A Survey of Analytic Number Theory

Artem Mavrin
Advisor: Dr. Alina Bucur

April 28, 2014

Acknowledgements

I am very thankful to my advisor Alina Bucur for her patience, guidance, and expertise during the course of my reading and eventual thesis-writing with her. This thesis would not have been possible without her support and encouragement, and it was my pleasure to have had her as my mentor.

I am also very grateful to have been a student in the classes of Alina Bucur, Cristian Popescu, Justin Roberts, Daniel Rogalski, and Alireza Salehi Golsefidy, all of whom taught me mathematics with enthusiasm and clarity during my time at UCSD. In particular, I am indebted to Alina Bucur and Cristian Popescu for exposing me to the beautiful world of number theory.

Contents

1 Introduction

1.1 Analytic Number Theory and This Thesis

Analytic number theory is, roughly, the study of the integers using tools and techniques from analysis. It is believed to have begun with the work of Dirichlet, who used analytic objects called *Dirichlet L-functions* to prove the purely number theoretic result that, for any pair of positive integers a and m which are coprime, the arithmetic progression

$$a, \qquad a+m, \qquad a+2m, \qquad a+3m, \qquad \dots$$

contains infinitely many prime numbers. We will prove this in Theorem 5.3.7.

Another cornerstone of analytic number theory is the *prime number theorem*, which describes the asymptotic behavior of the prime numbers. It states that if x is a positive real number and $\pi(x)$ denotes the number of primes less than or equal to x, then

$$\lim_{x\to\infty} \frac{\pi(x)\log(x)}{x} = 1.$$

We will prove this result in Theorem 4.5.7.

In this thesis we will survey just a small sample of classical analytic number theory, reproducing a few of the important result along the way. The reader is assumed to be familiar with the most basic facts of elementary number theory (such as properties of divisibility and prime factorization), some undergraduate abstract algebra, and a fair amount of undergraduate analysis, including complex analysis. Appendices covering the more niche topics that are needed are included at the end.

1.2 An Example: The Infinitude of Primes via Analysis

In this section, we will prove a very elementary number theoretic result in two ways—first, using an ancient argument; second, using an analytic argument. We will see that the analytic argument actually gives us more information.

One of the oldest theorems in number theory is the following one, proved by Euclid in his *Elements*.

Theorem 1.2.1 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. It suffices to show that, given finitely many prime numbers $p_1, \ldots, p_n$, there exists a prime number p different from each p_i. If we have a finite list of primes $p_1, \ldots, p_n$, then we consider $q = p_1 \cdots p_n + 1$. If q is prime, then we are done. Otherwise, q has some prime factor p. The prime p cannot divide any of the primes $p_1, \ldots, p_n$, since otherwise p would divide $q - p_1 \cdots p_1 = 1$. Therefore p is a prime number not listed in the sequence $p_1, \ldots, p_n$. □

Using elementary analysis, we can strengthen Euclid's Theorem in the following way. We will explain after why this is a stronger result.

Theorem 1.2.2 (Euler)**.** *The series*

$$\sum_p \frac{1}{p}, \tag{1.2.1}$$

taken over all prime numbers p, diverges. In particular, there are infinitely many primes.

Proof. Suppose the series (1.2.1) converges. Then there exists a prime number p_0 such that

$$\sum_{p>p_0} \frac{1}{p} < \frac{1}{2}.$$

In particular, the series

$$\sum_{n=1}^{\infty} \left(\sum_{p>p_0} \frac{1}{p} \right)^n = \sum_{n=1}^{\infty} \sum_{p_0<p_1\leq\cdots\leq p_n} \frac{1}{p_1 p_2 \cdots p_n} \tag{1.2.2}$$

converges by comparison with the convergent geometric series

$$\sum_{m=1}^{\infty} \left(\frac{1}{2} \right)^m.$$

Define Q to be the product of all the prime numbers less than or equal to p_0, and fix a positive integer n. Then each prime dividing $1 + nQ$ must be larger than p_0, which shows that $(1 + nQ)^{-1}$ occurs as a summand in the series (1.2.2). It follows that the series

$$\sum_{n=1}^{\infty} \frac{1}{1 + nQ} \tag{1.2.3}$$

converges by comparison with the convergent series (1.2.2). But this is absurd since (1.2.3) diverges. Therefore the series (1.2.1) diverges, and this implies that there are infinitely many prime numbers. □

This is our first example of using tools from analysis to say things about integers. Going beyond Theorem 1.2.1, Theorem 1.2.2 shows that, among the infinite subsets of the positive integers, the set of primes is "large," in the sense that the sum over the reciprocals of its elements diverges. Other infinite subsets—for example, the subset of perfect squares—is well-known to be "small" in this sense: the series $\sum_{n=1}^{\infty} 1/n^2$ converges.

1.3 Notation and Conventions

The bold letters

$$\mathbf{Z} \qquad \mathbf{Z}_+ \qquad \mathbf{Q} \qquad \mathbf{R} \qquad \mathbf{R}_{\geq 0} \qquad \mathbf{C}$$

denote, respectively, the set of integers, the set of positive integers, the set of rational numbers, the set of real numbers, the set of non-negative real numbers, and the set of complex numbers. The letter p will always denote a prime number unless stated otherwise. Notation such as $\sum_p$ and $\prod_{p \leq x}$ should be interpreted as sums and products taken over primes. We follow the common practice of interpreting empty sums as 0 and empty products as 1. The greatest common divisor of two integers m and n is denoted (m, n). For a real number x, we denote by $[x]$ the greater integer less than or equal to x, and by $\{x\}$ the fractional part of x (i.e., $\{x\} = x - [x]$). Context will always prevent ambiguity about issues like whether $\{x\}$ means the singleton set containing x or the fractional part of x. For a complex number $s = a + bi$, $\mathrm{Re}(s) = a$ and $\mathrm{Im}(s) = b$ are the real and imaginary parts of s, respectively. The function log will denote the principal branch of the complex logarithm unless stated otherwise.

We will occasionally use asymptotic notation, so we recall it here. Given two complex-valued functions f and g, defined on sets such that the limit below makes sense, we write

$$f(x) \sim g(x) \qquad \text{as } x \to a$$

if and only if

$$\lim_{x \to a} \frac{f(x)}{g(x)} = 1$$

(this includes $a = \infty$). In this case, $f(x)$ and $g(x)$ are said to be *asymptotically equivalent as* $x \to a$, and this relation is an equivalence relation. Moreover, we write

$$f(x) = O(g(x)) \qquad \text{as } x \to \infty$$

(to be read as "$f(x)$ is *big O* of $g(x)$") if and only if there exists a $C > 0$ and an x_0 such that

$$|f(x)| \leq C|g(x)|$$

for all $x \geq x_0$.

2 Arithmetic Functions

2.1 The Ring of Arithmetic Functions

Definition 2.1.1. An *arithmetic function* is a complex-valued function defined on the set $\mathbf{Z}_+$ of positive integers.

The set $\mathbf{C}^{\mathbf{Z}_+}$ of all arithmetic functions has a a natural $\mathbf{C}$-algebra structure: the sum $f+g$ and product fg of two arithmetic functions f and g is given by

$$(f+g)(n) = f(n) + g(n), \qquad (fg)(n) = f(n)g(n),$$

and the scalar multiple αh of an arithmetic function h by a complex number α is given by

$$(\alpha h)(n) = \alpha h(n).$$

With these operations, $\mathbf{C}^{\mathbf{Z}_+}$ is a unital, associative, commutative $\mathbf{C}$-algebra which has zero divisors but no nilpotent elements. However, there is a more useful multiplication operation on $\mathbf{C}^{\mathbf{Z}_+}$, which is defined as follows.

Definition 2.1.2. Given two arithmetic functions f and g, their *convolution* is the arithmetic function $f * g$ defined by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right),$$

where the sum ranges over all positive divisors d of n.

The binary operation $(f, g) \mapsto f * g$ on $\mathbf{C}^{\mathbf{Z}_+}$ is clearly $\mathbf{C}$-bilinear, associative, and commutative.

Definition 2.1.3. We define the arithmetic function δ, called the *convolution identity function*, by

$$\delta(n) = \left[\frac{1}{n}\right] = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases}$$

We check at once that

$$\delta * f = f * \delta = f$$

for every arithmetic function f, so δ is the identity for convolution. Thus $\mathbf{C}^{\mathbf{Z}_+}$ has a unital, associative, and commutative $\mathbf{C}$-algebra structure different from the one given before, with the same addition and scalar multiplication, but with multiplication given by convolution. Henceforth we adopt this $\mathbf{C}$-algebra structure on $\mathbf{C}^{\mathbf{Z}_+}$ as the default one. In particular, when we say (as in Lemma 2.1.4 below) that an arithmetic function f is *invertible*, we mean that it is a unit in $\mathbf{C}^{\mathbf{Z}_+}$ with respect to convolution. That is, f is invertible if and only if there exists a necessarily unique arithmetic function f^{-1} such that

$$f * f^{-1} = f^{-1} * f = \delta.$$

Lemma 2.1.4. *An arithmetic function f is invertible if and only if $f(1) \neq 0$. Moreover, if f is invertible, then its inverse f^{-1} is given recursively by*

$$f^{-1}(1) = \frac{1}{f(1)}$$

and

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)$$

for all integers $n > 1$.

Proof. Fix an arithmetic function f. If f is invertible, then we have

$$f(1)f^{-1}(1) = (f * f^{-1})(1) = \delta(1) = 1,$$

so $f(1) \neq 0$. Conversely, suppose $f(1) \neq 0$. Let g be the arithmetic function defined recursively by $g(1) = 1/f(1)$ and

$$g(n) = -\frac{1}{f(n)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) g(d)$$

for $n \neq 1$. We then see that

$$(f * g)(1) = f(1)g(1) = \frac{f(1)}{f(1)} = 1 = \delta(1).$$

Next, if $n > 1$, then we have

$$\begin{aligned}(f * g)(n) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d) &= \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) g(d) + f(1)g(n) \\ &= \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) g(d) - \frac{f(1)}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) g(d) = 0 = \delta(n).\end{aligned}$$

It follows that $f * g = \delta$, so f is invertible and $g = f^{-1}$. □

2.2 Multiplicative Functions

Definition 2.2.1. We say that an arithmetic function f is *multiplicative* if and only if f is not identically zero and for all coprime positive integers m and n, we have

$$f(mn) = f(m)f(n). \tag{2.2.1}$$

Moreover, if (2.2.1) holds for all pairs of positive integers m and n, then f is said to be *totally multiplicative.*

Note that the convolution identity function δ is totally multiplicative.

Lemma 2.2.2. *Let f be a multiplicative function. Then $f(1) = 1$, and consequently f is invertible.*

Proof. Since f is multiplicative, there exists a positive integer n for which $f(n) \neq 0$. Then $f(n) = f(n)f(1)$ since n and 1 are coprime, and hence $f(1) = 1$. Lemma 2.1.4 now implies that f is invertible. □

Lemma 2.2.3. *Let f and g be multiplicative functions. Then $f * g$ and f^{-1} are both multiplicative.*

Proof. First we prove that $f * g$ is multiplicative. By Lemma 2.2.2, $f(1) = g(1) = 1$, so

$$(f * g)(1) = f(1)g(1) = 1.$$

Next, let m and n be coprime positive integers. Then there is a one-to-one correspondence between the divisors of mn and pairs of divisors of m and n. Therefore we have

$$\begin{aligned}(f * g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{a|m,\, b|n} f(ab)g\left(\frac{m}{a}\cdot\frac{n}{b}\right)\\ &= \sum_{a|m,\, b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)\\ &= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right)\\ &= (f*g)(m)(f*g)(n),\end{aligned}$$

and hence $f * g$ is multiplicative.

Now we prove that f^{-1} is multiplicative. First we note that $f^{-1}(1) = 1/f(1) = 1$. Next, if p is a positive prime number and k is a positive integer, then by Lemmas 2.1.4 and 2.2.2 we have

$$\begin{aligned}f^{-1}(p^k) &= -\frac{1}{f(1)}\sum_{\substack{d|p^k\\ d<p^k}} f\left(\frac{p^k}{d}\right)f^{-1}(d)\\ &= -\sum_{j=1}^{k} f(p^j)f^{-1}(p^{k-j}).\end{aligned} \tag{2.2.2}$$

Let h be the arithmetic function defined by

$$h(n) = \prod_{p|n} f^{-1}(p^{v_p(n)}),$$

where the product is taken over the nonzero prime ideals of 1 that divide n and v_p is the p-adic valuation. Then h is clearly a multiplicative function, and h agrees with f^{-1} on powers of prime numbers. By the first part of this lemma, $f * h$ is a multiplicative function, and for every positive prime p and every positive integer k we have

$$(f*h)(p^k) = \sum_{d|p^k} f\left(\frac{p^k}{d}\right)h(d) = \sum_{j=0}^{k} f(p^j)f^{-1}(p^{k-j})$$

$$= f^{-1}(p^k) + \sum_{j=1}^{k} f(p^j) f^{-1}(p^{k-j}) = 0 = \delta(p^k)$$

by (2.2.2). Therefore $f * h$ agrees with δ on powers of primes. Since both $f * h$ and δ are multiplicative, it follows that $f * h = \delta$, and hence $f^{-1} = h$. Thus f^{-1} is a multiplicative function. □

Lemmas 2.2.2 and 2.2.3 show that the set of multiplicative functions is a subgroup (under convolution) of the group of units of the ring $\mathbf{C}^{\mathbf{Z}_+}$.

2.3 The Derivative of an Arithmetic Function

Definition 2.3.1. If f is an arithmetic function, then we define its *derivative* to be the arithmetic function f' given by

$$f'(n) = -\log(n) f(n).$$

Lemma 2.3.2. *The map $f \mapsto f'$ is a derivation on the $\mathbf{C}$-algebra $\mathbf{C}^{\mathbf{Z}_+}$.*

Proof. The only thing to verify is that the equation

$$(f * g)' = f' * g + f * g' \tag{2.3.1}$$

holds for all arithmetic functions f, g. Thus, fix two arithmetic functions f and g, and let $n \in \mathbf{Z}_+$ be given. Then we have

$$\begin{aligned}
(f * g)'(n) &= -\log(n) \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \\
&= -\sum_{d|n} \left(\log(d) + \log\left(\frac{n}{d}\right)\right) f(d) g\left(\frac{n}{d}\right) \\
&= -\sum_{d|n} \log(d) f(d) g\left(\frac{n}{d}\right) - \sum_{d|n} f(d) \log\left(\frac{n}{d}\right) g\left(\frac{n}{d}\right) \\
&= \sum_{d|n} f'(d) g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) g'\left(\frac{n}{d}\right) \\
&= (f' * g)(n) + (f * g')(n)
\end{aligned}$$

so (2.3.1) holds, and the proof is complete. □

2.4 The Euler Totient Function

Definition 2.4.1. The *Euler totient function* is the arithmetic function ϕ defined by

$$\phi(n) = \left|(\mathbf{Z}/n\mathbf{Z})^{\times}\right|,$$

the cardinality of the group of units of $\mathbf{Z}/n\mathbf{Z}$.

There are alternate interpretations of ϕ. For example, $\phi(n)$ counts the number of positive integers less than n which are coprime to n, and $\phi(n)$ is the number of generators of the cyclic group $\mathbf{Z}/n\mathbf{Z}$.

Lemma 2.4.2. *The Euler totient function ϕ is multiplicative.*

Proof. Let m and n be coprime positive integers, By the Chinese remainder theorem, we have the ring isomorphism

$$\mathbf{Z}/mn\mathbf{Z} \cong (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z}).$$

The functor mapping a ring to its group of units commutes with products, so the lemma follows. □

Lemma 2.4.3. *Let p be a prime number, and let k be a positive integer. Then*

$$\phi(p^k) = p^{k-1}\,(p-1)$$

Proof. Note that $\mathbf{Z}/p^k\mathbf{Z}$ is a local ring with maximal ideal $p\mathbf{Z}/p^k\mathbf{Z}$. It follows that $\mathbf{Z}/p^k\mathbf{Z}$ can be written as the disjoint union

$$\mathbf{Z}/p^k\mathbf{Z} = \left(p\mathbf{Z}/p^k\mathbf{Z}\right) \amalg \left(\mathbf{Z}/p^k\mathbf{Z}\right)^{\times},$$

whence

$$\phi(p^k) = p^k - [p\mathbf{Z} : p^k\mathbf{Z}].$$

Therefore it suffices to prove that

$$[p\mathbf{Z} : p^k\mathbf{Z}] = p^{k-1}. \tag{2.4.1}$$

This is clearly true if $k = 1$. Suppose $k > 1$. We have a canonical isomorphism

$$\left(\mathbf{Z}/p^k\mathbf{Z}\right) / \left(p^{k-1}\mathbf{Z}/p^k\mathbf{Z}\right) \cong \mathbf{Z}/p^{k-1}\mathbf{Z},$$

from which we conclude that

$$[p^{k-1}\mathbf{Z} : p^k\mathbf{Z}] = \frac{p^k}{p^{k-1}} = p.$$

Then we have

$$[p\mathbf{Z} : p^k\mathbf{Z}] = [p\mathbf{Z} : p^{k-1}\mathbf{Z}][p^{k-1}\mathbf{Z} : p^k\mathbf{Z}] = p[p\mathbf{Z} : p^{k-1}\mathbf{Z}],$$

and therefore (2.4.1) follows by induction. This completes the proof. □

Lemma 2.4.4. *For every $n \in \mathbf{Z}_+$ we have*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is taken over all prime divisors of n.

Proof. Fix $n \in \mathbf{Z}_+$. Then we have $n = \prod_{p|n} p^{v_p(n)}$. By Lemmas 2.4.2 and 2.4.3 we have

$$\begin{aligned}\phi(n) &= \prod_{p|n} \phi(p^{v_p(n)}) = \prod_{p|n} p^{v_p(n)-1}(p-1) \\ &= \prod_{p|n} p^{v_p(n)} \left(1 - \frac{1}{p}\right) = \prod_{p|n} p^{v_p(n)} \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right).\end{aligned}$$

□

Lemma 2.4.5. *For every $n \in \mathbf{Z}_+$, we have*

$$n = \sum_{d|n} \phi(d). \tag{2.4.2}$$

In the language of convolution, (2.4.2) says that

$$\mathrm{id} = \phi * 1, \tag{2.4.3}$$

where id *is the natural embedding $\mathbf{Z} \hookrightarrow \mathbf{C}$ and, by abuse of notation,* 1 *denotes the constant arithmetic function $n \mapsto 1$.*

Proof. If p is a prime number and r is a positive integer, then by Lemma 2.4.3 we have

$$\phi(p^r) = p^r - p^{r-1}.$$

Therefore

$$\begin{aligned}\sum_{d|p^k} \phi(d) &= \sum_{r=0}^{k} \phi(p^r) = 1 + \sum_{r=1}^{k} \left(p^r - p^{r-1}\right) \\ &= 1 + p^k + \sum_{r=1}^{k-1} p^r - \sum_{r=2}^{k} p^{r-1} - 1 = p^k.\end{aligned} \tag{2.4.4}$$

Thus we've proved (2.4.2) for the case of prime powers. The function ϕ is multiplicative by Lemma 2.4.2, and the constant arithmetic function 1 is clearly multiplicative. By Lemma 2.2.3, it follows that $\phi * 1$ is multiplicative. We have therefore shown in (2.4.4) that the multiplicative functions id and $\phi * 1$ agree on powers of primes. Thus we conclude that $\mathrm{id} = \phi * 1$. □

2.5 The Möbius Function, Möbius Inversion

Definition 2.5.1. The *Möbius function* is the arithmetic function μ defined by setting $\mu(1) = 1$, setting

$$\mu(p^k) = \begin{cases} -1, & \text{if } k = 1, \\ 0, & \text{if } k > 1 \end{cases}$$

for all prime numbers p and all positive integers k, and setting

$$\mu(n) = \prod_{p|n} \mu(p^{v_p(n)})$$

for composite $n \in \mathbf{Z}_+$ with at least two prime factors.

It is clear that μ is multiplicative.

Lemma 2.5.2. *For any $n \in \mathbf{Z}$, we have*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{2.5.1}$$

In the language of convolution, (2.5.1) says that

$$\mu * 1 = \delta$$

(recall that δ denotes the convolution identity function).

Proof. Formula (2.5.1) is clearly true when $n = 1$. Suppose $n \in \mathbf{Z}_+$ is greater than 1, and let $p_1, \dots, p_k$ be the distinct nonzero primes dividing n. By throwing away those divisors d of n for which $\mu(d) = 0$, we get

$$\begin{aligned}\sum_{d\mid n} \mu(d) &= \mu(1) + \sum_{j=1}^{k} \sum_{1\le i_1<\cdots<i_j\le k} \mu(p_{i_1}\cdots p_{i_j}) \\ &= 1 + \sum_{j=1}^{k} \binom{k}{j} (-1)^j = (1-1)^k = 0\end{aligned}$$

by the binomial theorem. □

Theorem 2.5.3 (Möbius inversion). *Let f and g be arithmetic functions on K. Then*

$$f = g * 1 \qquad \textit{if and only if} \qquad g = f * \mu. \tag{2.5.2}$$

That is, the equation

$$f(n) = \sum_{d\mid n} g(d)$$

holds for every $n \in \mathbf{Z}_+$ if and only if the equation

$$g(n) = \sum_{d\mid n} f(d)\mu\left(\frac{n}{d}\right)$$

holds for every $n \in \mathbf{Z}_+$.

