Introduction to Analytic Number Theory

Math 531 Lecture Notes, Fall 2005

A.J. Hildebrand
Department of Mathematics
University of Illinois

http://www.math.uiuc.edu/~hildebr/ant

Version 2005.12.06

Contents

List of Tables

Notation

$\mathbb{R}$	the set of real numbers
$\mathbb{C}$	the set of complex numbers
$\mathbb{Z}$	the set of integers
$\mathbb{N}$	the set of positive integers ("natural numbers")
$\mathbb{N}_0$	the set of nonnegative integers (i.e., $\mathbb{N} \cup \{0\}$)
$[x]$	the greatest integer $\leq x$ (floor function)
$\{x\}$	the fractional part of x, i.e., $x - [x]$
$d, n, m, \ldots$	integers (usually positive)
$p, p_i, q, q_i, \ldots$	primes
$p^m, p^\alpha, \ldots$	prime powers
$d \mid n$	d divides n
$d \nmid n$	d does not divide n
$p^m \mid\mid n$	p^m divides exactly n (i.e., $p^m \mid n$ and $p^{m+1} \nmid n$)
(a, b)	the greatest common divisor (gcd) of a and b
$[a, b]$	the least common multiple (lcm) of a and b
$n = \prod_{i=1}^{k} p_i^{\alpha_i}$	canonical prime factorization of an integer $n > 1$ (with distinct primes p_i and exponents $\alpha_i \geq 1$)
$n = \prod_p p^{\alpha(p)}$	the prime factorization of n in a different notation, with p running through all primes and exponents $\alpha(p) \geq 0$
$n = \prod_{p^m \mid\mid n} p^m$	yet another way of writing the canonical prime factorization of n
$\sum_{p \leq x}$	summation over all primes $\leq x$
$\sum_{p^m}$	summation over all prime powers p^m with p prime and m a positive integer
$\sum_{d \mid n}$	summation over all positive divisors of n (including the trivial divisors $d = 1$ and $d = n$)
$\sum_{d^2 \mid n}$	summation over all positive integers d for which d^2 divides n
$\sum_{p^m \mid\mid n}$	summation over all prime powers that divide exactly n (i.e., if $n = \prod_i^k p_i^{\alpha_i}$ is the standard prime factorization of n, then $\sum_{p^m \mid\mid n} f(p^m)$ is the same as $\sum_{i=1}^{k} f(p_i^{\alpha_i})$)
$\sum_{p \mid n}$	summation over all (distinct) primes dividing n.

Convention for empty sums and products: An empty sum (i.e., one in which the summation condition is never satisfied) is defined as 0; an empty product is defined as 1. Thus, for example, the relation $n = \prod_{p^m||n} p^m$ remains valid for $n = 1$ since the right-hand side is an empty product in this case.

Chapter 0

Primes and the Fundamental Theorem of Arithmetic

Primes constitute the holy grail of analytic number theory, and many of the famous theorems and problems in number theory are statements about primes. Analytic number theory provides some powerful tools to study prime numbers, and most of our current (still rather limited) knowledge of primes has been obtained using these tools.

In this chapter, we give a precise definition of the concept of a prime, and we state the Fundamental Theorem of Arithmetic, which says that every integer greater than 1 has a unique (up to order) representation as a product of primes. We conclude the chapter by proving the infinitude of primes.

The material presented in this chapter belongs to elementary (rather than analytic) number theory, but we include it here in order to make the course as self-contained as possible.

0.1 Divisibility and primes

In order to define the concept of a prime, we first need to define the notion of divisibility.

Given two integers $d \neq 0$ and n, we say that d **divides** n or n **is divisible by** d, if there exists an integer m such that $n = dm$. We write $d|n$ if d divides n, and $d \nmid n$ if d does not divide n.

Note that divisibility by 0 is not defined, but the integer n in the above definition may be 0 (in which case n is divisible by any non-zero integer d) or negative (in which case $d|n$ is equivalent to $d|(-n)$).

While the above definition allows for the number d in the relation "$d|n$"

to be negative, it is clear that $d|n$ if and only if $(-d)|n$, so there is a one-to-one correspondence between the positive and negative divisors of an integer n. In particular, no information is lost by focusing on the *positive* divisors of a given integer, and it will be convenient to restrict the notion of a divisor to that of a positive divisor. We therefore make the following convention: *Unless otherwise specified, by a divisor of an integer we mean a positive divisor, and in a notation like $d|n$ the variable d represents a positive divisor of n.* This convention allows us, for example, to write the sum-of-divisors function $\sigma(n)$ (defined as the sum of all *positive* divisors of n) simply as $\sigma(n) = \sum_{d|n} d$, without having to add the extra condition $d > 0$ under the summation symbol.

The **greatest common divisor (gcd)** of two integers a and b that are not both zero is the unique integer $d > 0$ satisfying (i) $d|a$ and $d|b$, and (ii) if $c|a$ and $c|b$, then $c|d$. The gcd of a and b is denoted by (a, b). If $(a, b) = 1$, then a and b are said to be **relatively prime** or **coprime**.

The **least common multiple (lcm)** of two non-zero integers a and b is the unique integer $m > 0$ satisfying (i) $a|m$ and $b|m$, and (ii) if $a|n$ and $b|n$, then $m|n$. The lcm of a and b is denoted by $[a, b]$.

The gcd and the lcm of more than two integers are defined in an analogous manner.

An integer $n > 1$ is called **prime** (or a **prime number**) if its only positive divisors are the trivial ones, namely 1 and n.

The sequence of primes, according to this (commonly accepted) definition is thus $2, 3, 5, 7, 11, \ldots$ Note, in particular, that 1 is not a prime, nor is 0 or any negative integer.

Primes in other algebraic structures. The notion of a "prime" can be defined in quite general algebraic structures. All that is needed for such a definition to make sense is an analog of the multiplication operation (so that divisibility can be defined), and the notion of "units" (which serve as "trivial" divisors, analogous to the numbers ± 1 among the integers). One can then define a prime as any element in the given structure that can only be factored in a trivial way, in the sense that one of the factors is a unit. The best-known examples of such structures are algebraic integers, which behave in many respects like the ordinary integers, and which form the subject of a separate branch of number theory, **algebraic number theory**.

Another example is given by the ring of polynomials with integer coefficients, with multiplication of ordinary polynomials as ring operation and the constant polynomials ± 1 as "units". The "primes" in such a polynomial

ring turn out to be the irreducible (over $\mathbb{Z}$) polynomials.

