_0| < r\}$, where $\varepsilon > 0$ is sufficiently small. The Euler product estimate (6.4) gives $\zeta(s_0) \asymp 1$. For s with $|s - s_0| = r$, we have by (6.9) $|f(s)| \le M|f(s_0)|$ for some $M \ll \log(3 + |t_0|)$. This gives (i).

For (ii), we argue as in (i) with $t_0 := \Im(s)$. We use the bound for the number of zeros to see that (6.10) doesn't change if we modify the sum by including or excluding any zeros that are at least some fixed distance away from s. This leads to the claimed estimate. □

Lemma 6.12. *For $C > \varepsilon > 0$ and $T \in \mathbb{R}$, we have*

$$\int_{\sigma=\varepsilon}^{C} \int_{t=T-1}^{T+1} \left| \frac{\zeta'}{\zeta}(\sigma + it) \right| dt\, d\sigma \ll_{\varepsilon, C} \log(3 + |T|).$$

Proof. This follows upon integrating (6.10), using that

$$\int_{-R}^{R} \int_{-R}^{R} \frac{1}{|x + iy|}\, dx\, dy < \infty.$$

□

6.6. **Contour shifting and an explicit formula.** We can now carry out the promised contour shifting arguments. Here's a typical result that one can obtain in this way. (Our arrangement is like Theorem 21 of these notes, but with smooth weights, and should be compared against standard references such as [1, Chapter 17] or [3, §5.5]. See also [5].)

Proposition 6.13. *Let $f \in C_c^\infty(\mathbb{R})$, with Mellin transform $F(s) = \int_{\mathbb{R}^+} y^s f(y)\, d^\times y$. Let $x \ge 1$ and $\varepsilon > 0$. Then*

$$\sum_n \Lambda(n) f\left(\frac{n}{x}\right) = F(1)x + \sum_{\rho : \Re(\rho) > \varepsilon} F(\rho) x^\rho + \mathrm{O}_\varepsilon\left(x^\varepsilon \mathcal{E}\right),$$

where

$$\mathcal{E} := \int_{T \in \mathbb{R}} E(T) \log(3 + |T|)\, dT, \qquad E(T) := \max_{\substack{\sigma \in [\varepsilon/2, \varepsilon] \\ t \in [T-1, T+1]}} |F(\sigma + it)|.$$

Note that since f is smooth, the quantity $\mathcal{E}$ is finite (see external Lemma 6 of these notes).

Proof. To simplify notation, we can absorb x into f: the function $f_1(y) := f(n/x)$ has Mellin transform $F_1(s) = x^s F(s)$, and from this we see easily that if we can establish the required conclusion for F_1 (with $x = 1$), then we obtain the required conclusion for F. Thus, let us suppose without loss of generality that $x = 1$.

As in (6.7), we have for each $c > 1$

$$\sum_n \Lambda(n) f(n) = \int_{(c)} F(s) D(s)\, \frac{ds}{2\pi i}, \quad D(s) := -\frac{\zeta'}{\zeta}(s).$$

Set $I_\sigma(t) := |F(\sigma+it)D(\sigma+it)|$. By the definition of $E(T)$ and Lemma 6.12, we have

$$\int_{\sigma=\varepsilon/2}^{\varepsilon}\int_{t\in\mathbb{R}} I_\sigma(t)\,dt\,d\sigma \le \int_{T\in\mathbb{R}} E(T)\int_{\sigma=\varepsilon/2}^{\varepsilon}\int_{t=T-1}^{T+1} |D(\sigma+it)|\,dt\,d\sigma\,dT \ll_\varepsilon \mathcal{E}.$$

By the pigeonhole principle, we can find some $c_0 \in (\varepsilon/2, \varepsilon)$ so that

$$\int_{t\in\mathbb{R}} I_{c_0}(t) \ll_\varepsilon \mathcal{E}. \tag{6.11}$$

By the triangle inequality, it follows that

$$\int_{(c_0)} F(s)D(s)\,\frac{ds}{2\pi i} \ll_\varepsilon \mathcal{E}.$$

We also have, by another application of Lemma 6.12,

$$\left|\sum_{\rho: c_0<\Re(\rho)\le\varepsilon} F(\rho)\right| \le \int_{T\in\mathbb{R}} E(T)\left(\sum_{\substack{\rho: c_0<\Re(\rho)\le\varepsilon,\\ \Im(\rho)\in[T-1,T+1]}} 1\right) dT \ll_\varepsilon \mathcal{E}.$$