Proof. We use the facts that convolution is associative and commutative together with Lemma 2.5.2. If $f = g * 1$, then

$$f * \mu = g * 1 * \mu = g * \delta = g,$$

proving one of the implications in (2.5.2). The other implication follows similarly. □

We mention a brief application of the Möbius inversion theorem. Formula (2.4.3) of Lemma 2.4.5 was

$$\mathrm{id} = \phi * 1.$$

Applying Theorem 2.5.3, we get

$$\phi = \mathrm{id} * \mu.$$

That is, for every $n \in \mathbf{Z}_+$, we have

$$\phi(n) = \sum_{d\mid \mathfrak{n}} \mu\left(\frac{n}{d}\right) d. \tag{2.5.3}$$

2.6 The Von Mangoldt Function

Definition 2.6.1. The *von Mangoldt function* is the arithmetic function Λ defined by

$$\Lambda(n) = \begin{cases} \log(p), & \text{if } n = p^k \text{ for some prime } p \text{ and } k \in \mathbf{Z}_+, \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 2.6.2. *For $n \in \mathbf{Z}_+$, we have*

$$\log(n) = \sum_{d|n} \Lambda(d). \tag{2.6.1}$$

In the language of convolution, (2.6.1) becomes

$$\log = \Lambda * 1.$$

Proof. It is clear that (2.6.1) is true when $n > 1$, so suppose $n \neq 1$. Write $n = p_1^{a_1} \cdots p_r^{a_r}$ for distinct primes $p_1, \ldots, p_r$. Then we have

$$\begin{aligned} \sum_{d|n} \Lambda(d) &= \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log(p_k) \\ &= \sum_{k=1}^{r} a_k \log(p_k) = \sum_{k=1}^{r} \log(p_k^{a_k}) \\ &= \log\left(p_1^{a_1} \ldots p_r^{a_r}\right) = \log(n). \end{aligned}$$ □

Theorem 2.6.3. *For a nonzero ideal n of 1, we have*

$$\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d) \log(d). \tag{2.6.2}$$

In the language of convolution, the first equality of (2.6.2) becomes

$$\Lambda = \mu * \log .$$

Proof. The first equality of (2.6.2) follows from Möbius inversion (Theorem 2.5.3) applied to formula (2.6.1) of Theorem 2.6.2. Moreover, we have

$$\sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = \log(n) \sum_{d|n} \mu(d) - \sum_{d|n} \mu(n) \log(d). \tag{2.6.3}$$

In Lemma 2.5.2 we showed that

$$\sum_{d|n} \mu(d) = \delta(n),$$

so we have

$$\log(n) \sum_{d|n} \mu(d) = \log(n)\delta(n) = 0$$

for all $n \in \mathbf{Z}_+$. Applying this to (2.6.3), we finish the proof the second equality of (2.6.2). □

2.7 Euler Products

We will frequently use infinite product starting with this section. The main facts about infinite products that we will need are summarized in §A.1.

Theorem 2.7.1. *Let f be a multiplicative function such that the series $\sum_{n=1}^{\infty} f(n)$ converges absolutely. Then we have*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \sum_{n=0}^{\infty} f(p^n), \tag{2.7.1}$$

where the infinite product on the right is taken over all prime numbers p and is absolutely convergent. Moreover, if f is totally multiplicative, then

$$\sum_{n=1}^{\infty} f(n) = \prod_p \frac{1}{1 - f(p)}. \tag{2.7.2}$$

In either (2.7.1) or (2.7.2), the product is called the *Euler product* of the series $\sum_{n=1}^{\infty} f(n)$.

Proof. By Lemma A.1.5, to prove that the infinite product

$$\prod_p \sum_{n=0}^{\infty} f(p^n), \tag{2.7.3}$$

converges absolutely, it suffices to show that the series

$$\sum_p \sum_{n=1}^{\infty} f(p^n) \tag{2.7.4}$$

converges absolutely. Given a positive integer N, we have

$$\sum_{p\le N}\left|\sum_{n=1}^{\infty} f(p^n)\right| \le \sum_{p\le N}\sum_{n=1}^{\infty}|f(p^n)| \le \sum_{n=1}^{\infty}|f(n)|$$

and the series on the right converges. Thus (2.7.4) converges absolutely, and so the infinite product (2.7.3) also converges absolutely.

Now let $\varepsilon > 0$ be given, and choose a positive integer N such that

$$\sum_{n=N+1}^{\infty}|f(n)| < \varepsilon.$$

Let A be the set containing 1 and all positive integers whose prime factors are all less than or equal to N, and let B be the set of all positive integers that have a prime factor greater than N. If $p_1, \ldots, p_m$ are the nonzero prime ideals less than or equal to N, then

$$\begin{aligned}\prod_{k=1}^{m}\sum_{n=0}^{\infty} f(p_k^n) &= \sum_{n=0}^{\infty}\sum_{\substack{\nu_1,\ldots,\nu_m\ge 0\\ \nu_1+\cdots+\nu_m=n}} f\left(p_1^{\nu_1}\cdots p_m^{\nu_m}\right)\\ &= \sum_{\nu_1,\ldots,\nu_m\ge 0} f\left(p_1^{\nu_1}\cdots p_m^{\nu_m}\right)\\ &= \sum_{n\in A} f(n).\end{aligned}$$

Here the rearrangement of the series is justified by absolute convergence. Now we have

$$\sum_{n=1}^{\infty} f(n) - \prod_{k=1}^{m}\sum_{n=0}^{\infty} f(p_k^n) = \sum_{b\in B} f(b).$$

Thus

$$\left|\sum_{n=1}^{\infty} f(n) - \prod_{k=1}^{m}\sum_{n=0}^{\infty} f(p_k^n)\right| \le \sum_{b\in B}|f(b)| \le \sum_{n>N}|f(n)| < \varepsilon.$$

Therefore we have proved (2.7.1).

Finally, if f is totally multiplicative, then every term of the product $\prod_p \sum_{n=0}^{\infty} f(p^n)$ is a convergent geometric series, and we have

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}\sum_{n=0}^{\infty} f(p)^n = \prod_{p}\frac{1}{1-f(p)}.$$

This finishes the proof. □

2.8 The Sieve of Eratosthenes

We end our discussion of arithmetic functions with a simple application. First, let us motivate the upcoming theory with an example.

Example 2.8.1. Consider the positive integers up to 30:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

Suppose we want to determine all the prime numbers in this set. We can immediately ignore 1 since it is not prime, and, for the rest, we note that a number is not prime (i.e., composite) if it has a prime divisor smaller than itself. The number 2 is the smallest prime in the list, and so all its multiples are composite. Therefore we circle 2 to signify that it is prime, and we cross out all the multiples of 2 in the list. We are left with

	②	3	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$	9	$\cancel{10}$
11	$\cancel{12}$	13	$\cancel{14}$	15	$\cancel{16}$	17	$\cancel{18}$	19	$\cancel{20}$
21	$\cancel{22}$	23	$\cancel{24}$	25	$\cancel{26}$	27	$\cancel{28}$	29	$\cancel{30}$

The next number uncrossed and uncircled is 3, so we repeat the preceding procedure, circling 3 and crossing out its multiples.

	②	③	$\cancel{4}$	5	$\xcancel{6}$	7	$\cancel{8}$	$\bcancel{9}$	$\cancel{10}$
11	$\xcancel{12}$	13	$\cancel{14}$	$\bcancel{15}$	$\cancel{16}$	17	$\xcancel{18}$	19	$\cancel{20}$
$\bcancel{21}$	$\cancel{22}$	23	$\xcancel{24}$	25	$\cancel{26}$	$\bcancel{27}$	$\cancel{28}$	29	$\xcancel{30}$

Notice that the numbers 6, 12, 18, 24, and 30 have now been crossed off twice. The process now repeats one more time, circling 5 and crossing off its multiples.

	②	③	$\cancel{4}$	⑤	$\xcancel{6}$	7	$\cancel{8}$	$\bcancel{9}$	$\sout{\cancel{10}}$
11	$\xcancel{12}$	13	$\cancel{14}$	$\sout{\bcancel{15}}$	$\cancel{16}$	17	$\xcancel{18}$	19	$\sout{\cancel{20}}$
$\bcancel{21}$	$\cancel{22}$	23	$\xcancel{24}$	$\sout{25}$	$\cancel{26}$	$\bcancel{27}$	$\cancel{28}$	29	$\sout{\xcancel{30}}$

Several more numbers are crossed out twice at this stage (all of which have at least two prime factors), and the number 30, the only product of three primes in the list, is crossed out three times. We could continue this procedure until everything would be either crossed out or circled. However, we notice that the only numbers remaining in the list are already prime. This is not a coincidence, but a consequence of the following elementary lemma.

Lemma 2.8.2. *If an integer $n > 1$ is composite, then it has a prime factor $p \leq \sqrt{n}$.*

Proof. If n is a perfect square, then we are done. Thus, suppose n is not a perfect square. Since n is composite, we can write $n = ab$, where $a, b > 1$ are some integers. Since n is not a square, $a \neq b$, so $a \neq \sqrt{n}$ and $b \neq \sqrt{n}$. If $a < \sqrt{n}$, then any prime divisor p of a is less than $\sqrt{n}$, and if $a > \sqrt{n}$, then $b < \sqrt{n}$, and any prime divisor of b is less than $\sqrt{n}$. In either case, there is a prime divisor of n which is less than $\sqrt{n}$. □

In Example 2.8.1 above, once we've circled the primes 2, 3, and 5, we have circled all the primes less than or equal to $\sqrt{30} \approx 5.477$. Therefore, if some number n in the list above were composite, then it would be a multiple of some prime $p \leq \sqrt{n} \leq \sqrt{30}$ by Lemma 2.8.2, and so it would already be crossed out. We may therefore complete the task of determining all the primes less than or equal to 30 by circling the remaining numbers.

$$\begin{array}{cccccccccc}
 & \textcircled{2} & \textcircled{3} & \cancel{4} & \textcircled{5} & \xcancel{6} & \textcircled{7} & \cancel{8} & \bcancel{9} & \xcancel{10} \\
\textcircled{11} & \xcancel{12} & \textcircled{13} & \cancel{14} & \xcancel{15} & \cancel{16} & \textcircled{17} & \xcancel{18} & \textcircled{19} & \xcancel{20} \\
\bcancel{21} & \cancel{22} & \textcircled{23} & \xcancel{24} & \cancel{25} & \cancel{26} & \bcancel{27} & \cancel{28} & \textcircled{29} & \xcancel{30}
\end{array}$$

Thus, the primes less than or equal to 30 are 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29; there are 10 of them. The preceding algorithm is attributed to the Ancient Greek mathematician Eratosthenes of Cyrene, and it is called the *sieve of Eratosthenes.*

The underlying idea of the sieve of Eratosthenes was later formalized by Legendre. The set-up is as follows. Given a finite set of integers $\mathcal{A}$, a finite set of primes $\mathcal{P}$, and an arithmetic function f, we define the following:

$$P = \prod_{p \in \mathcal{P}} p, \qquad \mathcal{S}(\mathcal{A}, \mathcal{P}, f) = \sum_{\substack{n \in \mathcal{A} \\ (n,P)=1}} f(n), \qquad \mathcal{A}_d(f) = \sum_{\substack{n \in \mathcal{A} \\ d \mid n}} f(n). \tag{2.8.1}$$

If $f(n) = 1$ for all n, then $\mathcal{S}(\mathcal{A}, \mathcal{P}, f)$ simply counts the number of $n \in \mathcal{A}$ that are not divisible by any prime $p \in \mathcal{P}$.

Theorem 2.8.3 (Legendre)**.** *With notation as above, we have*

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, f) = \sum_{d \mid P} \mu(d) \mathcal{A}_d(f).$$

Proof. In Lemma 2.5.2 we showed that

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{2.8.2}$$

Using (2.8.2), we can rewrite the definition of $\mathcal{S}(\mathcal{A}, \mathcal{P}, f)$ in (2.8.1) as

$$\begin{aligned} \mathcal{S}(\mathcal{A}, \mathcal{P}, f) &= \sum_{n \in \mathcal{A}} \sum_{d \mid (n,P)} \mu(d) f(n) \\ &= \sum_{d \mid P} \mu(d) \sum_{\substack{n \in \mathcal{A} \\ d \mid n}} f(n) \\ &= \sum_{d \mid P} \mu(d) \mathcal{A}_d(f). \end{aligned}$$

□

Definition 2.8.4. For any $x \in \mathbf{R}$, we define

$$\pi(x) = \sum_{p \leq x} 1,$$

the number of prime numbers less than or equal to x. The function $\pi(x)$ is called the *prime-counting function.*

The classical sieve of Eratosthenes demonstrated in Example 2.8.1 has one interpretation as the following result, a consequence of Theorem 2.8.3.

Corollary 2.8.5 (Sieve of Eratosthenes)**.** *For all $x > 0$, we have*

$$\pi(x) = \pi(\sqrt{x}) - 1 + \sum_{\substack{d \\ p \mid d \implies p \leq \sqrt{x}}} \mu(d) \left[\frac{x}{d} \right], \tag{2.8.3}$$

where the sum is taken over all positive integers d such that every prime divisor of d is less than or equal to $\sqrt{x}$.

Proof. Since we will use Theorem 2.8.3, we first need to make a choice of what the arithmetic function f and the sets $\mathcal{A}$ and $\mathcal{P}$ are. Let $\mathcal{A}$ be the set of all the positive integers less than or equal to x, and let $\mathcal{P}$ be the set of all primes less than or equal to $\sqrt{x}$. Also, let f be the constant arithmetic function $f(n) = 1$. Then the sum in (2.8.3) is exactly

$$\sum_{\substack{d \\ p|d \implies p \leq \sqrt{x}}} \mu(d) \left[\frac{x}{d}\right] = \sum_{d|P} \mu(d)\mathcal{A}_d(f) = \mathcal{S}(\mathcal{A}, \mathcal{P}, f)$$

by Theorem 2.8.3. Therefore, to prove (2.8.3), it suffices to show that

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, f) - 1 = \sum_{\sqrt{x} < p \leq x} 1, \tag{2.8.4}$$

since the sum on the right of (2.8.4) is $\pi(x) - \pi(\sqrt{x})$. For this, we have

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, f) - 1 = \sum_{\substack{1 < n \leq x \\ (n,P)=1}} 1 = \sum_{\substack{\sqrt{x} < n \leq x \\ (n,P)=1}} 1 = \sum_{\sqrt{x} < p \leq x} 1. \tag{2.8.5}$$

The second equality of (2.8.5) follows from the fact that if $1 < n \leq \sqrt{x}$, then $(n, P) > 1$. The third equality of (2.8.5) follows from Lemma 2.8.2, since if $\sqrt{x} < n \leq x$ and n has no prime divisors less than or equal to $\sqrt{x}$, then n must be prime. Thus we've proved (2.8.4), and the proof is complete. □

Let us now return to Example 2.8.1 from the beginning of this section to see Corollary 2.8.5 in action. Suppose that, instead of wanting to determine all the primes less than or equal to 30, we only want to perform the easier task of counting how many such primes there are. That is, we want to compute $\pi(30)$. By Corollary 2.8.5, we know that

$$\pi(30) = \pi(\sqrt{30}) - 1 + \sum_{\substack{d \\ p|d \implies p \leq \sqrt{30}}} \mu(d) \left[\frac{30}{d}\right]. \tag{2.8.6}$$

Note that there are 3 primes less than or equal to $\sqrt{30}$. They are 2, 3, and 5. Therefore, the sum above is equal to

$$[30] - \sum_{p_1 \leq \sqrt{30}} \left[\frac{30}{p_1}\right] + \sum_{p_1 < p_2 \leq \sqrt{30}} \left[\frac{30}{p_1 p_2}\right] - \sum_{p_1 < p_2 < p_3 \leq \sqrt{30}} \left[\frac{30}{p_1 p_2 p_2}\right]$$

$$= [30] - \left[\frac{30}{2}\right] - \left[\frac{30}{3}\right] - \left[\frac{30}{5}\right] + \left[\frac{30}{2\cdot 3}\right] + \left[\frac{30}{2\cdot 5}\right] + \left[\frac{30}{3\cdot 5}\right] - \left[\frac{30}{2\cdot 3\cdot 5}\right].$$

This formalizes our process of circling primes and crossing out their multiples step-by-step in Example 2.8.1. When we circled the prime 2, we circled or crossed out a total of $[30/2] = 15$ numbers in the list. Then when we circled the prime 3 next, we circled or crossed out a total of $[30/3] = 10$ numbers in the list, but $[30/(2\cdot 3)] = 5$ of those were already crossed out when we worked with the prime 2. Finally, when we circled the prime 5, we circled or crossed out a total of $[30/5] = 6$ numbers in the list. However, of these 6 numbers, $[30/10] = 3$ were crossed out in the prime 2 step, and $[30/15] = 2$ were already crossed out in the prime 3 step. Also, the number $30 = [30/(2\cdot 3\cdot 5)]$ was crossed out at each stage. This is the intuitive justification for the arrangements of plus and minus signs in the sums above, and it shows that the factor $\mu(d)$ occurring in (2.8.6), and more generally in (2.8.3) of Corollary 2.8.5 plays an "inclusion-exclusion" role to avoid over-counting.

Stepping away from our example and into more generality, one wonders if one can use Corollary 2.8.5 to give an estimate for

$$\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{\substack{d \\ p|d \implies p\le\sqrt{x}}} \mu(d)\left[\frac{x}{d}\right]$$

by bounding the right-hand side. An obvious first approach would be to replace $[t]$ by t, with some remainder term involving $\{t\}$, the fractional part of t. We immediately have

$$\begin{aligned}\pi(x) - \pi(\sqrt{x}) + 1 &= \sum_{\substack{d \\ p|d \implies p\le\sqrt{x}}} \mu(d)\left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) \\ &= x\sum_{d|P(\sqrt{x})}\frac{\mu(d)}{d} + R,\end{aligned} \tag{2.8.7}$$

where our "remainder" R is

$$R = -\sum_{d|P(\sqrt{x})}\mu(d)\left\{\frac{x}{d}\right\}.$$

Recall from §2.5 that the Möbius inversion formula (Theorem 2.5.3) allowed us to prove (2.5.3):

$$\phi(n) = \sum_{d|n}\mu\left(\frac{n}{d}\right)d.$$

Changing the order of summation, we see that

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}. \tag{2.8.8}$$

Next, recall from Lemma 2.4.4 that

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{2.8.9}$$

Combining (2.8.8) and (2.8.9), we get

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

and so (2.8.7) becomes

$$\pi(x) - \pi(\sqrt{x}) + 1 = x \prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) + R. \tag{2.8.10}$$

To estimate the product in (2.8.10), we use the following theorem, presented without proof.

Theorem 2.8.6 (Mertens)**.** *For $z > 0$, we have*

$$\prod_{p \leq z} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log(z)} \left(1 + O\left(\frac{1}{\log(z)}\right)\right) \qquad \textit{as } z \to \infty,$$

where γ is the Euler-Mascheroni constant (cf. Definition 4.2.5 below).

Proof. See [Mur08, Theorem 9.1.3]. □

One can now show, using Theorem 2.8.6 and (2.8.10), that

$$\pi(x) - \pi(\sqrt{x}) + 1 \sim 2e^{-\gamma} \left(\frac{x}{\log(x)}\right) \qquad \text{as } x \to \infty.$$

This is not optimal, and we will get a better estimate when we later prove the prime number theorem (Theorem 4.5.7), which states that

$$\pi(x) \sim \frac{x}{\log(x)} \qquad \text{as } x \to \infty.$$

Moreover, if we try to bound our remainder term R, we will get a cumbersome bound of $2^{\pi(\sqrt{x})}$, which is huge as $x \to \infty$. Therefore, the sieve of Eratosthenes has its limitations when used to bound sums.

In modern practice, the use of the sieve of Eratosthenes is usually superseded by more sophisticated sieve methods, such as the Brun sieve or the Selberg sieve. A popular resource for sieve theory that covers these and many other topics is [FI10].

Among the many application of sieves is the study of *twin primes*—primes p such that $p+2$ is also prime. A famous open problem is the following.

Conjecture 2.8.7 (Twin Primes Conjecture)**.** There are infinitely many twin primes.

Although this is still open, there has been some progress made in the direction of affirming the conjecture. In [Che73], Chen used sieve methods to prove the tantalizingly close result that there are infinitely many primes p such that $p+2$ is a product of two primes. More recently, in [Zha14], Zhang proved that

$$\liminf_{n\to\infty}(p_{n+1}-p_n) < 7\cdot 10^7,$$

where p_n denotes the nth prime. Even more recently, Maynard used sieve methods to prove that

$$\liminf_{n\to\infty}(p_{n+1}-p_n) \leq 600$$

in his pre-print [May13].

3 Dirichlet Series

3.1 Summation Lemmas

Lemma 3.1.1. *Let $(f_n)_{n=1}^{\infty}$ and $(g_n)_{n=1}^{\infty}$ be sequences of complex numbers, and let $a \leq b$ be positive integers. Then the following hold:*

(a) $\displaystyle\sum_{n=a}^{b} f_n g_n = f_b \sum_{n=a}^{b} g_n + \sum_{n=a}^{b-1}(f_n - f_{n+1}) \sum_{k=a}^{n} g_k.$

(b) $\displaystyle\sum_{n=a}^{b} f_n\left(g_{n+1}-g_n\right) = f_{b+1}g_{b+1} - f_a g_a - \sum_{n=a}^{b} g_{n+1}\left(f_{n+1}-f_n\right).$

Proof. The proof consists of re-indexing sums and gathering terms. We have $g_n = \sum_{k=a}^{n} g_k - \sum_{k=a}^{n-1} g_k$, whence

$$\begin{aligned}\sum_{n=a}^{b} f_n g_n &= \sum_{n=a}^{b} f_n \left(\sum_{k=a}^{n} g_k - \sum_{k=a}^{n-1} g_k\right)\\ &= f_b \sum_{n=a}^{b} g_n + \sum_{n=a}^{b-1} f_n \sum_{k=a}^{n} g_k - \sum_{n=a+1}^{b} f_n \sum_{k=a}^{n-1} g_k\\ &= f_b \sum_{n=a}^{b} g_n + \sum_{n=a}^{b-1} (f_n - f_{n+1}) \sum_{k=a}^{n} g_k,\end{aligned}$$

proving (a). For (b), we have

$$\begin{aligned}\sum_{n=a}^{b} f_n \left(g_{n+1} - g_n\right) &= \sum_{n=a}^{b} f_n g_{n+1} - \sum_{n=a-1}^{b-1} f_{n+1} g_{n+1}\\ &= \sum_{n=a}^{b} f_n g_{n+1} - f_a g_a - \sum_{n=a}^{b} f_{n+1} g_{n+1} + f_{b+1} g_{n+1}\\ &= f_{b+1} g_{b+1} - f_a g_a - \sum_{n=a}^{b} g_{n+1} \left(f_{n+1} - f_n\right). \qquad \square\end{aligned}$$

Lemma 3.1.2 (Abel's Lemma)**.** *Let f be an arithmetic function, and let g be a C^1 function defined on $[a, b]$, where $0 < a < b$. For any real number $x \geq 1$, define*

$$F(x) = \sum_{1 \leq n \leq x} f(n),$$

the sum being taken over integers n greater than 0 and not exceeding x. Then

$$\sum_{a<n\leq b} f(n)g(n) = F(b)g(b) - F(a)g(a) - \int_a^b F(t)g'(t)\,dt. \qquad (3.1.1)$$

Proof. The leftmost sum in (3.1.1) is the Riemann-Stieltjes integral

$$\sum_{a<n\leq b} f(n)g(n) = \int_a^b g(t)\,dF(t).$$

Therefore integration by parts gives

$$\begin{aligned}\sum_{a<n\leq b} f(n)g(n) &= F(b)g(b) - F(a)g(a) - \int_a^b F(t)\,dg(t) \\ &= F(b)g(b) - F(a)g(a) - \int_a^b F(t)g'(t)\,dt. \qquad \square\end{aligned}$$

3.2 The Dirichlet Series of an Arithmetic Function

Definition 3.2.1. Let f be an arithmetical function. To f we associate the complex-valued function

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

defined for all those $s \in \mathbf{C}$ for which the series converges, called the *Dirichlet series* of f.

