

COPYRIGHT NOTICE:

**Steven J. Miller and Ramin Takloo-Bighash:
An Invitation to Modern Number Theory**

is published by Princeton University Press and copyrighted, © 2006, by Princeton University Press. All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher, except for reading and browsing via the World Wide Web. Users are not permitted to mount this file on any network servers.

Follow links Class Use and other Permissions. For more information, send email to: permissions@pupress.princeton.edu

Chapter Three

Zeta and L -Functions

In §2.3 we gave two proofs that there are infinitely many primes. Euclid's proof led to a weak lower bound for $\pi(x)$, the number of primes at most x . Chebyshev proved that there exist constants A and B such that $\frac{Ax}{\log x} \leq \pi(x) \leq \frac{Bx}{\log x}$. Gauss conjectured that the correct order of magnitude of $\pi(x)$ is $\frac{x}{\log x}$. Hadamard and de la Vallée Poussin proved this and more in the 1890s: they were able to obtain bounds for $|\pi(x) - \frac{x}{\log x}|$. Their proofs involved powerful techniques from complex analysis, which might seem surprising as there are no complex numbers in sight. This is because the auxiliary functions (called L -functions) which are introduced to help study the primes are functions of complex variables. It was not until almost 50 years later that "elementary" (this does not mean easy: it means using the standard arithmetic functions of Chapter 2) proofs were found by Erdős and Selberg. See [Gol2] for the history and [Ed, EE] for an exposition of the elementary proof.

In this chapter we explain the connection of complex analysis to the study of primes. The introductory sections require only basic arithmetic and calculus; except for §3.2.2, the later sections assume some familiarity with complex analysis. While we give a quick review of some of the tools and techniques (both in this chapter and later in the book), this is meant only to give a flavor of the subject. The interested reader should read the statements of the theorems and then consult the references for more details. We shall use much of this material in Chapters 15 to 18 when we investigate the distribution of zeros of L -functions.

3.1 THE RIEMANN ZETA FUNCTION

A series of the form

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \tag{3.1}$$

with $s \in \mathbb{C}$ and $a(n)$ a sequence of complex numbers is called a **Dirichlet series**. It is common to write $s = \sigma + it$, with $\sigma, t \in \mathbb{R}$. Thus the real part of s is $\Re s = \sigma$ and the imaginary part is $\Im s = t$.

The most exciting Dirichlet series is the simplest one of the them all. The **Riemann zeta function** is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{3.2}$$

Exercise^(h) 3.1.1. Prove $\zeta(s)$ converges for $\Re s > 1$. If $s \in [0, 1]$, show the series for $\zeta(s)$ diverges.

While $\zeta(s)$ as defined only makes sense for $\Re s > 1$, we will show that we can “extend” this to a new function defined for all $s \in \mathbb{C}$. In §3.1.1 we show how $\zeta(s)$ is built from the primes, and it is this connection that will prove fruitful below. Explicitly, tools from elementary analysis and complex analysis allow us to pass from knowledge about $\zeta(s)$ to knowledge about the primes. See the survey article [Wei2] for the origins of $\zeta(s)$, and [Roc] for a popular account of its history and connections to various parts of mathematics. Riemann’s classic paper [Ri], as well as an expanded version, are available in [Ed]. This short paper is Riemann’s only published paper on $\zeta(s)$. It is one of the most influential papers in mathematics, and we strongly encourage everyone to read it.

3.1.1 Euler Product

The following property shows the connection between $\zeta(s)$ and the primes. The proof depends crucially on the **unique factorization** property of integers, namely any positive integer n can be written uniquely as a product of powers of primes (if $n = p_1^{r_1} \cdots p_k^{r_k} = q_1^{s_1} \cdots q_m^{s_m}$, then $k = m$ and after possibly reordering, $p_i = q_i$).

Exercise 3.1.2. Prove unique factorization.

Theorem 3.1.3 (Euler Product of $\zeta(s)$). We have

$$\zeta(s) = \sum_n \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \Re s > 1. \quad (3.3)$$

Sketch of Proof. The product expansion follows from the absolute convergence of the series for $\Re s > 1$, and the unique factorization property of the integers. Namely, by the geometric series formula we have

$$\frac{1}{1-r} = 1 + r + r^2 + r^3 + \cdots = \sum_{k=0}^{\infty} r^k \quad (3.4)$$

for $|r| < 1$. Applying this to $(1 - p^{-s})^{-1}$ for $\Re s > 1$ we obtain

$$\left(1 - \frac{1}{p^s}\right)^{-1} = 1 + \frac{1}{p^s} + \left(\frac{1}{p^s}\right)^2 + \cdots; \quad (3.5)$$

multiplying these expressions and using the unique factorization of natural numbers into products of prime powers completes the proof. \square

Exercise^(hr) 3.1.4. Prove the infinite geometric series formula (3.4), as well as the finite geometric series formula

$$\sum_{k=m}^n r^k = \frac{r^m - r^{n+1}}{1-r}. \quad (3.6)$$

Exercise^(h) 3.1.5. Rigorously prove Theorem 3.1.3.

The product expansion

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \quad (3.7)$$

is called the **Euler product** after Euler, who initiated such investigations. This product expansion is one of the most important properties of $\zeta(s)$. Initially $\zeta(s)$ is defined as a sum over integers — the Euler product connects $\zeta(s)$ to the primes. As the integers are well understood, this allows us to pass from knowledge of integers to knowledge of primes, as the next two exercises illustrate.

Exercise^(hr) 3.1.6 (Important: $\zeta(1)$). Show $\lim_{x \rightarrow \infty} \sum_{n \leq x} \frac{1}{n}$ diverges by comparing it with $\log x$ (use the Integral test). Use the Euler product to show that there are infinitely many prime numbers by investigating $\lim_{s \rightarrow 1} \zeta(s)$.

Exercise 3.1.7 (Important: $\zeta(2)$). Assume that π^2 is irrational; thus $\pi^2 \neq \frac{a}{b}$ for any $a, b \in \mathbb{N}$. We sketch a proof of the irrationality of π^2 in Exercise 5.4.17. In §11.3.4 we show that

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \quad (3.8)$$

Using the Euler product, show there must be infinitely many primes. See Theorem 205 of [HW] for a proof of the transcendence of π (which implies π^2 is irrational), and Chapter 11 of [BB] or [Sc] for a history of calculations of π (as well as many entertaining exercises). This is just one of many applications of Fourier analysis (Chapter 11) to Number Theory.

Exercise 3.1.8. Write $\frac{1}{\zeta(2)}$ as a sum over primes and prime powers, and interpret this number as the probability that as $N \rightarrow \infty$ a number less than N is square-free. See also Exercise 2.3.19.

The method of proof in Exercise 3.1.7 is known as a **special value proof**, and is the first example of a very important phenomenon: Dirichlet series evaluated at certain “natural” points encode interesting algebraic and arithmetic information (see also Exercise 3.3.28). Unlike Euclid and Chebyshev’s Theorems, $\zeta(2)$ irrational provides *no* information on how many primes there are at most x ; by Partial Summation one can obtain bounds on $\pi(x)$ from $\lim_{s \rightarrow 1} \zeta(s)$. See [BP] for connections between $\zeta(k)$ and continued fractions. For some results on the distribution of digits of values of $\zeta(s)$ and Benford’s Law, see Remark 9.4.5.

Exercise 3.1.9. Use the product expansion to prove $\zeta(s) \neq 0$ for $\Re s > 1$; this important property is not at all obvious from the series expansion. While it is clear from the series expansion that $\zeta(s) \neq 0$ for real $s > 1$, what happens for complex s is not apparent.

Exercise 3.1.10. Suppose a_n is a sequence of positive rational numbers such that $P = \prod_{n=1}^{\infty} a_n$ is convergent; this means that $\lim_{N \rightarrow \infty} \prod_{n=1}^N a_n$ converges to a finite non-zero number. Must P be rational? If so, this would provide a very easy proof of the irrationality of $\pi!$ See also Exercises 3.3.8 and 5.6.9.

Exercise^(h) 3.1.11. Prove (see Exercise 3.3.8) that $\prod_{n=2}^{\infty} \zeta(n)$ converges and is finite, and bound $\left| \prod_{n=2}^{\infty} \zeta(n) - \prod_{n=2}^N \zeta(n) \right|$. See [CL1, CL2] for applications of this number to average orders of groups.

3.1.2 Functional Equation and Analytic Continuation

The Euler product is the first of many important properties of $\zeta(s)$. The next is that $\zeta(s)$ has a meromorphic continuation to the entire plane. We first give a definition and an example of meromorphic continuation, and then return to our study of $\zeta(s)$.

Definition 3.1.12 (Zero, Pole, Order, Residue). Assume f has a convergent Taylor series expansion (see §A.2.3) about z_0 :

$$f(z) = a_n(z - z_0)^n + a_{n+1}(z - z_0)^{n+1} + \cdots = \sum_{m=n}^{\infty} a_m(z - z_0)^m, \quad (3.9)$$

with $a_n \neq 0$. Thus n is the location of the first non-zero coefficient. If $n > 0$ we say f has a zero of order n at z_0 ; if $n < 0$ we say f has a pole of order $-n$ at z_0 . If $n = -1$ we say f has a simple pole with residue a_{-1} . We denote the order of the f at z_0 by $\text{ord}_f(z_0) = n$.

Definition 3.1.13 (Meromorphic Function). We say f is meromorphic at z_0 if the Taylor expansion about z_0 converges for all z close to z_0 . In particular, there is a disk about z_0 of radius r and an integer n_0 such that for all z with $|z - z_0| < r$,

$$f(z) = \sum_{n \geq n_0} a_n(z - z_0)^n. \quad (3.10)$$

If f is meromorphic at each point in a disk, we say f is meromorphic in the disk. If $n_0 \geq 0$, we say f is **analytic**.

We have already seen an example of meromorphic continuation (to be defined below). Consider the geometric series $G(r) = \sum_{n=1}^{\infty} r^n$. This series converges for all r with $|r| < 1$, and for such r we have

$$\sum_{n=1}^{\infty} r^n = \frac{1}{1-r}. \quad (3.11)$$

Let us denote the right hand side of (3.11) by $H(r)$. By Exercise 3.1.4, $G(r) = H(r)$ for $|r| < 1$; however, $H(r)$ is well defined for *all* r except for $r = 1$, where $H(r)$ is undefined (it has a simple pole with residue -1). As $H(r)$ agrees with $G(r)$ wherever $G(r)$ is defined and is defined for additional r , we say H is a continuation of G . Since H has a pole, we say H is a **meromorphic continuation**; if H had no poles, we would have an **analytic continuation**. If a function defined for all $z \in \mathbb{C}$ has a convergent Taylor expansion at each point (which implies it has no poles), the function is said to be **entire**.

To study $\zeta(s)$, we need to recall the definition and basic properties of the Gamma function $\Gamma(s)$. For $\Re s > 0$ set

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt. \quad (3.12)$$

Exercise 3.1.14. Prove for $\Re s > 0$ that

$$\Gamma(s+1) = s\Gamma(s). \quad (3.13)$$

One can then use (3.13) to extend the definition of $\Gamma(s)$ to all values of s . It is then seen that the value of $\Gamma(s)$ is always finite unless $s = 0, -1, -2, \dots$

Exercise 3.1.15. Prove the above claims. For n a positive integer, show $\Gamma(n) = (n-1)!$ (remember $0!$ is defined to be 1). Thus $\Gamma(s)$ is a generalization of the factorial function $n!$.

The following theorem collects some of the most important properties of the Gamma function. We refer the reader to [WW], Chapters 12 and 13 for proofs.