Note that (6.11) implies in particular that ζ has no zeros with real part c_0. By combining the above estimates, we reduce to establishing the following identity:

$$\int_{(c)} F(s)D(s)\,\frac{ds}{2\pi i} = \int_{(c_0)} F(s)D(s)\,\frac{ds}{2\pi i} + F(1) - \sum_{\rho:\Re(\rho)>c_0} F(\rho).$$

Note that each the integrals and sums converge absolutely, due to (6.11), part (i) of Proposition 6.11, and the rapid decay of F in vertical strips. It will thus suffice to find a sequence of positive reals t, tending off to infinity, along which the quantities

$$J_t := \int_{c-it}^{c+it} F(s)D(s)\,\frac{ds}{2\pi i} - \int_{c_0-it}^{c_0+it} F(s)D(s)\,\frac{ds}{2\pi i} - F(1) + \sum_{\substack{\rho:\Re(\rho)>c_0,\\ |\Im(\rho)|<t}} F(\rho)$$

tend to zero. To that end, we observe first that if t is chosen not to coincide with the imaginary part of any zero of zeta, then Cauchy's residue theorem gives

$$J_t = \int_{c-it}^{c_0-it} F(s)D(s)\,\frac{ds}{2\pi i} - \int_{c+it}^{c_0+it} F(s)D(s)\,\frac{ds}{2\pi i}.$$

We next observe, using the rapid decay of F and the triangle inequality, that for each $T \in \mathbb{R}$,

$$\int_{t=T-1}^{T+1} |J_t|\,dt \ll_f (1+|T|)^{-100}\int_{t=T-1}^{T+1}\int_{\sigma=c_0}^{c} |D(\sigma+it)|\,dt\,d\sigma.$$

By another application of Lemma 6.12, this last double integral is $\ll \log T$. By another application of the pigeonhole principle, we can find $t \in [T-1, T+1]$ such that $J_t \ll (1+|T|)^{-99}$, say. Since T can be taken arbitrarily large, we obtain the required sequence of quantities t along which $J_t \to 0$. □

6.7. **Zero-free regions.** These results were presented in Sergey's lectures while I was travelling, following the reference [5, §3].

Theorem 6.14. *There exists $c > 0$ so that if $\zeta(s) = 0$ for $s = \sigma + it$, then*

$$1 - \sigma > \frac{c}{\log(2 + |t|)}.$$

In particular, $\zeta(s) = 0$ only if $\Re(s) < 1$.

6.8. **Prime number theorem.** We'll present the proof of the qualitative form, i.e., without giving an explicit error term. First, we treat the case of a smoothly weighted sum.

Theorem 6.15. *Fix $f \in C_c^\infty(\mathbb{R}^+)$, with Mellin transform F, and let $x \to \infty$. Then*

$$\sum_n \Lambda(n) f\left(\frac{n}{x}\right) = F(1)x + o(x).$$

Proof. We apply the explicit formula, as given in Proposition 6.13, with some small $\varepsilon > 0$. The error quantity $E(T)$ is $\ll T^{-100}$, say, by the rapid decay of F, and so $\mathcal{E} \ll \int_{T \in \mathbb{R}} (1 + |T|)^{-100} \log(3 + |T|)\, dT \ll 1$. Our task thereby reduces to showing that

$$\sum_{\rho : \Re(\rho) > \varepsilon} F(\rho) x^\rho = o(x). \tag{6.12}$$

To that end, let us observe first that

$$\sum_{\rho : \Re(\rho) > \varepsilon} |F(\rho)| < \infty.$$

Indeed, by the rapid decay of F, we have $F(\rho) \ll |\rho|^{-100}$, while by Proposition 6.11, the number of ρ with $|\rho| \le T$ is $\ll T \log T$ for $T \ge 3$; the claimed convergence then follows by summing over dyadic ranges $X \le |\rho| \le 2X$.

It follows that for each $\alpha > 0$, we choose a finite multiset $\mathcal{R}$ of zeros ρ as above such that the sum of $|F(\rho)|$ over the complement of $\mathcal{R}$ is at most $\alpha/2$. On the other hand, for each $\rho \in \mathcal{R}$, we have by Theorem 6.14 that $\Re(\rho) < 1$, and so $\lim_{x \to \infty} F(\rho) x^{\rho - 1} = 0$. It follows that for $x > x_0(\alpha)$, the left hand side of (6.12) is bounded in magnitude by α. Since $\alpha > 0$ was arbitrary, we conclude that (6.12) holds, as required. □

Now we successively pass from this to more elementary statements.