Theorem 3.2.2. *Let f be a multiplicative arithmetic function, and let s be a complex number for which $D(f,s)$ converges absolutely. Then we have*

$$D(f,s) = \prod_p \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}}.$$

Moreover, if f is totally multiplicative, then we have

$$D(f,s) = \prod_p \frac{1}{1 + f(p)p^{-s}}.$$

Proof. Both claims are immediate corollaries of Theorem 2.7.1. □

Theorem 3.2.3. *If f and g are two arithmetic functions and s is a complex number such that both $D(f,s)$ and $D(g,s)$ converge and at least one of $D(f,s)$ and $D(g,s)$ converges absolutely, then we have*

$$D(f,s)D(g,s) = D(f*g,s).$$

Proof. By absolute convergence of one of the Dirichlet series, we may rearrange the sums to get

$$D(f,s)D(g,s) = \left(\sum_{m=1}^{\infty} \frac{f(m)}{m^s}\right)\left(\sum_{n=1}^{\infty} \frac{g(n)}{n^s}\right)$$

$$= \sum_{m,n\in\mathbf{Z}_+} \frac{f(m)g(n)}{(mn)^s} = \sum_{n=1}^{\infty} \left(\sum_{d|n} f(d) g\left(\frac{n}{d}\right) \right) \frac{1}{n^s}$$

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

3.3 Convergence of General Dirichlet Series

Definition 3.3.1. Let $f : \mathbf{Z}_+ \to \mathbf{C}$ be an arithmetic function, and let $\lambda : \mathbf{Z}_+ \to \mathbf{R}$ be a strictly increasing and unbounded function. To f and λ we associate the *general Dirichlet series*

$$D(f,\lambda,s) = \sum_{n=1}^{\infty} f(n)e^{-\lambda(n)s}, \tag{3.3.1}$$

defined at all $s \in \mathbf{C}$ for which this series converges.

Note that when $\lambda = \log$, we have

$$D(f,\lambda,s) = D(f,s),$$

and when $\lambda(n) = n$, then $D(f,\lambda,s)$ is a power series in e^{-s}.

For the remainder of this section, we f and λ as in Definition 3.3.1.

Theorem 3.3.2. *Suppose $D(f,\lambda,s_0)$ converges for some $s_0 \in \mathbf{C}$. Then for every $\theta > 0$ with $\theta < \pi/2$, the general Dirichlet series $D(f,\lambda,s)$ converges uniformly in the domain of all $s \in \mathbf{C}$ satisfying*

$$|\operatorname{Arg}(s-s_0)| \leq \theta.$$

Proof. We may assume without loss of generality that $s_0 = 0$, since otherwise we could define

$$g(n) = f(n)e^{-\lambda(n)s_0}, \qquad s' = s - s_0$$

and consider the general Dirichlet series

$$D(g,\lambda,s') = \sum_{n=1}^{\infty} g(n)e^{-\lambda(n)s'},$$

which converges at $s = 0$. Thus, we henceforth assume that $s_0 = 0$. That is, the series

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

converges. For each $n \in \mathbf{Z}_+$, define

$$R(n) = \sum_{k=n+1}^{\infty} f(k).$$

Then $\lim_{n\to\infty} R(n) = 0$.

Now pick a real number θ strictly between 0 and $\pi/2$. Let $\varepsilon > 0$ be given. Then there exists a positive integer N so that $|R(n)| < \varepsilon$ for all integers $n \geq N$. Also, assume N is large enough so that $\lambda(n) > 0$ for every $n \geq N$.

Fix an $s \in \mathbf{C}$ with $|\operatorname{Arg}(s)| < \theta$. Write $s = \sigma + it$ with $\sigma, t \in \mathbf{R}$ (note that $\sigma > 0$). Then by trigonometry we have

$$\frac{|s|}{\sigma} = \sec(\operatorname{Arg}(s)) \leq \sec(\theta). \tag{3.3.2}$$

For $N \in \mathbf{Z}_+$, we define

$$S(N) = \sum_{n=1}^{N} f(n)e^{-\lambda(n)s}.$$

Suppose m and n are positive integers with $N \leq m \leq n$. Then we have

$$S(n) - S(m) = \sum_{k=m+1}^{n} f(k)e^{-\lambda(k)s} = \sum_{k=m+1}^{n} \left(R(k-1) - R(k)\right) e^{-\lambda(k)s},$$

so by partial summation (Lemma 3.1.1(b)) we get

$$\begin{aligned} &S(n) - S(m) \\ &= \sum_{k=m+1}^{n} R(k)\left(e^{-\lambda(k+1)s} - e^{-\lambda(k)s}\right) + R(m)e^{-\lambda(m+1)s} - R(n)e^{-\lambda(n+1)s} \end{aligned}$$

Taking absolute values gives us

$$|S(n) - S(m)| < \varepsilon \sum_{k=m+1}^{n} \left|e^{-\lambda(k+1)s} - e^{-\lambda(k)s}\right| + 2\varepsilon. \tag{3.3.3}$$

Moreover, we have

$$\begin{aligned}\sum_{k=m+1}^{n} \left|e^{-\lambda(k+1)s} - e^{-\lambda(k)s}\right| &= \sum_{k=m+1}^{n} \left|-s \int_{\lambda(k)}^{\lambda(k+1)} e^{-us}\, du\right| \\ &\leq |s| \sum_{k=m+1}^{n} \int_{\lambda(k)}^{\lambda(k+1)} e^{-u\sigma}\, du \\ &= |s| \int_{\lambda(m+1)}^{\lambda(n+1)} e^{-u\sigma}\, du \\ &= \frac{|s|}{\sigma}\left(e^{\lambda(m+1)\sigma} - e^{\lambda(n+1)\sigma}\right) \leq \frac{|s|}{\sigma},\end{aligned}$$

so now (3.3.2) and (3.3.3) give us

$$|S(n) - S(m)| < \varepsilon\left(\frac{|s|}{\sigma} + 2\right) \leq \varepsilon(\sec\theta + 2). \tag{3.3.4}$$

The right-hand side of (3.3.4) goes to zero as $\varepsilon \to 0$ and does not depend on s, so it follows that $D(f, \lambda, s)$ is uniformly Cauchy in the domain of all $s \in \mathbf{C}$ with $|\operatorname{Arg}(s - s_0)| \leq \theta$. Thus the lemma follows. □

Corollary 3.3.3. *If $D(f, \lambda, s_0)$ converges for some $s_0 \in \mathbf{C}$, then $D(f, \lambda, s)$ converges uniformly in all compact subsets of the domain of all $s \in \mathbf{C}$ with $\operatorname{Re}(s) > \operatorname{Re}(s_0)$.*

Proof. Suppose $D(f, \lambda, s_0)$ converges, and let K be a compact subset of the half-plane $\{s \in \mathbf{C} \mid \operatorname{Re}(s) > \operatorname{Re}(s_0)\}$. Since K is compact, there exists a $\theta \in (0, \pi/2)$ such that $|\operatorname{Arg}(s - s_0)| \leq \theta$ for all $s \in K$, so the claim follows from Theorem 3.3.2. □

Definition 3.3.4. Let S be the set of all $\sigma \in \mathbf{R}$ such that there exists an $s \in \mathbf{C}$ with $\operatorname{Re}(s) = \sigma$ and for which $D(f, \lambda, s)$ converges. The number $\sigma_c = \inf S$ (possibly $\pm\infty$) is called the *abscissa of convergence* of $D(f, \lambda, s)$. Moreover, the open set $H_c = \{s \in \mathbf{C} \mid \operatorname{Re}(s) > \sigma_c\}$ is called the *half-plane of convergence* of $D(f, \lambda, s)$.

The name of H_c is justified by the following theorem.

Theorem 3.3.5. *For all $s \in \mathbf{C}$, if $\operatorname{Re}(s) > \sigma_c$, then $D(f, \lambda, s)$ converges, and if $\operatorname{Re}(s) < \sigma_c$, then $D(f, \lambda, s)$ diverges.*

Proof. If $s \in \mathbf{C}$ and $\mathrm{Re}(s) < \sigma_c$, then $D(f, s)$ diverges by the definition of σ_c. Now suppose $\mathrm{Re}(s) > \sigma_c$, and suppose $D(f, \lambda, s)$ diverges. Then, by the definition of σ_c, there necessarily exists an $s' \in \mathbf{C}$ with $\sigma_c \leq \mathrm{Re}(s') < \mathrm{Re}(s)$ such that $D(f, \lambda, s')$ converges. But the convergence of $D(f, \lambda, s')$ implies the convergence of $D(f, \lambda, s)$ by Corollary 3.3.3 since $\mathrm{Re}(s') < \mathrm{Re}(s)$. This contradiction implies that $D(f, \lambda, s)$ in fact converges. □

In Theorem 3.3.7 we will derive an explicit formulas for σ_c in the case that $\sum_{n=1}^{\infty} f(n)$ converges. We will need to use the following lemma.

Lemma 3.3.6. *Suppose that there exists an $s_0 \in \mathbf{C}$ with $\mathrm{Re}(s_0) > 0$ for which $D(f, \lambda, s_0)$ converges. Let*

$$\alpha = \limsup_{n \to \infty} \frac{1}{\lambda(n)} \log \left| \sum_{k=1}^{n} f(k) \right|.$$

Then

$$\alpha \leq \mathrm{Re}(s_0).$$

Proof. For every $n \in \mathbf{Z}_+$, let

$$A(n) = \sum_{k=1}^{n} f(k) e^{-\lambda(k) s_0}.$$

Since $D(f, \lambda, s_0)$ converges, there exists an $M > 0$ such that

$$|A(n)| < M \tag{3.3.5}$$

for all $n \in \mathbf{Z}_+$. Partial summation (Lemma 3.1.1(a)) yields

$$\begin{aligned} \sum_{k=1}^{n} f(k) &= \sum_{k=1}^{n} e^{\lambda(k) s_0} f(k) e^{-\lambda(k) s_0} \\ &= e^{\lambda(n) s_0} A(n) + \sum_{k=1}^{n-1} \left(e^{\lambda(k) s_0} - e^{-\lambda(k+1) s_0} \right) A(k). \end{aligned}$$

After taking absolute values and applying (3.3.5), it follows that

$$\left| \sum_{k=1}^{n} f(k) \right| < M e^{\lambda(n) \mathrm{Re}(\sigma_0)} + M \sum_{k=1}^{n-1} \left| e^{\lambda(k) s_0} - e^{-\lambda(k+1) s_0} \right|. \tag{3.3.6}$$

Moreover, we have

$$\begin{aligned}\sum_{k=1}^{n-1}\left|e^{\lambda(k)s_0}-e^{\lambda(k+1)s_0}\right| &= \sum_{k=1}^{n-1}\left|-s_0\int_{\lambda(k)}^{\lambda(k+1)} e^{us_0}\,du\right| \\ &\leq |s_0|\sum_{k=1}^{n-1}\int_{\lambda(k)}^{\lambda(k+1)} e^{u\,\mathrm{Re}(s_0)}\,du \\ &= |s_0|\int_{\lambda(1)}^{\lambda(n)} e^{u\,\mathrm{Re}(s_0)}\,du \\ &= \frac{|s_0|}{\mathrm{Re}(s_0)}\left(e^{\lambda(n)\,\mathrm{Re}(s_0)}-e^{\lambda(1)\,\mathrm{Re}(s_0)}\right) \\ &\leq \frac{|s_0|}{\mathrm{Re}(s_0)}e^{\lambda(n)\,\mathrm{Re}(s_0)}.\end{aligned}$$

This and (3.3.6) imply that

$$\left|\sum_{k=1}^{n} f(k)\right| \leq e^{\lambda(n)\,\mathrm{Re}(s_0)}M\left(1+\frac{|s_0|}{\mathrm{Re}(s_0)}\right).$$

Applying the logarithm and dividing by $\lambda(n)$, we see that

$$\frac{1}{\lambda(n)}\log\left|\sum_{k=1}^{n} f(k)\right| \leq \mathrm{Re}(s_0)+\frac{1}{\lambda(n)}\log\left(M+\frac{|s_0|M}{\mathrm{Re}(s_0)}\right). \tag{3.3.7}$$

Let $\varepsilon > 0$ be given. The function λ is strictly increasing and unbounded, so there exists a positive integer N such that for $n \geq N$ we have

$$\lambda(n) > \frac{1}{\varepsilon}\log\left(M+\frac{|s_0|M}{\mathrm{Re}(s_0)}\right)$$

and hence

$$\frac{1}{\lambda(n)}\log\left(M+\frac{|s_0|M}{\mathrm{Re}(s_0)}\right) < \varepsilon,$$

Now (3.3.7) yields

$$\frac{1}{\lambda(n)}\log\left|\sum_{k=1}^{n} a_k\right| < \mathrm{Re}(s_0)+\varepsilon. \tag{3.3.8}$$

Since (3.3.8) holds for all ε sufficiently small and all n sufficiently large, it follows that $\alpha \leq \mathrm{Re}(s)$. □

Theorem 3.3.7. *As in Lemma 3.3.6, define*

$$\alpha = \limsup_{n\to\infty} \frac{1}{\lambda(n)} \log \left| \sum_{k=1}^{n} f(k) \right| .$$

If the series $\sum_{n=1}^{\infty} f(n)$ diverges, then $\sigma_c = \alpha$.

Proof. The divergence of the series $\sum_{n=1}^{\infty} f(n)$ implies that $\sigma_c \geq 0$. We will first prove that $\alpha \leq \sigma_c$. Since there is nothing to prove if $\sigma_c = \infty$, we assume that $\sigma_c < \infty$. For a given $s \in \mathbf{C}$ with $\sigma_c < \mathrm{Re}(s)$, Theorem 3.3.5 implies that $D(f, \lambda, s)$ converges, and so $\alpha \leq \mathrm{Re}(s)$ by Lemma 3.3.6. Thus the definition of σ_c implies that $\alpha \leq \sigma_c$.

Next we prove that $\sigma_c \leq \alpha$. There is nothing to prove if $\alpha = \infty$, so assume $\alpha < \infty$. It is sufficient to prove that the series $D(f, \lambda, \alpha + \delta)$ converges for every $\delta > 0$. Therefore we fix a $\delta > 0$ and let $s = \alpha + \delta$. Choose a $\varepsilon > 0$ with $\varepsilon < \delta$. For every $n \in \mathbf{Z}_+$, define

$$A(n) = \sum_{k=1}^{n} f(k).$$

By the definition of α, there exists a positive integer N such that for all $n \geq N$ we have

$$\log |A(n)| < \lambda(n)(s - \varepsilon),$$

and so

$$|A(n)| < e^{\lambda(n)(s-\varepsilon)}, \tag{3.3.9}$$

From partial summation (Lemma 3.1.1(a)) it follows that

$$\sum_{m=1}^{n} f(m) e^{-\lambda(m)s} = e^{-\lambda(n)s} A(n) + \sum_{k=1}^{n-1} \left(e^{-\lambda(k)s} - e^{-\lambda(k+1)s} \right) A(k). \tag{3.3.10}$$

By (3.3.9), we have

$$\left| e^{-\lambda(n)s} A(n) \right| < e^{-\lambda(n)s} e^{\lambda(n)(s-\varepsilon)} = e^{-\lambda(n)\varepsilon}$$

for $n \geq N$. Therefore, by (3.3.9) and (3.3.10), to prove that $D(f, \lambda, s)$ converges it suffices to prove that the series

$$\sum_{n=1}^{\infty} \left(e^{-\lambda(n)s} - e^{-\lambda(n+1)s} \right) e^{\lambda(n)(s-\varepsilon)} \tag{3.3.11}$$

converges. For this, note that

$$\left(e^{-\lambda(n)s} - e^{-\lambda(n+1)s}\right) e^{\lambda(n)(s-\varepsilon)} = s \int_{\lambda(n)}^{\lambda(n+1)} e^{\lambda(n)(s-\varepsilon)-st}\, dt \leq s \int_{\lambda(n)}^{\lambda(n+1)} e^{-\varepsilon t}\, dt,$$

so that

$$\sum_{n=1}^{\infty} \left(e^{-\lambda(n)s} - e^{-\lambda(n+1)s}\right) e^{\lambda(n)(s-\varepsilon)} \leq s \sum_{n=1}^{\infty} \int_{\lambda(n)}^{\lambda(n+1)} e^{-\varepsilon t}\, dt = s \int_{\lambda(1)}^{\infty} e^{-\varepsilon t}\, dt.$$

The rightmost integral above converges, whence so does the series (3.3.11), finishing the proof. □

3.4 Absolute Convergence of General Dirichlet Series

As in §3.3, $f : \mathbf{Z}_+ \to \mathbf{C}$ will denote a fixed arithmetic function and $\lambda : \mathbf{Z}_+ \to \mathbf{R}$ will denote a fixed increasing and unbounded function.

Definition 3.4.1. The *abscissa of absolute convergence* σ_a of $D(f, \lambda, s)$ is the abscissa of convergence of the general Dirichlet series $D(|f|, \lambda, s)$.

Theorem 3.4.2. *For $s \in \mathbf{C}$, if $s > \sigma_a$, then $D(f, \lambda, s)$ converges absolutely, and if $s < \sigma_a$, then $D(f, \lambda, s)$ does not converge absolutely. Moreover, if $\sum_{n=1}^{\infty} |f(n)|$ diverges, then*

$$\sigma_a = \limsup_{n\to\infty} \frac{1}{\lambda(n)} \log \left(\sum_{k=1}^{n} |f(n)| \right).$$

Proof. This follows immediately from Definition 3.4.1, Theorem 3.3.5, and Theorem 3.3.7. □

Theorem 3.4.3. *We have the inequality*

$$0 \leq \sigma_a - \sigma_c \leq \limsup_{n\to\infty} \frac{\log(n)}{\lambda(n)}.$$

Proof. It is clear that $\sigma_a - \sigma_c \geq 0$. The difference $\sigma_a - \sigma_c$ is invariant under a change of variable in the corresponding general Dirichlet series, so we may assume without loss of generality that $\sigma_c > 0$. Then Theorems 3.3.7 and 3.4.2 apply, and we have

$$\sigma_c = \limsup_{n\to\infty} \frac{1}{\lambda(n)} \log \left| \sum_{k=1}^{n} f(n) \right|, \qquad \sigma_a = \limsup_{n\to\infty} \frac{1}{\lambda(n)} \log \left(\sum_{k=1}^{n} |f(n)| \right)$$

Let $\varepsilon > 0$ be given. Choose a positive integer N such that for all $n \geq N$ we have

$$\left| \sum_{k=1}^{n} f(k) \right| < e^{\lambda(n)(\sigma_a+\varepsilon)}, \quad \sum_{k=1}^{n} |f(k)| < e^{\lambda(n)(\sigma_c+\varepsilon)}, \quad e^{\lambda(n)\varepsilon} > 2. \tag{3.4.1}$$

Therefore

$$|f(n)| = \left| \sum_{k=1}^{n} f(k) - \sum_{k=1}^{n-1} f(k) \right| \leq 2e^{\lambda(n)(\sigma_c+\varepsilon)} < e^{\lambda(n)(\sigma_c+2\varepsilon)} \tag{3.4.2}$$

when $n \geq N$. Then for sufficiently large $n \geq N$, (3.4.1) and (3.4.2) imply that

$$\begin{aligned} \sum_{k=1}^{n} |f(k)| &= \sum_{k=1}^{N} |f(k)| + \sum_{k=N+1}^{n} |f(k)| \\ &< \sum_{k=1}^{N} |f(k)| + ne^{\lambda(n)(\sigma_c+2\varepsilon)} \\ &< ne^{\lambda(n)(\sigma_c+3\varepsilon)}, \end{aligned}$$

whence

$$\sigma_a \leq \frac{1}{\lambda(n)} (\log(n) + \lambda(n)(\sigma_c + 3\varepsilon)) = \frac{\log(n)}{\lambda(n)} + \sigma_c + 3\varepsilon.$$

Letting ε go to zero, we prove the theorem. □

3.5 Dirichlet Series as Analytic Functions

Lemma 3.5.1. *Let U be an open subset of $\mathbf{C}$, and let $\{f_n\}$ be a sequence of analytic functions that converges uniformly on every compact subset of U. Let f be the limit of $\{f_n\}$. Then f is analytic and for every $z \in U$ and every positive integer k we have*

$$f^{(k)}(z) = \lim_{n\to\infty} f_n^{(k)}(z).$$

Proof. Let D be a closed disk in U, and let C be its boundary, oriented in the usual way. Then for every positive integer n, every nonnegative integer k, and every point $z_0 \in D$ we have

$$f_n^{(k)}(z_0) = \frac{k!}{2\pi i} \oint_C \frac{f_n(z)}{(z - z_0)^{k+1}} \, dz$$

The uniform convergence of $\{f_n\}$ on D implies that we may pull limits through the integral above, and hence the lemma follows. □

Theorem 3.5.2. *Let f be an arithmetic function, and let $D(f,s)$ be its Dirichlet series. Then there exist $\sigma_f, \sigma_{|f|} \in \mathbf{R} \cup \{\pm\infty\}$ such that*

(a) *we have the inequality*

$$0 \le \sigma_{|f|} - \sigma_f \le 1;$$

(b) *$D(f,s)$ diverges if $\operatorname{Re}(s) < \sigma_f$;*

(c) *$D(f,s)$ converges uniformly in every compact subset of the half-plane*

$$H_f = \{s \in \mathbf{C} \mid \operatorname{Re}(s) > \sigma_f\};$$

(d) *$D(f,s)$ converges absolutely in the half-plane*

$$H_{|f|} = \{s \in \mathbf{C} \mid \operatorname{Re}(s) > \sigma_{|f|}\};$$

(e) *$D(f,s)$ defines an analytic function for $\operatorname{Re}(s) > \sigma_f$, and*

$$D(f,s)' = D(f',s),$$

where $f'(n) = -\log(n) f(n)$ as in §2.3;

(f) *If $\sum_{n=1}^{\infty} f(n)$ diverges, then*

$$\sigma_f = \limsup_{n\to\infty} \frac{\log \left|\sum_{k=1}^{n} f(k)\right|}{\log(n)}.$$

(g) *If $\sum_{n=1}^{\infty} |f(n)|$ diverges, then*

$$\sigma_{|f|} = \limsup_{n\to\infty} \frac{\log \left(\sum_{k=1}^{n} |f(k)|\right)}{\log(n)}.$$

Proof. Everything except for (e) follows from the results of §3.3. Part (e) follows from Lemma 3.5.1 since the partial sums of a Dirichlet series are clearly analytic. □

The numbers σ_f and $\sigma_{|f|}$ of Theorem 3.5.2 are called the *abscissa of convergence* and the *abscissa of absolute convergence* of the Dirichlet series $D(f, s)$.