0.2 The Fundamental Theorem of Arithmetic

As the name suggests, this result, which we now state, is of fundamental importance in number theory, and many of the results in later chapters depend in a crucial way on this theorem and would fail if the theorem were false.

Theorem 0.1 (Fundamental Theorem of Arithmetic). *Every integer $n > 1$ can be written as a product of primes, and the representation is unique up to the order of the factors.*

The proof of this result, while elementary, is somewhat involved, and we will not give it here. (It can be found in any text on elementary number theory.) We only note here that the crux of the proof lies in showing the *uniqueness* of a prime factorization; the proof of the *existence* of such a factorization is an easy exercise in induction.

Notation. There are several common ways to denote the prime factorization guaranteed by the Fundamental Theorem of Arithmetic. First, we can write the prime factorization of an integer $n \geq 2$ as

$$n = p_1 \dots p_r,$$

where the p_i's are primes, but *not necessarily distinct*.

In most situations it is more useful to combine identical factors in the above representation and write

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

where, this time, the p_i's are *distinct* primes, and the exponents α_i positive integers.

Using the notation $p^m || n$ if p^m is the exact power of p that divides n (i.e., $p^m | n$, but $p^{m+1} \nmid n$), we can write the above representation as

$$n = \prod_{p^m || n} p^m.$$

Yet another useful representation of the prime factorization of n is

$$n = \prod_p p^{\alpha(p)},$$

where the product is extended over *all* prime numbers and the exponents $\alpha(p)$ are nonnegative integers with $\alpha(p) \neq 0$ for at most finitely many p.

The last notation is particularly convenient when working with the greatest common divisor or the least common multiple, since these concepts have a simple description in terms of this notation: Indeed, if n and m are positive integers with prime factorization $n = \prod_p p^{\alpha(p)}$ and $m = \prod_p p^{\beta(p)}$, then the gcd and lcm of n and m are given by

$$(n, m) = \prod_p p^{\min(\alpha(p),\beta(p))}, \quad [n, m] = \prod_p p^{\max(\alpha(p),\beta(p))},$$

respectively. Similarly, divisibility is easily characterized in terms of the exponents arising in the representation: Given $n = \prod_p p^{\alpha(p)}$ and $m = \prod_p p^{\beta(p)}$, we have $m|n$ if and only if $\beta(p) \leq \alpha(p)$ for all p.

With the convention that an empty product is to be interpreted as 1, all of the above formulas remain valid when $n = 1$.

Unique factorization in more general algebraic structures. As mentioned above, the concept of a prime can be defined in very general algebraic structures. One can then ask if an analog of the Fundamental Theorem of Arithmetic also holds in these structures. It turns out that the existence part of this result, i.e., the assertion that every (non-unit) element in the given structure has a representation as a product of "prime" elements, remains valid under very general conditions. By contrast, the uniqueness of such a representation (up to the order of the factors or multiplication by units) is no longer guaranteed and can fail, even in some simple examples. For instance, in the ring of algebraic integers $\{n + m\sqrt{6}i : m, n \in \mathbb{Z}\}$, the number 10 can be factored as $10 = 2 \cdot 5$ and $10 = (2+i\sqrt{6})(2-i\sqrt{6})$, and one can show that each of the four factors $2, 5, 2 \pm i\sqrt{6}$ arising here are "primes" in the appropriate sense.

Beurling generalized primes. By the Fundamental Theorem of Arithmetic the positive integers are exactly the products of the form $(*)$ $\prod_{i \in I} p_i^{\alpha_i}$, where $p_1 < p_2 < \cdots$ is the sequence of primes, I a finite (possibly empty) subset of the positive integers, and the exponents α_i are positive integers. This characterization of the positive integers suggests the following generalization of the concepts of a "prime" and a (positive) "integer", which was first proposed some 50 years ago by Arne Beurling. Instead of starting with an appropriate analog of the integers and then trying to define a notion of a

prime, the idea of Beurling was to start with an appropriate generalization of the primes and then define generalized integers as above in terms of these generalized primes. Specifically, let $\mathcal{P} = \{p_1 < p_2 < \cdots\}$ be an arbitrary sequence of positive numbers (which need not even be integers), and let $\mathbb{N}_{\mathcal{P}}$ be the set of all finite products of the form $(*)$ with the p_i's taken from $\mathcal{P}$. Then $\mathcal{P}$ is called a system of *Beurling generalized primes*, and $\mathbb{N}_{\mathcal{P}}$ the associated system of *Beurling generalized integers*. One can study such systems in great generality, and ask, for instance, how the "growth" of such a sequence of generalized primes is related with that of the associated sequence of generalized integers.

0.3 The infinitude of primes

We conclude this chapter with a proof of the infinitude of primes, a result first proved some two thousand years ago by Euclid.

Theorem 0.2. *There are infinitely many primes.*

Proof. We give here a somewhat nonstandard proof, which, while not as short as some other proofs, has a distinctly analytic flavor. It is based on the following lemma, which is of interest in its own right.

Lemma 0.3. *Let $\mathcal{P} = \{p_1, \dots, p_k\}$ be a finite set of primes, let*

$$\mathbb{N}_{\mathcal{P}} = \{n \in \mathbb{N} : p|n \Rightarrow p \in \mathcal{P}\},$$

i.e., $\mathbb{N}_{\mathcal{P}}$ is the set of positive integers all of whose prime factors belong to the set $\mathcal{P}$ (note that $1 \in \mathbb{N}_{\mathcal{P}}$), and let

$$N_{\mathcal{P}}(x) = \#\{n \in \mathbb{N}_{\mathcal{P}} : n \le x\} \quad (x \ge 1).$$

Then there exist constants c and x_0 (depending on $\mathcal{P}$) such that $N_{\mathcal{P}}(x) \le c(\log x)^k$ for $x \ge x_0$.