First, we approximate sharp cutoffs by smooth ones to deduce a sharply truncated dyadic estimate.

Theorem 6.16. *As $x \to \infty$, we have*

$$\sum_{x \le n \le 2x} \Lambda(n) \sim x. \tag{6.13}$$

Proof. For each fixed $\varepsilon > 0$, we may find $f, f_+ \in C_c^\infty(\mathbb{R}^+)$ such that, writing 1_A for the character function of a set A and F, F_+ for the Mellin transforms,

$$\big|f(x) - 1_{[1,2]}(x)\big| \le f_+(x) \quad \text{and} \quad F_+(1) = \int f_+ < \varepsilon. \tag{6.14}$$

(We can do this by modifying the standard proof that nonzero smooth compactly supported functions exist.) Write S for the left hand side of (6.13), and write

$$S_f := \sum_n \Lambda(n) f\left(\frac{n}{x}\right), \quad S_{f_+} := \sum_n \Lambda(n) f_+\left(\frac{n}{x}\right)$$

for the analogous smoothly-weighted sums. We then have

$$|S - S_f| \leq S_{f_+}. \tag{6.15}$$

By Theorem 6.15, we have $S_f = F(1)x + o(x)$ and $S_{f_+} = F_+(1)x + o(x)$. By (6.14), we have $|F(1) - 1| \leq F_+(1) < \varepsilon$. In particular, for x large enough, we deduce that $|S_f - x| < 2\varepsilon x$ and $\left|S_{f_+}\right| < 2\varepsilon x$. By the triangle inequality, it follows that $|S - x| < 4\varepsilon x$. Since $\varepsilon > 0$ was arbitrary, we thereby deduce the claimed estimate (6.13). □

Next, we apply dyadic summation to obtain an estimate for the sum over all $n \leq x$:

Theorem 6.17. *As $x \to \infty$, we have*

$$\sum_{n \leq x} \Lambda(n) \sim x. \tag{6.16}$$

Proof. For $x \geq 1$, let us define $\alpha(x)$ by writing

$$\sum_{x < n \leq 2x} \Lambda(n) = x(1 + \alpha(x)). \tag{6.17}$$

By Theorem 6.16, we have

$$\alpha(x) \to 0 \tag{6.18}$$

as $x \to \infty$. In particular, for x sufficiently large, we have $|\alpha(x)| \leq 1$. On the other hand, for small x, we see by trivial estimation that $\alpha(x)$ is uniformly bounded. Thus there exists $C \geq 0$ so that

$$|\alpha(x)| \leq C \tag{6.19}$$

for all $x \geq 1$.

Next, letting $x \to \infty$, we write

$$\sum_{n \leq x} \Lambda(n) = \sum_{\frac{x}{2} < n \leq x} + \sum_{\frac{x}{4} < n \leq \frac{x}{2}} + \sum_{\frac{x}{8} < n \leq \frac{x}{4}} + \cdots + \sum_{\frac{x}{2^{m+1}} < n \leq \frac{x}{2^m}},$$

where m is chosen so that

$$\frac{x}{2^{m+1}} < 2 \leq \frac{x}{2^m}. \tag{6.20}$$

By applying (6.17) to each summand, we obtain

$$\sum_{n \leq x} \Lambda(n) = x\left(1 - \frac{1}{2^{m+1}}\right) + x \sum_{k=1}^{m+1} \frac{1}{2^k} \alpha\left(\frac{x}{2^k}\right).$$

Fix $\varepsilon > 0$. We can choose $k_1 \geq 1$ so that

$$C \sum_{k > k_1} \frac{1}{2^k} \leq \varepsilon.$$

By (6.19), we then have

$$\left| x \sum_{k=k_1+1}^{m+1} \frac{1}{2^k} \alpha\left(\frac{x}{2^k}\right) \right| \leq \varepsilon x.$$

On the other hand, for each $k \leq k_1$, we see by (6.18) that

$$x \frac{1}{2^k} \alpha\left(\frac{x}{2^k}\right) = o(x)$$

as $x \to \infty$. By combining these estimates with (6.20), we deduce that

$$\left| \sum_{n \leq x} \Lambda(n) - x \right| \leq 3\varepsilon x$$

for x sufficiently large. Since $\varepsilon > 0$ was arbitrary, we are done. □

We next aim to deduce from this the prime number theorem in unweighted form:

Theorem 6.18. *As $x \to \infty$, we have*

$$\sum_{p \leq x} 1 \sim \frac{x}{\log x}.$$

The proof uses the following identity.