Theorem 3.1.16. The Γ -function has the following properties:

1. $\Gamma(s)$ has a meromorphic continuation to the entire complex plane with simple poles at $s = 0, -1, -2, \dots$, and the residue at $s = -k$ is $\frac{(-1)^k}{k!}$. The meromorphically continued function is never zero.
2. For all s we have

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s} \quad (3.14)$$

and

$$\Gamma(s)\Gamma\left(s + \frac{1}{2}\right) = 2^{1-2s}\pi^{\frac{1}{2}}\Gamma(2s). \quad (3.15)$$

3. For any fixed $\delta > 0$, as $|s| \rightarrow \infty$ in $-\pi + \delta < \arg s < \pi - \delta$,

$$\log \Gamma(s) = \left(s - \frac{1}{2}\right) \log s - s + \frac{1}{2} \log 2\pi + O(|s|^{-1}). \quad (3.16)$$

Remark 3.1.17. Theorem 3.1.16(3) is called Stirling's Formula. It can be used to give an asymptotic formula for $n!$. See also Lemma 8.4.5.

Exercise^(h) 3.1.18. Show $\Gamma(s)$ has a simple pole with residue 1 at $s = 0$. We will need this in Chapter 18 when we derive the explicit formula (which relates sums over zeros of $\zeta(s)$ to sums over primes; this formula is the starting point for studying properties of the zeros of $\zeta(s)$). More generally, for each non-negative integer k show that $\Gamma(s)$ has a pole at $s = -k$ with residue $\frac{(-1)^k}{k!}$. Finally, show $\Gamma(s)$ is never zero.

The following theorem is one of the most important theorems in mathematics:

Theorem 3.1.19 (Analytic Continuation of the Completed Zeta Function). Define the completed zeta function by

$$\xi(s) = \frac{1}{2}s(s-1)\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s); \quad (3.17)$$

$\xi(s)$, originally defined for $\Re s > 1$, has an analytic continuation to an entire function and satisfies the functional equation $\xi(s) = \xi(1-s)$.

Proof. For the functional equation we follow Riemann's original argument as described in [Da2]. For $\Re s > 0$, by definition of the Gamma function and change of variables we have

$$\int_0^{\infty} x^{\frac{1}{2}s-1} e^{-n^2\pi x} dx = \frac{\Gamma\left(\frac{s}{2}\right)}{n^s \pi^{\frac{s}{2}}}. \quad (3.18)$$

Summing over $n \in \mathbb{N}$, with $\Re s > 1$ to guarantee convergence, we obtain

$$\begin{aligned} \pi^{-\frac{1}{2}s} \Gamma\left(\frac{s}{2}\right) \zeta(s) &= \int_1^{\infty} x^{\frac{1}{2}s-1} \left(\sum_{n=1}^{\infty} e^{-n^2\pi x} \right) dx \\ &= \int_0^{\infty} x^{\frac{1}{2}s-1} \omega(x) dx \\ &= \int_1^{\infty} x^{\frac{1}{2}s-1} \omega(x) dx + \int_1^{\infty} x^{-\frac{1}{2}s-1} \omega\left(\frac{1}{x}\right) dx, \end{aligned} \quad (3.19)$$

with $\omega(x) = \sum_{n=1}^{+\infty} e^{-n^2\pi x}$. Note we divided the integral into two pieces and changed variables by $x \mapsto x^{-1}$ in the second integral; this leads to rapidly converging integrals. The absolute convergence of the sum-integral justifies the rearrangement of the terms in (3.19) (see Theorem A.2.8, but see Exercise 11.4.12 for an example where the orders cannot be interchanged). We will show in a moment that the function ω satisfies the functional equation

$$\omega\left(\frac{1}{x}\right) = -\frac{1}{2} + -\frac{1}{2}x^{\frac{1}{2}} + x^{\frac{1}{2}}\omega(x) \quad (3.20)$$

for $x > 0$. Simple algebra then shows that for $\Re s > 1$ we have

$$\pi^{-\frac{1}{2}s} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \frac{1}{s(s-1)} + \int_1^{\infty} (x^{\frac{1}{2}s-1} + x^{-\frac{1}{2}s-\frac{1}{2}}) \omega(x) dx. \quad (3.21)$$

Because of the rapid decay of $\omega(x)$, the integral on the right converges absolutely for *any* s and represents an entire function of s . The remaining assertions of the theorem are easy consequences of the location of poles of $1/s(s-1)$ and the invariance of the right hand side of (3.21) under $s \mapsto 1-s$. It remains to verify the functional equation of ω . For this we write

$$\omega(x) = \frac{\theta(x) - 1}{2} \quad (3.22)$$

with

$$\theta(x) = \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 x}. \quad (3.23)$$

Note this series is rapidly converging for $x > 0$. The desired functional equation for ω easily follows from

$$\theta(x^{-1}) = x^{\frac{1}{2}}\theta(x), \quad x > 0, \quad (3.24)$$

which we now prove. Without worrying about convergence, we have

$$\begin{aligned} \theta(x^{-1}) &= \sum_{n=-\infty}^{\infty} e^{-\pi n^2 x^{-1}} \\ &= \sum_{\nu=-\infty}^{\infty} \int_{-\infty}^{\infty} e^{-\pi t^2 x^{-1} + 2\pi i \nu t} dt = x^{\frac{1}{2}}\theta(x) \end{aligned} \quad (3.25)$$

by the Poisson summation formula (see §11.4.2) and Exercise 3.1.22. \square

Remark 3.1.20. Theorem 3.1.19 furnishes us with a meromorphic continuation of $\zeta(s)$ to all $s \in \mathbb{C}$, with its only pole at $s = 1$. We denote the meromorphic continuation by $\zeta(s)$; note, however, that $\zeta(s)$ is only given by the series and product expansions if $\Re s > 1$.

Remark 3.1.21 (Technique: Splitting the Integral). A common method in number theory for obtaining analytic properties of functions defined by integral transforms (here a multiple of $\zeta(s)$ equals $\int_0^\infty x^{\frac{1}{2}s-1}\omega(x)dx$) is to write the integration as $\int_0^1 + \int_1^\infty$ and then use functional relations of the integrand to relate values at $\frac{1}{x}$ to those at x .

Exercise 3.1.22 (Advanced). *Justify the use of the Poisson summation formula in the proof of Theorem 3.1.19. In particular, if $f(t) = e^{-\pi t^2}$ then calculate $\hat{f}(u) = \int_{\mathbb{R}} f(t)e^{2\pi i t u} dt$. See §11.4 for the definition of the Fourier transform.*

Weil [Wei2] calls the Euler product expansion the pre-history of the Riemann zeta function. It seems that the functional equation and the meromorphic continuation were first obtained by Riemann in the monumental paper [Ri]. Because the functional equation connects values of $\zeta(s)$ with those of $\zeta(1-s)$, it suffices to investigate $\zeta(s)$ for $\Re s \geq \frac{1}{2}$.

Exercise^(h) 3.1.23. *The following gives an elementary proof that $\zeta(s)$ can be continued to a meromorphic function for $\Re s > 0$. Show*

$$\zeta(s) = \frac{s}{s-1} - s \int_1^\infty \{x\}x^{-s-1}dx, \quad (3.26)$$

where $\{x\}$ is the fractional part of x .

3.1.3 Values of the Zeta Function at Integer Points

In Exercises 3.1.6 and 3.1.7 we showed how knowledge of $\zeta(s)$ at special s led to information about primes. We needed a result, to be proved in §11.3.4, that

$$\zeta(2) = \frac{\pi^2}{6}. \quad (3.27)$$

In fact, for positive integers n , $\zeta(2n)$ can be explicitly computed. It turns out that

$$\zeta(2n) = r(n)\pi^{2n}, \quad (3.28)$$

where for each n , $r(n)$ is a rational number. For example,

$$\zeta(4) = \frac{\pi^4}{90}. \quad (3.29)$$

The rational number $r(n)$ is expressible in terms of Bernoulli numbers (see [Ed, La6, Se] for a proof, and [CG] or Exercise 3.1.24 for properties of Bernoulli numbers). It is then clear that $\zeta(2n)$ is always irrational, indeed transcendental (see definitions 5.0.3 and 5.0.4 for definitions of algebraic and transcendental numbers). The question of whether the values of $\zeta(s)$ are irrational at odd positive numbers not equal to one is a much more complex problem. The irrationality of $\zeta(3)$ was established by Apéry [Ap] in 1979 (see also the simple proof [Mill]). It is not known

whether $\zeta(3)$ is transcendental. It is a very recent theorem that infinitely many of $\zeta(2n+1)$ are irrational [BR]. We invite the reader to consult the above references for details and further remarks.

Exercise 3.1.24. *The Bernoulli numbers B_n are defined by*

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n. \quad (3.30)$$

Calculate the first few Bernoulli numbers, especially B_{2m+1} .

Exercise^(h) 3.1.25 (Advanced). *Show*

$$\zeta(2n) = \frac{(-1)^{n-1} B_{2n}}{2(2n)!} (2\pi)^{2n}. \quad (3.31)$$

Exercise^(h) 3.1.26. *Verify that $\zeta(s)$ has a simple pole at $s = 1$, with residue equal to 1. Prove that $\zeta(0) = -\frac{1}{2}$, $\zeta(-1) = -\frac{1}{12}$. Compute the values of zeta at all negative integers.*

Remark 3.1.27. Note that the value of $\zeta(-1)$ comes from the continuation of $\zeta(s)$, and not from substituting $s = 1$ in the series expansion: $1 + 2 + 3 + 4 + \dots \neq -\frac{1}{12}$.

Exercise 3.1.28. *Here is another way of computing $\zeta(2)$ (due to G. Simmons). Show that*

$$\zeta(2) = \int_0^1 \int_0^1 \frac{dx dy}{1 - xy}. \quad (3.32)$$

Now compute the integral using the change of variable

$$\begin{aligned} x &= (u - v)\sqrt{2}/2, \\ y &= (u + v)\sqrt{2}/2. \end{aligned} \quad (3.33)$$

Exercise 3.1.29. *Show the number of square-free numbers at most x is $\frac{x}{\zeta(2)} + o(x)$. Generalize to k^{th} -power-free numbers.*

For more on $\zeta(2)$, including complete details of the above exercise, see the entry “Riemann Zeta Function Zeta(2)” in [We].

3.2 ZEROS OF THE RIEMANN ZETA FUNCTION

For this section we assume the reader has more than a passing familiarity with complex analysis, except for §3.2.1 and §3.2.2 where we give an explanation of the interplay between zeros of $\zeta(s)$ and the distribution of primes. In §3.2.1 we introduce the terminology, and in §3.2.2 highlight some of the key results from complex analysis (with sketches of proofs) and describes how these results connect the zeros of $\zeta(s)$ to properties of the primes.

3.2.1 Definitions

From the functional equation of $\zeta(s)$, it is clear that $\zeta(s)$ cannot have any zeros for $\Re s < 0$ except for those forced upon it by the poles of the Γ -function, namely at $-2m$ for $m \in \mathbb{N}$; these are called the **trivial zeros**. In the **critical strip** $0 \leq \Re s \leq 1$, again a simple application of the functional equation implies that the zeros must lie symmetrically around the critical line $\Re s = \frac{1}{2}$, called the **critical line**. The **Riemann Hypothesis** asserts that all the zeros of the zeta function in the critical strip lie on the critical line. These are called the **non-trivial zeros**. The Riemann Hypothesis is an extremely difficult unsolved problem, and it has been the subject of much research since its announcement in 1860. The Riemann Hypothesis (often abbreviated RH) has very important consequences in number theory, especially in problems related to the study of the distribution of prime numbers. It is justly one of the central themes of research in modern mathematics. It was proved by Hardy in 1914 that infinitely many of the zeros lie on the critical line, and by Selberg in 1942 that a positive proportion of all the zeros lie on the line. While we cannot prove the Riemann Hypothesis in its full strength, one can still obtain some interesting results regarding the distribution of the zeros of the zeta function. For example, the following proposition was stated by Riemann in his 1860 paper and was proved by von Mangoldt in 1905:

Proposition 3.2.1. *The number $N(T)$ of zeros of $\zeta(s)$ in the critical strip with $0 < t \leq T$ satisfies*

$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T). \quad (3.34)$$

For a proof see [Da2], §15. This proposition will be used in Chapter 18 as a guide for scaling the zeros of the zeta function.