Proof. Note that

$$\mathbb{N}_{\mathcal{P}} = \{p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} : a_i \in \mathbb{N}_0\},$$

and that by the Fundamental Theorem of Arithmetic each element in $\mathbb{N}_{\mathcal{P}}$ corresponds to a *unique* k-tuple $(a_1, \dots, a_k)$ of nonnegative integers. Thus,

$$\begin{aligned} \mathbb{N}_{\mathcal{P}}(x) &= \#\{(a_1, \dots, a_k) : a_i \in \mathbb{N}_0, p_1^{a_1} \dots p_k^{a_k} \le x\} \\ &= \#\{(a_1, \dots, a_k) : a_i \in \mathbb{N}_0, a_1 \log p_1 + \cdots + a_k \log p_k \le \log x\}. \end{aligned}$$

Now note that the inequality $a_1 \log p_1 + \cdots + a_k \log p_k \le \log x$ implies $a_i \le \log x / \log p_i \le \log x / \log 2$ for each i. Hence, for each a_i there are at most $[\log x / \log 2] + 1$ choices, and the number of tuples $(a_1, \ldots, a_k)$ counted in $\mathbb{N}_{\mathcal{P}}(x)$ is therefore

$$\le \left(\left[\frac{\log x}{\log 2} \right] + 1 \right)^k .$$

If we now restrict x by $x \ge 2$, then $[\log x / \log 2] + 1 \le 2 \log x / \log 2$, so the above becomes

$$\le \left(2 \frac{\log x}{\log 2} \right)^k = (2/\log 2)^k (\log x)^k .$$

This gives the asserted bound for $\mathbb{N}_{\mathcal{P}}(x)$ with $c = (2/\log 2)^k$ and $x_0 = 2$. □

With this lemma at hand, the infinitude of primes follows easily: If there were only finitely many primes, then we could apply the lemma with $\mathcal{P}$ equal to the set of all primes and, consequently, $\mathbb{N}_{\mathcal{P}}$ the set of all positive integers, so that $\mathbb{N}_{\mathcal{P}}(x) = [x]$ for all $x \ge 1$. But the lemma would give the bound $\mathbb{N}_{\mathcal{P}}(x) \le c(\log x)^k$ for all $x \ge 2$ with some constant c, and since $(\log x)^k / [x]$ tends to zero as $x \to \infty$, this is incompatible with the equality $\mathbb{N}_{\mathcal{P}}(x) = [x]$. □

0.4 Exercises

0.1 Show that there exist arbitrarily large intervals that are free of primes, i.e., for every positive integer k there exist k consecutive positive integers none of which is a prime.

0.2 Call a set of positive integers a *PC-set* if it has the property that any pair of distinct elements of the set is coprime. Given $x \geq 2$, let $N(x) = \max\{|A| : A \subset [2,x],\ A \text{ is a PC-set}\}$, i.e., $N(x)$ is the maximal number of integers with the PC property that one can fit into the interval $[2,x]$. Prove that $N(x)$ is equal to $\pi(x)$, the number of primes $\leq x$.

0.3 A positive integer n is called squarefull if it satisfies $(*)$ $p|n \Rightarrow p^2|n$. (Note that $n = 1$ is squarefull according to this definition, since 1 has no prime divisors and the above implication is therefore trivially true.)

(i) Show that n is squarefull if and only if n can be written in the form $n = a^2b^3$ with $a, b \in \mathbb{N}$.

(ii) Find a similar characterization of "k-full" integers, i.e., integers $n \in \mathbb{N}$ that satisfy $(*)$ with 2 replaced by k (where $k \geq 3$).

0.4 Let $\mathcal{P} = \{p_1, \ldots, p_k\}$ be a finite set of primes, let

$$\mathbb{N}_{\mathcal{P}} = \{n \in \mathbb{N} : p|n \Rightarrow p \in \mathcal{P}\}$$

i.e., $\mathbb{N}_{\mathcal{P}}$ is the set of positive integers all of whose prime factors belong to the set $\mathcal{P}$ (note that $1 \in \mathbb{N}_{\mathcal{P}}$), and let

$$N_{\mathcal{P}}(x) = \#\{n \in \mathbb{N}_{\mathcal{P}} : n \leq x\} \quad (x \geq 1).$$

In Lemma 0.3 we showed that $N_{\mathcal{P}}(x) \leq c_1(\log x)^k$ for a suitable constant c_1 (depending on the set $\mathcal{P}$, but not on x) and for all sufficiently large x, say $x \geq x_1$. Prove that a bound of the same type holds in the other direction, i.e., there exist constants $c_2 > 0$ and x_2, depending on $\mathcal{P}$, such that $N_{\mathcal{P}}(x) \geq c_2(\log x)^k$ holds for all $x \geq x_2$.

Chapter 1

Arithmetic functions I: Elementary theory

1.1 Introduction and basic examples

A simple, but very useful concept in number theory is that of an **arithmetic function**. An arithmetic function is any real- or complex-valued function defined on the set $\mathbb{N}$ of positive integers. (In other words, an arithmetic function is just a *sequence* of real or complex numbers, though this point of view is not particularly useful.)

Examples

(1) **Constant function:** The function defined by $f(n) = c$ for all n, where c is a constant, is denoted by c; in particular, 1 denotes the function that is equal to 1 for all n.

(2) **Unit function:** $e(n)$, defined by $e(1) = 1$ and $e(n) = 0$ for $n \geq 2$.

(3) **Identity function:** $\mathrm{id}(n)$; defined by $\mathrm{id}(n) = n$ for all n.

(4) **Logarithm:** $\log n$, the (natural) logarithm, restricted to $\mathbb{N}$ and regarded as an arithmetic function.

(5) **Moebius function:** $\mu(n)$, defined by $\mu(1) = 1$, $\mu(n) = 0$ if n is not squarefree (i.e., divisible by the square of a prime), and $\mu(n) = (-1)^k$ if n is composed of k *distinct* prime factors (i.e., $n = \prod_i^k p_i$).

(6) **Characteristic function of squarefree integers:** $\mu^2(n)$ or $|\mu(n)|$. From the definition of the Moebius function, it follows that the absolute value (or, equivalently, the square) of μ is the characteristic function of the squarefree integers.

(7) **Liouville function:** $\lambda(n)$, defined by $\lambda(1) = 1$ and $\lambda(n) = (-1)^k$ if n is composed of k *not necessarily distinct* prime factors (i.e., if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ then $\lambda(n) = \prod_{i=1}^{k}(-1)^{\alpha_i}$).

(8) **Euler phi (totient) function:** $\phi(n)$, the number of positive integers $m \leq n$ that are relatively prime to n; i.e., $\phi(n) = \sum_{m=1,(m,n)=1}^{n} 1$.

(9) **Divisor function:** $d(n)$, the number of positive divisors of n (including the trivial divisors $d = 1$ and $d = n$); i.e., $d(n) = \sum_{d|n} 1$. (Another common notation for this function is $\tau(n)$.)