Theorem 3.5.3. *If f is an arithmetic function taking only nonnegative real number values, then there is no extension of $D(f, s)$ to a function which is analytic at σ_f.*

Proof. Without loss of generality, we may assume $\sigma_f = 0$. For the sake of contradiction, suppose that there exists a complex function F extending $D(f, s)$ which is analytic at 0. Then F is analytic at 1 and can therefore be written locally as a Taylor series centered at 1 with radius of convergence strictly greater than 1. Let s be a negative number for which this Taylor series converges. Then we have

$$\begin{aligned} F(s) &= \sum_{k=0}^{\infty} \frac{D(f,s)^{(k)}\big|_{s=1}}{k!} (s-1)^k \\ &= \sum_{k=0}^{\infty} \frac{(1-s)^k}{n!} \sum_{n=1}^{\infty} \frac{f(n)\log(n)^k}{n} \\ &= \sum_{n=1}^{\infty} \frac{f(n)}{n} \sum_{k=0}^{\infty} \frac{(1-s)^k \log(n)^k}{k!} \\ &= \sum_{n=1}^{\infty} \frac{f(n)}{n} \sum_{k=0}^{\infty} \frac{\log\left(n^{1-s}\right)^k}{k!}, \end{aligned}$$

where changing the order of summation is justified since everything is nonnegative. Therefore, since

$$\frac{1}{n^{s-1}} = e^{\log(n^{1-s})} = \sum_{k=0}^{\infty} \frac{\log\left(n^{1-s}\right)^k}{k!},$$

we have

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n} \cdot \frac{1}{n^{s-1}} = \sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

which shows that $D(f,s)$ converges as a Dirichlet series at $s<0$, contradicting the fact that $\sigma_f = 0$. □

Lemma 3.5.4. *Let f be an arithmetic function, and suppose that*

$$F(x) = \sum_{1\le n\le x} f(n) = O(x^\delta) \tag{3.5.1}$$

as $x\to\infty$ for some $\delta>0$. Then for $\mathrm{Re}(s)>\delta$ *we have*

$$D(f,s) = s\int_1^\infty \frac{F(t)}{t^{s+1}}\,dt.$$

Proof. Fix an $s\in\mathbf{C}$ with $\mathrm{Re}(s)>\delta$. By Abel's lemma (Lemma 3.1.2) we have

$$\sum_{1\le n\le x}\frac{f(n)}{n^s} = \frac{F(x)}{x^s} + s\int_1^x \frac{F(t)}{t^{s-1}}\,dt. \tag{3.5.2}$$

Since $F(x)=O(x^\delta)$ and $\mathrm{Re}(s)>\delta$, it follows that

$$\lim_{x\to\infty}\left|\frac{F(x)}{x^s}\right| = \lim_{x\to\infty}\frac{|F(x)|}{x^{\mathrm{Re}(s)}} = 0.$$

Therefore the limit in (3.5.2) is zero, and the lemma follows. □

4 The Riemann Zeta Function

4.1 Elementary Properties of $\zeta(s)$

Definition 4.1.1. The *Riemann zeta function* is the Dirichlet series

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

associated to the constant arithmetic function $n\mapsto 1$.

By the general theory of Dirichlet series developed in §3 (in particular, Theorems 3.2.2, 3.5.2, and 3.5.3), we immediately see that $\zeta(s)$ has abscissa of regular and absolute convergence 1, that for $\mathrm{Re}(s)>1$ we have

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}, \tag{4.1.1}$$

that $\zeta(s)$ is analytic for $\mathrm{Re}(s) > 1$, satisfying

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

and that $\zeta(s)$ has a pole at $s = 1$. The convergence of the Euler product (4.1.1) implies that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$.

Lemma 4.1.2. *If $s \in \mathbf{C}$ and $\mathrm{Re}(s) > 1$, then*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}. \tag{4.1.2}$$

Proof. Fix $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. For all $n \in \mathbf{Z}_+$, we have $|\mu(n)| \leq 1$, so that

$$\left| \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^{\mathrm{Re}(s)}} \leq \zeta(\mathrm{Re}(s)),$$

which shows that the right side of (4.1.2) converges absolutely for $\mathrm{Re}(s) > 1$. By Theorem 3.2.3 and Lemma 2.5.2 (which states that $\mu * 1 = \delta$), we have

$$\zeta(s) D(\mu, s) = D(1 * \mu, s) = D(\delta, s) = 1. \tag{4.1.3}$$

Since $\zeta(s) \neq 0$, we divide (4.1.3) by $\zeta(s)$ to get

$$\frac{1}{\zeta(s)} = D(\mu, s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$ □

Lemma 4.1.3. *If $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 2$, then*

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

Proof. Fix $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 2$, so that both $\zeta(s)$ and $\zeta(s-1)$ converge (absolutely). Then we have

$$\zeta(s-1) = \sum_{n=1}^{\infty} \frac{1}{n^{s-1}} = \sum_{n=1}^{\infty} \frac{n}{n^s} = D(\mathrm{id}, s). \tag{4.1.4}$$

Thus $D(\mathrm{id}, s)$ converges absolutely. Since for all $n \in \mathbf{Z}_+$ we have

$$0 \le \phi(n) \le n,$$

it follows that $D(\phi, s)$ also converges absolutely. In Lemma 2.4.5 we proved the identity

$$\mathrm{id} = \phi * 1,$$

so using Theorem 3.2.3 and (4.1.4), we obtain the equality

$$\zeta(s)D(\phi, s) = D(1 * \phi, s) = D(\mathrm{id}, s) = \zeta(s-1).$$

Therefore we conclude that

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}. \qquad \square$$

Lemma 4.1.4. *If $s \in \mathbf{C}$ and $\mathrm{Re}(s) > 1$, then*

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = \sum_{p} \frac{\log(p)}{p^s - 1}, \tag{4.1.5}$$

where the second series is taken over all positive prime numbers p.

Proof. Fix $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$, and let $\sigma = \mathrm{Re}(s)$. Since

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

converges absolutely, it follows that the series

$$\sum_{p} \frac{\log(p)}{p^s}$$

converges absolutely. By the limit comparison test, the series

$$\sum_{p} \frac{\log(p)}{p^s - 1} = \sum_{p} \sum_{k=1}^{\infty} \frac{\log(p)}{p^{ks}} = \sum_{p} \sum_{k=1}^{\infty} \frac{\Lambda(p^k)}{p^{ks}} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

also converges absolutely. We have thus proved the second equality of (4.1.5). Next, by Theorem 2.6.2, we have

$$\log = \Lambda * 1,$$

so since

$$-\zeta'(s) = \sum_{n=1}^{\infty} \frac{\log(n)}{n^s} = D(\log, s),$$

it follows from Theorem 3.2.3 that

$$D(\Lambda, s)\zeta(s) = -\zeta'(s),$$

proving the first equality of (4.1.5). □

4.2 Analytic Continuation of $\zeta(s)$ to $\mathrm{Re}(s) > 0$

Theorem 4.2.1. *The function*

$$\zeta(s) - \frac{1}{s-1},$$

defined a priori for $\mathrm{Re}(s) > 1$*, extends to a holomorphic function in the half-plane* $\mathrm{Re}(s) > 0$*. In particular, the residue of* $\zeta(s)$ *at* $s = 1$ *is* 1*.*

Proof. First note that for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$ we have

$$\begin{aligned} \zeta(s) - \frac{1}{s-1} &= \sum_{n=1}^{\infty} \frac{1}{n^s} - \int_1^{\infty} \frac{1}{x^s}\, dx \\ &= \sum_{n=1}^{\infty} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{x^s}\right) dx. \end{aligned} \tag{4.2.1}$$

Let $\varepsilon > 0$ be given, and let K be a compact subset of the half-plane $\mathrm{Re}(s) > \varepsilon$. Define

$$M = \sup_{s \in K} |s|.$$

Then for $s \in K$ we have

$$\begin{aligned} \left| \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{x^s}\right) dx \right| &= \left| s \int_n^{n+1} \int_n^{x} \frac{1}{u^{s+1}}\, du\, dx \right| \\ &\le |s| \int_n^{n+1} \int_n^{n+1} \frac{1}{u^{\mathrm{Re}(s)+1}}\, du\, dx \\ &= |s| \int_n^{n+1} \frac{1}{u^{\mathrm{Re}(s)+1}}\, du \end{aligned}$$

$$\begin{aligned}&\le |s| \max_{n\le u\le n+1} \frac{1}{u^{\mathrm{Re}(s)+1}}\\ &= \frac{|s|}{n^{\mathrm{Re}(s)+1}} \le \frac{M}{n^{\varepsilon+1}}.\end{aligned}$$

It follows that the final series of (4.2.1) converges absolutely and uniformly in compact subsets of the half-plane $\mathrm{Re}(s) > \varepsilon$ for every $\varepsilon > 0$, and hence this series defines a holomorphic function for $\mathrm{Re}(s) > 0$ by Lemma 3.5.1. □

Corollary 4.2.2. *We have*

$$\sum_p \frac{1}{p^s} \sim \log\left(\frac{1}{s-1}\right) \qquad \text{as } s \to 1^+.$$

(Recall that this means that $\lim_{s\to 1^+}\left(\sum_p p^{-s}\right) / \log\left(\frac{1}{s-1}\right) = 1$.*) Moreover, the series*

$$\sum_p \sum_{k=2}^{\infty} \frac{1}{p^{ks}}$$

is bounded as $s \to 1^+$.

Proof. For $s > 1$, the Euler product (4.1.1) of $\zeta(s)$ implies

$$\begin{aligned}\log(\zeta(s)) &= \sum_p \log\left(\frac{1}{1-p^{-s}}\right)\\ &= \sum_p \sum_{k=1}^{\infty} \frac{1}{kp^{ks}} = \sum_p \frac{1}{p^s} + \psi(s),\end{aligned} \tag{4.2.2}$$

where we define

$$\psi(s) = \sum_p \sum_{k=2}^{\infty} \frac{1}{kp^{ks}}.$$

We then have

$$\begin{aligned}\psi(s) &\le \sum_p \sum_{k=2}^{\infty} \frac{1}{p^{ks}} = \sum_p \frac{1}{p^s\left(p^s-1\right)}\\ &\le \sum_p \frac{1}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1.\end{aligned}$$

Therefore $\psi(s)$ is bounded for $s > 1$. By Theorem 4.2.1, we know that

$$\zeta(s) \sim \frac{1}{s-1} \qquad \text{as } s \to 1,$$

so that

$$\log(\zeta(s)) \sim \log\left(\frac{1}{s-1}\right) \qquad \text{as } s \to 1^+.$$

Now (4.2.2) implies that

$$\sum_p \frac{1}{p^s} \sim \log\left(\frac{1}{s-1}\right) \qquad \text{as } s \to 1^+.$$

since $\psi(s)$ is bounded. □

Lemma 4.2.3. *For all $s \neq 1$ with $\operatorname{Re}(s) > 0$ we have*

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

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

Proof. If $F(x)$ denotes

$$F(x) = \sum_{1 \leq n \leq x} 1$$

for $x \geq 1$, then $F(x) = [x] = x - \{x\}$, where $[x]$ is the greatest integer less than or equal to x. Then $F(x) = O(x)$, so by Lemma 3.5.4 we have

$$\begin{aligned} \zeta(s) &= s\int_1^\infty \frac{x - \{x\}}{x^{s+1}}\,dx \\ &= \frac{s}{s+1} - s\int_1^\infty \frac{\{x\}}{x^{s+1}}\,dx \end{aligned} \tag{4.2.3}$$

for $\operatorname{Re}(s) > 1$. The bottom expression of (4.2.3) is analytic for $\operatorname{Re}(s) > 0$ (away from $s = 1$) and it agrees with ζ for $\operatorname{Re}(s) > 1$, so it must agree with ζ for $\operatorname{Re}(s) > 0$ and $s \neq 1$. □

Lemma 4.2.4. *If $\operatorname{Re}(s) > 0$ and $s \neq 1$, then we have*

$$\left(1 - \frac{1}{2^{s-1}}\right)\zeta(s) = -\sum_{n=1}^\infty \frac{(-1)^n}{n^s}. \tag{4.2.4}$$

Proof. For $\mathrm{Re}(s) > 1$, the absolute convergence of the Dirichlet series $\zeta(s)$ lets us write

$$\begin{aligned}\left(1 - \frac{1}{2^{s-1}}\right)\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{\infty} \frac{2}{(2n)^s} \\ &= \sum_{2\nmid n} \frac{1}{n^s} + \sum_{2\mid n} \left(\frac{1}{n^s} - \frac{2}{n^s}\right) \\ &= -\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}.\end{aligned}$$

Thus we have proved (4.2.4) for $\mathrm{Re}(s) > 1$. Note that the right-hand Dirichlet series in (4.2.4) converges (not necessarily absolutely) for $\mathrm{Re}(s) > 0$ by the alternating series test, so (4.2.4) must hold for all $s \neq 1$ with $\mathrm{Re}(s) > 0$. □

Definition 4.2.5. Write the Laurent expansion of ζ at $s = 1$ as

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=0}^{\infty} A_n (s-1)^n.$$

Then for each nonnegative integer n, the nth *Stieltjes constant* is

$$\gamma_n = (-1)^n n! A_n.$$

The number $\gamma = \gamma_0$ is called the *Euler-Mascheroni constant.*

That is, for s in some sufficiently small punctured neighborhood of 1, we have

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \frac{(-1)^n \gamma_n}{n!} (s-1)^n.$$

Lemma 4.2.6. *We have*

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

Proof. By Lemma 4.2.3, we have

$$\begin{aligned}\zeta(s) &= \frac{s}{s-1} + s\int_1^{\infty} \frac{[x]-x}{x^{s+1}}\,dx \\ &= \frac{1}{s-1} + 1 + s\int_1^{\infty} \frac{[x]-x}{x^{s+1}}\,dx\end{aligned}$$

for $\mathrm{Re}(s) > 0$. Therefore

$$\begin{aligned}
\gamma &= \lim_{s\to 1}\left(\zeta(s) - \frac{1}{s-1}\right) \\
&= 1 + \int_1^\infty \frac{[x]-x}{x^2}\,dx \\
&= \lim_{n\to\infty}\left(1 + \sum_{k=1}^{n-1}\int_k^{k+1}\frac{k-x}{x^2}\,dx\right) \\
&= \lim_{n\to\infty}\left(1 + \sum_{k=1}^{n-1}\left(1 - \frac{k}{k+1} + \log(k) - \log(k+1)\right)\right) \\
&= \lim_{n\to\infty}\left(1 + \sum_{k=1}^{n-1}\left(1 - \frac{k}{k+1}\right) - \log(n)\right) \\
&= \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \log(n)\right).
\end{aligned}$$

□

4.3 A Zero-Free Region of $\zeta(s)$

In this section we will prove the following theorem, which will help us in proving the prime number theorem in §4.5.

Theorem 4.3.1. *If* $\mathrm{Re}(s) \geq 1$ *and* $s \neq 1$, *then* $\zeta(s) \neq 0$.

Proof. We know that $\zeta(s) \neq 0$ when $\mathrm{Re}(s) > 1$ from the convergence of the Euler product (4.1.1) of $\zeta(s)$, so it suffices to prove that $\zeta(s) \neq 0$ when $\mathrm{Re}(s) = 1$ and $s \neq 1$. For any $t \in \mathbf{R}$ we have

$$\begin{aligned}
3 + 4\cos(t) + \cos(2t) &= 2 + 4\cos(t) + 2\cos(t)^2 \\
&= 2(1+\cos(t))^2 \geq 0.
\end{aligned} \tag{4.3.1}$$

Next, for $\sigma, t \in \mathbf{R}$ with $\sigma > 1$ we use the Euler product of $\zeta(s)$ to get

$$\begin{aligned}
\log|\zeta(\sigma+it)| &= \mathrm{Re}(\log(\zeta(\sigma+it)) \\
&= \mathrm{Re}\left(-\sum_p \log\left(1 - \frac{1}{p^{\sigma+it}}\right)\right)
\end{aligned}$$

$$= \mathrm{Re}\left(\sum_p \sum_{n=1}^{\infty} \frac{1}{np^{n(\sigma+it)}}\right)$$

$$= \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{n\sigma}} \cos(t\log(n)),$$

so that by (4.3.1) we have

$$\begin{aligned} &\log\left|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)\right| \\ &= \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{n\sigma}} \left(3 + 4\cos(t\log(n)) + \cos(2t\log(n))\right) \geq 0. \end{aligned} \tag{4.3.2}$$

Applying the exponential function and dividing by $\sigma - 1$ in (4.3.2), it follows that

$$((\sigma-1)\zeta(\sigma))^3 \left|\frac{\zeta(\sigma+it)}{\sigma-1}\right|^4 |\zeta(\sigma+2it)| \geq \frac{1}{\sigma-1}. \tag{4.3.3}$$

From Theorem 4.2.1 we know that the residue of $\zeta(s)$ at the simple pole $s = 1$ is 1, so

$$\lim_{\sigma\to 1}(\sigma-1)\zeta(\sigma) = 1. \tag{4.3.4}$$

Now assume $t \in \mathbf{R}^\times$ and $\zeta(1+it) = 0$. Then

$$\lim_{\sigma\to 1} \frac{\zeta(\sigma+it)}{\sigma-1} = \zeta'(1+it).$$

Thus taking the limit as $\sigma \to 1$ in (4.3.3) and using (4.3.4), we get

$$(\zeta'(1+it))^4 \lim_{\sigma\to 1} |\zeta(\sigma+2it)| \geq \lim_{\sigma\to\infty} \frac{1}{\sigma-1} = \infty.$$

It follows that

$$\lim_{\sigma\to 1} |\zeta(\sigma+2it)| = \infty,$$

and so $1 + 2it$ is a pole of ζ, contradicting Theorem 4.2.1 since $t \neq 0$. Thus $\zeta(1+it) \neq 0$. □

4.4 An Analytic Theorem

This section is devoted to the following theorem, which will be crucial to our proof of the prime number theorem in §4.5.

Theorem 4.4.1. *Let $f : \mathbf{R}_{\geq 0} \to \mathbf{C}$ be a bounded and locally integrable function such that the function*

$$g(z) = \int_0^\infty f(t)e^{-zt}\,dt,$$

defined for $\operatorname{Re}(z) > 0$, *extends to a holomorphic function for* $\operatorname{Re}(z) \geq 0$. *Then* $g(0) = \int_0^\infty f(t)\,dt$.

Proof. First, fix an $M > 0$ such that

$$|f(x)| \leq M$$

for all $x \geq 0$. For each $T > 0$, define $g_T : \mathbf{C} \to \mathbf{C}$ by

$$g_T(z) = \int_0^T f(t)e^{-zt}\,dt.$$

By differentiating under the integral sign, we see that each g_T is an entire function.