Remark 3.2.2 (Important). Using techniques from complex analysis, Riemann [Ri] calculated (but did not mention in his paper!) that the first few zeros of $\zeta(s)$ lie on the critical line. This is one of the most powerful examples of numerical evidence leading to an important conjecture. An English translation of Riemann's paper is available in [Ed]. The first trillion zeros have all been shown to lie on the critical line; for an introduction to such researches see [Od1, Od2] and Zeta-Grid [Wed], where one can download a screensaver to join a world-wide, parallel process investigation of the zeros where more than a billion zeros are checked each day. See [Con2] for a survey of some of the approaches towards proving RH.

Exercise 3.2.3. *Prove that the only zeros of $\zeta(s)$ for $\Re s < 0$ are at $s = -2m$ for $m \in \mathbb{N}$. In the critical strip, prove that the zeros lie symmetrically around the critical line $\Re s = \frac{1}{2}$ (if $\rho = \sigma + it$ is a zero, so is $1 - \sigma + it$).*

3.2.2 Zeros of $\zeta(s)$ and Primes

The connection between the zeros of the Riemann zeta function and the distribution of primes was mentioned earlier. The connection comes through the Euler product expansion (the Euler factors play the role of the polynomial coefficients in the heuristic below).

Why does knowledge about the zeros of $\zeta(s)$ yield information about prime numbers? A simple heuristic is the following. Let $P(x)$ be a polynomial with zeros r_1, \dots, r_N and leading term Ax^n . Then

$$\begin{aligned} P(x) &= A \cdot (x - r_1)(x - r_2) \cdots (x - r_n) \\ &= A(x^n + a_{n-1}(r_1, \dots, r_n)x^{n-1} + \cdots + a_0(r_1, \dots, r_n)), \end{aligned} \quad (3.35)$$

where

$$\begin{aligned} a_{n-1}(r_1, \dots, r_n) &= -(r_1 + \cdots + r_n) \\ &\vdots \\ a_0(r_1, \dots, r_n) &= r_1 r_2 \cdots r_n. \end{aligned} \quad (3.36)$$

Hence knowledge of the zeros gives knowledge about the coefficients of the polynomial, and vice versa. See [J] for more on relations between roots and coefficients, as well as other related materials (i.e., Newton's identities and symmetric polynomials). For $\zeta(s)$ the coefficients are related to the primes.

Exercise 3.2.4. *Are there nice formulas for the roots r_i in terms of the coefficients a_i ? Investigate for various choices of n .*

A better explanation of the connection between primes and zeros of $\zeta(s)$ is through complex analysis and contour integration, which we now quickly review and then apply. Two functions play a central role in what follows. The first one (see §2.1) is the von Mangoldt function Λ , defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, p \text{ prime} \\ 0 & \text{otherwise.} \end{cases} \quad (3.37)$$

We also define a function ψ on the set of positive real numbers by

$$\psi(x) = \sum_{n \leq x} \Lambda(x). \quad (3.38)$$

Exercise 3.2.5. *Use Chebyshev's Theorem (Theorem 2.3.9) to prove*

$$x \ll \psi(x) \ll x. \quad (3.39)$$

Exercise 3.2.6. *Prove most of the contribution to $\psi(x)$ comes from primes and not prime powers. Explicitly, show the contribution from p^k ($k \geq 2$) is $O(x^{1/2} \log x)$. Note $\psi(x)$ is a weighted counting function of primes, and the techniques of §2.3.4 allow us to remove these weights easily. See also §3.2.2 and §14.7.*

We assume basic knowledge of complex numbers, though knowledge of Green's Theorem from multivariable calculus (see Theorem A.2.9) is needed to complete the proofs of some claims. We provide a heuristic as to how properties of the zeros of $\zeta(s)$ give information about the primes. Any complex number z can be written either as $x + iy$ or as $re^{i\theta}$, with $r \in [0, \infty)$ and $\theta \in [0, 2\pi)$; note by De Moivre's Theorem that $e^{i\theta} = \cos(\theta) + i \sin(\theta)$. If $z \neq 0$ then there is a unique representation of z as $re^{i\theta}$, with r and θ restricted as above.

Exercise 3.2.7. Write down the change of variables from $(x, y) \rightarrow (r, \theta)$ and from $(r, \theta) \rightarrow (x, y)$.

Theorem 3.2.8. Let $r > 0$ and $n \in \mathbb{Z}$. Then

$$\frac{1}{2\pi i} \int_{\theta=0}^{2\pi} (re^{i\theta})^n ire^{i\theta} d\theta = \begin{cases} 1 & \text{if } n = -1 \\ 0 & \text{otherwise.} \end{cases} \quad (3.40)$$

Sketch of the proof. In (3.40) we have $e^{i(n+1)\theta} = \cos((n+1)\theta) + i \sin((n+1)\theta)$ (de Moivre's Theorem). If $n = -1$ the integrand is 1 and the result follows; if $n \neq -1$ the integral is zero because we have an integral number of periods of \sin and \cos (see the following exercise). \square

Exercise 3.2.9. For $m > 0$, show that $\sin(mx)$ and $\cos(mx)$ are periodic functions of period $\frac{2\pi}{m}$ (i.e., $f(x + \frac{2\pi}{m}) = f(x)$). If m is a positive integer, these functions have an integral number of periods in $[0, 2\pi]$.

If we consider all $z \in \mathbb{C}$ with $|z| = r > 0$, this set is a circle of radius r about the origin. As only θ varies, we have $dz = izd\theta$, and the integral in (3.40) becomes

$$\frac{1}{2\pi i} \oint_{|z|=r} z^n dz = \begin{cases} 1 & \text{if } n = -1 \\ 0 & \text{otherwise.} \end{cases} \quad (3.41)$$

The symbol \oint denotes that we are integrating about a closed curve, and $|z| = r$ states which curve. Note the answer is independent of the radius.

Exercise 3.2.10. Prove

$$\frac{1}{2\pi i} \oint_{|z-z_0|=r} (z-z_0)^n dz = \begin{cases} 1 & \text{if } n = -1 \\ 0 & \text{otherwise.} \end{cases} \quad (3.42)$$

We state, but do not prove, the following theorems on **contour integration** (see, for example, [Al, La6, SS2]):

Theorem 3.2.11. Let $f(z)$ be a meromorphic function (see Definition 3.1.13) in a disk of radius r about z_0 , say

$$f(z) = \sum_{n \geq n_0} a_n (z - z_0)^n. \quad (3.43)$$

If $f(z)$ is not identically zero, for r sufficiently small f has no poles in this disk except possibly at z_0 ; it has a pole if $n_0 < 0$. Then

$$\frac{1}{2\pi i} \oint_{|z-z_0|=r} f(z) dz = a_{-1}. \quad (3.44)$$

Sketch of the proof. If we could interchange summation and integration, we would have

$$\frac{1}{2\pi i} \oint f(z) dz = \frac{1}{2\pi i} \oint \sum_{n \geq n_0} a_n (z - z_0)^n dz = \sum_{n \geq n_0} a_n \frac{1}{2\pi i} \oint (z - z_0)^n dz. \quad (3.45)$$

The only non-zero integral is when $n = -1$, which gives 1. The difficulty is in justifying the interchange. \square

Theorem 3.2.12. Let $f(z)$ be a meromorphic function in a disk of radius r about the origin, with finitely many poles (at z_1, z_2, \dots, z_N). Then

$$\frac{1}{2\pi i} \oint_{|z|=r} f(z) dz = \sum_{n=1}^N a_{-1}(z_n), \quad (3.46)$$

where $a_{-1}(z_n)$ is the **residue** (the -1 coefficient) of the Taylor series expansion of $f(z)$ at z_n .

The proof is similar to the standard proof of Green's Theorem (see Theorem A.2.9). In fact, the result holds not just for integrating over circular regions, but over any "nice" region. All that matters are whether there are any poles of f in the region, and if so, what their residues are.

Exercise 3.2.13 (Logarithmic Derivative). Let $f(z) = a_n(z - z_0)^n$, $n \neq 0$. Show

$$\frac{f'(z)}{f(z)} = \frac{na_n}{z - z_0}. \quad (3.47)$$

Note $\frac{f'(z)}{f(z)} = \frac{d \log f(z)}{dz}$. In particular, this implies

$$\frac{1}{2\pi i} \oint_{|z-b|=r} \frac{f'(z)}{f(z)} dz = \begin{cases} na_n & \text{if } z_0 \text{ is in the disk of radius } r \text{ about } b \\ 0 & \text{otherwise.} \end{cases} \quad (3.48)$$

In the above exercise, note it does not matter if $n > 0$ (z_0 is a zero) or $n < 0$ (z_0 is a pole): $\frac{f'(z)}{f(z)}$ has a simple pole at z_0 with residue na_n . The above result generalizes to $f(z) = \sum_{m \geq n} a_m(z - z_0)^m$. One can show

$$\frac{f'(z)}{f(z)} = \frac{n}{z - z_0} + h(z), \quad (3.49)$$

where

$$h(z) = \sum_{m=0}^{\infty} b_m(z - z_0)^m, \quad (3.50)$$

and if $f(z)$ has at most one zero or pole in the disk of radius r about b (namely, z_0), then

$$\frac{1}{2\pi i} \oint_{|z-b|=r} \frac{f'(z)}{f(z)} dz = \begin{cases} n & \text{if } z_0 \text{ is in the disk of radius } r \text{ about } b \\ 0 & \text{otherwise.} \end{cases} \quad (3.51)$$

Theorem 3.2.14. Let $f(z)$ be a meromorphic function on a disk of radius r about z_0 . Assume the only zeros or poles of $f(z)$ inside a disk of radius r about b are z_1, \dots, z_N . Then

$$\frac{1}{2\pi i} \oint_{|z-b|=r} \frac{f'(z)}{f(z)} dz = \sum_{n=1}^N \text{ord}_f(z_n). \quad (3.52)$$

(See Definition 3.1.12 for the definition of $\text{ord}_f(z_n)$.)

This result is also true if we consider “nice” regions instead of a disk. Note $\frac{f'(z)}{f(z)} = \frac{d \log f(z)}{dz}$ is the logarithmic derivative of $f(z)$; these results state that the logarithmic derivative encodes information about the zeros and poles of f . We now use these results to sketch the link between primes and zeros of $\zeta(s)$.

Exercise^(h) 3.2.15 (Important). For $\Re s > 1$ show that

$$\frac{\zeta'(s)}{\zeta(s)} = - \sum_n \frac{\Lambda(n)}{n^s}. \quad (3.53)$$

A common method to deal with products is to take the logarithm (see Theorem 10.2.4 for another example) because this converts a product to a sum, and we have many methods to understand sums.

The idea is as follows: we integrate each side of (3.53) over the perimeter of a box (the location is chosen to ensure convergence of all integrals). For convenience, we first multiply each side by $\frac{x^s}{s}$, where x is an arbitrary parameter that we send to infinity. This will yield estimates for $\pi(x)$. We then have

$$\oint_{\text{perimeter}} \frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} ds = - \oint_{\text{perimeter}} \sum_n \frac{\Lambda(n)}{n^s} \frac{x^s}{s} ds. \quad (3.54)$$

Using results from complex analysis, one shows that $\oint \frac{(x/n)^s}{s} ds$ is basically 1 if $n < x$ and 0 otherwise. For the left hand side, we get contributions from the zeros and poles of $\zeta(s)$ in the region. $\zeta(s)$ has a pole at $s = 1$ of residue 1. Let ρ range over the zeros of $\zeta(s)$. One needs to do some work to calculate the residues of $\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s}$ at the zeros and poles of $\zeta(s)$; the answer is basically $\frac{x^\rho}{\rho}$. Combining the pieces and multiplying by -1 yields

$$x - \sum_{\rho: \zeta(\rho)=0} \frac{x^\rho}{\rho} = \sum_{n \leq x} \Lambda(n). \quad (3.55)$$

The $x = x^1$ is from the pole of $\zeta(s)$ at $s = 1$. The above is known as an Explicit Formula (to be discussed in detail in §3.2.5). Note $|x^\rho| = x^{\Re \rho}$. If we knew all the zeros had $\Re \rho = \frac{1}{2}$, then the left hand side of (3.55) is approximately $x + O(x^{1/2})$ (we are ignoring numerous convergence issues in an attempt to describe the general features). One can pass from knowledge of $\sum_{n \leq x} \Lambda(x)$ to $\pi(x) = \sum_{n \leq x} 1$: first note the contributions from the prime powers in the sum is at most $x^{1/2} \log x$, and then use Partial Summation (see §2.3.4 for details).