(10) **Sum-of-divisors function:** $\sigma(n)$, the sum over all positive divisors of n; i.e., $\sigma(n) = \sum_{d|n} d$.

(11) **Generalized sum-of-divisors functions:** $\sigma_\alpha(n)$, defined by $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. Here α can be any real or complex parameter. This function generalizes the divisor function ($\alpha = 0$) and the sum-of-divisors function ($\alpha = 1$).

(12) **Number of distinct prime factors:** $\omega(n)$, defined by $\omega(1) = 0$ and $\omega(n) = k$ if $n \geq 2$ and $n = \prod_{i=1}^{k} p_i^{\alpha_i}$; i.e., $\omega(n) = \sum_{p|n} 1$.

(13) **Total number of prime divisors:** $\Omega(n)$, defined in the same way as $\omega(n)$, except that prime divisors are counted with multiplicity. Thus, $\Omega(1) = 0$ and $\Omega(n) = \sum_{i=1}^{k} \alpha_i$ if $n \geq 2$ and $n = \prod_{i=1}^{k} p_i^{\alpha_i}$; i.e., $\Omega(n) = \sum_{p^m|n} 1$. For squarefree integers n, the functions $\omega(n)$ and $\Omega(n)$ are equal and are related to the Moebius function by $\mu(n) = (-1)^{\omega(n)}$. For all integers n, $\lambda(n) = (-1)^{\Omega(n)}$.

(14) **Ramanujan sums:** Given a positive integer q, the Ramanujan sum c_q is the arithmetic function defined by $c_q(n) = \sum_{a=1,(a,q)=1}^{q} e^{2\pi i a n/q}$.

(15) **Von Mangoldt function:** $\Lambda(n)$, defined by $\Lambda(n) = 0$ if n is not a prime power, and $\Lambda(p^m) = \log p$ for any prime power p^m.

1.2 Additive and multiplicative functions

Many important arithmetic functions are multiplicative or additive functions, in the sense of the following definition.

Definition. An arithmetic function f is called **multiplicative** if $f \not\equiv 0$ and

$$f(n_1 n_2) = f(n_1) f(n_2) \quad \text{whenever } (n_1, n_2) = 1; \tag{1.1}$$

f is called **additive** if it satisfies

$$f(n_1 n_2) = f(n_1) + f(n_2) \quad \text{whenever } (n_1, n_2) = 1. \tag{1.2}$$

If this condition holds without the restriction $(n_1, n_2) = 1$, then f is called **completely (or totally) multiplicative** resp. **completely (or totally) additive**.

The condition (1.1) can be used to prove the multiplicativity of a given function. (There are also other, indirect, methods for establishing multiplicativity, which we will discuss in the following sections.) However, in order to exploit the multiplicativity of a function known to be multiplicative, the criterion of the following theorem is usually more useful.

Theorem 1.1 (Characterization of multiplicative functions). *An arithmetic function f is multiplicative if and only if $f(1) = 1$ and, for $n \geq 2$,*

$$f(n) = \prod_{p^m || n} f(p^m). \tag{1.3}$$

The function f is completely multiplicative if and only if the above condition is satisfied and, in addition, $f(p^m) = f(p)^m$ for all prime powers p^m.

Remarks. (i) The result shows that a multiplicative function is uniquely determined by its values on prime powers, and a completely multiplicative function is uniquely determined by its values on primes.

(ii) With the convention that an empty product is to be interpreted as 1, the condition $f(1) = 1$ can be regarded as the special case $n = 1$ of (1.3). With this interpretation, f is multiplicative if and only if f satisfies (1.3) for all $n \in \mathbb{N}$.

Proof. Suppose first that f satisfies $f(1) = 1$ and (1.3) for $n \geq 2$. If n_1 and n_2 are positive integers with $(n_1, n_2) = 1$, then the prime factorizations of n_1 and n_2 involve disjoint sets of prime powers, so expressing each of $f(n_1)$,

$f(n_2)$, and $f(n_1 n_2)$ by (1.3) we see that f satisfies (1.1). Moreover, since $f(1) = 1$, f cannot be identically 0. Hence f is multiplicative.

Conversely, suppose that f is multiplicative. Then f is not identically 0, so there exists $n \in \mathbb{N}$ such that $f(n) \neq 0$. Applying (1.3) with $(n_1, n_2) = (n, 1)$, we obtain $f(n) = f(1 \cdot n) = f(1)f(n)$, which yields $f(1) = 1$, upon dividing by $f(n)$.

Next, let $n \geq 2$ be given with prime factorization $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. "Shaving off" prime powers one at a time, and applying (1.3) inductively, we have

$$\begin{aligned} f(n) &= f\left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) = f\left(p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}}\right) f\left(p_k^{\alpha_k}\right) \\ &= \cdots = f\left(p_1^{\alpha_1}\right) \cdots f\left(p_k^{\alpha_k}\right), \end{aligned}$$

so (1.3) holds.

If f is completely multiplicative, then for any prime power p^m we have

$$f(p^m) = f(p^{m-1} \cdot p) = f(p^{m-1})f(p) = \cdots = f(p)^{m-1}.$$

Conversely, if f is multiplicative and satisfies $f(p^m) = f(p)^m$ for all prime powers p^m, then (1.3) can be written as $f(n) = \prod_{i=1}^{r} f(p_i)$, where now $n = \prod_{i=1}^{r} p_i$ is the factorization of n into single *(not necessarily distinct)* prime factors p_i. Since, for any two positive integers n_1 and n_2, the product of the corresponding factorizations is the factorization of the product, it follows that the multiplicativity property $f(n_1 n_2) = f(n_1)f(n_2)$ holds for any pair (n_1, n_2) of positive integers. Hence f is completely multiplicative. □

Theorem 1.2 (Products and quotients of multiplicative functions). *Assume f and g are multiplicative function. Then:*

(i) The (pointwise) product fg defined by $(fg)(n) = f(n)g(n)$ is multiplicative.

(ii) If g is non-zero, then the quotient f/g (again defined pointwise) is multiplicative.

Proof. The result is immediate from the definition of multiplicativity. □

Analogous properties hold for additive functions: an additive function satisfies $f(1) = 0$ and $f(n) = \sum_{p^m || m} f(p^m)$, and the pointwise sums and differences of additive functions are additive.

Tables 1.1 and 1.2 below list the most important multiplicative and additive arithmetic functions, along with their values at prime powers, and basic properties. (Properties that are not obvious from the definition will be established in the following sections.)