Lemma 6.19 (Abel summation). *Let f be a continuously differentiable function on the interval $[a, b]$, where $a < b$ are real numbers, and let c_n be a sequence of scalars, indexed by the integers, with $c_n = 0$ for n sufficiently close to $-\infty$. Then, writing*

$$S(t) := \sum_{n \leq t} c_n,$$

we have

$$\sum_{a < n \leq b} f(n) c_n = f(b) S(b) - f(a) S(a) - \int_a^b S(t) f'(t)\, dt. \tag{6.21}$$

Proof. The left hand side of (6.21) may be understood as the Riemann–Stieltjes integral

$$\int_a^b f(t)\, dS(t).$$

The claimed formula follows by integration by parts for such integrals.

Alternatively, we can reduce by linearity to the case that $c_m = 1$ and $c_n = 0$ for $n \neq m$. Then $S(t) = 1_{t \geq m}$. The claimed identity can be verified by considering separately the cases that $m \leq a$ or $a < m \leq b$ or $b < m$, in which it reads respectively

$$0 = f(b) - f(a) - \int_a^b f'(t)\, dt,$$

$$f(m) = f(b) - \int_m^b f'(t)\, dt,$$

$$0 = 0.$$

□

Example 6.20. If $f \equiv 1$, then (6.21) says

$$\sum_{a<n\leq b} c_n = S(b) - S(a),$$

which is clear.

Example 6.21. If $f(t) = t$, then (6.21) says

$$\sum_{a<n\leq b} nc_n = bS(b) - aS(a) - \int_a^b S(t)\,dt.$$

Proof of Theorem 6.18. We apply Lemma 6.19 with $[a,b] = [\frac{3}{2}, x]$, $c_n = \Lambda(n)$, and $f(t) = 1/\log t$. Then $S(t) = \sum_{n\leq t} \Lambda(t)$. Since $f'(t) = -1/(t\log^2 t)$, we obtain

$$\sum_{n\leq x} \frac{\Lambda(n)}{\log n} = \frac{S(x)}{\log x} + \int_{\frac{3}{2}}^x \frac{S(t)}{t\log^2 t}\,dt.$$

By Theorem (6.16), the first term on the right hand side is $\sim x/\log x$, while the second term is

$$\ll \int_{\frac{3}{2}}^x \frac{dt}{\log^2 t}.$$

We can estimate this last integral by splitting it into the ranges $t \leq \sqrt{x}$ and $t > \sqrt{x}$. In the former range, we obtain $\ll \sqrt{x}$, while in the latter, we obtain $\ll x/\log^2 x$, using that $\log\sqrt{x} \asymp \log x$. It follows that

$$\sum_{n\leq x} \frac{\Lambda(n)}{\log n} \sim \frac{x}{\log x}.$$

Recall that, by definition, we have $\Lambda(n)/\log n = 0$ unless n is of the form p^k for some prime p and natural number k, in which case $\Lambda(n) = \log p = \frac{1}{k}\log n$. Since $p^k \leq x$ if and only if $p \leq x^{1/k}$, it follows that

$$\sum_{n\leq x} \frac{\Lambda(n)}{\log n} = \pi(x) + \pi(x^{1/2}) + \pi(x^{1/3}) + \cdots + \pi(x^{1/k}),$$

where $\pi(x)$ is the number of primes $p \leq x$ and k is the natural number for which

$$x^{\frac{1}{k}} \geq 2 > x^{\frac{1}{k+1}}.$$

By trivial estimation, we have $|\pi(x)| \leq x$ and $k \ll \log x$, hence

$$\pi(x^{1/2}) + \pi(x^{1/3}) + \cdots + \pi(x^{1/k}) \ll x^{1/2}\log x.$$

This is much smaller than $x/\log x$, so we conclude as required that $\pi(x) \sim x/\log x$. □

7. Primes in arithmetic progressions

7.1. **Goal.** Next goal is to establish the prime number theorem in arithmetic progressions.