We begin to see now why the Euler Product is such an important property of $\zeta(s)$. In Exercise 3.2.15 we considered the logarithmic derivative of $\zeta(s)$; because of the Euler Product we have a very tractable expression in terms of sums over the primes. Contour integration then relates sums over zeros to sums over primes. If we did not have an Euler Product then we would not have a nice expression on the prime side.

Exercise 3.2.16. Using Partial Summation, show if $\sum_{n \leq x} \Lambda(x) = x + O(x^{\frac{1}{2} + \epsilon})$ then $\pi(x) = \frac{x}{\log x}$ plus a smaller error term. How small can one take the error term to be?

Thus, using complex analysis, information on the location of the zeros of $\zeta(s)$ translates to information on the number of primes. To date, it is unknown that there is some number $\sigma_0 \in (\frac{1}{2}, 1)$ such that all zeros have real part at most σ_0 . The best known results are that there are no zeros on the line $\Re s = 1$, and there are no zeros “slightly” to the left of this line (the amount we can move left decreases with how high we are on the line). In fact, $\zeta(1 + it) \neq 0$ is equivalent to the Prime Number Theorem! See [Da2, EE] for more details.

Remark 3.2.17. Another way to see the connection between zeros of $\zeta(s)$ and primes is through the product expansion of $\zeta(s)$ in terms of its zeros (see §3.2.3).

Remark 3.2.18. As we saw in Remark 2.3.20, because the logarithmic derivative of $\zeta(s)$ involves the von Mangoldt $\Lambda(n)$ -function, we see it is often easier to weight the primes by slowly varying logarithmic factors. This is present throughout modern number theory, namely it is a common technique to study weighted prime sums because they occur more naturally and then remove the weights by partial summation.

Exercise 3.2.19. *The Prime Number Theorem is essentially equivalent to the statement that if $\zeta(\rho) = 0$ then $\Re(\rho) < 1$ (the technical difficulty is exchanging the summation on ρ with the limit as $x \rightarrow \infty$ in (3.55): see [Ed] for details). Mertens gave an elegant proof that $\Re(\rho) < 1$ by a clever application of a trigonometric identity. We sketch his argument. Prove the following statements:*

1. $3 + 4 \cos \theta + \cos 2\theta \geq 0$ (Hint: Consider $(\cos \theta - 1)^2$);
2. For $s = \sigma + it$, $\log \zeta(s) = \sum_p \sum_{k=1}^{\infty} \frac{p^{-k\sigma}}{k} e^{-itk \log p}$;
3. $\Re \log \zeta(s) = \sum_p \sum_{k=1}^{\infty} \frac{p^{-k\sigma}}{k} \cos(t \log p^k)$;
4. $3 \log \zeta(\sigma) + 4 \Re \log \zeta(\sigma + it) + \Re \log \zeta(\sigma + 2it) \geq 0$;
5. $\zeta(\sigma)^3 |\zeta(\sigma + it)^4 \zeta(\sigma + 2it)| \geq 1$;
6. If $\zeta(1 + it) = 0$, then as σ decreases to 1 from above, $|\zeta(\sigma + it)| < A(\sigma - 1)$ for some A ;
7. As $\zeta(\sigma) \sim (\sigma - 1)^{-1}$ ($\zeta(s)$ has a simple pole of residue 1 at $s = 1$) and $\zeta(\sigma + 2it)$ is bounded as $\sigma \rightarrow 1$ (the only pole of $\zeta(s)$ is at $s = 1$), the above implies that if $\zeta(1 + it) = 0$ then as $\sigma \rightarrow 1$, $\zeta(\sigma)^3 |\zeta(\sigma + it)^4 \zeta(\sigma + 2it)| \rightarrow 0$. As the product must be at least 1, this proves $\zeta(1 + it) \neq 0$.

The key to Mertens’ proof is the positivity of a certain trigonometric expression.

3.2.3 Product Expansion

Below we assume the reader is familiar with complex analysis [Al, La6, SS2]. Another interesting property, first noted in Riemann’s original paper, is the following:

Proposition 3.2.20. *The function $\xi(s)$ has the following product representation*

$$\xi(s) = e^{A+Bs} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}}, \quad (3.56)$$

with A, B are constants and ρ runs through the non-trivial zeros of the zeta function.

Sketch of proof. A non-constant entire function $f(z)$ is said to be of **finite order** if there exists a number $\alpha > 0$ such that

$$|f(z)| = O(e^{|z|^\alpha}) \quad \text{as } |z| \rightarrow \infty. \quad (3.57)$$

If $f(z)$ is of finite order, the infimum of the numbers α is called the order of $f(z)$. If r_1, r_2, \dots are the absolute values of the zeros of $f(z)$, then it follows from Jensen's formula that for $\beta > \text{order of } f(z)$, the series $\sum_1^\infty r_n^{-\beta}$ converges, provided of course $f(0) \neq 0$. It is then a theorem of Weierstrass that if $f(z)$ is an entire function of order 1 with zeros z_1, z_2, \dots (none of which are zero), then there are constants A, B with

$$f(z) = e^{A+Bz} \prod_n \left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}}. \quad (3.58)$$

To prove the proposition we need to show that for any $\alpha > 1$ we have

$$|\xi(s)| = O(e^{|s|^\alpha}) \quad (3.59)$$

as $|s| \rightarrow \infty$. In fact, one shows

$$|\xi(s)| < \exp(C|s| \log |s|) \quad (3.60)$$

as $|s| \rightarrow \infty$. It is clear that there is a constant C_1 with

$$\left| \frac{1}{2}s(s-1)\pi^{-\frac{1}{2}s} \right| < \exp(C_1|s|). \quad (3.61)$$

Also Stirling's formula (Theorem 3.1.16(3)) shows the existence of C_2 such that

$$\left| \Gamma\left(\frac{s}{2}\right) \right| < \exp(C_2|s| \log |s|). \quad (3.62)$$

We need to control $\zeta(s)$. For this we have the following:

$$\begin{aligned} \zeta(s) &= \sum_{n=1}^{\infty} n \left[\frac{1}{n^s} - \frac{1}{(n+1)^s} \right] \\ &= s \sum_{n=1}^{\infty} n \int_n^{n+1} t^{-s-1} dt \\ &= s \sum_{n=1}^{\infty} \int_n^{n+1} [t] t^{-s-1} dt \\ &= s \int_1^{\infty} [t] t^{-s-1} dt \\ &= s \int_1^{\infty} t^{-s} dt - s \int_1^{\infty} \{t\} t^{-s-1} dt \\ &= \frac{s}{s-1} + O(s). \end{aligned} \quad (3.63)$$

This shows that $|\zeta(s)| < C_3|s|$ for $|s|$ large. Multiplying the inequalities gives (3.60). \square

Remark 3.2.21. Fine tuning the same argument shows that $\zeta(s)$ has an infinite number of zeros in the critical strip; see Chapter 12 of [Da2] for more details. Comparing formula (3.58) with the Euler product hints at a mysterious relationship between the zeros of the zeta function and prime numbers!

Remark 3.2.22. Note the above argument gives a meromorphic continuation of $\zeta(s)$ to $\Re s > 0$ with a simple pole of residue 1 at $s = 1$.

3.2.4 Riemann-Siegel Zeta Function and Hardy's Theorem

The Riemann-Siegel zeta function $\Xi(t)$ is defined by

$$\Xi(t) = -\frac{1}{2} \left(t^2 + \frac{1}{4} \right) \pi^{-\frac{1}{4} - \frac{it}{2}} \Gamma \left(\frac{1}{4} + \frac{it}{2} \right) \zeta \left(\frac{1}{2} + it \right). \quad (3.64)$$

Exercise^(h) 3.2.23. Prove that $\Xi(t)$ is an entire function. It is real for real t , and is an even function: $\Xi(t) = \Xi(-t)$.

A zero of $\zeta(s)$ on $\Re s = \frac{1}{2}$ corresponds to a real zero of $\Xi(t)$. As $\Xi(t)$ is continuous, in order to detect a real zero we simply need to search for places where the sign of $\Xi(t)$ changes (see also Exercise 5.3.21). This is a very useful observation, and in fact is one of the most important methods to locate zeros of $\zeta(s)$.

Remark 3.2.24 (Divide and Conquer). In practice one chooses a small step size h and evaluates $\Xi(t_0 + nh)$ for $n \in \{0, \dots, N\}$. Every sign change corresponds to a zero of $\zeta(s)$, and repeating the calculation near the sign change with a smaller step size yields better approximations to the zero; see Exercise 5.3.21. If there is a zero of even order, however, there will not be a sign change to detect while for zeros of odd order there is only one sign change and only one zero is detected. Thus the method cannot detect multiplicities of zeros. Using contour integration (which gives the number of zeros in a region), we can ensure that we have found all the zeros. Moreover, once we have seen there are M zeros with imaginary part at most T , and if we have shown there are M such zeros on the critical line, we will have experimentally verified RH in this region. See [Od1, Od2] for more on these algorithms, and Chapter 15 for a connection between zeros of $\zeta(s)$ and eigenvalues of matrices!

In the following series of exercises we show that infinitely many of the zeros of the Riemann zeta function lie on the critical line. This was originally proved by Hardy in 1914; in 1942 Selberg proved that in fact a positive proportion of the zeros lie on the line. The proof of this fact, though within the scope of this manuscript, is very technical. See [Ed, EE, Ti] for details.

Theorem 3.2.25 (Hardy, 1914). *Infinitely many of the zeros of the Riemann zeta function lie on the line $\Re s = \frac{1}{2}$.*

There are various proofs of this fact; a few are recorded in [Ti]. We sketch the argument on page 258 of [Ti].

Sketch of proof. We show that the function $\Xi(t)$ has infinitely many sign changes. For this we use the following theorem of Fejér:

Theorem 3.2.26 (Fejér). *Let n be a positive integer. Then the number of sign changes in the interval $(0, a)$ of a continuous function $f(x)$ is not less than the number of sign changes of the sequence*

$$f(0), \int_0^a f(t) dt, \dots, \int_0^a f(t)t^n dt. \quad (3.65)$$

We prove Fejér's theorem after proving Hardy's theorem. To apply Fejér's theorem, one proves

$$\lim_{\alpha \rightarrow \frac{\pi}{4}} \int_0^\infty \frac{\Xi(t)}{t^2 + \frac{1}{4}} t^{2n} \cosh \alpha t dt = \frac{(-1)^n \pi \cos \frac{\pi}{8}}{2^{2n}}. \quad (3.66)$$

as sketched in the following exercise:

Exercise 3.2.27. *Use (3.21) to prove that*

$$\int_0^\infty \frac{\Xi(t)}{t^2 + \frac{1}{4}} \cos xt dt = \frac{1}{2} \pi \left[e^{\frac{1}{2}x} - 2e^{-\frac{1}{2}x} \omega(e^{-2x}) \right]. \quad (3.67)$$

Inserting $x = -i\alpha$ gives

$$\frac{2}{\pi} \int_0^\infty \frac{\Xi(t)}{t^2 + \frac{1}{4}} \cosh \alpha t dt = e^{-\frac{1}{2}i\alpha} - 2e^{\frac{1}{2}i\alpha} \omega(e^{2i\alpha}). \quad (3.68)$$

1. Show that the above can be differentiated with respect to α any number of times if $\alpha < \frac{1}{4}\pi$.
2. Use the first part to show

$$\begin{aligned} \frac{2}{\pi} \int_0^\infty \frac{\Xi(t)}{t^2 + \frac{1}{4}} t^{2n} \cosh \alpha t dt \\ = \frac{(-1)^n \cos \frac{1}{2}\alpha}{2^{2n-1}} - 2 \left(\frac{d}{d\alpha} \right)^{2n} e^{\frac{1}{2}i\alpha} \left[\frac{1}{2} + \omega(e^{2i\alpha}) \right]. \end{aligned} \quad (3.69)$$

3. Show that $\omega(x+i) = 2\omega(4x) - \omega(x)$. Use the functional equation of ω to conclude

$$\omega(x+i) = \frac{1}{\sqrt{x}} \omega\left(\frac{1}{4x}\right) - \frac{1}{\sqrt{x}} \omega\left(\frac{1}{x}\right) - \frac{1}{2}. \quad (3.70)$$

4. Use (3.70) to show that $\frac{1}{2} + \omega(x)$ and all its derivatives tend to zero as $x \rightarrow i$ in the angle $|\arg(x-i)| < \frac{1}{2}\pi$. Show that this observation combined with (3.69) gives (3.66).