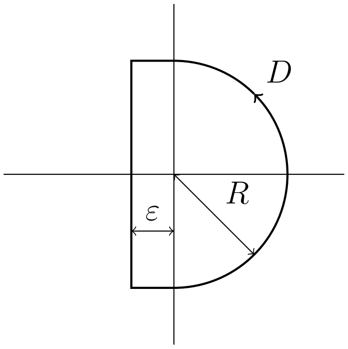
For $T > 0$ and $R > 0$, the function

$$(g(z) - g_T(z))\,e^{zT}\left(\frac{1}{z} + \frac{1}{R^2}\right) \tag{4.4.1}$$

is analytic for $\operatorname{Re}(z) \geq 0$ and $z \neq 0$ with a simple pole at $z = 0$ with residue $g(0) - g_T(0)$. Moreover, a simple calculation shows that, on the circle $|z| = R$, the rightmost factor in the right-hand side of (4.4.1) becomes

$$\left(\frac{1}{z} + \frac{1}{R^2}\right) = \frac{2\operatorname{Re}(z)}{R^2} \tag{4.4.2}$$

Having fixed $R > 0$, there exists an $\varepsilon \in (0, 1)$ such that g is analytic in the region of all $z \in \mathbf{C}$ satisfying $\operatorname{Re}(z) > \varepsilon$, $|\operatorname{Im}(z)| < R$. Let D be the following contour in $\mathbf{C}$:



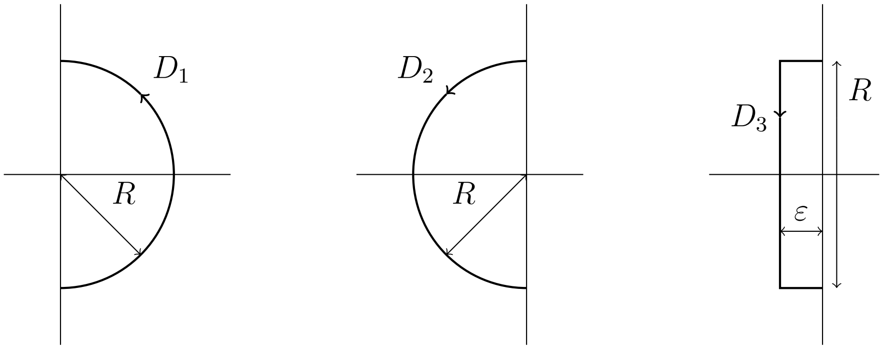
Now define

$$I = \int_D (g(z) - g_T(z))\, e^{zT} \left(\frac{1}{z} + \frac{1}{R^2} \right) dz,$$

so that, by the residue theorem, we have

$$I = 2\pi i (g(0) - g_T(0)) \tag{4.4.3}$$

We also define the following contours:



Finally, we define three integrals:

$$\begin{aligned} I_1 &= \int_{D_1} (g(z) - g_T(z))\, e^{zT} \left(\frac{1}{z} + \frac{1}{R^2} \right) dz \\ I_2 &= \int_{D_2} g_T(z) e^{zT} \left(\frac{1}{z} + \frac{1}{R^2} \right) dz \\ I_3 &= \int_{D_3} g(z) e^{zT} \left(\frac{1}{z} + \frac{1}{R^2} \right) dz \end{aligned}$$

Then by the residue theorem and (4.4.3) we have

$$I_1 - I_2 + I_3 = 2\pi i g(0) - 2\pi i g_T(0) = I. \tag{4.4.4}$$

Now for $z \in \mathbf{C}$ with $\mathrm{Re}(z) > 0$ we have

$$\begin{aligned} |g(z) - g_T(z)| &= \left| \int_T^\infty f(t) e^{-zt}\, dt \right| \\ &\leq M \int_T^\infty e^{-\mathrm{Re}(z) t}\, dt = M \frac{e^{-\mathrm{Re}(z) T}}{\mathrm{Re}(z)}. \end{aligned}$$

It follows from (4.4.2) that

$$|I_1| \leq \pi R \sup_{z \in D_1} \left(M \frac{e^{-\operatorname{Re}(z)T}}{\operatorname{Re}(z)} e^{\operatorname{Re}(z)T} \frac{2\operatorname{Re}(z)}{R^2} \right) = \frac{2\pi M}{R} \tag{4.4.5}$$

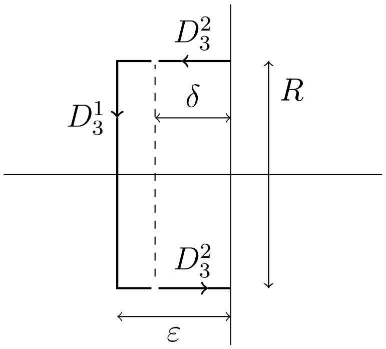
Next, for $z \in \mathbf{C}$ with $\operatorname{Re}(z) < 0$ we have

$$|g_T(z)| \leq M \int_0^T e^{-\operatorname{Re}(z)t}\, dt = \frac{e^{-\operatorname{Re}(z)T} - 1}{|\operatorname{Re}(z)|} \leq \frac{e^{-\operatorname{Re}(z)T}}{|\operatorname{Re}(z)|},$$

so from (4.4.2) it follows that

$$|I_2| \leq \pi R \sup_{z \in D_2} \left(M \frac{e^{-\operatorname{Re}(z)T}}{|\operatorname{Re}(z)|} e^{\operatorname{Re}(z)T} \frac{2|\operatorname{Re}(z)|}{R^2} \right) = \frac{2\pi M}{R}. \tag{4.4.6}$$

Thus we have bounded I_1 and I_2. We now proceed to bound I_3. Pick a δ between 0 and ε, and consider the following pair of contours in $\mathbf{C}$:



so that $D_3 = D_3^1 \cup D_3^2$. The function $g(z)\left(\frac{1}{z} + \frac{1}{R^2}\right)$ is analytic on D_3, so it is bounded in absolute value by some constant $C > 0$. Therefore we have

$$\begin{aligned} |I_3| &\leq \left| \int_{D_3^1} g(z) e^{zT} \left(\frac{1}{z} + \frac{1}{R^2} \right) dz \right| + \left| \int_{D_3^2} g(z) e^{zT} \left(\frac{1}{z} + \frac{1}{R^2} \right) dz \right| \\ &\leq (2\varepsilon - 2\delta + R) C e^{-\delta T} + 2\delta C \\ &\leq C(2 + R) C e^{-\delta T} + 2\delta C \end{aligned}$$

As $T \to \infty$, we have

$$0 \leq \liminf_{T \to \infty} |I_3| \leq \limsup_{T \to \infty} |I_3| \leq 2\delta C,$$

and taking the limit $\delta \to 0^+$, we get

$$\lim_{T\to\infty} |I_3| = 0 \tag{4.4.7}$$

Now we can finish the proof. From (4.4.3) and (4.4.4) we get that

$$|g(0) - g_T(0)| = \left|\frac{I}{2\pi i}\right| \leq |I_1| + |I_2| + |I_3|.$$

As $T \to \infty$, we get from (4.4.5), (4.4.6), and (4.4.7) that

$$0 \leq \liminf_{T\to\infty} |g(0) - g_T(0)| \leq \limsup_{T\to\infty} |g(0) - g_T(0)| \leq \frac{4\pi M}{R}.$$

Letting $R \to \infty$, we get

$$\lim_{T\to\infty} |g(0) - g_T(0)| = 0,$$

so we conclude that

$$g(0) = \lim_{T\to\infty} g_T(0) = \int_0^\infty f(t)\,dt. \qquad \square$$

4.5 The Prime Number Theorem

The proof of the prime number theorem given here is based heavily on Zagier's modification of Newman's 1980 proof (cf. [New80], [Zag97]). We rely on complex analysis instead of elementary methods, and our main tool will be Theorem 4.4.1 of §4.4.

Recall the definition of the prime-counting function $\pi(x)$ from Definition 2.8.4:

$$\pi(x) = \sum_{p\leq x} 1$$

for $x \in \mathbf{R}$. We already know from Euclid's Theorem 1.2.1 that

$$\pi(x) \to \infty \qquad \text{as } x \to \infty,$$

but we would like to know more about the asymptotic behavior of $\pi(x)$. The goal of this section is to prove the *prime number theorem*:

$$\pi(x) \sim \frac{x}{\log(x)} \qquad \text{as } x \to \infty. \tag{4.5.1}$$

That is, we want to prove that

$$\lim_{x\to\infty} \frac{\pi(x)\log(x)}{x} = 1.$$

We will prove (4.5.1) in Theorem 4.5.7 at the end of this section. Before that, we need several definitions and lemmas.

Definition 4.5.1. For $x \in \mathbf{R}$, we define

$$\vartheta(x) = \sum_{p\le x} \log(p),$$

where p ranges over the positive prime numbers less than or equal to x.

Lemma 4.5.2. *For $x \geq 2$, we have*

$$\vartheta(x) \le 2x\log(4).$$

In particular,

$$\vartheta(x) = O(x) \qquad \text{as } x \to \infty.$$

Proof. For any positive integer n we have

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k}$$

by the binomial theorem. Therefore

$$4^n \ge \binom{2n}{n} \ge \prod_{\substack{n<p\le 2n\\ p \text{ prime}}} p = e^{\vartheta(2n)-\vartheta(n)},$$

and so

$$\vartheta(2n) - \vartheta(n) \le n\log(4). \tag{4.5.2}$$

For any $k \in \mathbf{Z}_+$, repeated application of (4.5.2) gives

$$\vartheta(2^{k+1}) = \sum_{i=0}^{k} \big(\vartheta(2^{i+1}) - \vartheta(2^i)\big) \le \log(4)\sum_{i=0}^{k} 2^i \le 2^{k+1}\log(4). \tag{4.5.3}$$

Now if $x \geq 2$, there exists a $k \in \mathbf{Z}_+$ such that

$$2^k \le x < 2^{k+1} \le 2x,$$

and so by (4.5.3) we have

$$\vartheta(x) \le \vartheta(2^{k+1}) \le 2^{k+1}\log(4) \le 2x\log(4). \qquad \square$$

Definition 4.5.3. For $s \in \mathbf{C}$, we define

$$\Phi(s) = \sum_p \frac{\log(p)}{p^s},$$

wherever this series, taken over all prime numbers, converges.

Lemma 4.5.4. *The function* $\Phi(s)$ *converges for* $\operatorname{Re}(s) > 1$*, and*

$$\Phi(s) - \frac{1}{s-1}$$

extends to a holomorphic function for $\operatorname{Re}(s) \geq 1$*.*

Proof. From Lemma 4.1.4 it follows that

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log(p)}{p^s - 1} = \Phi(s) + \sum_p \frac{\log(p)}{p^s(p^s-1)}, \tag{4.5.4}$$

which shows the convergence of $\Phi(s)$ for $\operatorname{Re}(s) > 1$. Moreover, from (4.5.4) we now have

$$\Phi(s) = -\frac{\zeta'(s)}{\zeta(s)} - \sum_p \frac{\log(p)}{p^s(p^s-1)}, \tag{4.5.5}$$

and the series here converges absolutely for $\operatorname{Re}(s) > \frac{1}{2}$. Thus (4.5.5) gives a meromorphic extension of Φ to $\operatorname{Re}(s) > \frac{1}{2}$, with poles at 1 and at the zeros of $\zeta(s)$ in the strip $\frac{1}{2} < \operatorname{Re}(s) \leq 1$. Since $\zeta(s)$ has no zeros on the line $\operatorname{Re}(s) = 1$ by Theorem 4.3.1, it follows that $\Phi(s) - \frac{1}{s-1}$ is holomorphic for $\operatorname{Re}(s) \geq 1$. □

Lemma 4.5.5. *The integral*

$$\int_1^\infty \frac{\vartheta(x) - x}{x^2}\, dx$$

converges.

Proof. Let $f : \mathbf{R}_{\geq 0} \to \mathbf{C}$ be the function given by

$$f(t) = \frac{\vartheta(e^t)}{e^t} - 1.$$

Lemma 4.5.2 implies that there exists a $C > 0$ such that for t sufficiently large we have

$$f(t) = \frac{\vartheta(e^t)}{e^t} - 1 \leq C - 1.$$

Thus f is a bounded function, and it is clearly locally integrable.

Next, let $g(s)$ denote the integral

$$g(s) = \int_0^\infty f(t)e^{-st}\,dt$$

for all $s \in \mathbf{C}$ where this makes sense. We note that for all $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$ we can use integration by parts to obtain the formula

$$\begin{aligned}\Phi(s) &= \sum_p \frac{\log p}{p^s} = \int_1^\infty \frac{1}{x^s}\,d\vartheta(x) \\ &= \lim_{x\to\infty} \frac{\vartheta(x)}{x^s} + s\int_1^\infty \frac{\vartheta(x)}{x^{s+1}}\,dx.\end{aligned} \tag{4.5.6}$$

The limit in (4.5.6) is zero since

$$\lim_{x\to\infty}\left|\frac{\vartheta(x)}{x^s}\right| \le \lim_{x\to\infty}\frac{C}{x^{\mathrm{Re}(s)-1}} = 0.$$

Thus (4.5.6) implies that

$$\frac{\Phi(s)}{s} = \int_1^\infty \frac{\vartheta(x)}{x^{s+1}}\,dx, = \int_0^\infty \vartheta(e^t)e^{-st}\,dt$$

after we make the change of variables $x = e^t$. Since $1/s = \int_0^\infty e^{-st}\,dt$, it follows that

$$\frac{\Phi(s+1)}{s+1} - \frac{1}{s} = \int_0^\infty \left(\frac{\vartheta(e^t)}{e^t} - 1\right)e^{-st}\,dt = g(s). \tag{4.5.7}$$

By Lemma 4.5.4, $\Phi(s+1)$ is holomorphic for $\mathrm{Re}(s) \ge 0$ except for a simple pole at $s = 0$ with residue 1. Therefore the function $\Phi(s+1)/(s+1)$ has a simple pole at $s = 0$ with residue

$$\lim_{s\to 0} s\frac{\Phi(s+1)}{s+1} = \frac{\lim_{s\to 0} s\Phi(s+1)}{\lim_{s\to 0}(s+1)} = 1.$$

Thus (4.5.7) shows that $g(s)$ is holomorphic for $\mathrm{Re}(s) \ge 0$. We now apply the analytic theorem of §4.4 (Theorem 4.4.1) to conclude that the integral

$$g(0) = \int_0^\infty f(t)\,dt = \int_0^\infty \left(\frac{\vartheta(e^t)}{e^t} - 1\right)dt = \int_1^\infty \frac{\vartheta(x) - x}{x^2}\,dx$$

converges, proving the lemma. □

Lemma 4.5.6. *$\vartheta(x) \sim x$ as $x \to \infty$.*

Recall that this means that $\lim_{x\to\infty} \vartheta(x)/x = 1$.

Proof. First suppose that there is a $\lambda > 1$ such that

$$\vartheta(x) \geq \lambda x$$

for all x sufficiently large. We would then have

$$\int_x^{\lambda x} \frac{\vartheta(t) - t}{t^2}\, dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt = \int_1^{\lambda} \frac{\lambda - u}{u^2}\, du > 0$$

for sufficiently large x, contradicting Lemma 4.5.5. Next, suppose that there is a $\lambda < 1$ such that

$$\vartheta(x) \leq \lambda x$$

for all x sufficiently large. We would then have

$$\int_{\lambda x}^{x} \frac{\vartheta(t) - t}{t^2}\, dt \leq \int_{\lambda x}^{x} \frac{\lambda x - t}{t^2}\, dt = \int_{\lambda}^{1} \frac{\lambda - u}{u^2}\, du < 0$$

for sufficiently large x, again contradicting Lemma 4.5.5. Thus it must be the case that $\vartheta(x)/x \to 1$ as $x \to \infty$, and so the lemma is proved. □

Theorem 4.5.7 (The Prime Number Theorem)**.**

$$\pi(x) \sim \frac{x}{\log(x)} \qquad \text{as } x \to \infty.$$

Proof. First, note that

$$\vartheta(x) = \sum_{p \leq x} \log(p) \leq \pi(x)\log(x) \tag{4.5.8}$$

for $x > 0$. Next, for a fixed $\varepsilon > 0$ we have

$$\vartheta(x) \geq \sum_{x^{1-\varepsilon} < p \leq x} \log(p) \geq (\pi(x) - \pi(x^{1-\varepsilon}))\log(x^{1-\varepsilon}) \tag{4.5.9}$$

Combining (4.5.8) and (4.5.9), we get

$$\frac{\vartheta(x)}{x} \leq \frac{\pi(x)\log(x)}{x} \leq \frac{1}{1-\varepsilon}\frac{\vartheta(x)}{x} + \frac{\log(x)}{x^{\varepsilon}}.$$

By Lemma 4.5.6, it follows that

$$1 \leq \liminf_{x\to\infty} \frac{\pi(x)\log(x)}{x} \leq \limsup_{x\to\infty} \frac{\pi(x)\log(x)}{x} \leq \frac{1}{1-\varepsilon},$$

and since this holds for arbitrary $\varepsilon > 0$, it follows that

$$\lim_{x\to\infty} \frac{\pi(x)\log(x)}{x} = 1,$$

which proves the prime number theorem. □

4.6 The Functional Equation of $\zeta(s)$

This section relies heavily on facts about the gamma function and the Fourier transform. See §A.2 and §B.3, respectively, for an overview of these topics.

Lemma 4.6.1. *Let $h : \mathbf{R} \to \mathbf{C}$ be the function defined by*

$$h(x) = e^{-\pi x^2}.$$

Then h is its own Fourier transform: $\widehat{h} = h$.

Proof. Note that

$$\frac{dh(x)}{dx} = -2\pi x h(x).$$

Applying the Fourier transform to both sides and using Lemmas B.3.2 and B.3.3, we get the differential equation

$$\frac{d\widehat{h}(y)}{dy} + 2\pi y\widehat{h}(y) = 0,$$

whence

$$\widehat{h}(y) = ce^{-\pi y^2}$$

for some $c \in \mathbf{R}$. We have

$$c = \widehat{h}(0) = \int_{\mathbf{R}} e^{-\pi x^2}\, dx = 1,$$

and hence $\widehat{h} = h$. □

Lemma 4.6.2. *Let $g \in L^1(\mathbf{R})$, $r \in \mathbf{R}$, and $s > 0$ be given. If $g_{r,s}$ denotes the function*

$$g_{r,s}(x) = g(rs + sx),$$

then we have

$$\widehat{g_{r,s}}(y) = s^{-1} e^{2\pi i r y} \widehat{g}(s^{-1} y).$$

Proof. A simple substitution shows that

$$\begin{aligned} \widehat{g_{r,s}}(y) &= \int_{\mathbf{R}} g(rs + sx) e^{-2\pi i x y}\, dx \\ &= s^{-1} \int_{\mathbf{R}} g(u) e^{-2\pi i (u - rs) s^{-1} y}\, du \\ &= s^{-1} e^{2\pi i r y} \int_{\mathbf{R}} g(u) e^{-2\pi i u s^{-1} y}\, du \\ &= s^{-1} e^{2\pi i r y} \widehat{g}(s^{-1} y). \end{aligned}$$

□

Lemma 4.6.3. *For all $a \in \mathbf{R}$ and $t > 0$ we have*

$$\sum_{n \in \mathbf{Z}} e^{-\pi (n+a)^2 / t} = t^{1/2} \sum_{n \in \mathbf{Z}} e^{-\pi n^2 t + 2\pi i n a}.$$

Proof. The function $h(x) = e^{-\pi x^2}$ is its own Fourier transform by Lemma 4.6.1. Fix an $a \in \mathbf{R}$ and a $t > 0$, and let g be the function

$$g(x) = h(a t^{-1/2} + t^{-1/2} x) = e^{-\pi (a + x)^2 / t}.$$

By Lemma 4.6.2 we have

$$\widehat{g}(y) = t^{1/2} e^{2\pi i a y} \widehat{h}(t^{1/2} y) = t^{1/2} e^{2\pi i a y - \pi y^2 t}. \tag{4.6.1}$$

The Poisson summation formula (Theorem B.3.5) and (4.6.1) then give

$$\sum_{n \in \mathbf{Z}} e^{-\pi (n+a)^2 / t} = \sum_{n \in \mathbf{Z}} g(n) = \sum_{n \in \mathbf{Z}} \widehat{g}(n) = t^{1/2} \sum_{n \in \mathbf{Z}} e^{-\pi n^2 t + 2\pi i n a}.$$

□

Definition 4.6.4. For $t > 0$, we define

$$\theta(t) = \sum_{n \in \mathbf{Z}} e^{-\pi n^2 t}, \qquad \omega(t) = \sum_{n=1}^{\infty} e^{-\pi n^2 t} = \frac{\theta(t) - 1}{2}.$$

Lemma 4.6.5. *As $t \to \infty$, we have*

$$\theta(t) = O(e^{-\pi t}), \qquad \omega(t) = O(e^{-\pi t}).$$

Proof. For $t \geq 1$, we have

$$\begin{aligned}\theta(t) &\leq \sum_{n \in \mathbf{Z}} e^{-\pi n^2 t} \\ &= e^{-\pi t} \sum_{n \in \mathbf{Z}} e^{-\pi (n^2-1)t} \\ &\leq e^{-\pi t} \sum_{n \in \mathbf{Z}} e^{-\pi (n^2-1)}.\end{aligned}$$

This proves that $\theta(t) = O(e^{-\pi t})$. Since $\omega(t) \leq \theta(t)$, it also follows that $\omega(t) = O(e^{-\pi t})$. □

Lemma 4.6.6. *For all $t > 0$, we have*

$$\theta(t^{-1}) = t^{1/2}\theta(t) \tag{4.6.2}$$

and

$$\omega(t^{-1}) = -\frac{1}{2} + \frac{t^{1/2}}{2} + t^{1/2}\omega(t). \tag{4.6.3}$$

Proof. Setting $a = 0$ in Lemma 4.6.3 immediately gives us (4.6.2). Moreover, since

$$\omega(t) = \frac{\theta(t) - 1}{2} \qquad \text{and} \qquad \theta(t) = 1 + 2\omega(t),$$

we use (4.6.2) to get

$$\begin{aligned}\omega(t^{-1}) &= \frac{\theta(t^{-1}) - 1}{2} = \frac{t^{1/2}\theta(t) - 1}{2} \\ &= \frac{t^{1/2}(1 + 2\omega(t)) - 1}{2} = -\frac{1}{2} + \frac{t^{1/2}}{2} + t^{1/2}\omega(t),\end{aligned}$$

proving (4.6.3). □

Definition 4.6.7. We define

$$\xi(s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \left(t^{s/2} + t^{(1-s)/2}\right) \omega(t) \, \frac{dt}{t}, \tag{4.6.4}$$

for all $s \in \mathbf{C}$ where this makes sense.

Lemma 4.6.8. *The function $\xi(s)$ is meromorphic on $\mathbf{C}$, with only simple poles at $s = 0$ and $s = 1$, with residues -1 and 1, respectively. Morevoer, we have the functional equation*

$$\xi(s) = \xi(1-s) \tag{4.6.5}$$

for all s different from $s = 0$ and $s = 1$.

Proof. The integral defining $\xi(s)$ in (4.6.4) is absolutely and uniformly convergent on compact subsets of $\mathbf{C}$ since $\omega(t) = O(e^{-\pi t})$ as $t \to \infty$ by Lemma 4.6.5. Therefore this integral defines an entire function, and from the definition of $\xi(s)$ we conclude that $\xi(s)$ is analytic everywhere except $s = 0$ and $s = 1$, with poles -1 and 1, respectively. Finally, the functional equation (4.6.5) follows from the simple observation that (4.6.4) is invariant under the change of variables $s \mapsto 1-s$. □

Theorem 4.6.9. *For all $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$, we have*

$$\xi(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s). \tag{4.6.6}$$

The right-hand side of (4.6.6) extends to a meromorphic function on $\mathbf{C}$ with only simple poles at $s = 0$ and $s = 1$, with residues -1 and 1, respectively, and we have

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) \tag{4.6.7}$$

for all $s \in \mathbf{C}$ different from 0 and 1.