Let (a,b) denote the greatest common divisor of a pair of integers a and b. We recall that (a,b) is then the nonnegative generator of the ideal generated by a and b, hence may be written in the form $ax + by$ for some integers x and y. We recall that a and b are called coprime if $(a,b) = 1$.

For a natural number q, we denote by $\mathbb{Z}/q := \mathbb{Z}/q\mathbb{Z}$ the ring of residue classes modulo q and by $(\mathbb{Z}/q)^\times$ its unit group, consisting of what we call the *reduced* residue classes. Each residue class $a \in \mathbb{Z}/q$ may be identified with an arithmetic progression $a + q\mathbb{Z}$. A residue class is reduced if and only if it consists of integers coprime to q. We sometimes write simply $a\ (q)$ and $a\ (q)^*$ to denote respectively that $a \in \mathbb{Z}/q$ and that $a \in (\mathbb{Z}/q)^\times$. We write

$$\phi(q) := (\mathbb{Z}/q)^\times$$

for the Euler ϕ function, which counts the reduced residue classes modulo q.

If the residue class $a\ (q)$ is not reduced, then it contains at most one prime number. Indeed, our hypothesis implies that a and q have a common divisor $d > 1$. Then any prime $p \equiv a\ (q)$ is in particular divisible by d, hence $p = d$, as required.

It follows that all but finitely many prime numbers lie in one of the reduced residue classes modulo q. By the prime number theorem, we thus have for fixed q, as $x \to \infty$, the estimate

$$\sum_{a(q)^*} \sum_{\substack{p \le x \\ p \equiv a(q)}} 1 \sim \frac{x}{\log x}.$$

The prime number theorem says that the primes distribute evenly modulo the reduced residue classes, i.e., for each $a(q)^*$,

$$\sum_{\substack{p \le x \\ p \equiv a(q)}} \frac{1}{\phi(q)} \frac{x}{\log x}.$$

The proof will boil down to nonvanishing properties of the Dirichlet L-functions $L(s, \chi)$, where χ is a Dirichlet character modulo q.

In particular, such estimates imply the infinitude of primes in arithmetic progressions (Dirichlet's theorem).

7.2. **Structure of the group of reduced residue classes.** Let q be a natural number. Here we describe the structure of the group $(\mathbb{Z}/q)^\times$. In particular, we write that group as a product of cyclic groups.

By the fundamental theorem of arithmetic, we may factor q as a product of prime numbers, say $q = \prod_i p_i^{a_i}$. By the Chinese remainder theorem, the natural map

$$\mathbb{Z}/q \to \prod_i \mathbb{Z}/p_i^{a_i}$$

is an isomorphism of rings, hence induces an isomorphism of unit groups

$$(\mathbb{Z}/q)^\times \cong \prod_i (\mathbb{Z}/p_i^{a_i})^\times. \tag{7.1}$$

We can therefore reduce our study to the case that q is a prime power.

In the case that q is a prime, we have the following fundamental fact from basic algebra:

Lemma 7.1. *For a prime number p, the group $(\mathbb{Z}/p)^\times$ is cyclic.*

Proof. We sketch the standard proof. Since the group $(\mathbb{Z}/p)^\times$ has order $\phi(p) = p-1$, we have $x^{p-1} = 1$ for each $x \in (\mathbb{Z}/p)^\times$. The order of x is thus some divisor d of $p-1$. On the other hand, using that $\mathbb{Z}/p$ is a field and the fundamental theorem of algebra, we know that the number of elements x of order d is at most what it would

be if the group $(\mathbb{Z}/q)^\times$ were cyclic. By a counting argument, it follows that that number is in fact exactly what it would be if that group were cyclic. In particular, by taking $d = p - 1$, we deduce that there exists a cyclic element. □

A *primitive root* modulo p is a generator g of the cyclic group $(\mathbb{Z}/p)^\times$.