Note (3.66) implies that given any N there is an $a = a(N)$ large and an $\alpha = \alpha(N)$ very close to $\frac{\pi}{4}$ such that the expression

$$\int_0^a \frac{\Xi(t)}{t^2 + \frac{1}{4}} t^{2n} \cosh \alpha t dt \quad (3.71)$$

has the same sign as $(-1)^n$ for $n \in \{0, \dots, N\}$. Now Fejér's theorem implies that $\Xi(t)$ has at least N sign changes in $a(N)$. As N is arbitrary the theorem follows. \square

Proof of Fejér's theorem. We first need a lemma:

Lemma 3.2.28 (Fekete). *The number of changes in sign in the interval $(0, a)$ of a continuous function $f(x)$ is not less than the number of changes in sign in the sequence*

$$f_0(a), f_1(a), \dots, f_n(a), \quad (3.72)$$

where $f_0(x) = f(x)$ and

$$f_\nu(x) = \int_0^x f_{\nu-1}(t) dt \quad (\nu = 1, 2, \dots, n). \quad (3.73)$$

Exercise^(h) 3.2.29. *Use induction and interchanging the order of integration to show that*

$$f_\nu(x) = \frac{1}{(\nu-1)!} \int_0^x (x-t)^{\nu-1} f(t) dt, \quad (3.74)$$

and prove that Fekete's Lemma implies Fejér's Theorem.

By the above exercise, we just need to prove Fekete's Lemma. We proceed by induction. If $n = 1$, the lemma is obvious. Now assume the lemma for $n - 1$. Suppose there are at least k changes of sign in the sequence $f_1(a), \dots, f_n(a)$. Then $f_1(x)$ has at least k changes of sign. The following exercise completes the proof:

Exercise 3.2.30. *In the above setting,*

1. *if $f(a)$ and $f_1(a)$ have the same sign, $f(x)$ has at least k changes of sign;*
2. *if $f(a)$ and $f_1(a)$ have different signs, $f(x)$ has at least $k + 1$ changes of sign.*

This completes the proof of Fejér's theorem. □

3.2.5 Explicit Formula

The following proposition, first proved by von Magnoldt in 1895, highlights the relationship between the prime numbers and the zeros of the Riemann zeta function that we alluded to in (3.55). For more on Explicit Formulas, see Chapter 18. Recall

$$\psi(x) = \sum_{n \leq x} \Lambda(n). \quad (3.75)$$

Theorem 3.2.31 (Explicit Formula for $\zeta(s)$). *We have*

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2} \log(1 - x^2), \quad (3.76)$$

where ρ ranges over all the non-trivial zeros of the Riemann zeta function (i.e., $\Re \rho \in [0, 1]$).

Exercise 3.2.32. *This exercise is the starting point of the proof of the above theorem. Set*

$$I(x, R) = \frac{1}{2\pi i} \int_{c-iR}^{c+iR} \frac{x^s}{s} ds, \quad (3.77)$$

and

$$\delta(x) = \begin{cases} 0 & 0 < x < 1 \\ \frac{1}{2} & x = 1 \\ 1 & x > 1. \end{cases} \quad (3.78)$$

Prove that

$$|I(x, R) - \delta(x)| < \begin{cases} x^c \min(1, R^{-1} |\log x|^{-1}) & \text{if } x \neq 1 \\ \frac{c}{R} & \text{if } x = 1. \end{cases} \quad (3.79)$$

Exercise 3.2.33. *Prove that*

$$\psi(x) = \sum_{n=1}^{\infty} \Lambda(n) \delta\left(\frac{n}{x}\right) \quad (3.80)$$

and

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}. \quad (3.81)$$

The proof of the proposition then follows from a careful analysis of the difference

$$\left| \psi(x) - \frac{1}{2\pi i} \int_{c-iR}^{c+iR} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) \frac{x^s}{s} ds \right|, \quad (3.82)$$

using the previous exercise with appropriate choices of c and $R \rightarrow \infty$. One then shows that with such choices the difference approaches 0, and the proposition then follows from the computation of the integral appearing in the expression. For this one uses Cauchy's theorem, noting the function $\frac{\zeta'(s)}{\zeta(s)}$ has its poles at the zeros of $\zeta(s)$ with an additional pole coming from $s = 0$ which is responsible for the term $-\frac{\zeta'(0)}{\zeta(0)}$. The non-trivial zeros of the zeta contribute $-\sum_{\rho} x^{\rho}/\rho$ and the trivial ones contribute $-\frac{1}{2} \log(1-x^2)$. We refer the reader to §17 of [Da2] for the details; see also [Sch].

Exercise 3.2.34. *Assuming the Riemann hypothesis, prove that*

$$\psi(x) = x + O(x^{\frac{1}{2}} \log^2 x), \quad (3.83)$$

and vice versa.

3.2.6 Li's constants and the Riemann Hypothesis

We state an interesting criterion for the validity of the Riemann hypothesis. This section is independent of the rest of the book, and the interested reader should see [BoLa, Vo] for more details. Our exposition of this topic closely follows [BoLa].

As usual, denote a typical complex zero of $\zeta(s)$ by ρ . For each positive integer n we define Li's constants λ_n by

$$\lambda_n = \sum_{\rho} \left[1 - \left(1 - \frac{1}{\rho} \right)^n \right], \quad (3.84)$$

where the sum over ρ is taken as

$$\sum_{\rho} \left[1 - \left(1 - \frac{1}{\rho} \right)^n \right] = \lim_{T \rightarrow \infty} \sum_{|\Im \rho| \leq T} \left[1 - \left(1 - \frac{1}{\rho} \right)^n \right]. \quad (3.85)$$

Theorem 3.2.35 (Li's criterion). *The Riemann hypothesis is equivalent to $\lambda_n > 0$ for $n = 1, 2, 3, \dots$*

Another interpretation of the sequence λ_n is the following. As before we set

$$\xi(s) = \frac{1}{2} s(s-1) \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s). \quad (3.86)$$

Then

$$\lambda_n = \frac{1}{(n-1)!} \frac{d^n}{ds^n} [s^{n-1} \log \xi(s)] \Big|_{s=1}. \quad (3.87)$$

Exercise 3.2.36. *Prove the above statement.*

We sketch the proof in [BoLa] of Li's criterion. This simple proof shows that Li's criterion is combinatorial in nature, and holds for much more general settings. We begin with some needed terminology.

Definition 3.2.37. A **multiset** is a set whose elements have positive integral multiplicities assigned to them.

Definition 3.2.38. Let \mathcal{R} be a multiset and $(a_{\rho})_{\rho \in \mathcal{R}}$ a sequence indexed by the elements of \mathcal{R} . Then if the limit

$$\lim_{T \rightarrow \infty} \sum_{|\Im \rho| \leq T} a_{\rho} \quad (3.88)$$

exists we say the sum is **-convergent*, and we denote this by $\sum_{\rho \in \mathcal{R}} a_{\rho}$.

As we will ultimately be interested in multisets defined by zeros of $\zeta(s)$, we will assume that our multisets appearing below do not contain 0 or 1.

Lemma 3.2.39. *Let \mathcal{R} be a multiset of complex numbers ρ with*

$$\sum_{\rho \in \mathcal{R}} \frac{1 + |\Re \rho|}{(1 + |\rho|)^2} < \infty. \quad (3.89)$$

Then for all integers n the sum

$$\sum_{\rho \in \mathcal{R}} \Re \left[1 - \left(1 - \frac{1}{\rho} \right)^n \right] \quad (3.90)$$

*converges absolutely. Moreover, if $\sum_{\rho \in \mathcal{R}} \frac{1}{\rho}$ is *-convergent, then*

$$\lambda_n = \sum_{\rho \in \mathcal{R}} \left[1 - \left(1 - \frac{1}{\rho} \right)^n \right] \quad (3.91)$$

*is also *-convergent.*

Exercise^(h) 3.2.40. Prove Lemma 3.2.39.

The main result is the following:

Theorem 3.2.41. Let \mathcal{R} be a multiset that satisfies the conditions of Lemma 3.2.39. Then the following conditions are equivalent:

1. $\Re \rho \leq \frac{1}{2}$;
2. $\sum_{\rho \in \mathcal{R}} \Re \left[1 - \left(1 - \frac{1}{\rho} \right)^{-n} \right] \geq 0$ for $n = 1, 2, 3, \dots$;
3. for every $\epsilon > 0$ there is a constant $c(\epsilon)$ such that for $n = 1, 2, 3, \dots$

$$\sum_{\rho \in \mathcal{R}} \Re \left[1 - \left(1 - \frac{1}{\rho} \right)^{-n} \right] \geq -c(\epsilon)e^{\epsilon n}. \quad (3.92)$$

The following exercise shows how Li's criterion for $\zeta(s)$ (Theorem 3.2.35) follows from Theorem 3.2.41 (in particular, how we pass from having an exponent of $-n$ in Theorem 3.2.41 to an exponent of n in Theorem 3.2.35).

Exercise^(h) 3.2.42. Prove the following:

1. Let \mathcal{R}_ζ be the multiset consisting of the non-trivial zeros of $\zeta(s)$. Prove that \mathcal{R}_ζ satisfies the conditions of Lemma 3.2.39. Also prove that if $\rho \in \mathcal{R}_\zeta$, then $\bar{\rho}, 1 - \rho, 1 - \bar{\rho} \in \mathcal{R}_\zeta$.
2. Apply Theorem 3.2.41 to \mathcal{R}_ζ and $1 - \mathcal{R}_\zeta = \{1 - \rho; \rho \in \mathcal{R}_\zeta\}$ to deduce Theorem 3.2.35.