Proof. Fix a positive integer n, and note that

$$\begin{aligned}\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)n^{-s} &= \pi^{-s/2}n^{-s}\int_0^\infty x^{s/2}e^{-x}\,\frac{dx}{x}\\ &= \int_0^\infty t^{s/2}e^{-\pi n^2 t}\,\frac{dt}{t}\end{aligned}$$

after a change of variables. Summing over all positive n, we get

$$\begin{aligned}\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \sum_{n=1}^\infty\int_0^\infty t^{s/2}e^{-\pi n^2 t}\,\frac{dt}{t}\\ &= \int_0^\infty t^{s/2}\omega(t)\,\frac{dt}{t}.\end{aligned} \tag{4.6.8}$$

The interchange of integral and summation in (4.6.8) is justified by the absolute convergence of the the final integral (since $\omega(t) = O(e^{-\pi t})$ by Lemma 4.6.5). The functional equation for ω (4.6.3) now give

$$\begin{aligned}
\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \int_0^1 t^{s/2}\omega(t)\,\frac{dt}{t} + \int_1^\infty t^{s/2}\omega(t)\,\frac{dt}{t} \\
&= \int_1^\infty t^{-s/2}\omega(t^{-1})\,\frac{dt}{t} + \int_1^\infty t^{s/2}\omega(t)\,\frac{dt}{t} \\
&= \int_1^\infty \left(\frac{t^{(1-s)/2}}{2} - \frac{t^{-s/2}}{2} + \left(t^{s/2} + t^{(1-s)/2}\right)\omega(t)\right)\frac{dt}{t} \\
&= \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \left(t^{s/2} + t^{(1-s)/2}\right)\omega(t)\,\frac{dt}{t} = \xi(s).
\end{aligned}$$

This proves that (4.6.6) holds. The remaining assertions of this theorem are immediate consequences of Lemma 4.6.8. □

Corollary 4.6.10. *The Riemann zeta function $\zeta(s)$ extends to a meromorphic function for all $s \in \mathbf{C}$ with only a simple pole at $s = 1$.*

Proof. Theorem 4.6.9 implies that $\zeta(s)$ has a meromorphic continuation to $\mathbf{C}$. We already know that $\zeta(s)$ has a simple pole at $s = 1$ by Theorem 4.2.1. From the facts that $\Gamma(s)$ is non-vanishing and has a simple pole at 0, that $\xi(s)$ only has simple poles at $s = 0$ and $s = 1$ (Lemma 4.6.8), and that

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

for all $s \neq 0, 1$, it follows that $\zeta(s)$ cannot have any other poles. □

Corollary 4.6.11. *We have $\zeta(0) = -1/2$.*

Proof. The gamma function has a simple pole at $s = 0$ with residue 1, so

$$\lim_{s\to 0} s\Gamma\left(\frac{s}{2}\right) = 2\lim_{s\to 0}\frac{s}{2}\Gamma\left(\frac{s}{2}\right) = 2.$$

On the one hand, from Theorem 4.6.9 we get

$$\lim_{s\to 0} s(s-1)\xi(s) = \lim_{s\to 0}(s-1)\pi^{-s/2}s\Gamma\left(\frac{s}{2}\right)\zeta(s) = -2\zeta(0). \tag{4.6.9}$$

On the other hand, by the functional equation (4.6.5) we have

$$\lim_{s\to 0} s(s-1)\xi(s) = \lim_{s\to 1} s(s-1)\xi(1-s)$$

$$\begin{aligned}
&= \lim_{s\to 1} s(s-1)\xi(s) \\
&= \lim_{s\to 1} s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) \\
&= \frac{1}{\sqrt{\pi}}\Gamma\left(\frac{1}{2}\right)\lim_{s\to 1}(s-1)\zeta(s) = 1.
\end{aligned}$$

The last equality holds since $\Gamma(1/2) = \sqrt{\pi}$ and $\zeta(s)$ has a simple pole of residue 1 at $s = 1$. Thus from (4.6.9), we get

$$\zeta(0) = -\frac{1}{2}. \qquad \square$$

Corollary 4.6.12. *For every positive integer n, $\zeta(s)$ has a simple zero at $s = -2n$. Moreover, if $s \in \mathbf{C}$ is a zero of $\zeta(s)$, then either s is a negative even integer, or $0 < \mathrm{Re}(s) < 1$.*

Proof. For every positive integer n, $\Gamma(s)$ has a simple pole at $s = -n$. Since

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

is analytic when $\mathrm{Re}(s) < 0$, it follows that

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

is well-defined, so $\zeta(s)$ must have a simple zero at $s = -2n$.

Next, suppose $s \in \mathbf{C}$ is a zero of $\zeta(s)$ different from a negative even integer. By Corollary 4.6.11, $s \neq 0$, and so s is not a pole of $\Gamma(s/2)$. By Theorem 4.3.1, we know that $\zeta(z) \neq 0$ when $\mathrm{Re}(z) \geq 1$, so $\mathrm{Re}(s) < 1$. Moreover, we have $\xi(s) = 0$, and so $\xi(1-s) = 0$ by the functional equation (4.6.5) of $\xi(s)$. Since the gamma function is never zero, it follows that $\zeta(1-s) = 0$. Now if $\mathrm{Re}(s) \leq 0$, then $\mathrm{Re}(1-s) \geq 1$, contradicting the non-vanishing of $\zeta(z)$ on $\mathrm{Re}(z) \geq 1$. Therefore $\mathrm{Re}(s) > 0$, and so

$$0 < \mathrm{Re}(s) < 1. \qquad \square$$

Definition 4.6.13. The *trivial zeros* of $\zeta(s)$ are the non-negative integers. The *non-trivial zeros* of $\zeta(s)$ are the zeros of $\zeta(s)$ in the strip $0 < \mathrm{Re}(s) < 1$.

Conjecture 4.6.14 (The Riemann Hypothesis)**.** Every non-trivial zero of $\zeta(s)$ lies on the line $\mathrm{Re}(s) = \frac{1}{2}$.

Currently, the Riemann Hypothesis is one of the most important open problems in mathematics. Among other things, the Riemann hypothesis being true would improve the estimate of the prime-counting function $\pi(x)$ of §4.5 given by the prime number theorem. Recall that the prime number theorem (Theorem 4.5.7) stated that

$$\pi(x) \sim \frac{x}{\log(x)} \qquad \text{as } x \to \infty.$$

In [Sch76], Schoenfeld proved that, if the Riemann hypothesis were true, then the stronger statement

$$|\pi(x) - \mathrm{li}(x)| < \frac{1}{8\pi}\sqrt{x}\log(x) \qquad \text{for all } x \geq 2657$$

would hold, where

$$\mathrm{li}(x) = \lim_{\varepsilon \to 0^+} \left(\int_0^{1-\varepsilon} \frac{1}{\log(t)}\,dt + \int_{1+\varepsilon}^{x} \frac{1}{\log(t)}\,dt \right)$$

for $x > 1$.

5 Dirichlet L-Functions

5.1 Dirichlet Characters, Dirichlet L-Functions

Definition 5.1.1. Let m be a positive integer. A character of the multiplicative group $(\mathbf{Z}/m\mathbf{Z})^\times$ is called a *Dirichlet character modulo m.*

The trivial character of $(\mathbf{Z}/m\mathbf{Z})^\times$ will be denoted $\mathbf{1}_m$.

If χ is a Dirichlet character modulo m, then it is useful to extend χ to all of $\mathbf{Z}/m\mathbf{Z}$ by setting

$$\chi(n) = 0$$

if $(n, m) > 1$. Moreover, it is useful to extend χ to all of $\mathbf{Z}$ by defining (via abuse of notation) $\chi(n) = \chi(\overline{n})$, where $\overline{n}$ is the residue class of n modulo m. Viewed as functions $\mathbf{Z} \to \mathbf{C}$, the Dirichlet characters modulo q are precisely those functions χ satisfying

(1) $\chi(n + m) = \chi(n)$ for every $n \in \mathbf{Z}$;

(2) $\chi(n) = 0$ if $(n, m) > 1$, and $|\chi(n)| = 1$ if $(n, m) = 1$;

(3) $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$ for all $n_1, n_2 \in \mathbf{Z}$.
If $d \mid m$, then there is a natural surjective homomorphism

$$\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}.$$

Thus for any Dirichlet character modulo d we obtain the *induced* Dirichlet character modulo m via composition with this homomorphism.

Definition 5.1.2. A Dirichlet character modulo m is called *primitive* if it is not induced by any Dirichlet character modulo d for any divisor $d \neq m$ of m. A Dirichlet character χ is called *odd* if $\chi(-1) = -1$, and it is called *even* if $\chi(-1) = 1$.

Definition 5.1.3. For a Dirichlet character χ modulo m, viewed as a function $\chi : \mathbf{Z}_+ \to \mathbf{C}$, we define the associated *Dirichlet L-function* $L(s, \chi)$ by the Dirichlet series

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

Fix a Dirichlet character χ modulo m. By Theorem 3.5.2, the abscissa of absolute convergence of $L(s, \chi)$ is

$$\sigma_{|\chi|} = \limsup_{n\to\infty} \frac{\log\left(\sum_{k=1}^{n} |\chi(k)|\right)}{\log(n)} \leq \limsup_{n\to\infty} \frac{\log(n)}{\log(n)} = 1.$$

Thus $L(s, \chi)$ is at least absolutely convergent and analytic for $\mathrm{Re}(s) > 1$. Moreover, the absolute convergence of $L(s, \chi)$ and Theorem 3.2.2 imply that for $\mathrm{Re}(s) > 1$, we have the Euler product representation

$$L(s, \chi) = \prod_{p} \frac{1}{1 - \chi(p)p^{-s}} = \prod_{p \nmid m} \frac{1}{1 - \chi(p)p^{-s}}. \tag{5.1.1}$$

In particular, the convergence of the Euler product (5.1.1), whose factors are all nonzero, implies that $L(s, \chi) \neq 0$ for $\mathrm{Re}(s) > 1$.

We note that if $\chi = \mathbf{1}_m$ is the trivial Dirichlet character modulo m, then by (5.1.1) we have

$$L(s, \mathbf{1}_m) = \zeta(s) \prod_{p \mid m} \left(1 - \frac{1}{p^s}\right). \tag{5.1.2}$$

Lemma 5.1.4. *If χ is a nontrivial Dirichlet character modulo m, then $L(s,\chi)$ converges and is analytic for* $\mathrm{Re}(s) > 0$.

Proof. Suppose $\chi \neq \mathbf{1}_m$, and let σ_χ be the abscissa of convergence of $L(s,\chi)$. Note that $L(0,\chi)$ diverges by the periodicity of χ, so $\sigma_\chi \geq 0$. For $n \in \mathbf{Z}_+$, pick the smallest $r \in \mathbf{Z}_+$ such that $n \equiv r \pmod{m}$. Then Lemma C.2.1 (one of the orthogonality relations for characters of finite abelian groups) implies that

$$\sum_{k=1}^{n} \chi(k) = \sum_{k=1}^{r} \chi(k) + \sum_{k=r+1}^{n} \chi(k) = \sum_{k=1}^{r} \chi(k)$$

since the sum $\sum_{k=r+1}^{n} \chi(k)$ cycles over all elements of $\mathbf{Z}/m\mathbf{Z}$. Therefore

$$\left| \sum_{k=1}^{n} \chi(k) \right| \leq \sum_{k=1}^{\phi(m)} 1 = \phi(m),$$

and hence the formula for σ_χ obtained from Theorem 3.5.2 gives

$$0 \leq \sigma_\chi = \limsup_{n\to\infty} \frac{\log |\sum_{k=1}^{n} \chi(k)|}{\log(n)} \leq \limsup_{n\to\infty} \frac{\log(\phi(m))}{\log(n)} = 0.$$

Therefore $\sigma_\chi = 0$, and so $L(s,\chi)$ converges and is analytic for $\mathrm{Re}(s) > 0$. □

5.2 Non-Vanishing of $L(1,\chi)$

In this section we will prove that if χ is a nontrivial Dirichlet character modulo m, then $L(1,\chi) \neq 0$. We closely follow Serre's exposition in [Ser73] in this section and the next one.

Let m denote a fixed positive integer, let $G(m) = (\mathbf{Z}/m\mathbf{Z})^\times$, and for every prime p not dividing m, let $f(p)$ denote the order of the image of p in $G(m)$. Also define

$$g(p) = \frac{\phi(m)}{f(p)},$$

which is equal to the order of the quotient of $G(m)$ by the subgroup generated by the image of p.

Lemma 5.2.1. *Let p be a prime not dividing m. Then in the polynomial ring* $\mathbf{C}[T]$ *we have*

$$\prod_{\chi\in\widehat{G(m)}} (1-\chi(p)T) = \left(1-T^{f(p)}\right)^{g(p)}.$$

Proof. Let W denote the group of $f(p)$-th roots of unity in $\mathbf{C}$. Then we have

$$1 - T^{f(p)} = \prod_{\omega \in W} (1 - \omega T).$$

Moreover, for each $\omega \in W$, there are exactly $g(p)$ Dirichlet characters χ modulo m such that $\chi(p) = \omega$. Therefore the lemma follows. □

Definition 5.2.2. For $\mathrm{Re}(s) > 1$, define

$$\zeta_m(s) = \prod_{\chi \in \widehat{G(m)}} L(s, \chi).$$

Since each $L(s, \chi)$ is analytic for $\mathrm{Re}(s) > 1$, so is $\zeta_m(s)$.

Lemma 5.2.3. *For* $\mathrm{Re}(s) > 1$, *we have*

$$\zeta_m(s) = \prod_{p \nmid m} \frac{1}{(1 - p^{-f(p)s})^{g(p)}}, \tag{5.2.1}$$

and $\zeta_m(s)$ *can be expressed as the Dirichlet series of a positive arithmetic function.*

Proof. The Euler products (5.1.1) of the Dirichlet L-functions together with Lemma 5.2.1 (setting $T = p^{-s}$) immediately give us (5.2.1). Moreover, the product expansion of $\zeta_m(s)$ clearly shows that $\zeta_m(s)$ can be written as the Dirichlet series of a positive arithmetic function. □

Theorem 5.2.4. *Suppose* χ *is a nontrivial Dirichlet character modulo* m. *Then* $L(1, \chi) \neq 0$.

Proof. Suppose that $L(1, \chi) = 0$. Then this zero cancels the simple pole of $L(s, \mathbf{1}_m)$ at $s = 1$, and so $\zeta_m(s)$ is analytic for $\mathrm{Re}(s) > 0$. By Lemma 5.2.3, $\zeta_m(s)$ has a Dirichlet series expansion with positive coefficients. By Theorem 3.5.3, $\zeta_m(s)$ must have a pole at its abscissa of convergence. Since $\zeta_m(s)$ is analytic for $\mathrm{Re}(s) > 0$, it follows that its Dirichlet series converges at least for $\mathrm{Re}(s) > 0$. However, for each prime p not dividing m we have

$$\frac{1}{(1 - p^{-f(p)s})^{g(p)}} = \left(\sum_{n=0}^{\infty} p^{-nf(p)s} \right)^{g(p)} \geq \sum_{n=0}^{\infty} p^{-n\phi(m)s}.$$

Therefore the coefficients of the Dirichlet series $\zeta_m(s)$ are all greater than those of the series

$$\sum_{(n,m)=1} \frac{1}{n^{\phi(m)s}},$$

and this series diverges for $s = 1/\phi(m)$. Therefore, $L(1/\phi(m), \chi)$ must diverge as a Dirichlet series, and so $L(1, \chi) \neq 0$. □

Corollary 5.2.5. *$\zeta_m(s)$ has a simple pole at $s = 1$.*

Proof. By (5.1.2), the L-function $L(s, \mathbf{1}_m)$ has a simple pole at $s = 1$ (since $\zeta(s)$ has a simple pole at $s = 1$ by Theorem 4.2.1). Moreover, if χ is a nontrivial Dirichlet character modulo m, then $L(s, \chi)$ is analytic for $\mathrm{Re}(s) > 0$ by Lemma 5.1.4, and $L(1, \chi) \neq 0$ by Theorem 5.2.4. Therefore, since

$$\zeta_m(s) = \prod_{\chi \in \widehat{G(m)}} L(s, \chi),$$

we see immediately that $\zeta_m(s)$ has a simple pole at $s = 1$. □

5.3 Primes in Arithmetic Progressions

Definition 5.3.1. Let A be any set of prime numbers. We say that A has *density* $\alpha \in \mathbf{R}$ if

$$\lim_{s \to 1^+} \frac{\sum_{p \in A} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)} = \alpha.$$

We have previously shown that the density of the set of all primes is 1 (Corollary 4.2.2). In this section we will prove that for a positive integer m and an integer a such that $(a, m) = 1$, the set of primes congruent to a modulo m has density $1/\phi(m)$. This is a refinement of a theorem of Dirichlet which states that the arithmetic progression

$$a, \qquad a + m, \qquad a + 2m, \qquad a + 3m, \qquad \ldots$$

contains infinitely many primes (because the density of any finite set is zero).

For the remainder of this section, fix a positive integer m and an integer a with $(a, m) = 1$.

Definition 5.3.2. If χ is a Dirichlet character modulo m, define

$$f_\chi(s) = \sum_{p \nmid m} \frac{\chi(p)}{p^s}.$$

Lemma 5.3.3. *We have*

$$f_{\mathbf{1}_m}(s) \sim \log\left(\frac{1}{s-1}\right) \qquad \textit{as } s \to 1^+,$$

where $\mathbf{1}_m$ *is the trivial Dirichlet character modulo* m*.*

Proof. By Corollary 4.2.2, we have

$$\sum_p \frac{1}{p^s} \sim \log\left(\frac{1}{s-1}\right) \qquad \text{as } s \to 1^+.$$

The lemma follows since $f_{\mathbf{1}_m}(s)$ differs from $\sum_p \frac{1}{p^s}$ by only the summands corresponding to primes dividing m. □

Lemma 5.3.4. *If* χ *is a nontrivial Dirichlet character modulo* m*, then* $f_\chi(s)$ *is bounded as* $s \to 1^+$*.*

Proof. Using the Euler product (5.1.1) of $L(s,\chi)$ for $s > 1$, we have

$$\begin{aligned} \log(L(s,\chi)) &= \sum_p \log\left(\frac{1}{1-\chi(p)p^{-s}}\right) \\ &= \sum_p \sum_{n=0}^{\infty} \frac{\chi(p)^n}{np^{ns}} = f_\chi(s) + F_\chi(s), \end{aligned} \tag{5.3.1}$$

where

$$F_\chi(s) = \sum_p \sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}$$

By Corollary 4.2.2, the series $\sum_p \sum_{n=2}^{\infty} \frac{1}{p^{ns}}$ is bounded as $s \to 1^+$. By comparison with this series, it follows that $F_\chi(s)$ is also bounded as $s \to 1^+$. Moreover, $L(1,\chi) \neq 0$ by Theorem 5.2.4, so $\log(L(s,\chi))$ is also bounded as $s \to 1^+$. Therefore from (5.3.1) we conclude that $f_\chi(s)$ is bounded as $s \to 1^+$. □

Definition 5.3.5. Let P_a denote the set of all prime numbers p such that $p \equiv a \pmod{m}$. Moreover, for $s > 1$, define

$$g_a(s) = \sum_{p \in P_a} \frac{1}{p^s}.$$

Lemma 5.3.6. *For $s > 1$, we have*

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi \in \widehat{G(m)}} \chi(a)^{-1} f_\chi(s).$$

Proof. We have

$$\sum_{\chi \in \widehat{G(m)}} \chi(a)^{-1} f_\chi(s) = \sum_{p \nmid m} \left(\sum_{\chi \in \widehat{G(m)}} \chi(a^{-1}p) \right) \frac{1}{p^s} \tag{5.3.2}$$

by the definition of f_χ. The orthogonality relations for characters of finite abelian groups (cf. Lemma C.2.2) imply that

$$\sum_{\chi \in \widehat{G(m)}} \chi(a^{-1}p) = \begin{cases} \phi(m), & \text{if } p \equiv a \pmod{m}, \\ 0, & \text{otherwise.} \end{cases}$$

Now from (5.3.2) we get

$$\sum_{\chi \in \widehat{G(m)}} \chi(a)^{-1} f_\chi(s) = \sum_{p \in P_a} \frac{\phi(m)}{p^s} = \phi(m) g_a(s),$$

finishing the proof. □

We are now ready to prove our version of Dirichlet's theorem on primes in arithmetic progressions.

Theorem 5.3.7. *The set P_a has density $1/\phi(m)$.*

Proof. It suffices to prove that

$$\lim_{s \to 1^+} \frac{g_a(s)}{\log\left(\frac{1}{s-1}\right)} = \frac{1}{\phi(m)}. \tag{5.3.3}$$

By Lemma 5.3.6, we have

$$g_a(s) = \frac{f_{\mathbf{1}_m}(s)}{\phi(m)} + \frac{1}{\phi(m)} \sum_{\chi \neq \mathbf{1}_m} \chi(a)^{-1} f_\chi(s).$$

The sum above is bounded as $s \to 1^+$ by Lemma 5.3.4, so (5.3.3) follows from Lemma 5.3.3 since

$$f_{\mathbf{1}_m}(s) \sim \log\left(\frac{1}{s-1}\right) \qquad \text{as } s \to 1^+. \qquad \square$$

5.4 Gauss Sums

Definition 5.4.1. Let χ be a Dirichlet character modulo m. For $n \in \mathbf{Z}_+$, we define

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

The *Gauss sum* associated to χ is

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

Lemma 5.4.2. *Suppose χ is a Dirichlet character modulo m, and suppose that either*

(a) $(m, n) = 1$, *or*

(b) $(m, n) > 1$ *and χ is primitive and non-trivial.*

Then

$$\tau(\chi, n) = \overline{\chi(n)}\tau(\chi). \tag{5.4.1}$$

Proof. First suppose (a) holds. Then n is invertible in $\mathbf{Z}/m\mathbf{Z}$, and so we have

$$\begin{aligned} \overline{\chi(n)}\tau(\chi) &= \sum_{k=0}^{m-1} \chi(k)\overline{\chi(n)} e^{2\pi i k/m} \\ &= \sum_{k=0}^{m-1} \chi(kn^{-1} \pmod{m}) e^{2\pi i k/m} \\ &= \sum_{h=0}^{m-1} \chi(h) e^{2\pi i h n/m} = \tau(\chi, n) \end{aligned}$$

by changing the order of summation.