Function	**value at n**	**value at p^m**	**properties**
$e(n)$	1 if $n = 1$, 0 else	0	unit element w.r.t. Dirichlet product, $\boxed{e * f = f * e = f}$
$\mathrm{id}(n)$ (identity function)	n	p^m	
$s(n)$ (char. fct. of squares)	1 if $n = m^2$ with $m \in \mathbb{N}$, 0 else	1 if m is even, 0 if m is odd	
$\mu^2(n)$ (char. fct. of squarefree integers)	1 if n is squarefree, 0 else	1 if $m = 1$, 0 if $m > 1$	
$\mu(n)$ (Moebius function)	1 if $n = 1$, $(-1)^k$ if $n = \prod_{i=1}^k p_i$ (p_i distinct), 0 otherwise	-1 if $m = 1$, 0 if $m > 1$	$\sum_{d\|n} \mu(d) = 0$ if $n \geq 2$ $\boxed{\mu * 1 = e}$
$\lambda(n)$ (Liouville function)	1 if $n = 1$, $(-1)^{\sum_{i=1}^k \alpha_i}$ if $n = \prod_{i=1}^k p_i^{\alpha_i}$	$(-1)^m$	$\sum_{d\|n} \lambda(d) = n^2$ $\boxed{\lambda * 1 = s}$
$\phi(n)$ (Euler phi function)	$\#\{1 \leq m \leq n : (m, n) = 1\}$	$p^m(1 - 1/p)$	$\sum_{d\|n} \phi(d) = n$ $\boxed{\phi * 1 = \mathrm{id}}$
$d(n)\,(= \tau(n))$ (divisor function)	$\sum_{d\|n} 1$	$m + 1$	$\boxed{d = 1 * 1}$
$\sigma(n)$ (sum of divisor function)	$\sum_{d\|n} d$	$\dfrac{p^{m+1} - 1}{p - 1}$	$\boxed{\sigma = 1 * \mathrm{id}}$

Table 1.1: Some important multiplicative functions

Function	**value at n**	**value at p^m**	**properties**
$\omega(n)$ (number of distinct prime factors)	0 if $n = 1$, k if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$	1	additive
$\Omega(n)$ (total number of prime factors)	0 if $n = 1$, $\sum_{i=1}^{k} \alpha_i$ if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$	m	completely additive
$\log n$ (logarithm)	$\log n$	$\log p^m$	completely additive
$\Lambda(n)$ (von Mangoldt function)	$\log p$ if $n = p^m$, 0 if n is not a prime power	$\log p$	neither additive nor multiplicative $\boxed{\log = \Lambda * 1}$

Table 1.2: Some other important arithmetic functions

1.3 The Moebius function

The fundamental property of the Moebius function is given in the following theorem.

Theorem 1.3 (Moebius identity). *For all $n \in \mathbb{N}$, $\sum_{d|n} \mu(d) = e(n)$; i.e., the sum $\sum_{d|n} \mu(d)$ is zero unless $n = 1$, in which case it is 1.*

Proof. There are many ways to prove this important identity; we give here a combinatorial proof that does not require any special tricks or techniques. We will later give alternate proofs, which are simpler and more elegant, but which depend on some results in the theory of arithmetic functions.

If $n = 1$, then the sum $\sum_{d|n} \mu(d)$ reduces to the single term $\mu(1) = 1$, so the asserted formula holds in this case. Next, suppose $n \geq 2$ and let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ be the canonical prime factorization of n. Since $\mu(d) = 0$ if d is not squarefree, the sum over d can be restricted to divisors of the form $d = \prod_{i \in I} p_i$, where $I \subset \{1, 2, \ldots, k\}$, and each such divisor contributes a

term $\mu(d) = (-1)^{|I|}$. Hence,

$$\sum_{d|n} \mu(d) = \sum_{I \subset \{1,\ldots,k\}} (-1)^{|I|}.$$

Now note that, for any $r \in \{0, 1, \ldots, k\}$, there are $\binom{k}{r}$ subsets I with $|I| = r$, and for each such subset the summand $(-1)^{|I|}$ is equal to $(-1)^r$. Hence the above sum reduces to

$$\sum_{r=0}^{k} (-1)^r \binom{k}{r} = (1-1)^k = 0,$$

by the binomial theorem. (Note that $k \geq 1$, since we assumed $n \geq 2$.) Hence we have $\sum_{d|n} \mu(d) = 0$ for $n \geq 2$, as claimed. □

Motivation for the Moebius function. The identity given in this theorem is the main reason for the peculiar definition of the Moebius function, which may seem rather artificial. In particular, the definition of $\mu(n)$ as 0 when n is not squarefree appears to be unmotivated. The Liouville function $\lambda(n)$, which is identical to the Moebius function on squarefree integers, but whose definition extends to non-squarefree integers in a natural way, appears to be a much more natural function to work with. However, this function does not satisfy the identity of the theorem, and it is this identity that underlies most of the applications of the Moebius function.

Application: Evaluation of sums involving a coprimality condition. The identity of the theorem states that $\sum_{d|n} \mu(d)$ is the characteristic function of the integer $n = 1$. This fact can be used to extract specific terms from a series. A typical application is the evaluation of sums over integers n that are relatively prime to a given integer k. By the theorem, the characteristic function of integers n with $(n, k) = 1$ is given by $\sum_{d|(n,k)} \mu(d)$. Since the condition $d|(n, k)$ is equivalent to the simultaneous conditions $d|n$ and $d|k$, one can formally rewrite a sum $\sum_{n,(n,k)=1} f(n)$ as follows:

$$\begin{aligned}\sum_{\substack{n \\ (n,k)=1}} f(n) &= \sum_{n} f(n) e((n,k)) = \sum_{n} f(n) \sum_{d|(n,k)} \mu(n) \\ &= \sum_{d|k} \mu(d) \sum_{\substack{n \\ d|n}} f(n) = \sum_{d|k} \mu(d) \sum_{m} f(dm).\end{aligned}$$

The latter sum can usually be evaluated, and doing so yields a formula for the original sum. (Of course, one has to make sure that the series involved converge.) The following examples illustrate the general method.

Evaluation of the Euler phi function. By definition, the Euler phi function is given by $\phi(n) = \sum_{m \le n, (m,n)=1} 1$. Eliminating the coprimality condition $(m, n) = 1$, as indicated above, yields the identity

$$\phi(n) = \sum_{m \le n} \sum_{d \mid (m,n)} \mu(d) = \sum_{d \mid n} \mu(d) \sum_{m \le n, d \mid m} 1 = \sum_{d \mid n} \mu(d)(n/d).$$

(For an alternative proof of this identity see Section 1.7.)