Proof of Theorem 3.2.41. For $\rho \neq 1$ we have

$$\left| 1 - \frac{1}{\rho} \right|^{-2} = 1 + \frac{2\Re \rho - 1}{|1 - \rho|^2}; \quad (3.93)$$

giving (1) \Rightarrow (2). Note (2) \Rightarrow (3) is obvious. To see (3) \Rightarrow (1), we proceed as follows. Suppose (1) does not hold. Then for at least one $\rho \in \mathcal{R}$ we have $\Re \rho > \frac{1}{2}$. On the other hand, as

$$\sum_{\rho \in \mathcal{R}} \frac{1}{(1 + |\rho|)^2} < +\infty \quad (3.94)$$

we have $|\rho| \rightarrow \infty$, which then implies that $\rho^{-1} \rightarrow 0$ and consequently

$$\left| 1 - \frac{1}{\rho} \right| \rightarrow 1. \quad (3.95)$$

This combined with the elementary inequality (3.93) from above gives

$$\frac{2\Re \rho - 1}{|1 - \rho|^2} \rightarrow 0, \quad (3.96)$$

hence the maximum over ρ of this quantity is attained and there are finitely many elements $\rho_k \in \mathcal{R}$, $k = 1, 2, \dots, K$, such that

$$\left|1 - \frac{1}{\rho}\right|^{-1} = 1 + t \quad (3.97)$$

is a maximum. We have $t > 0$ as $\Re \rho > \frac{1}{2}$ for at least one ρ . For the other ρ we have

$$\left|1 - \frac{1}{\rho}\right|^{-1} < 1 + t - \delta \quad (3.98)$$

for a fixed small positive δ . Let ϕ_k be the argument of $1 - 1/\rho_k$. Then by definition

$$1 - \left(1 - \frac{1}{\rho_k}\right)^{-n} = 1 - (1 + t)^n e^{-in\phi_k}. \quad (3.99)$$

For $\rho \neq \rho_k$ we have

$$\left|1 - \frac{1}{\rho}\right|^{-1} < (1 + t - \delta)^n, \quad (3.100)$$

and also if $|\rho| > n$ then

$$\Re \left[1 - \left(1 - \frac{1}{\rho_k}\right)^{-n}\right] = O\left(\frac{n|\Re \rho| + n^2}{|\rho|^2}\right). \quad (3.101)$$

Exercise^(h) 3.2.43. *Verify the last inequality.*

The last inequality implies that the sum over $|\rho| > n$ is $O(n^2)$ (prove this). Also the number of elements with $|\rho| \leq n$ is $O(n^2)$ (prove this). Hence elements other than the ρ_k contribute at most $O(n^2(1 + t - \delta)^n)$ to $\sum \Re [1 - (1 - 1/\rho)^{-n}]$. The remaining elements ρ_k contribute

$$K - (1 + t)^n \sum_{k=1}^K \cos(n\phi_k). \quad (3.102)$$

Consequently

$$\sum_{\rho \in \mathcal{R}} \Re [1 - (1 - 1/\rho)^{-n}] = K - (1 + t)^n \sum_{k=1}^K \cos(n\phi_k) + O(n^2(1 + t - \delta)^n). \quad (3.103)$$

By Exercise A.4.7 there are infinitely many n with $\sum_{k=1}^K \cos(n\phi_k)$ arbitrarily close to K . For such n the expression is negative and arbitrarily large in absolute value. This shows $3 \implies 1$. \square

Exercise 3.2.44. *Complete the details.*

The paper of Bombieri-Lagarias contains the following interesting interpretation of Li's constants:

$$\begin{aligned} \lambda_n = & - \sum_{j=1}^n \binom{n}{j} \frac{(-1)^{j-1}}{(j-1)!} \lim_{\epsilon \rightarrow 0^+} \left\{ \sum_{m \leq \frac{1}{\epsilon}} \frac{\Lambda(m)(\log m)^{j-1}}{m} - \frac{1}{j} \left(\log \frac{1}{\epsilon}\right)^j \right\} \\ & + 1 - (\log 4\pi + \gamma) \frac{n}{2} - \sum_{j=2}^n (-1)^{j-1} \binom{n}{j} (1 - 2^{-j}) \zeta(j). \end{aligned} \quad (3.104)$$

The observant reader will notice that as λ_n is a sum over the zeros of $\zeta(s)$, (3.104) very much resembles an explicit formula (see §3.2.5). In fact, the proof of (3.104) uses a variant of an explicit formula due to Weil. We advise the reader to consult the very interesting paper [BoLa] for a detailed proof.

Exercise 3.2.45. Use the Bombieri-Lagarias' formula to evaluate $\sum_{\rho} \frac{1}{\rho}$.

Remark 3.2.46. It would be very interesting to numerically test the values of Li's constants to check the validity of the Riemann Hypothesis. Recently, Voros [Vo] has found the following equivalent formulation of the Riemann Hypothesis:

$$\lambda_n \sim \frac{1}{2}n(\log n - \log 2\pi - 1 + \gamma) \quad (3.105)$$

as $n \rightarrow \infty$. He has verified that for $n < 3300$ the above formula agrees well with numerical data.

3.3 DIRICHLET CHARACTERS AND L -FUNCTIONS

We have seen that knowledge of $\zeta(s)$ translates to knowledge of primes, and that many questions concerning the distribution of primes are related to questions on the distribution of zeros of $\zeta(s)$. The zeta function is the first of many L -**functions**. To us, an L -function is a Dirichlet series that converges for $\Re s$ sufficiently large, has some type of Euler product expansion, and is "built" from arithmetic information. Similar to $\zeta(s)$, we can glean much from an analysis of these L -functions. In this section we concentrate on L -functions from Dirichlet characters with different moduli (to be defined below). Just as $\zeta(s)$ can be used to prove there are infinitely many primes and count how many there are less than x , the L -functions from Dirichlet characters give information about primes in arithmetic progressions. With the exception of L -functions of elliptic curves (see §4.2.2), we only investigate the Riemann zeta function and Dirichlet L -functions. See [Se] for an excellent introduction to additional L -functions and their connections to the arithmetic functions of Chapter 2.

Fix two positive integers m and a and look at all numbers congruent to a modulo m : $\{x : x = nm + a, n \in \mathbb{N}\}$. If m and a have a common divisor, there can be at most one prime congruent to a modulo m . If m and a are relatively prime, Dirichlet proved that not only are there infinitely many primes in this progression, but also that all such progressions have to first order the same number of primes in the limit. Explicitly, there are $\phi(m)$ numbers a that are relatively prime to m and $\pi(x)$ primes at most x . Let $\pi_{m,a}(x)$ denote the number of primes at most x congruent to a modulo m . Then

$$\pi_{m,a}(x) = \frac{1}{\phi(m)} \frac{x}{\log x} + o_a \left(\frac{1}{\phi(m)} \frac{x}{\log x} \right). \quad (3.106)$$

The main term is independent of a ; how the error term varies with a , and what is its true dependence on m , is another story (see for example [Mon1, RubSa, Va]). Probabilistic arguments (see [Mon1] and the remark below) lead to natural conjectures for the m -dependence, and these have far reaching consequences for number theory; for one example, see §18.2.3.

Remark 3.3.1. We sketch some heuristics for the observations mentioned above. For ease of exposition, instead of keeping track of factors of $\log x$ we absorb these into an error x^ϵ . Assuming the Riemann Hypothesis (RH), the error in counting the number of primes at most x is of size $x^{\frac{1}{2}+\epsilon}$. For a fixed m , there are $\phi(m)$ residue classes. To first order, Dirichlet's Theorem asserts each residue class has the same number of primes, roughly $\frac{\pi(x)}{\phi(m)}$. By the Central Limit Theorem (see §8.4), if $\eta_1, \dots, \eta_N \in \{-1, 1\}$, we expect a typical sum $\eta_1 + \dots + \eta_N$ to be of size \sqrt{N} ; the philosophy of square root cancellation asserts similar behavior happens in many situations (see also §4.4, §13.3.2 and Remark 13.3.7). If $\pi_{m,a}(x) = \frac{\pi(x)}{\phi(m)} + E_{m,a}(x)$, then the errors $E_{m,a}(x)$ can be positive or negative and assuming the RH sum to something of size $x^{\frac{1}{2}+\epsilon}$. If we assume they are roughly of the same size, say $\pm E_m$, then as there are $\phi(m)$ terms, the philosophy of square root cancellation predicts their sum is of size $\sqrt{\phi(m)}E_m$. Hence the errors should roughly be of size $x^{\frac{1}{2}+\epsilon}/\sqrt{\phi(m)}$. In many applications we are interested in results that hold for all residue classes as $m \rightarrow \infty$. Unfortunately, if even just one class had a much larger error, say of size $x^{\frac{1}{2}+\epsilon}/\phi(m)^{\frac{1}{4}}$ or even $o(x^{\frac{1}{2}+\epsilon})$, it would not noticeably affect the sum of the errors and hence cannot be ruled out. This would have profound consequences. So while we expect the typical $E_{m,a}(x)$ to be of size at most $x^{\frac{1}{2}+\epsilon}/\sqrt{\phi(m)}$, no bounds of this strength are known to hold uniformly in a for fixed m .

3.3.1 General Dirichlet Series

We will consider **Dirichlet series**

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad (3.107)$$

where the a_n encode arithmetic information. We first prove some general results about convergence of such series, and then investigate Dirichlet series related to primes in arithmetic progressions.

Theorem 3.3.2. *If the above Dirichlet series converges for $s_0 = \sigma_0 + it_0$, then it converges for all s with $\Re s > \sigma_0$.*

Proof. The idea of the proof is to express the tail of the Dirichlet series at s in terms of the tail of the Dirichlet series at s_0 (which is known to converge). We put $C(n) = a(n)/n^{s_0}$, $h(x) = x^{-(s-s_0)}$ and $\sigma = \Re s$. Then

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \sum_{n=1}^{\infty} C(n)h(n). \quad (3.108)$$

To show the Dirichlet series in (3.108) converges, it suffices (see for example [Rud]) to show that given any $\epsilon' > 0$ there exists an N such that for all $M > N$ then

$$\left| \sum_{n=N+1}^M \frac{a_n}{n^s} \right| = \epsilon'. \quad (3.109)$$

If (3.109) holds, we say the sequence satisfies the **Cauchy convergence condition**. Letting $M \rightarrow \infty$ shows the sum of the tail of the series can be made arbitrarily small. By Partial Summation (Theorem 2.2.6) we have

$$\sum_{n=1}^K \frac{a(n)}{n^s} = S(K)K^{-(s-s_0)} + (s-s_0) \int_1^K S(t)t^{-1-(s-s_0)} dt, \quad (3.110)$$

where $S(x) = \sum_{n \leq x} \frac{a(n)}{n^{s_0}}$. Note $S(x)$ is a truncation of the Dirichlet series at s_0 (summing only those n up to x). We use the convergence at s_0 to obtain convergence at s . Subtracting (3.110) with $K = N$ from (3.110) with $K = M$ yields

$$\begin{aligned} \sum_{n=N+1}^M \frac{a(n)}{n^s} &= (S(M) - S(N))M^{-(s-s_0)} + S(N)(M^{-(s-s_0)} - N^{-(s-s_0)}) \\ &\quad + (s-s_0) \int_N^M S(t)t^{-1-(s-s_0)} dt. \end{aligned} \quad (3.111)$$

By direct integration we see the second term in (3.111) equals

$$-(s-s_0) \int_N^M t^{-1-(s-s_0)} S(N) dt, \quad (3.112)$$

which implies

$$\begin{aligned} \sum_{n=N+1}^M \frac{a(n)}{n^s} &= (S(M) - S(N))M^{-(s-s_0)} \\ &\quad + (s-s_0) \int_N^M (S(t) - S(N))t^{-1-(s-s_0)} dt. \end{aligned} \quad (3.113)$$

Since we have assumed that the series converges for s_0 , for $\epsilon > 0$ there is an N_0 such that for $x \geq N \geq N_0$ we have $|S(x) - S(N)| < \epsilon$. Thus

$$\left| \sum_{n=N+1}^M \frac{a(n)}{n^s} \right| \leq |(S(M) - S(N))M^{-(s-s_0)}| + \epsilon |s-s_0| \int_N^M |t^{-1-(s-s_0)}| dt. \quad (3.114)$$

For $\sigma > \sigma_0$,

$$\int_N^M |t^{-1-(s-s_0)}| dt = \int_N^M t^{-1-(\sigma-\sigma_0)} dt = \frac{N^{-(\sigma-\sigma_0)} - M^{-\sigma-\sigma_0}}{\sigma-\sigma_0}. \quad (3.115)$$

Since $|s-s_0| \geq \sigma-\sigma_0$, we get

$$\begin{aligned} \left| \sum_{n=N+1}^M \frac{a(n)}{n^s} \right| &\leq \epsilon \frac{|s-s_0|}{\sigma-\sigma_0} \left(M^{-(\sigma-\sigma_0)} + N^{-(\sigma-\sigma_0)} - M^{-(\sigma-\sigma_0)} \right) \\ &= \epsilon \frac{|s-s_0|}{\sigma-\sigma_0} N^{-(\sigma-\sigma_0)} \\ &\leq \epsilon \frac{|s-s_0|}{\sigma-\sigma_0}. \end{aligned} \quad (3.116)$$

Since ϵ is arbitrary, the convergence of the series in (3.108) for s now follows. \square

Exercise 3.3.3. Assume a Dirichlet series converges absolutely for s_0 . Prove this implies that for any $\epsilon > 0$ there is an N_0 such that if $x \geq N \geq N_0$ then $|S(x) - S(N)| < \epsilon$.