Now suppose (b) holds. Then $\chi(n) = 0$, so to prove (5.4.1), it suffices to prove that

$$\tau(\chi, n) = 0.$$

Choose positive integers m_1, n_1, d such that $m = m_1 d$, $n = n_1 d$, $d > 1$, and $(m_1, n_1) = 1$. Then we have

$$\tau(\chi, n) = \sum_{k=0}^{m-1} \chi(k) e^{2\pi i n_1 k/m_1}.$$

Since m_1 is a proper divisor of m and χ is a primitive Dirichlet character modulo m, it follows that there exists an integer c_0 such that $(c_0, m) = 1$, $c_0 \equiv 1 \pmod{m}_1$, and $\chi(c_0) \neq 1$. Let c_1 be an inverse of c_0 modulo m_1. Then we have

$$n_1 c_1 k \equiv n_1 k \pmod{m_1}.$$

Therefore

$$\begin{aligned} \chi(c_0)\tau(\chi, n) &= \sum_{k=0}^{m-1} \chi(c_0 k) e^{2\pi i n_1 k/m_1} \\ &= \sum_{k=0}^{m-1} \chi(k) e^{2\pi i n_1 c_1 k/m_1} \\ &= \sum_{k=0}^{m-1} \chi(k) e^{2\pi i n_1 k/m_1} = \tau(\chi, n). \end{aligned}$$

Since $\chi(c_0) \neq 1$, it follows that $\tau(\chi, n) = 0$, proving (5.4.1) for case (b). □

Lemma 5.4.3. *Suppose χ is a primitive Dirichlet character modulo m. Then*

$$|\tau(\chi)| = \sqrt{m}.$$

Proof. Using Lemma 5.4.2, we have

$$\begin{aligned} |\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} &= \sum_{k=0}^{m-1} \overline{\chi(n)} \tau(\chi) e^{-2\pi i k/n} \\ &= \sum_{k=0}^{m-1} \tau(\chi, n) e^{-2\pi i k/n} = \sum_{k=0}^{m-1} \sum_{\ell=0}^{m-1} \chi(\ell) e^{2\pi i (\ell - 1)k/n} \end{aligned}$$

$$= \sum_{\ell=0}^{m-1} \chi(\ell) \sum_{k=0}^{m-1} e^{2\pi i(\ell-1)k/n} = m$$

since

$$\sum_{k=0}^{m-1} e^{2\pi i(\ell-1)k/n} = \begin{cases} m, & \text{if } n = 1 \\ 0, & \text{if } n \neq 1. \end{cases}$$

□

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

In this section, we prove that for a primitive Dirichlet character χ modulo m, the L-function $L(s,\chi)$ is related to the L-function $L(s,\overline{\chi})$ by a functional equation similar to that of the Riemann zeta function (cf. §4.6). The proof strategy will be very similar, relying heavily on the Poisson summation formula (Theorem B.3.5). We must divide the discussion into the cases where χ is even and where χ is odd. Recall that χ is *even* if $\chi(-1) = 1$, and χ is *odd* if $\chi(-1) = -1$.

5.5.1 The Even Case

Definition 5.5.1. For every primitive even Dirichlet character χ modulo m and $t > 0$, we define

$$\theta(t,\chi) = \sum_{n\in\mathbf{Z}} \chi(n) e^{-\pi n^2 t/m}.$$

Lemma 5.5.2. *For χ a primitive even Dirichlet character modulo m, we have*

$$\theta(t,\chi) = O(e^{-\pi t})$$

as $t \to \infty$.

Proof. For $t \geq 1$, we have

$$\begin{aligned} |\theta(t,\chi)| &\leq \sum_{n\in\mathbf{Z}} e^{-\pi n^2 t/m} \\ &= e^{-\pi t} \sum_{n\in\mathbf{Z}} e^{-\pi(n^2-m)t/m} \\ &\leq e^{-\pi t} \sum_{n\in\mathbf{Z}} e^{-\pi(n^2-m)/m}. \end{aligned}$$

□

Lemma 5.5.3. *Let χ be a primitive even Dirichlet character modulo m. For $t > 0$, we have*

$$\tau(\overline{\chi})\theta(t,\chi) = \left(\frac{m}{t}\right)^{1/2} \theta(t^{-1},\overline{\chi}). \tag{5.5.1}$$

Proof. Note that

$$\tau(\overline{\chi})\theta(t,\chi) = \sum_{k=0}^{m-1} \overline{\chi}(k) \sum_{n\in\mathbf{Z}} e^{-\pi n^2 t/m + 2\pi i nk/m}. \tag{5.5.2}$$

By Lemma 4.6.3, the inner sum in (5.5.2) is

$$\sum_{n\in\mathbf{Z}} e^{-\pi n^2 t/m + 2\pi i nk/m} = \left(\frac{m}{t}\right)^{1/2} \sum_{n\in\mathbf{Z}} e^{-\pi(n+k/m)^2 m/t},$$

so (5.5.2) becomes

$$\begin{aligned}\tau(\overline{\chi})\theta(t,\chi) &= \left(\frac{m}{t}\right)^{1/2} \sum_{k=0}^{m-1} \overline{\chi}(k) \sum_{n\in\mathbf{Z}} e^{-\pi(nm+k)^2/(tm)} \\ &= \left(\frac{m}{t}\right)^{1/2} \sum_{\ell=0}^{m-1} \overline{\chi}(\ell) \sum_{n\in\mathbf{Z}} e^{-\pi \ell^2/(tm)} \\ &= \left(\frac{m}{t}\right)^{1/2} \theta(t^{-1},\overline{\chi}).\end{aligned}$$

□

Definition 5.5.4. For a primitive even Dirichlet character χ modulo m, we define

$$\xi(s,\chi) = \frac{1}{2}\int_1^\infty t^{s/2}\theta(t,\chi)\,\frac{dt}{t} + \frac{\sqrt{m}}{2\tau(\overline{\chi})}\int_1^\infty t^{(1-s)/2}\theta(t,\overline{\chi})\,\frac{dt}{t} \tag{5.5.3}$$

for all $s \in \mathbf{C}$ where this makes sense.

Lemma 5.5.5. *Let χ be a primitive even Dirichlet character modulo m. The function $\xi(s,\chi)$ is entire, and for all $s \in \mathbf{C}$ we have*

$$m^{1/2}\xi(s,\chi) = \tau(\chi)\xi(1-s,\overline{\chi}). \tag{5.5.4}$$

Proof. The integrals defining $\xi(s,\chi)$ in (5.5.3) are absolutely and uniformly convergent on compact subsets of $\mathbf{C}$ by Lemma 5.5.3 since $\theta(t,\chi) = O(e^{-\pi t})$. This proves that $\xi(s,\chi)$ is an entire function. Moreover, the functional equation (5.5.4) of $\xi(s,\chi)$ follows from the functional equation (5.5.1) of $\theta(t,\chi)$ and the change of variables $s \mapsto 1-s$ in the integrals defining $\xi(s,\chi)$. □

Theorem 5.5.6. *Let χ be a primitive even Dirichlet character modulo m. For all $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$, we have*

$$\xi(s, \chi) = \pi^{-s/2} m^{s/2} \Gamma\left(\frac{s}{2}\right) L(s, \chi). \tag{5.5.5}$$

The right-hand side of (5.5.5) extends to an entire function, and we have

$$\pi^{-s/2} m^{s} \Gamma\left(\frac{s}{2}\right) L(s, \chi) = \pi^{-(1-s)/2} \tau(\chi) \Gamma\left(\frac{1-s}{2}\right) L(1-s, \overline{\chi}) \tag{5.5.6}$$

for all $s \in \mathbf{C}$ different from 0 and 1.

Proof. Let n be a positive integer, and note that

$$\begin{aligned}\pi^{-s/2} m^{s/2} \Gamma\left(\frac{s}{2}\right) \chi(n) n^{-s} &= \pi^{-s/2} m^{s/2} \chi(n) n^{-s} \int_0^\infty x^{s/2} e^{-x} \, \frac{dx}{x} \\ &= \chi(n) \int_0^\infty t^{s/2} e^{-\pi n^2 t/m} \, \frac{dt}{t}\end{aligned}$$

after a change of variables. Summing over all positive n, we get

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

Since $\chi(-1) = 1$ and $\chi(0) = 0$, it follows that

$$\begin{aligned}\pi^{-s/2} m^{s/2} \Gamma\left(\frac{s}{2}\right) L(s, \chi) &= \frac{1}{2} \sum_{n \in \mathbf{Z}} \int_0^\infty t^{s/2} \chi(n) e^{-\pi n^2 t/m} \, \frac{dt}{t} \\ &= \frac{1}{2} \int_0^\infty t^{s/2} \theta(t, \chi) \, \frac{dt}{t}.\end{aligned} \tag{5.5.7}$$

The last equality of (5.5.7) holds because the final integral converges absolutely by Lemma 5.5.2. From (5.5.7) and the functional equation of $\theta(t, \chi)$ (5.5.1) it follows that

$$\begin{aligned}\pi^{-s/2} m^{s/2} \Gamma\left(\frac{s}{2}\right) L(s, \chi) &= \frac{1}{2} \int_1^\infty t^{s/2} \theta(t, \chi) \, \frac{dt}{t} + \frac{1}{2} \int_0^1 t^{s/2} \theta(t, \chi) \, \frac{dt}{t} \\ &= \frac{1}{2} \int_1^\infty t^{s/2} \theta(t, \chi) \, \frac{dt}{t} + \frac{1}{2} \int_1^\infty t^{-s/2} \theta(t^{-1}, \chi) \, \frac{dt}{t}\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2}\int_1^\infty t^{s/2}\theta(t,\chi)\,\frac{dt}{t} + \frac{\sqrt{m}}{2\tau(\overline{\chi})}\int_1^\infty t^{(1-s)/2}\theta(t,\overline{\chi})\,\frac{dt}{t}\\
&= \xi(s,\chi).
\end{aligned}
$$

Thus we've proved (5.5.5), and the rest of the theorem follows from Lemma 5.5.3. □

Corollary 5.5.7. *For any primitive even Dirichlet character modulo m, the L-function $L(s,\chi)$ extends to an entire function on $\mathbf{C}$.*

Proof. This is an immediate consequence of Theorem 5.5.6 since $\xi(s,\chi)$ is entire and the gamma function is never zero. □

5.5.2 The Odd Case

The same method used in §5.5.1 to prove the functional equation (5.5.6) of $L(s,\chi)$ when χ is even cannot be used if χ is odd since the function

$$\theta(t,\chi) = \sum_{n\in\mathbf{Z}} \chi(n)e^{-\pi n^2 t/m}$$

is identically zero in this case. We define a replacement for $\theta(t,\chi)$ when χ is odd as follows.

Definition 5.5.8. Let χ be a primitive odd Dirichlet character modulo m. For $t>0$, define

$$\theta_1(t,\chi) = \sum_{n\in\mathbf{Z}} n\chi(n)e^{-\pi n^2 t/m}.$$

Lemma 5.5.9. *For $t>0$ and χ a primitive odd Dirichlet character modulo m, we have*

$$\tau(\overline{\chi})\theta_1(t,\chi) = im^{1/2}t^{-3/2}\theta_1(t^{-1},\overline{\chi}). \tag{5.5.8}$$

Proof. We have

$$\tau(\overline{\chi})\theta_1(t,\chi) = \sum_{k=0}^{m-1}\overline{\chi}(k)\sum_{n\in\mathbf{Z}} ne^{-\pi n^2 t/m + 2\pi ink/m}$$

Thus to prove (5.5.8), it suffices to prove that

$$\sum_{n\in\mathbf{Z}} ne^{-\pi n^2 t/m + 2\pi ikn/m} = i\left(\frac{m}{t}\right)^{3/2}\sum_{n\in\mathbf{Z}}\left(n+\frac{k}{m}\right)e^{-\pi(n+k/m)^2 m/t},$$

and this follows from differentiating both sides of the equation

$$\sum_{n\in\mathbf{Z}} e^{-n^2\pi t/m+2\pi ink/m} = \left(\frac{m}{t}\right)^{1/2} \sum_{n\in\mathbf{Z}} e^{-\pi(n+k/m)^2 m/t} \tag{5.5.9}$$

given by Lemma 4.6.3. □

Definition 5.5.10. For a primitive odd Dirichlet character χ modulo m, we define

$$\xi(s,\chi) = \frac{1}{2}\int_1^\infty t^{s/2}\theta_1(t,\chi)\,\frac{dt}{\sqrt{t}} + \frac{i\sqrt{m}}{2\tau(\overline{\chi})}\int_1^\infty t^{(1-s)/2}\theta_1(t,\overline{\chi})\,\frac{dt}{\sqrt{t}} \tag{5.5.10}$$

for all $s\in\mathbf{C}$ where this makes sense.

Lemma 5.5.11. *Let χ be a primitive odd Dirichlet character modulo m. The function $\xi(s,\chi)$ is entire, and for all $s\in\mathbf{C}$ we have*

$$im^{1/2}\xi(s,\chi) = \tau(\chi)\xi(1-s,\overline{\chi}). \tag{5.5.11}$$

Proof. Like in the corresponding even case, the integrals defining $\xi(s,\chi)$ in (5.5.10) are absolutely and uniformly convergent on compact subsets of $\mathbf{C}$, so $\xi(s,\chi)$ is an entire function. The functional equation (5.5.11) of $\xi(s,\chi)$ follows from the functional equation (5.5.8) of $\theta_1(t,\chi)$ and a change of variables. □

Theorem 5.5.12. *Let χ be a primitive odd Dirichlet character modulo m. For all $s\in\mathbf{C}$ with $\mathrm{Re}(s)>1$, we have*

$$\xi(s,\chi) = \pi^{-(s+1)/2}m^{(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi). \tag{5.5.12}$$

The right-hand side of (5.5.12) extends to an entire function, and $L(s,\chi)$ extends to an entire function on $\mathbf{C}$.

Proof. For a positive integer n, note that

$$\pi^{-(s+1)/2}m^{(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)\chi(n)n^{-s} = \chi(n)\int_0^\infty ne^{-\pi n^2 t/m}t^{(s+1)/2}\,\frac{dt}{t},$$

so that, using the functional equation (5.5.8) of $\theta_1(t,\chi)$, we get

$$\pi^{-(s+1)/2}m^{(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi) = \sum_{n=1}^\infty \int_0^\infty n\chi(n)e^{-\pi n^2 t/m}t^{(s+1)/2}\,\frac{dt}{t}$$

$$
\begin{aligned}
&= \frac{1}{2}\int_0^\infty t^{(s+1)/2}\theta_1(t,\chi)\,\frac{dt}{t} \\
&= \frac{1}{2}\int_1^\infty t^{(s+1)/2}\theta_1(t,\chi)\,\frac{dt}{t} + \frac{1}{2}\int_1^\infty t^{-(s+1)/2}\theta_1(t^{-1},\chi)\,\frac{dt}{t} \\
&= \xi(s,\chi).
\end{aligned}
$$

Thus we've proved (5.5.12). Since $\Gamma(s)$ is never zero, it follows from the functional equation (5.5.11) of $\xi(s,\chi)$ that $L(s,\chi)$ has no poles. □

We have seen in this section that the Dirichlet L-functions $L(s,\chi)$ behave much like the Riemann zeta function $\zeta(s)$ in that they have a continuation to the entire plane $\mathbf{C}$ and satisfy a functional equation involving the gamma function. In fact, both Dirichlet L-functions and the Riemann zeta function are a special case of so-called *Artin L-functions*, which arise from Galois representations of number fields. Like the Riemann zeta function and the Dirichlet L-functions (which arise from one-dimensional Galois representations), Artin L-functions also satisfy properties like possessing a meromorphic continuation and satisfying a functional equation. The theory of Artin L-functions is a much larger and richer area of study, and they fit into a much broader framework of the Langlands program. For an good overview of this current area of research, see [Gel84].

A Complex Analysis

A.1 Infinite Products

Definition A.1.1. Let $\alpha_1, \alpha_2, \alpha_3, \ldots$ be a sequence of complex numbers. Suppose that the following conditions hold:

(1) there exists a positive integer N such that $\alpha_n \neq 0$ for all $n \geq N$;

(2) the limit
$$L = \lim_{m\to\infty} \prod_{n=N}^{m} \alpha_m$$
exists and is different from zero.

If the preceding conditions hold for some N, then we say that the *infinite product* $\prod_{n=1}^\infty \alpha_i$ *converges*, and its value is, by definition,

$$\prod_{n=1}^{\infty} \alpha_i = L \prod_{n=1}^{N-1} \alpha_n.$$

We follow the convention that any product taken over the empty set is 1.

Lemma A.1.2. *Suppose the infinite product* $\prod_{n=1}^{\infty} \alpha_n$ *converges. Then*

$$\lim_{n\to\infty} \alpha_n = 1.$$

Proof. Without loss of generality, assume $\alpha_n \neq 0$ for all $n \in \mathbf{Z}_+$. In particular, $\prod_{n=1}^{\infty} \alpha_n \neq 0$. Then we have

$$\alpha_n = \frac{\prod_{k=1}^{n} \alpha_k}{\prod_{k=1}^{n-1} \alpha_k},$$

and letting $n \to \infty$, the lemma follows. □

Lemma A.1.3. *The infinite product* $\prod_{n=1}^{\infty} \alpha_n$ *converges if and only if there exists a positive integer* N *such that the series* $\sum_{n=N}^{\infty} \log(\alpha_n)$ *converges (here* log *denotes the principal branch of the logarithm).*

Proof. Without loss of generality, assume $\alpha_n \neq 0$ for each $n \in \mathbf{Z}_+$, so we may take $N = 1$ in the statement of the lemma. For every positive integer n, define

$$P_n = \prod_{k=1}^{n} \alpha_k, \qquad S_n = \sum_{k=1}^{n} \log(\alpha_k).$$

Suppose first that the series $\sum_{n=1}^{\infty} \log(\alpha_n) = \lim_{n\to\infty} S_n$ converges to the complex number S. Then we have

$$P_n = e^{S_n}$$

for each n, so the convergence of S_n to S implies the convergence of P_n to $e^S \neq 0$. In particular, the product $\prod_{n=1}^{\infty} \alpha_n$ converges.

Conversely, suppose the infinite product $\prod_{n=1}^{\infty} \alpha_n = \lim_{n\to\infty} P_n$ converges to the nonzero complex number P. Then $P_n/P \to 1$ as $n \to \infty$, whence $\log(P_n/P) \to 0$ as $n \to \infty$. For each $n \in \mathbf{Z}_+$, there exists an $h_n \in \mathbf{Z}$ such that

$$\log\left(\frac{P_n}{P}\right) = S_n - \log(P) + 2\pi i h_n. \tag{A.1.1}$$

Thus we have

$$2\pi i(h_{n+1} - h_n) = \log\left(\frac{P_{n+1}}{P}\right) - \log\left(\frac{P_n}{P}\right) - \log(\alpha_n).$$

Looking at the imaginary parts of the equation above, we get

$$2\pi(h_{n+1} - h_n) = \operatorname{Arg}\left(\frac{P_{n+1}}{P}\right) - \operatorname{Arg}\left(\frac{P_n}{P}\right) - \operatorname{Arg}(\alpha_n).$$

Since $|\operatorname{Arg}(\alpha_n)| \leq \pi$ for all n, and since $\operatorname{Arg}(P_n/P) \to 0$ as $n \to \infty$, it follows that the sequence of integers $h_1, h_2, h_3, \ldots$ is eventually constant. That is, there exists an $h \in \mathbf{Z}$ with $h_n = h$ for all n sufficiently large, and so by (A.1.1) we have

$$\lim_{n\to\infty} S_n = \log(P) - 2\pi i h.$$

In particular, the series $\sum_{n=1}^{\infty} \log(\alpha_n)$ converges. □

Definition A.1.4. The infinite product $\prod_{n=1}^{\infty} \alpha_n$ is said to *converge absolutely* if and only if there exists an $N \in \mathbf{Z}_+$ such that the series $\sum_{n=N}^{\infty} \log(\alpha_n)$ converges absolutely.

Lemma A.1.5. *The infinite product $\prod_{n=1}^{\infty}(1 + \alpha_n)$ converges absolutely if and only if the series $\sum_{n=1}^{\infty} \alpha_n$ converges absolutely.*

Proof. Without loss of generality, assume $1 + \alpha_n \neq 0$ for all $n \in \mathbf{Z}_+$. By Lemma A.1.3, it suffices to show that $\sum_{n=1}^{\infty} \log(1 + \alpha_n)$ converges absolutely if and only if $\sum_{n=1}^{\infty} \alpha_n$ converges absolutely. But this follows from the limit comparison test and the fact that

$$\lim_{s\to 0} \frac{\log(1+s)}{s} = 1.$$ □

A.2 The Gamma Function

In this section we will list the fundamental and well-known properties of the gamma function without proof. The proofs of the properties are contained in many texts (e.g., [Ahl78]).

Definition A.2.1. For every $s \in \mathbf{C}$ different from a non-positive integer, we define $\Gamma(s)$ by the infinite product

$$\Gamma(s) = \frac{e^{-\gamma s}}{s} \prod_{n\in\mathbf{Z}_+} \frac{e^{s/n}}{1 + \frac{s}{n}} \qquad \text{(A.2.1)}$$

The function Γ is called the *gamma function*.

The number γ in (A.2.1) is the Euler-Mascheroni constant, which by Definition 4.2.5 and Lemma 4.2.6 is equal to

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

Theorem A.2.2. *The gamma function satisfies the following properties:*

(a) Γ *is a non-vanishing meromorphic function with a simple pole at each non-positive integer;*

(b) *the residue of* Γ *at* $-k$ *for* k *a non-negative integer is* $\frac{(-1)^k}{k!}$*;*

(c) *we have*

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

whenever $\mathrm{Re}(s) > 0$*;*

(d) *we have*

$$\Gamma(s+1) = s\Gamma(s)$$

for all $s \in \mathbf{C}$ *where* $\Gamma(s)$ *and* $\Gamma(s+1)$ *are defined;*

(e) *we have*

$$\Gamma(n+1) = n!$$

for every non-negative integer n*;*

(f) *we have*

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

for all non-integer $s \in \mathbf{C}$*;*

(g) *we have*

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

B Fourier Analysis

B.1 Fourier Series

Let $f : \mathbf{R} \to \mathbf{C}$ be a periodic function with period $T > 0$ which is integrable on every bounded interval.