How about for prime powers? For an odd prime p and an integer $k \geq 2$, the group $(\mathbb{Z}/p^k)^\times$ is likewise cyclic. Indeed, we can lift a primitive root g mod p to a $(p-1)$st root of unity in $(\mathbb{Z}/p^k)^\times$. Then the map

$$\begin{aligned} \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{k-1} &\to (\mathbb{Z}/p^k)^\times \\ (a, b) &\mapsto g^a(1+p)^b \end{aligned} \tag{7.2}$$

is an isomorphism. At the prime 2, we have the slightly more complicated isomorphism

$$\begin{aligned} \mathbb{Z}/2 \times \mathbb{Z}/2^{k-2} &\to (\mathbb{Z}/2^k)^\times \\ (a, b) &\mapsto (-1)^a 5^b. \end{aligned} \tag{7.3}$$

Example 7.2. What are the squares in $(\mathbb{Z}/q)^\times$? Under the isomorphism (7.1), they correspond to products of squares in $(\mathbb{Z}/p^k)^\times$, where p^k runs over the prime power factors of q. If p is odd, then the squares in $(\mathbb{Z}/p^k)^\times$ are the elements of the form $g^a(1+p)^b$ for which $a \equiv 0 \pmod 2$. If $p^k = 2$, then everything is a square. If $p = 2$ and $k \geq 2$, then the squares are the elements of the form $(-1)^a 5^b$ for which $a \equiv 0 \pmod 2$ and $b \equiv 0 \pmod 2$.

7.3. **Characters of finite abelian groups.** We recall some basics from Sergey's lecture concerning the discrete Fourier transform.

Let G be a finite abelian group. A *character* of G is a homomorphism $\chi : G \to \mathbb{C}^\times$. Since G is torsion, the image of any character consists of roots of unity, and in particular lies in the subgroup $\mathrm{U}(1) \leq \mathbb{C}^\times$.

We write $\hat{G}$ for the set of characters of G. Equipped with the operation of pointwise multiplication, this set is naturally a finite abelian group. The identity element of $\hat{G}$ is the trivial character $1 \in \hat{G}$, which assigns the scalar 1 to each element of G.

The groups G and $\hat{G}$ are (non-canonically) isomorphic. One can see this using the fact that G is isomorphic to a finite product of cyclic groups, together with the following explicit isomorphism in the case of a cyclic group $G = \mathbb{Z}/n$: with $e(x) := e^{2\pi i x}$, we have

$$\begin{aligned} \mathbb{Z}/n &\xrightarrow{\cong} \widehat{\mathbb{Z}/n}, \\ a &\mapsto [b \mapsto e(ab/n)]. \end{aligned}$$

To each $f : G \to \mathbb{C}$, we associate its *Fourier transform* $\hat{f} : \hat{G} \to \mathbb{C}$, defined by

$$\hat{f}(\chi) := \frac{1}{|G|} \sum_{a \in G} f(a)\chi^{-1}(a).$$

We then have the Fourier inversion formula

$$f = \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi$$

and the Parseval formula

$$\frac{1}{|G|} \sum_{a \in G} f_1(a)\overline{f_2(a)} = \sum_{\chi \in \hat{G}} f_1(\chi)\overline{f_2(\chi)}.$$

These may be verified by reduction to the case of cyclic groups, where they follow by summing geometric series.

7.4. **Dirichlet characters.** A *Dirichlet character* χ modulo q is a character χ of the group $(\mathbb{Z}/q)^\times$.

It is convenient to identify a character χ modulo q with the function $\chi : \mathbb{Z} \to \mathbb{C}$ supported on the integers a coprime to q and given there by $\chi(a) := \chi(a \ (q))$.

The discussion of §7.2 and §7.3 makes the Dirichlet characters fairly explicit:

- Suppose q factors as a product of prime powers $p_i^{a_i}$. Then any Dirichlet character χ modulo q factors as a product of Dirichlet characters χ_i, where χ_i factors through a Dirichlet character modulo $p_i^{a_i}$ via the map $(\mathbb{Z}/q)^\times \to (\mathbb{Z}/p_i^{a_i})^\times$.
- Suppose $q = p^k$ for some odd prime p and $k \geq 1$. Then, via the isomorphism (7.2), every Dirichlet character is uniquely of the form
$$\chi_{\xi,\eta}(g^a(1+p)^b) = e\left(\frac{\xi a}{p-1} + \frac{\eta b}{p^{k-1}}\right) \tag{7.4}$$
for some $(\xi, \eta) \in \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{k-1}$.
- The group $(\mathbb{Z}/2)^\times$ is trivial, so every Dirichlet character modulo 2 is trivial.
- Suppose $q = 2^k$ for some $k \geq 2$. Then, via 7.2, every Dirichlet character is given by
$$\chi_{\xi,\eta}((-1)^a 5^b) = (-1)^{\xi a} e\left(\frac{\eta b}{2^{k-2}}\right)$$
for some $(\xi, \eta) \in \mathbb{Z}/2 \times \mathbb{Z}/2^{k-2}$.