Ramanujan sums. The functions $c_q(n) = \sum_{a=1,(a,q)=1}^{q} \exp(2\pi i a n/q)$, where q is a positive integer, are called Ramanujan sums. By eliminating the condition $(a, q) = 1$ using the above method, one can show that $c_q(n) = \sum_{d \mid (q,n)} d\mu(q/d)$. When $n = 1$, this formula reduces to $c_q(1) = \mu(q)$, and we obtain the remarkable identity $\sum_{a=1,(a,q)=1}^{q} \exp(2\pi i a/q) = \mu(q)$, which shows that the sum over all "primitive" k-th roots of unity is equal to $\mu(q)$.

A weighted average of the Moebius function. While the estimation of the partial sums of the Moebius function $\sum_{n \le x} \mu(n)$ is a very deep (and largely unsolved) problem, remarkably enough a weighted version of this sum, namely $\sum_{n \le x} \mu(n)/n$ is easy to bound. In fact, we will prove:

Theorem 1.4. *For any real $x \ge 1$ we have*

$$\left| \sum_{n \le x} \frac{\mu(n)}{n} \right| \le 1. \tag{1.4}$$

Proof. Note first that, without loss of generality, one can assume that $x = N$, where N is a positive integer. We then evaluate the sum $S(N) = \sum_{n \le N} e(n)$ in two different ways. On the one hand, by the definition of $e(n)$, we have $S(N) = 1$; on the other hand, writing $e(n) = \sum_{d \mid n} \mu(d)$ and interchanging summations, we obtain $S(N) = \sum_{d \le N} \mu(d)[N/d]$, where $[t]$ denotes the greatest integer $\le t$. Now, for $d \le N - 1$, $[N/d]$ differs from N/d by an amount that is bounded by 1 in absolute value, while for $d = N$, the

quantities $[N/d]$ and N/d are equal. Replacing $[N/d]$ by N/d and bounding the resulting error, we therefore obtain

$$\left| S(N) - N \sum_{d \le N} \frac{\mu(d)}{d} \right| \le \sum_{d \le N} |\mu(d)| \cdot |[N/d] - (N/d)| \le \sum_{d \le N-1} |\mu(d)| \le N - 1.$$

Hence,

$$\left| N \sum_{d \le N} \frac{\mu(d)}{d} \right| \le (N-1) + |S(N)| = (N-1) + 1 = N,$$

which proves (1.4). □

The Moebius function and the Prime Number Theorem. Part of the interest in studying the Moebius function stems from the fact that the behavior of this function is intimately related to the Prime Number Theorem (PNT), which says that the number $\pi(x)$ of primes below x is asymptotically equal to $x/\log x$ as $x \to \infty$ and which is one of the main results of Analytic Number Theory. We will show later that the PNT is "equivalent" to the fact that $\mu(n)$ has average value ("mean value") zero, i.e., $\lim_{x\to\infty}(1/x)\sum_{n\le x}\mu(n) = 0$. The latter statement can has the following probabilistic interpretation: If a squarefree integer is chosen at random, then it is equally likely to have an even and an odd number of prime factors.

Mertens' conjecture. A famous conjecture, attributed to Mertens (though it apparently was first stated by Stieltjes who mistakenly believed that he had proved it) asserts that $|\sum_{n\le x}\mu(n)| \le \sqrt{x}$ for all $x \ge 1$. This conjecture had remained open for more than a century, but was disproved (though only barely!) in 1985 by A. Odlyzko and H. te Riele, who used extensive computer calculations, along with some theoretical arguments, to show that the above sum exceeds $1.06\sqrt{x}$ for infinitely many x. Whether the constant 1.06 can be replaced by any constant c is still an open problem. Heuristic arguments, based on the assumption that the values ± 1 of the Moebius function on squarefree integers are distributed like a random sequence of numbers ± 1, strongly suggest that this is the case, but a proof has remained elusive so far.

1.4 The Euler phi (totient) function

Theorem 1.5. *The Euler phi function satisfies:*

(i) $\sum_{d|n} \phi(d) = n$ *for all* $n \in \mathbb{N}$.

(ii) $\phi(n) = \sum_{d|n} \mu(d)(n/d)$.

(iii) ϕ *is multiplicative.*

(iv) $\phi(n) = \prod_{p^m||n}(p^m - p^{m-1}) = n\prod_{p|n}(1 - 1/p)$ *for all* $n \in \mathbb{N}$.

Proof. (i) Split the set $A = \{1, 2, \ldots, n\}$ into the pairwise disjoint subsets $A_d = \{m \in A : (m, n) = d\}$, $d|n$. Writing an element $m \in A_d$ as $m = dm'$, we see that $A_d = \{dm' : 1 \leq m' \leq n/d, (m', n/d) = 1\}$, and so $|A_d| = \phi(n/d)$. Since $n = |A| = \sum_{d|n} |A_d|$, it follows that $n = \sum_{d|n} \phi(n/d)$. Writing $d' = n/d$ and noting that, as d runs over all positive divisors of n, so does d', we obtain the desired identity.

(ii) This identity was proved in the last section. Alternatively, as we shall show in Section 1.7, one can derive it from the identity (i).

(ii) We defer the proof of the multiplicativity until Section 1.7.

(iv) This follows immediately from the multiplicativity of ϕ and the fact that, at $n = p^m$, $\phi(p^m) = p^m - p^{m-1}$. To see the latter formula, note that an integer is relatively prime to p^m if and only if it is not a multiple of p and that of the p^m positive integers $\leq p^m$ exactly p^{m-1} are multiples of p. □

Formula (iii) of the theorem can be used to quickly compute values of ϕ. For example, the first 7 values are $\phi(1) = 1$, $\phi(2) = (2 - 1) = 1$, $\phi(3) = (3-1) = 2$, $\phi(4) = (2^2-2) = 2$, $\phi(5) = (5-1) = 4$, $\phi(6) = \phi(2\cdot 3) = (2 - 1)(3 - 1) = 2$, $\phi(7) = (7 - 1) = 6$.