Exercise 3.3.4 (Important). Assume the partial sums of a_n are bounded. Prove that $\sum \frac{a_n}{n^s}$ converges for $\Re s > 0$. This exercise will be needed in our investigations of primes in arithmetic progressions.

The following theorems assume some familiarity with uniform convergence and complex analysis (for a review, see Appendix A.3), and are not used in the remainder of the text.

Theorem 3.3.5. Notation as in Theorem 3.3.2, the convergence is uniform inside any angle for which $|\arg(s - s_0)| \leq \frac{\pi}{2} - \delta$ for $0 < \delta < \frac{\pi}{2}$.

Proof. Let s be a point in the angle. Then we have

$$\frac{|s - s_0|}{\sigma - \sigma_0} = \frac{1}{\sigma - \sigma_0} \frac{\sigma - \sigma_0}{\cos \arg |s - s_0|} \leq \frac{1}{\cos(\frac{\pi}{2} - \delta)} = \frac{1}{\sin \delta}. \quad (3.117)$$

Arguing as in the proof of Theorem 3.3.2, we have

$$\left| \sum_{n=N+1}^M \frac{a(n)}{n^s} \right| \leq \frac{\epsilon}{\sin \delta}, \quad (3.118)$$

and the convergence is thus uniform inside the angle. \square

Let R be the collection of all $\gamma \in \mathbb{R}$ with the property that the Dirichlet series converges for $\sigma > \gamma$. By Theorem 3.3.2, R must have an infimum (which may be $-\infty$ if the series converges for all s , or $+\infty$ if it never converges). Let α be this infimum, which is called the **abscissa of convergence**. The Dirichlet series converges if $\sigma > \alpha$ and diverges if $\sigma < \alpha$. As in the case of the convergence of power series on the boundary of the disk of convergence, the behavior of Dirichlet series for $\sigma = \alpha$ is in general undetermined. The following is an easy consequence of the above theorems:

Theorem 3.3.6. *The Dirichlet series*

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \quad (3.119)$$

converges for $\Re s > \alpha$, and it defines an analytic function on that domain.

In general one must be very careful in dealing with conditionally convergent series, as the following exercise shows.

Exercise 3.3.7 (Rearrangement Theorem). Let a_n be any series that conditionally converges but does not absolutely converge (thus $\sum a_n$ exists but $\sum |a_n|$ does not). Given $a < b$, show by rearranging the order of the a_n 's (instead of a_1, a_2, \dots , we now have the order a_{n_1}, a_{n_2}, \dots), we can get the new partial sums arbitrarily close to a and b infinitely often.

Exercise 3.3.8. Let $\{a_n\}$ be a sequence of complex numbers. We say that the infinite product

$$\prod_{n=1}^{\infty} a_n \quad (3.120)$$

converges if the sequence $\{p_m\}$ defined by

$$p_m = \prod_{n=1}^m a_n \quad (3.121)$$

converges; i.e., if $\lim_{m \rightarrow \infty} p_m$ exists and is non-zero. We assume that $a_n \neq 0$ for all n .

1. State and prove a Cauchy convergence criterion for infinite products. If the infinite product (3.121) converges to a non-zero number, what is $\lim_{n \rightarrow \infty} a_n$?
2. Suppose for all n , $a_n \neq -1$. Prove that $\prod_n (1 + a_n)$ converges if and only if $\sum_n a_n$ converges.
3. Determine $\prod_{n=1}^{\infty} (1 + \frac{1}{n})$ and $\prod_{n=2}^{\infty} (1 - \frac{1}{n^2})$.

The basic theory of Dirichlet series can be found in many references. We have used [Ay] in the above exposition.

3.3.2 Dirichlet Characters

Let m be a positive integer. A completely multiplicative (see Definition 2.1.2) arithmetic function with period m that is not identically zero is called a **Dirichlet character**. In other words, we have a function $f : \mathbb{Z} \rightarrow \mathbb{C}$ such that $f(xy) = f(x)f(y)$ and $f(x+m) = f(x)$ for all integers x, y . Often we call the period m the **conductor** or **modulus** of the character.

Exercise 3.3.9. Let χ be a Dirichlet character with conductor m . Prove $\chi(1) = 1$. If χ is not identically 1, prove $\chi(0) = 0$.

Because of the above exercise, we adopt the convention that a Dirichlet character has $\chi(0) = 0$. Otherwise, given any character, there is another character which differs only at 0.

A complex number z is a **root of unity** if there is some positive integer n such that $z^n = 1$. For example, numbers of the form $e^{2\pi ia/q}$ are roots of unity; if a is relatively prime to q , the smallest n that works is q , and we often say it is a q^{th} **root of unity**. Let

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n, m) = 1 \\ 0 & \text{otherwise.} \end{cases} \quad (3.122)$$

We call χ_0 the **trivial** or **principal character** (with conductor m); the remaining characters with conductor m are called **non-trivial** or **non-principal**.

Exercise 3.3.10. Let χ be a non-trivial Dirichlet character with conductor m . Prove that if $(n, m) = 1$ then $\chi(n)$ is a root of unity, and if $(n, m) \neq 1$ then $\chi(n) = 0$.

Theorem 3.3.11. The number of Dirichlet characters with conductor m is $\phi(m)$.

Proof. We prove the theorem for the special case when m equals a prime p . By Theorem 1.4.29 the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, generated by some g of order $p - 1$. Thus any $x \in (\mathbb{Z}/p\mathbb{Z})^*$ is equivalent to g^k for some k depending on x . As $\chi(g^k) = \chi(g)^k$, once we have determined the Dirichlet character at a generator, its values are determined at all elements (of course, $\chi(0) = \chi(m) = 0$).

By Exercise 3.3.10, $\chi(g)$ is a root of unity. As $g^{p-1} \equiv 1 \pmod{p}$ and $\chi(1) = 1$, $\chi(g)^{p-1} = 1$. Therefore $\chi(g) = e^{2\pi ia/(p-1)}$ for some $a \in \{1, 2, \dots, p-1\}$. The proof is completed by noting each of these possible choices of a gives rise to a Dirichlet character, and all the characters are distinct (they have different values at g). \square

Not only have we proved (in the case of m prime) how many characters there are, but we have a recipe for them. If $a = p - 1$ in the above proof, we have the trivial character χ_0 .

Exercise^(h) 3.3.12 (Important). Let r and m be relatively prime. Prove that if n ranges over all elements of $\mathbb{Z}/m\mathbb{Z}$ then so does rn (except in a different order if $r \not\equiv 1 \pmod{m}$).

Exercise 3.3.13. If χ and χ' are Dirichlet characters with conductor m , so is $\chi'' = \chi\chi'$, given by $\chi''(n) = \chi(n)\chi'(n)$. Define $\bar{\chi}(n) = \overline{\chi(n)}$. Prove $\bar{\chi}$ is a Dirichlet character with conductor m , and $\bar{\chi}\chi = \chi_0$.

Exercise^(h) 3.3.14 (Important). Prove the Dirichlet characters with conductor m form a multiplicative group with $\phi(m)$ elements and identity element χ_0 . In particular, if χ' is a fixed character with conductor m , if χ ranges over all Dirichlet characters with conductor m , so does $\chi'\chi$.

The following lemma is often called the **orthogonality relations** for characters (orthogonal is another word for perpendicular). See Definition B.1.5 and §11.1 for other examples of orthogonality. By $\chi \pmod{m}$ we mean the set of all Dirichlet characters with conductor m .

Lemma 3.3.15 (Orthogonality Relations). The Dirichlet characters with conductor m satisfy

$$\sum_{n \pmod{m}} \chi(n) = \begin{cases} \phi(m) & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases} \quad (3.123)$$

$$\sum_{\chi \pmod{m}} \chi(n) = \begin{cases} \phi(m) & \text{if } n \equiv 1 \pmod{m} \\ 0 & \text{otherwise.} \end{cases} \quad (3.124)$$

Proof. We only prove (3.123) as the proof of (3.124) is similar. By $\chi \pmod m$ we mean χ ranges over all Dirichlet characters with conductor m . Let r be an integer with $(r, m) = 1$. Then

$$\chi(r) \sum_{n \pmod m} \chi(n) = \sum_{n \pmod m} \chi(rn) = \sum_{n \pmod m} \chi(n), \quad (3.125)$$

as when n ranges over a complete system of residues $\pmod m$, so does rn (Exercise 3.3.12). Consequently, denoting the sum in question by S , we have

$$\chi(r)S = S, \quad (3.126)$$

implying that $S = 0$ unless $\chi(r) = 1$ for all $(r, m) = 1$ (in this case, χ is the trivial character χ_0 , and $S = \phi(m)$). This finishes the proof. \square

Exercise^(h) 3.3.16. Prove (3.124).

Exercise 3.3.17. Give an alternate proof of (3.123) and (3.124) by using the explicit formulas for the characters χ with prime conductors. Specifically, for any character χ of prime conductor p with g a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ there is an a such that $\chi(g) = e^{2\pi ia/(p-1)}$.

Another useful form of the orthogonality relations is

Exercise 3.3.18 (Orthogonality Relations). Show Lemma 3.3.15 implies

$$\frac{1}{\phi(m)} \sum_{n \pmod m} \chi(n) \overline{\chi'}(n) = \begin{cases} 1 & \text{if } \chi' = \chi \\ 0 & \text{otherwise.} \end{cases} \quad (3.127)$$

To each character χ we can associate a vector of its values

$$\vec{\chi} \longleftrightarrow (\chi(1), \chi(2), \dots, \chi(m-1), \chi(m)), \quad (3.128)$$

and we may interpret (3.127) as saying $\vec{\chi}$ is perpendicular to $\vec{\chi}'$, where the dot product is

$$\langle \vec{\chi}, \vec{\chi}' \rangle = \sum_{n \pmod m} \chi(n) \overline{\chi'}(n). \quad (3.129)$$

Exercise 3.3.19 (Important). Given n and a integers, prove

$$\frac{1}{\phi(m)} \sum_{\chi \pmod m} \overline{\chi}(a) \chi(n) = \begin{cases} 1 & \text{if } n \equiv a \pmod m \\ 0 & \text{otherwise.} \end{cases} \quad (3.130)$$

This exercise provides a way to determine if $a \equiv n \pmod m$, and is used below to find primes congruent to a modulo m .

3.3.3 L -functions and Primes in Arithmetic Progressions

The L -function of a general Dirichlet character with conductor m is defined by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \quad (3.131)$$

Exercise^(h) 3.3.20. Prove $L(s, \chi)$ converges for $\Re s > 1$. If $\chi \neq \chi_0$, prove that $L(s, \chi)$ can be extended to $\Re s > 0$.

As in the case of the Riemann zeta function, because integers have unique factorization and because the Dirichlet characters are multiplicative, we have an **Euler product** defined for $\Re s > 1$:

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s} \right)^{-1}. \quad (3.132)$$

Arguing as in Exercise 3.1.9, for $\Re s > 1$, $L(s, \chi) \neq 0$ (again, this is not obvious from the series expansion).

Exercise^(h) 3.3.21. Prove (3.132).

We sketch how these L -functions can be used to investigate primes in arithmetic progressions (see [Da2, EE, Se] for complete details); another application is in counting solutions to congruence equations in §4.4. For example, say we wish to study primes congruent to a modulo m . Using Dirichlet characters modulo m , by Lemma 3.3.15 we have (at least for $\Re s > 1$)

$$\begin{aligned} \sum_{\chi \bmod m} \chi(a) L(s, \chi) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{\chi \bmod m} \chi(a) \chi(n) \\ &= \sum_{\substack{n=1 \\ n \equiv a \pmod{m}}}^{\infty} \frac{\phi(m)}{n^s}. \end{aligned} \quad (3.133)$$

Thus, by using *all* the Dirichlet characters modulo m , we have obtained a sum over integers congruent to a modulo m . We want to study not integers but primes; thus, instead of studying $\chi(a)L(s, \chi)$ we study $\chi(a) \log L(s, \chi)$ (because of the Euler product, the logarithm of $L(s, \chi)$ will involve a sum over primes).