Definition 7.3. We say that a Dirichlet character χ is *real* or *quadratic* if it takes real values, or equivalently, in view of the identity $\chi(a)^{-1} = \overline{\chi(a)}$, if it satisfies $\chi^2 = 1$.

Example 7.4. Suppose p is an odd prime. The *Legendre symbol* $x \mapsto (x|p)$ is the Dirichlet character modulo p given by taking $\xi = (p-1)/2$ in (7.4), or equivalently, by
$$(x|p) = \begin{cases} +1 & \text{if } x \text{ is a square modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$
It is the only nontrivial real character modulo p. Here is a table of the Legendre symbols modulo 7:

x	1	2	3	4	5	6
$(x\|7)$	+1	+1	−1	+1	−1	−1

Example 7.5. There is one nontrivial character modulo 4. It is real, and given by
$$x \mapsto (-1)^{\frac{x-1}{2}} = \begin{cases} +1 & \text{if } x \equiv 1 \quad (4), \\ -1 & \text{if } x \equiv -1 \quad (4). \end{cases} \tag{7.5}$$

Example 7.6. There are three nontrivial characters modulo 8. They are all real, and given either by (7.5), by
$$x \mapsto (-1)^{\frac{x^2-1}{8}} = \begin{cases} +1 & \text{if } x \equiv \pm 1 \quad (8), \\ -1 & \text{if } x \equiv \pm 5 \quad (8), \end{cases} \tag{7.6}$$
or by the product of (7.5) and (7.6).

Remark 7.7. The nontrivial real characters modulo higher prime powers all factor through some real character modulo 4, 8 or an odd prime. The real characters modulo a composite number factor as products of real characters modulo its prime power factors.

7.5. **Primitive characters.** For a divisor d of q, we have a natural quotient map of rings $\mathbb{Z}/q \to \mathbb{Z}/d$, hence a map of unit groups $\pi_{q,d} : (\mathbb{Z}/q)^\times \to (\mathbb{Z}/d)^\times$. This map is surjective. (In verifying this, we may assume that q is a prime power. For $d = 1$, we use that $(\mathbb{Z}/q)^\times$ is nontrivial. For $d > 1$, we use that any integer coprime to d is also coprime to q.) Letting $K_{q,d}$ denote its kernel, we obtain a short exact sequence of groups

$$1 \to K_{q,d} \to (\mathbb{Z}/q)^\times \xrightarrow{\pi_{q,d}} (\mathbb{Z}/d)^\times \to 1. \tag{7.7}$$

We say that a character χ of $(\mathbb{Z}/q)^\times$ is *induced* by a character χ_d of $(\mathbb{Z}/d)^\times$ if $\chi = \chi_d \circ \pi_{q,d}$. Being induced by some character modulo d is equivalent to having trivial restriction to $K_{q,d}$. We say that a character is *imprimitive* if it is induced from a character modulo d for some proper divisor d of q (where "proper" means that $d \neq q$). Otherwise, we say that a character is *primitive*. Thus, a character is primitive precisely when it has nontrivial restriction to $K_{q,d}$ for each proper divisor d of q.

Exercise 2. For Dirichlet character χ modulo q, there is a unique divisor f of q and a Dirichlet characters χ' modulo f so that χ is induced by χ'.

We refer to f as in Exercise 2 as the *conductor* of χ, and denoted it by $C(\chi) := f$. Thus, a character χ modulo q is primitive if and only if $C(\chi) = q$.

7.6. **Gauss sums.** Given characters $\psi : \mathbb{Z}/q \to \mathbb{C}^\times$ and $\chi : (\mathbb{Z}/q)^\times \to \mathbb{C}^\times$, the corresponding *Gauss sum* is defined by

$$g_\psi(\chi) := \sum_{a \in (\mathbb{Z}/q)^\times} \chi(a)\psi(a).$$

In the special case that ψ is the "standard" character

$$\psi(x) := \exp(2\pi i x/q), \tag{7.8}$$

we abbreviate $g(\chi) := g_\psi(\chi)$.

These sums will arise naturally in our study of the functional equation for Dirichlet L-functions.