Lemma B.1.1. *For all $a, b \in \mathbf{R}$ we have*

$$\int_a^{a+T} f(x)\,dx = \int_b^{b+T} f(x)\,dx$$

Proof. Let $g : \mathbf{R} \to \mathbf{C}$ be given by

$$g(a) = \int_a^{a+T} f(\xi)\,d\xi.$$

Then the fundamental theorem of calculus implies that

$$g'(a) = f(a+T) - f(a) = 0$$

for all $a \in \mathbf{R}$, so g is a constant function, and the lemma follows. □

For every integer n, we define a function $\chi_n : \mathbf{R} \to \mathbf{C}$ by

$$\chi_n(x) = e^{2\pi i n x/T}.$$

We then have $\overline{\chi_n(x)} = \chi_{-n}(x) = 1/\chi_n(x)$ and $\chi_m(x)\chi_n(x) = \chi_{m+n}(x)$, as well as

$$\frac{1}{T}\int_{-T/2}^{T/2} \chi_n(\xi)\,d\xi = \begin{cases} 1, & \text{if } n = 0, \\ 0, & \text{if } n \neq 0. \end{cases} \tag{B.1.1}$$

Definition B.1.2. For an integer n, the *nth Fourier coefficient* c_n of f is

$$c_n = \frac{1}{T}\int_{-T/2}^{T/2} f(\xi)\overline{\chi_n(\xi)}\,d\xi.$$

Theorem B.1.3 (Bessel's Inequality)**.**

$$\sum_{-\infty}^{\infty} |c_n|^2 \leq \frac{1}{T}\int_{-T/2}^{T/2} |f(\xi)|^2\,d\xi.$$

Proof. Fix a positive integer N. For $\xi \in [-T/2, T/2]$ we have

$$\left| f(\xi) - \sum_{n=-N}^{N} c_n \chi_n(\xi) \right|^2$$

$$= \left(f(\xi) - \sum_{n=-N}^{N} c_n \chi_n(\xi) \right) \left(\overline{f(\xi)} - \sum_{n=-N}^{N} \overline{c_n} \chi_{-n}(\xi) \right)$$

$$= |f(\xi)|^2 - \sum_{n=-N}^{N} \left(c_n \overline{f(\xi)} \chi_n(\xi) + \overline{c_n} f(\xi) \overline{\chi_n}(\xi) \right) + \sum_{m,n=-N}^{N} c_m \overline{c_n} \chi_{m-n}(\xi)$$

Now by (B.1.1) we have

$$\begin{aligned} 0 &\leq \frac{1}{T} \int_{-T/2}^{T/2} \left| f(\xi) - \sum_{n=-N}^{N} c_n \chi_n(\xi) \right|^2 d\xi \\ &= \frac{1}{T} \int_{-T/2}^{T/2} |f(\xi)|^2 \, d\xi - \sum_{n=-N}^{N} (c_n \overline{c_n} + \overline{c_n} c_n) + \sum_{n=-N}^{N} c_n \overline{c_n} \\ &= \frac{1}{T} \int_{-T/2}^{T/2} |f(\xi)|^2 \, d\xi - \sum_{n=-N}^{N} |c_n|^2 , \end{aligned}$$

so

$$\sum_{n=-N}^{N} |c_n|^2 \leq \frac{1}{T} \int_{-T/2}^{T/2} |f(\xi)|^2 \, d\xi.$$

The monotone sequence of partial sums $\sum_{n=-N}^{N} |c_n|^2$ is therefore bounded by $\frac{1}{T} \int_{-T/2}^{T/2} |f(\xi)|^2 \, d\xi$, whence the theorem follows. □

We now wish to find a condition on f under which we have

$$f(x) = \sum_{n=-\infty}^{\infty} c_n \chi_n(x) = \lim_{N \to \infty} \sum_{n=-N}^{N} c_n \chi_n(x).$$

The infinite series above is the *Fourier series* of f. Given a positive integer N, let $S_N(x)$ denote the Nth partial sum of the Fourier series of f at x. That is,

$$S_N(x) = \sum_{n=-N}^{N} c_n \chi_n(x) = \frac{1}{T} \sum_{n=-N}^{N} \int_{-T/2}^{T/2} f(\xi) e^{2\pi i n (x-\xi)/T} \, d\xi.$$

Using a change of variables and reversing the order of summation, we get

$$S_N(x) = \frac{1}{T} \sum_{n=-N}^{N} \int_{-T/2+x}^{T/2+x} f(x+\phi) e^{2\pi i n \phi/T} \, d\phi.$$

The integrand above is periodic with period T, so Lemma B.1.1 implies that

$$S_N(x) = \frac{1}{T}\sum_{n=-N}^{N}\int_{-T/2}^{T/2} f(x+\phi)e^{2\pi in\phi/T}\,d\phi.$$

If we define

$$D_N(\phi) = \frac{1}{T}\sum_{n=-N}^{N} e^{2\pi in\phi/T}, \tag{B.1.2}$$

then we have

$$S_N(x) = \int_{-T/2}^{T/2} f(x+\phi)D_N(\phi)\,d\phi. \tag{B.1.3}$$

We call D_N the *Nth Dirichlet kernel.* By (B.1.2) and the formula for a geometric sum, we have

$$D_N(\phi) = \frac{1}{T}e^{-2\pi iN\phi/T}\sum_{n=0}^{2N}\left(e^{2\pi i\phi/T}\right)^n = \frac{1}{T}\frac{e^{2\pi i(N+1)\phi/T}-e^{-2\pi iN\phi/T}}{e^{2\pi i\phi/T}-1}. \tag{B.1.4}$$

Lemma B.1.4. *For any positive integer N, we have*

$$\int_{-T/2}^{0} D_N(\phi)\,d\phi = \int_{0}^{T/2} D_N(\phi)\,d\phi = \frac{1}{2}$$

Proof. From the definition of D_N in (B.1.2), we see that

$$D_N(\phi) = \frac{1}{T} + \frac{1}{T}\sum_{n=1}^{N}\left(e^{2\pi in\phi/T}+e^{-2\pi in\phi/T}\right) = \frac{1}{T} + \frac{2}{T}\sum_{n=1}^{N}\cos\left(2\pi n\phi/T\right),$$

so

$$\int_{-T/2}^{0} D_N(\phi)\,d\phi = \left[\frac{\phi}{T} + \sum_{n=1}^{N}\frac{\sin\left(2\pi n\phi/T\right)}{\pi n}\right]_{-T/2}^{0} = \frac{1}{2}.$$

The integral from 0 to $T/2$ is evaluated similarly. □

Theorem B.1.5. *Suppose f is piecewise smooth on* $\mathbf{R}$*. Then for every $x \in \mathbf{R}$ we have*

$$\lim_{N\to\infty} S_N(x) = \frac{1}{2}\left[f(x-)+f(x+)\right],$$

where

$$f(x\pm) = \lim_{h\to 0+} f(x\pm h).$$

Proof. Fix $x \in \mathbf{R}$. By Lemma B.1.4, we have

$$\frac{1}{2}\left(f(x-)+f(x+)\right) = f(x-)\int_{-T/2}^{0} D_N(\phi)\,d\phi + f(x+)\int_{0}^{T/2} D_N(\phi)\,d\phi,$$

so from (B.1.3) it follows that

$$\begin{aligned} & S_N(x) - \frac{1}{2}\left(f(x-)+f(x+)\right) \\ & = \int_{-T/2}^{0} \left(f(x+\phi) - f(x-)\right) D_N(\phi)\,d\phi \\ & + \int_{0}^{T/2} \left(f(x+\phi) - f(x+)\right) D_N(\phi)\,d\phi. \end{aligned}$$

Let $g : (-T/2, T/2) \to \mathbf{C}$ be given by

$$g(\phi) = \begin{cases} \dfrac{f(x+\phi)-f(x-)}{e^{2\pi i\phi/T}-1} & \text{if } -T/2 < \phi \le 0 \\ \dfrac{f(x+\phi)-f(x+)}{e^{2\pi i\phi/T}-1} & \text{if } 0 < \phi < T/2. \end{cases}$$

Then by (B.1.4) we have

$$\begin{aligned} & S_N(x) - \frac{1}{2}\left(f(x-)+f(x+)\right) \\ & = \frac{1}{T}\int_{-T/2}^{T} g(\phi)\left(e^{2\pi i(N+1)\phi/T} - e^{-2\pi i N\phi/T}\right)\,d\phi \end{aligned} \tag{B.1.5}$$

If C_n denotes the nth Fourier coefficient of g, then Bessel's inequality (Theorem B.1.3) applied to g implies that the series $\sum_{n=-\infty}^{\infty} |C_n|^2$ converges, whence $\lim_{n\to 0} C_n = 0$. Moreover, (B.1.5) becomes

$$S_N(x) - \frac{1}{2}\left(f(x-)+f(x+)\right) = C_{N+1} - C_N,$$

and the right hand side of this equation tends to zero as $N \to \infty$. This concludes the proof of the theorem. □

B.2 Schwartz Functions

Definition B.2.1. A function $f : \mathbf{R} \to \mathbf{C}$ is said to be a *Schwartz function* if and only if f is smooth and for all positive integers m, n there exist $M, N > 0$ such that

$$\left| x^m \frac{d^n f(x)}{dx^n} \right| < N$$

if $|x| > M$. The set $\mathcal{S}$ of all Schwartz functions is called the *Schwartz space.*

Clearly $\mathcal{S}$ has a natural structure of a $\mathbf{C}$-vector space.

Example B.2.2. Any smooth function on $\mathbf{R}$ with compact support is in $\mathcal{S}$. In particular, for any $a, b \in \mathbf{R}$ with $a < b$, $\mathcal{S}$ contains the function

$$x \mapsto \begin{cases} e^{-\frac{1}{(x-a)(b-x)}} & \text{if } a < x < b \\ 0 & \text{otherwise} \end{cases}$$

which is smooth and vanishes on $\mathbf{R} \setminus [a, b]$.

Lemma B.2.3. *For every $f \in \mathcal{S}$, the integral $\int_{\mathbf{R}} |f(x)|\, dx$ is finite.*

Proof. Let $f \in \mathcal{S}$ be given. Then there exist constants $M, N > 0$ such that

$$|f(x)| < \frac{N}{x^2}$$

if $|x| > M$. Then we have

$$\int_{\mathbf{R}} |f(x)|\, dx \leq \int_{-M}^{M} |f(x)|\, dx + 2N \int_{M}^{\infty} \frac{1}{x^2}\, dx = \int_{-M}^{M} |f(x)|\, dx + \frac{2N}{M},$$

which proves the lemma. □

If $L^1(\mathbf{R})$ denotes the $\mathbf{C}$-vector space of all measurable functions $f : \mathbf{R} \to \mathbf{C}$ for which $\int_{\mathbf{R}} |f(x)|\, dx$ is finite, then Lemma B.2.3 is the assertion that $\mathcal{S} \subseteq L^1(\mathbf{R})$.

B.3 The Fourier Transform

Definition B.3.1. Let $f \in L^1(\mathbf{R})$ be given. The *Fourier transform* of f is the function $\widehat{f} : \mathbf{R} \to \mathbf{C}$ defined by

$$\widehat{f}(y) = \int_{\mathbf{R}} f(x) e^{-2\pi i x y}\, dx.$$

For a function $f : \mathbf{R} \to \mathbf{C}$, we denote by Mf the function $x \mapsto xf(x)$. Moreover, if f is differentiable, then we denote by Df the function $x \mapsto f'(x)$.

Lemma B.3.2. *If $f \in \mathcal{S}$, then $\widehat{f}$ is smooth and*

$$D^n \widehat{f} = (-2\pi i)^n \, \widehat{M^n f}$$

for every positive integer n.

Proof. By induction it suffices to prove only the case $n = 1$. Let $g : \mathbf{R}^2 \to \mathbf{C}$ denote the function $(x, y) \mapsto f(x)e^{-2\pi ixy}$, so that $\widehat{f}(y) = \int_{\mathbf{R}} g(x, y)\, dx$. Then

$$\frac{\partial}{\partial y} g(x, y) = -2\pi ixf(x)e^{-2\pi ixy}.$$

Differentiating under the integral, we get

$$D\widehat{f}(y) = \frac{d}{dy} \int_{\mathbf{R}} g(x, y)\, dx = \int_{\mathbf{R}} \frac{\partial}{\partial y} g(x, y)\, dx = -2\pi i\widehat{Mf}(y). \qquad \square$$

Lemma B.3.3. *If $f \in \mathcal{S}$, then*

$$M^n \widehat{f} = \frac{1}{(2\pi i)^n} \widehat{D^n f}$$

for every positive integer n.

Proof. If f is a Schwartz function, then integration by parts gives

$$y\widehat{f}(y) = \int_{\mathbf{R}} f(x)ye^{-2\pi ixy}\, dx = \frac{1}{2\pi i} \int_{\mathbf{R}} Df(x)e^{-2\pi ixy}\, dx = \frac{1}{2\pi i} \widehat{Df}(y),$$

which proves the lemma when $n = 1$. The general case follows by induction. □

Lemma B.3.4. *If $f \in \mathcal{S}$, then $\widehat{f} \in \mathcal{S}$.*

Proof. Let $f \in \mathcal{S}$ be given, and let m and n be arbitrary positive integers. Lemmas B.3.2 and B.3.3 imply that $\widehat{f}$ is smooth and that we have

$$M^m D^n \widehat{f} = (-1)^m \, (2\pi i)^{m-n} \, \widehat{D^m M^n} f. \tag{B.3.1}$$

It is clear that $D^m M^n f \in \mathcal{S}$ since $f \in \mathcal{S}$, and if $g \in \mathcal{S}$, then

$$|\widehat{g}(y)| \leq \int_{\mathbf{R}} |g(x)| \, dx,$$

so g is bounded. Thus (B.3.1) implies that $M^n D^n \widehat{f}$ is bounded. and hence $\widehat{f} \in \mathcal{S}$. □

Theorem B.3.5 (Poisson summation formula)**.** *Let $f \in \mathcal{S}$. Then*

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

Proof. Let $g : \mathbf{R} \to \mathbf{C}$ be given by

$$g(x) = \sum_{k\in\mathbf{Z}} f(x+k).$$

Note that this series converges for every x since f is a Schwartz function. The function g is smooth and periodic of period 1, so by Theorem B.1.5 it is the limit of its Fourier series. Let c_n be the nth Fourier coefficient of g. That is,

$$\begin{aligned} c_n &= \int_0^1 g(\xi)e^{-2\pi in\xi}\,d\xi \\ &= \sum_{k\in\mathbf{Z}} \int_0^1 f(\xi+k)e^{-2\pi in\xi}\,d\xi \\ &= \sum_{k\in\mathbf{Z}} \int_0^1 f(\xi+k)e^{-2\pi in(\xi+k)}\,d\xi \\ &= \int_{\mathbf{R}} f(x)e^{-2\pi inx}\,dx = \widehat{f}(n), \end{aligned}$$

whence

$$\sum_{m\in\mathbf{Z}} f(m) = g(0) = \sum_{m\in\mathbf{Z}} c_m = \sum_{m\in\mathbf{Z}} \widehat{f}(m). \qquad \square$$

C Characters of Finite Abelian Groups

C.1 The Dual Group

Throughout this section, let G denote a finite abelian group of order n.

Definition C.1.1. A *character* of G is a group homomorphism $\chi : G \to \mathbf{C}^\times$.

If χ is a character of G, then the image of χ is contained in the set of complex roots of unity of order n. The *trivial character* on G is the function $x \mapsto 1$ from G to $\mathbf{C}^\times$.

If χ and ϕ are characters of G, then so is the function $\chi\phi : G \to \mathbf{C}^\times$ given by $(\chi\phi)(x) = \chi(x)\phi(x)$. With respect to the operation $(\chi, \phi) \mapsto \chi\phi$, the set $\mathrm{Hom}(G, \mathbf{C}^\times)$ of characters of G is a finite abelian group, called the *dual* of G and denoted $\widehat{G}$.

Lemma C.1.2. *If G is a cyclic group, then $\widehat{G} \cong G$.*

Proof. Let g be a generator of G, and let ω be a primitive nth root of unity in $\mathbf{C}$. If $g^a = g^b$ for some positive integers a, b, then n divides $a - b$, whence $\omega^{a-b} = 1$, and so $\omega^a = \omega^b$. Thus we may define a character $\chi_0 : G \to \mathbf{C}^\times$ by $\chi_0(g^a) = \omega^a$. For each $i \in \{0, \dots, n-1\}$, we have $\chi_0^i(g) = \omega^i$, so $\chi_0^i \neq \chi_0^j$ for all $i, j \in \{0, \dots, n-1\}$ with $i \neq j$. Now if $\chi \in \widehat{G}$, then $\chi(g) = \omega^i$ for some $i \in \{0, \dots, n-1\}$. It follows that $\chi = \chi_0^i$, and hence $\widehat{G} = \langle \chi_0 \rangle$. □

Lemma C.1.3. *If G and H are finite abelian groups, then $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$.*

Proof. Let $i_G : G \to G \times H$ and $i_H : H \to G \times H$ be the canonical homomorphisms. We define a function $f : \widehat{G \times H} \to \widehat{G} \times \widehat{H}$ by $f(\chi) = (\chi \circ i_G, \chi \circ i_H)$. We also define a function $g : \widehat{G} \times \widehat{H} \to \widehat{G \times H}$ by $g(\chi, \phi)(x, y) = \chi(x)\phi(y)$. Clearly f and g are homomorphisms and are inverse to each other, proving the lemma. □

Theorem C.1.4. *For any finite abelian group G, we have $G \cong \widehat{G}$.*

Proof. Since G is a finite abelian group, we have $G \cong C_1 \times \cdots \times C_r$, where each C_i is s finite cyclic group. By Lemma C.1.2, we have $C_i \cong \widehat{C_i}$ for each i, and by Lemma C.1.3, we have

$$\widehat{G} \cong \widehat{C}_1 \times \cdots \times \widehat{C}_r \cong C_1 \times \cdots \times C_r \cong G. \qquad \square$$

Theorem C.1.5. *Let G be a finite abelian group. For every subgroup H of G and every $\phi \in \widehat{H}$, there exists a $\chi \in \widehat{G}$ such that $\chi\big|_H = \phi$.*

Proof. We induct on $[G : H]$, with the claim being trivially true if $[G : H] = 1$. Suppose H is a proper subgroup of G and ϕ is a character of H. Choose an $x \in G \setminus H$, and let n be the least positive integer such that $x^n \in H$. Let z be a complex root of unity such that $z^n = \phi(x^n)$. Suppose $h_1 x^{m_1} = h_2 x^{m_2}$ for some $h_1, h_2 \in H$ and $m_1, m_2 \in \mathbf{N}$, so that $x^{m_2 - m_1} = h_1 h_2^{-1} \in H$. Without loss of generality, assume $m_1 \leq m_2$, so that by the minimality of n we have $n \mid m_2 - m_1$. Then

$$z^{m_1 - m_2} = \phi(x^{m_1 - m_2}) = \phi(h_2)\phi(h_1)^{-1},$$

and so $z^{m_1}\phi(h_1) = z^{m_2}\phi(h_2)$. Therefore, if H' denotes the subgroup of G generated by H and x, then we may extend ϕ to a character ϕ' of H' by $\phi'(hx^m) = z^m\phi(h)$. Since $[G : H'] < [G : H]$, we may extend ϕ' to a character χ on G by induction. □

Theorem C.1.6. *The map $\varepsilon : G \to \widehat{\widehat{G}}$ given by $\varepsilon(x)(\chi) = \chi(x)$ is an isomorphism.*

Proof. Since G and $\widehat{\widehat{G}}$ are isomorphic finite groups by Theorem C.1.4, it suffices to prove that ε is injective. Thus it suffices to show that if $x \in G$ is not the identity, then there exists a $\chi \in \widehat{G}$ for which $\chi(x) \neq 1$. Let $x \in G$ be a non-identity element, and let H be the cyclic subgroup generated by x. There must exist a nontrivial character on H (otherwise $H \cong \widehat{H}$ would be trivial), and by Theorem C.1.5, we can extend this nontrivial character to a character χ of G. Since χ is nontrivial on H, we have $\chi(x) \neq 1$. □

C.2 Orthogonality Relations

Lemma C.2.1. *Let G be a finite abelian group of order n, and let $\chi \in \widehat{G}$. Then*

$$\sum_{x\in G} \chi(x) = \begin{cases} n, & \textit{if } \chi \textit{ is the trivial character,} \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. The claim is clearly true if χ is the trivial character. If χ is nontrivial, then there exists a y such that $\chi(y) \neq 1$. Then

$$\chi(y)\sum_{x\in G}\chi(x) = \sum_{x\in G}\chi(xy) = \sum_{x\in G}\chi(x),$$

so $\sum_{x\in G}\chi(x) = 0$. □

Lemma C.2.2. *Let G be a finite abelian group of order n, and let $x \in G$. Then*

$$\sum_{\chi\in\widehat{G}} \chi(x) = \begin{cases} n, & \textit{if } x \textit{ is the identity,} \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. This follows from applying Lemma C.2.1 to the dual group $\widehat{G}$ and using Theorem C.1.6. □

D References

[Ahl78] Lars V. Ahlfors. *Complex analysis*. McGraw-Hill Book Co., New York, third edition, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics.

[Apo76] Tom M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York-Heidelberg, 1976. Undergraduate Texts in Mathematics.

[Che73] Jing Run Chen. On the representation of a larger even integer as the sum of a prime and the product of at most two primes. *Sci. Sinica*, 16:157–176, 1973.

[Dav00] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[FI10] John Friedlander and Henryk Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[Fol92] Gerald B. Folland. *Fourier analysis and its applications*. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1992.

[Gel84] Stephen Gelbart. An elementary introduction to the Langlands program. *Bull. Amer. Math. Soc. (N.S.)*, 10(2):177–219, 1984.

[HR64] G. H. Hardy and M. Riesz. *The general theory of Dirichlet's series*. Cambridge Tracts in Mathematics and Mathematical Physics, No. 18. Stechert-Hafner, Inc., New York, 1964.

[May13] J. Maynard. Small gaps between primes. *arXiv pre-print*, 2013.

[Mur08] M. Ram Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2008. Readings in Mathematics.

[New80] D. J. Newman. Simple analytic proof of the prime number theorem. *Amer. Math. Monthly*, 87(9):693–696, 1980.

[Sch76] Lowell Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Math. Comp.*, 30(134):337–360, 1976.

[Ser73] J.-P. Serre. *A course in arithmetic.* Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Tit86] 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.

[Zag97] D. Zagier. Newman's short proof of the prime number theorem. *Amer. Math. Monthly*, 104(8):705–708, 1997.

[Zha14] Yitang Zhang. Bounded gaps between primes. *Ann. of Math. (2)*, 179(3):1121–1174, 2014.