Similar to the Riemann zeta function, there is a Riemann Hypothesis, the **Generalized Riemann Hypothesis** (GRH), which asserts that all the non-trivial zeros of the L -function $L(s, \chi)$ lie on the line $\Re s = \frac{1}{2}$. This is, of course, beyond the reach of current technology, and if proven will have immense arithmetic implications. In fact, very interesting arithmetic information has already been obtained from progress towards GRH. The following exercise sketches one of these.

Exercise 3.3.22 (Dirichlet's Theorem on Primes in Arithmetic Progression). *The purpose of this exercise is sketch the ideas for Dirichlet's Theorem for primes in arithmetic progressions. Suppose for all Dirichlet characters $\chi \neq \chi_0$ modulo m , we have $L(1, \chi) \neq 0$. Then for any $(a, m) = 1$, there are infinitely many prime numbers $p \equiv a \pmod{m}$.*

1. Using the Euler product for $L(s, \chi)$, and the Taylor series expansion for $\log(1 - u)$ about $u = 0$, prove that for $\Re s > 1$,

$$\log L(s, \chi) = \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{k p^{ks}}. \quad (3.134)$$

2. Use Exercise 3.3.19 to show that

$$\frac{1}{\phi(m)} \sum_{\chi} \bar{\chi}(a) \log L(s, \chi) = \sum_p \sum_{k=1}^{\infty} \sum_{p^k \equiv a \pmod{m}} \frac{1}{k p^{ks}}. \quad (3.135)$$

3. Show that the right hand side of (3.135) is

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} + O(1) \quad (3.136)$$

as $s \rightarrow 1$ from the right (i.e., $s > 1$ converges to 1, often denoted $s \rightarrow 1+$).

4. Verify that

$$L(s, \chi_0) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right), \quad (3.137)$$

and conclude that $\lim_{s \rightarrow 1+} L(s, \chi_0) = +\infty$.

5. Show that if for all $\chi \neq \chi_0$, $L(1, \chi) \neq 0$, then

$$\lim_{s \rightarrow 1+} \sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = \infty, \quad (3.138)$$

which of course implies there are infinitely many primes congruent to a modulo m . Proving $L(1, \chi) \neq 0$ is the crux of Dirichlet's proof; see [Da2, EE, IR, Se] for details.

Note even if we are only interested in one residue class modulo m , in this proof we need to study $L(s, \chi)$ for all Dirichlet characters with conductor m .

Exercise 3.3.23. The previous exercise allows us to reduce the question on whether or not there are infinitely many primes congruent to a modulo m to evaluating a finite number of L -functions at 1; thus any specific case can be checked. For $m = 4$ and $m = 6$, for each character χ use a good numerical approximation to $L(1, \chi)$ to show that it is non-zero. Note if one has a good bound on the tail of a series it is possible to numerically approximate an infinite sum and show it is non-zero; however, it is not possible to numerically prove an infinite sum is exactly zero.

Exercise 3.3.24. In the spirit of the previous problem, assume we know an infinite sum is rational and we know the denominator is at most Q . Prove that if we can show that $|\sum_{n=1}^{\infty} a_n - 0| < \frac{1}{Q}$ then this estimate improves itself to $\sum_{n=1}^{\infty} a_n = 0$. Unfortunately, it is difficult in practice to prove a sum is rational and to bound the denominator, though there are some instances involving L -functions attached to elliptic curves where this can be done. What is more common is to show a sum is a non-negative integer less than 1, which then implies the sum is 0. We shall see numerous applications of this in Chapter 5 (for example §5.4, where we prove e is irrational and transcendental).

Exercise^(hr) 3.3.25. The difficult part of Dirichlet's proof is showing $L(1, \chi) \neq 0$ for real characters χ ; we show how to handle the non-real characters (this means $\bar{\chi} \neq \chi$; for example, the Legendre symbol is a real character). Using $a = 1$ in Exercise 3.3.22, show

$$\sum_{\chi} \log L(\sigma, \chi) \geq 0 \quad (3.139)$$

for real $\sigma \geq 1$; note this sum may be infinite. Therefore $\prod_{\chi} L(\sigma, \chi) \geq 1$ for $\sigma \geq 1$. Show that if $L(1, \chi) = 0$ so too does $L(1, \bar{\chi})$. Show for a non-real character χ that $L(1, \chi) \neq 0$.

Exercise 3.3.26. We saw in Exercise 2.3.5 that for certain choices of m and a it is easy to prove there are infinitely many primes congruent to a modulo m . Modifying Euclid's argument (Theorem 2.3.1), prove there are infinitely many primes congruent to -1 modulo 4. Can you find an a modulo 5 (or 6 or 7) such that there are infinitely many primes? See [Mu1] for how far such elementary arguments can be pushed.

Remark 3.3.27. One can show that, to first order, $\pi_{m,a}(x) \sim \frac{\pi(x)}{\phi(m)}$, where $\pi_{m,a}(x)$ is the number of primes at most x congruent to a modulo m . We can see evidence of this in (3.135). The left hand side of that equation depends very weakly on a . The contribution from the non-principal characters is finite as $s \rightarrow 1$; thus the main contribution comes from $\chi_0(a)L(s, \chi_0) = L(s, \chi_0)$. Therefore the main term in (3.136), $\sum_{p \equiv a \pmod{q}} p^{-s}$, has a similar $s \rightarrow 1$ limit for all a ; specifically, the piece that diverges, diverges at the same rate for all a relatively prime to q . The behavior of the correction terms exhibit interesting behavior: certain congruence classes seem to have more primes. See [EE, RubSa] for details.

Exercise 3.3.28. By Exercise 3.3.29 or 11.3.17,

$$\frac{\pi}{4} = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2n-1}. \quad (3.140)$$

Note π is irrational (see [NZM], page 309). Define

$$\chi_4(n) = \begin{cases} (-1)^{(n-1)/2} & \text{if } n \text{ is odd} \\ 0 & \text{otherwise.} \end{cases} \quad (3.141)$$

Prove χ_4 is a Dirichlet character with conductor 4. By evaluating just $L(1, \chi_4)$ and noting π is irrational, show there are infinitely many primes; we sketch a proof of the irrationality of π^2 in Exercise 5.4.17. This is another special value proof and provides no information on the number of primes at most x . Using this and properties of $\zeta(s)$, can you deduce that there are infinitely many primes congruent to 1 modulo 4 or -1 modulo 4? Infinite products of rational numbers can be either rational or transcendental; see Exercise 5.6.9.

Exercise^(hr) 3.3.29 (Gregory-Leibniz Formula). Prove

$$\frac{\pi}{4} = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2n-1}. \quad (3.142)$$

Exercise^(h) 3.3.30 (Wallis' Formula). *Prove*

$$\frac{2}{\pi} = \frac{1}{2} \cdot \frac{3 \cdot 3}{2 \cdot 4} \cdot \frac{5 \cdot 5}{4 \cdot 6} \cdot \frac{7 \cdot 7}{6 \cdot 8} \cdots \quad (3.143)$$

See Exercise 5.6.9 for more on infinite products and Chapter 11 of [BB] for more formulas for π . A good starting point is

$$\begin{aligned} \int_0^{\pi/2} (\sin x)^{2m} dx &= \frac{1 \cdot 3 \cdot 5 \cdots (2m-1) \pi}{2 \cdot 4 \cdot 6 \cdots 2m} \frac{\pi}{2} \\ \int_0^{\pi/2} (\sin x)^{2m+1} dx &= \frac{2 \cdot 4 \cdot 6 \cdots 2m}{1 \cdot 3 \cdot 5 \cdots (2m+1)}. \end{aligned} \quad (3.144)$$

3.3.4 Imprimitve Characters

We conclude with some remarks about imprimitive characters. Except for the definitions of primitive and imprimitive, the rest of this subsection may safely be skipped.

By definition a character χ modulo m is periodic. If the smallest period of χ is equal to m , χ is called a **primitive character**, otherwise it is **imprimitive**. Usually statements regarding characters and their L -functions are easier for primitive characters. All characters are built out of primitive ones:

Lemma 3.3.31. *Let χ be a non-principal imprimitive character modulo m . Then there is a divisor $m_1 \neq 1$ of m and a character ψ modulo m_1 such that*

$$\chi(n) = \begin{cases} \psi(n) & \text{if } (n, m) = 1 \\ 0 & \text{otherwise.} \end{cases} \quad (3.145)$$

Proof. Let m_1 be the least period of χ ; $m_1 \neq 1$ because this would imply χ is periodic modulo 1, contradicting the assumption that χ is not principal. If $m_1 \nmid m$, then $(m_1, m) < m_1$ is also a period of χ , which contradicts the choice of m_1 . We now construct the character ψ . If $(n, m) = 1$ we set $\psi(n) = \chi(n)$; if $(n, m_1) \neq 1$ we set $\psi(n) = 0$. The only remaining case is when $(n, m_1) = 1$ but $(n, m) \neq 1$. Here we choose an integer t with $(n+tm_1, m) = 1$, and we set $\psi(n) = \chi(n+tm_1)$. We leave it to the reader to verify that ψ is a well defined primitive character modulo m_1 , and we say that ψ **induces** χ . \square

Exercise 3.3.32. *Show that the Legendre symbol $\left(\frac{*}{p}\right)$ is a non-primitive character modulo p^α for $\alpha > 1$, which is induced by the same character modulo p . Here $\chi(n) = \left(\frac{n}{p}\right)$.*

Exercise 3.3.33. *Let χ be an imprimitive character modulo m , induced by a character ψ . Prove for $\Re s > 1$,*

$$L(s, \chi) = L(s, \psi) \prod_{p|m} \left(1 - \frac{\psi(p)}{p^s}\right). \quad (3.146)$$

3.3.5 Functional Equation

Let χ be a primitive character mod m . Similar to $\zeta(s)$, $L(s, \chi)$ satisfies a functional equation. Before proving this we need to define certain sums involving Dirichlet characters. Let the **Gauss Sum** $c(m, \chi)$ be defined by

$$c(m, \chi) = \sum_{k=0}^{m-1} \chi(k) e^{2\pi i k/m}. \quad (3.147)$$

Exercise^(hr) 3.3.34. Prove that $|c(m, \chi)| = m^{\frac{1}{2}}$. See [BEW, IR] for additional results on Gauss and related sums.

Exercise 3.3.35. Prove that

$$\chi(n) = \frac{1}{c(m, \bar{\chi})} \sum_{k=0}^{m-1} \bar{\chi}(k) e^{2\pi i \frac{kn}{m}}. \quad (3.148)$$

Note the right hand side is well defined for all $n \in \mathbb{R}$. This useful formula interpolates χ from a function on \mathbb{Z} to one on \mathbb{R} .

Theorem 3.3.36 (Meromorphic Continuation of $L(s, \chi)$). *The function $L(s, \chi)$, originally defined only for $\Re s > 1$, has a meromorphic continuation to the entire complex plane. The meromorphic continuation of $L(s, \chi)$ has a unique pole at $s = 1$ when $\chi = \chi_0$; otherwise, it is entire. Furthermore, if we set*

$$\Lambda(s, \chi) = \left(\frac{m}{\pi}\right)^{\frac{1}{2}(s+\epsilon)} \Gamma\left(\frac{s+\epsilon}{2}\right) L(s, \chi), \quad (3.149)$$

where

$$\epsilon = \begin{cases} 0 & \text{if } \chi(-1) = 1 \\ 1 & \text{if } \chi(-1) = -1, \end{cases}$$

then we have

$$\Lambda(s, \chi) = (-i)^\epsilon \frac{c(m, \chi)}{m^{\frac{1}{2}}} \Lambda(1-s, \bar{\chi}). \quad (3.150)$$

Observe that

$$\left| (-i)^\epsilon \frac{c(m, \chi)}{m^{\frac{1}{2}}} \right| = 1. \quad (3.151)$$

The proof of this theorem is similar to the proof of the similar theorem for the Riemann zeta function as sketched above. We refer the reader to [Da2] for details.