Remark 7.8. Gauss sums are analogous to the integrals $\Gamma(s) = \int_{\mathbb{R}^+} y^s e^{-y}\, d^\times y$ defining the Γ-function, with χ playing the role of $\mathbb{R}^+ \ni y \mapsto y^s$ and ψ that of $\mathbb{R} \ni y \mapsto e^{-y}$.

Theorem 7.9. *Let χ be a primitive Dirichlet character modulo q. Then*

$$|g(\chi)| = q^{1/2}$$

Proof. We consider the function $f : \mathbb{Z}/q \to \mathbb{C}$ given by the extension-by-zero of χ:

$$f(a) := 1_{(a,q)=1}\chi(a).$$

We define its Fourier transform $\hat{f} : \mathbb{Z}/q \to \mathbb{C}$ using the standard character (7.8) to be

$$\hat{f}(\xi) := \frac{1}{q} \sum_{a \in \mathbb{Z}/q} f(a)\psi(\xi a). \tag{7.9}$$

We then have $q\hat{f}(1) = g(\chi)$, so our task is to show that

$$|\hat{f}(1)| = q^{-1/2}.$$

To that end, we will show that

$$|f(\xi)| = |f(1)| \quad \text{for } \xi \in (\mathbb{Z}/q)^\times \tag{7.10}$$

and

$$\hat{f}(\xi) = 0 \quad \text{for } \xi \in \mathbb{Z}/q - (\mathbb{Z}/q)^\times. \tag{7.11}$$

The claim (7.10) then follows from the Parseval formula, as follows:

$$\frac{\phi(q)}{q} = \frac{1}{q} \sum_{a \in \mathbb{Z}/q} |f(a)|^2 = \sum_{\xi \in \mathbb{Z}/q} |\hat{f}(\xi)|^2 = \phi(q)|\hat{f}(1)|^2.$$

To verify (7.10), we apply the invertible substitution $a \mapsto \xi^{-1}a$ in (7.9) and appeal to the multiplicativity property $f(\xi^{-1}a) = \chi(\xi)^{-1}f(a)$ and the unitarity $|\chi(\xi)| = 1$.

For (7.11), suppose that $\xi \notin (\mathbb{Z}/q)^\times$. Then $d := q/(q, \xi)$ is a proper divisor of q, and for each element b of the subgroup $K_{q,d}$ as in (7.7), we have $\xi b \equiv x \ (q)$, hence $\psi(\xi ab) = \psi(\xi a)$. Averaging over such identities in (7.9) and substituting $a \mapsto ab^{-1}$ yields

$$\hat{f}(\xi) = \frac{1}{q|K_{q,d}|} \sum_{a \in \mathbb{Z}/q} \psi(\xi a) \sum_{b \in K_{q,d}} f(ab).$$

Each term of this inner sum vanishes unless $a \in (\mathbb{Z}/q)^\times$, in which case that inner sum evaluates to

$$\sum_{b \in K_{q,d}} \chi(ab) = \chi(a) \sum_{b \in K_{q,d}} \chi(b).$$

Since χ is assumed primitive, it has nontrivial restriction to $K_{q,d}$. By the orthogonality of characters of finite abelian groups, that restriction is thus orthogonal to the trivial character, hence the inner sum vanishes. We conclude as required that $\hat{f}(\xi) = 0$. □

Remark 7.10. The evaluation of $g(\chi)$ for non-primitive χ can be reduced to the primitive case, see for instance [3, Lemma 3.1].

References

[1] Harold Davenport. *Multiplicative Number Theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1980. Revised by Hugh L. Montgomery.

[2] Anton Deitmar and Siegfried Echterhoff. *Principles of harmonic analysis*. Universitext. Springer, Cham, second edition, 2014.

[3] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[4] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier analysis on number fields*, volume 186 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[5] E. C. Titchmarsh. *The theory of the Riemann zeta-function*. The Clarendon Press Oxford University Press, New York, second edition, 1986. Edited and with a preface by D. R. Heath-Brown.

[6] Herbert S. Wilf. *generatingfunctionology*. A K Peters, Ltd., Wellesley, MA, third edition, 2006.

[7] Don Zagier. The mellin transform and other useful analytic techniques. `http://people.mpim-bonn.mpg.de/zagier/files/tex/MellinTransform/fulltext.pdf`, 2006.