Carmichael's conjecture. It is easy to see that not every positive integer occurs as a value of ϕ; for example, $\phi(n)$ is never equal to an odd prime. In other words, the range of ϕ is a proper subset of $\mathbb{N}$. At the beginning of this century, R.D. Carmichael, a professor at the University of Illinois and author of a textbook on number theory, observed that there seems to be no integer that appears exactly once as a value of ϕ; in other words, for each $m \in \mathbb{N}$, the pre-image $\phi^{-1}(m) = \{n \in \mathbb{N} : \phi(n) = m\}$ has either cardinality 0 or has cardinality ≥ 2. In fact, Carmichael claimed to have a proof of this result and included the "proof" as an exercise in his number theory textbook, but his "proof" was incorrect, and he later retracted the claim; he changed the

wording of the exercise, calling the result an "empirical theorem." This "empirical theorem" is still open to this date, and has become a famous conjecture, known as "Carmichael's conjecture," The numerical evidence for the conjecture is overwhelming: the conjecture (that the cardinality of $\phi^{-1}(m)$ is never 1) is true for values m up to $10^{10^{10}}$. While the conjecture is still open, Kevin Ford, a former UIUC graduate student and now a faculty member here, proved a number of related conjectures. In particular, he showed that for every integer $k \geq 2$ there exist infinitely many m such that $\phi^{-1}(m)$ has cardinality k. This was known as "Sierpinski's conjecture", and it complements Carmichael's conjecture which asserts that in the case $k = 1$, the only case not covered by Sierpinski's conjecture, the assertion of Sierpinski's conjecture is not true.

1.5 The von Mangoldt function

The definition of the von Mangoldt function may seem strange at first glance. One motivation for this peculiar definition lies in the following identity.

Theorem 1.6. *We have*

$$\sum_{d|n} \Lambda(d) = \log n \quad (n \in \mathbb{N}).$$

Proof. For $n = 1$, the identity holds since $\Lambda(1) = 0 = \log 1$. For $n \geq 2$ we have, by the definition of Λ,

$$\sum_{d|n} \Lambda(d) = \sum_{p^m|n} \log p = \log n.$$

(For the last step note that, for each prime power $p^\alpha||n$, each of the terms $p^1, p^2, \ldots, p^\alpha$ contributes a term $\log p$ to the sum, so the total contribution arising from powers of p is $\alpha(\log p) = \log p^\alpha$. Adding up those contributions over all prime powers $p^\alpha||n$, gives $\sum_{p^\alpha||n} \log p^\alpha = \log \prod_{p^\alpha||n} p^\alpha = \log n$.) □

The main motivation for introducing the von Mangoldt function is that the partial sums $\sum_{n\leq x} \Lambda(n)$ represent a weighted count of the prime powers $p^m \leq x$, with the weights being $\log p$, the "correct" weights to offset the density of primes. It is not hard to show that higher prime powers (i.e., those with $m \geq 2$) contribute little to the above sum, so the sum is essentially a weighted sum over prime numbers. In fact, studying the asymptotic behavior of the above sum is essentially equivalent to studying the behavior

of the prime counting function $\pi(x)$; for example, the PNT is equivalent to the assertion that $\lim_{x\to\infty}(1/x)\sum_{n\le x}\Lambda(n) = 1$. In fact, most proofs of the PNT proceed by first showing the latter relation, and then deducing from this the original form of the PNT. The reason for doing this is that, because of the identity in the above theorem (and some similar relations), working with $\Lambda(n)$ is technically easier than working directly with the characteristic function of primes.

1.6 The divisor and sum-of-divisors functions

Theorem 1.7. *The divisor function $d(n)$ and the sum-of-divisors function $\sigma(n)$ are multiplicative. Their values at prime powers are given by*

$$d(p^m) = m+1, \quad \sigma(p^m) = \frac{p^{m+1}-1}{p-1}.$$

Proof. To prove the multiplicativity of $d(n)$, let n_1 and n_2 be positive integers with $(n_1, n_2) = 1$. Note that if $d_1|n_1$ and $d_2|n_2$, then $d_1d_2|n_1n_2$. Conversely, by the coprimality condition and the fundamental theorem of arithmetic, any divisor d of n_1n_2 factors *uniquely* into a product $d = d_1d_2$, where $d_1|n_1$ and $d_2|n_2$. Thus, there is a $1-1$ correspondence between the set of divisors of n_1n_2 and the set of pairs (d_1, d_2) with $d_1|n_1$ and $d_2|n_2$. Since there are $d(n_1)d(n_2)$ such pairs and $d(n_1n_2)$ divisors of n_1n_2, we obtain $d(n_1n_2) = d(n_1)d(n_2)$, as required. The multiplicativity of $\sigma(n)$ can be proved in the same way. (Alternate proofs of the multiplicativity of d and σ will be given in the following section.)

The given values for $d(p^m)$ and $\sigma(p^m)$ are obtained on noting that the divisors of p^m are exactly the numbers $p^0, p^1, \ldots, p^m$. Since there are $m+1$ such divisors, we have $d(p^m) = m+1$, and applying the geometric series formula to the sum of these divisors gives the asserted formula for $\sigma(p^m)$. □

Perfect numbers. The sum-of-divisors function is important because of its connection to so-called **perfect numbers**, that is, positive integers n that are equal to the sum of all their *proper* divisors, i.e., all positive divisors except n itself. Since the divisor $d = n$ is counted in the definition of $\sigma(n)$, the sum of proper divisors of n is $\sigma(n) - n$. Thus, *an integer n is perfect if and only if $\sigma(n) = 2n$*. For example, 6 is perfect, since $6 = 1+2+3$. It is an unsolved problem whether there exist infinitely many perfect numbers. However, a result of Euler states:

Theorem (Euler). *An* even *integer n is perfect if and only if n is of the form $n = 2^{p-1}(2^p - 1)$ where p is a prime and $2^p - 1$ is also prime.*

This result is not hard to prove, using the multiplicity of $\sigma(n)$. The problem with this characterization is that it is not known whether there exist infinitely many primes p such that $2^p - 1$ is also prime. (Primes of this form are called Mersenne primes, and whether there exist infinitely many of these is another famous open problem.)

There is no analogous characterization of odd perfect numbers; in fact, no single odd perfect number has been found, and it is an open problem whether odd perfect numbers exist.

1.7 The Dirichlet product of arithmetic functions

The two obvious operations on the set of arithmetic functions are pointwise addition and multiplication. The constant functions $f = 0$ and $f = 1$ are neutral elements with respect to these operations, and the additive and multiplicative inverses of a function f are given by $-f$ and $1/f$, respectively.

While these operations are sometimes useful, by far the most important operation among arithmetic functions is the so-called **Dirichlet product**, an operation that, at first glance, appears mysterious and unmotivated, but which has proved to be an extremely useful tool in the theory of arithmetic functions.

Definition. Given two arithmetic functions f and g, the **Dirichlet product** (or **Dirichlet convolution**) of f and g, denoted by $f * g$, is the arithmetic function defined by

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

In particular, we have $(f * g)(1) = f(1)g(1)$, $(f * g)(p) = f(1)g(p) + f(p)g(1)$ for any prime p, and $(f * g)(p^m) = \sum_{k=0}^{m} f(p^k)g(p^{m-k})$ for any prime power p^m.

It is sometimes useful to write the Dirichlet product in the symmetric form

$$(f * g)(n) = \sum_{ab=n} f(a)g(b),$$

where the summation runs over all pairs (a, b) of positive integers whose product equals n. The equivalence of the two definitions follows immediately

from the fact that the pairs $(d, n/d)$, where d runs over all divisors of n, are exactly the pairs (a, b) of the above form.

One motivation for introducing this product is the fact that the definitions of many common arithmetic functions have the form of a Dirichlet product, and that many identities among arithmetic functions can be written concisely as identities involving Dirichlet products. Here are some examples:

Examples

(1) $d(n) = \sum_{d|n} 1$, so $d = 1 * 1$.

(2) $\sigma(n) = \sum_{d|n} d$, so $\sigma = \mathrm{id} * 1$.

(3) $\sum_{d|n} \mu(d) = e(n)$ (see Theorem 1.3), so $\mu * 1 = e$.

(4) $\sum_{d|n} \mu(d)(n/d) = \phi(n)$ (one of the applications of the Moebius identity, Theorem 1.3), so $\mu * \mathrm{id} = \phi$.

(5) $\sum_{d|n} \phi(d) = n$ (Theorem 1.5), so $\phi * 1 = \mathrm{id}$.

(6) $\sum_{d|n} \Lambda(d) = \log n$ (Theorem 1.6), so $\Lambda * 1 = \log$.

A second motivation for defining the Dirichlet product in the above manner is that this product has nice algebraic properties.

Theorem 1.8 (Properties of the Dirichlet product).

(i) The function e acts as a unit element for $*$, i.e., $f * e = e * f = f$ for all arithmetic functions f.

(ii) The Dirichlet product is commutative, i.e., $f * g = g * f$ for all f and g.

(iii) The Dirichlet product is associative, i.e., $(f * g) * h = f * (g * h)$ for all f, g, h.

(iv) If $f(1) \neq 0$, then f has a unique Dirichlet inverse, i.e., there is a unique function g such that $f * g = e$.

Proof. (i) follows immediately from the definition of the Dirichlet product. For the proof of (ii) (commutativity) and (iii) (associativity) it is useful to work with the symmetric version of the Dirichlet product, i.e., $(f * g)(n) = \sum_{ab=n} f(a)g(b)$. The commutativity of $*$ is immediate from

this representation. To obtain the associativity, we apply this representation twice to get

$$((f*g)*h)(n) = \sum_{dc=n} (f*g)(d)h(c) = \sum_{dc=n}\sum_{ab=d} f(a)g(b)h(c)$$
$$= \sum_{abc=n} f(a)g(b)h(c),$$

where the last sum runs over all triples (a,b,c) of positive integers whose product is equal to n. Replacing (f,g,h) by (g,h,f) in this formula yields the same final (triple) sum, and we conclude that $(f*g)*h = (g*h)*f = f*(g*h)$, proving that $*$ is associative.

It remains to prove (iv). Let f be an arithmetic function with $f(1) \neq 0$. By definition, a function g is a Dirichlet inverse of f if $(f*g)(1) = e(1) = 1$ and $(f*g)(n) = e(n) = 0$ for all $n \geq 2$. Writing out the Dirichlet product $(f*g)(n)$, we see that this is equivalent to the infinite system of equations

$$(A_1) \qquad f(1)g(1) = 1,$$
$$(A_n) \qquad \sum_{d|n} g(d)f(n/d) = 0 \quad (n \geq 2).$$

We need to show that the system $(A_n)_{n=1}^{\infty}$ has a unique solution g. We do this by inductively constructing the values $g(n)$ and showing that these values are uniquely determined.

For $n = 1$, equation (A_1) gives $g(1) = 1/f(1)$, which is well defined since $f(1) \neq 0$. Hence, $g(1)$ is uniquely defined and (A_1) holds. Let now $n \geq 2$, and suppose we have shown that there exist unique values $g(1), \ldots, g(n-1)$ so that equations (A_1)–(A_{n-1}) hold. Since $f(1) \neq 0$, equation (A_n) is equivalent to

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} g(d)f(n/d). \tag{1.5}$$

Since the right-hand side involves only values $g(d)$ with $d < n$, this determines $g(n)$ uniquely, and defining $g(n)$ by (1.5) we see that (A_n) (in addition to (A_1)–(A_{n-1})) holds. This completes the induction argument. □

Examples

(1) Since $\mu * 1 = e$, the Moebius function is the Dirichlet inverse of the function 1.

(2) Multiplying the identity $\phi = \mu * \mathrm{id}$ (obtained in the last section) by 1 gives $\phi * 1 = 1 * \phi = 1 * \mu * \mathrm{id} = e * \mathrm{id} = \mathrm{id}$, so we get the identity $\phi * 1 = \mathrm{id}$ stated in Theorem 1.5.

The last example is a special case of an important general principle, which we state as a theorem.

Theorem 1.9 (Moebius inversion formula). *If $g(n) = \sum_{d|n} f(d)$ for all $n \in \mathbb{N}$, then $f(n) = \sum_{d|n} g(d)\mu(n/d)$ for all n.*

Proof. The given relation can be written as $g = f * 1$. Taking the Dirichlet product of each side in this relation with the function μ we obtain $g * \mu = (f * 1) * \mu = f * (1 * \mu) = f * e = f$, which is the asserted relation. □

Finally, a third motivation for the definition of the Dirichlet product is that it preserves the important property of multiplicativity of a function, as shown in the following theorem. This is, again, by no means obvious.

Theorem 1.10 (Dirichlet product and multiplicative functions).

(i) If f and g are multiplicative, then so is $f * g$.

(ii) If f is multiplicative, then so is the Dirichlet inverse f^{-1}.

(iii) If $f * g = h$ and if f and h are multiplicative, then so is g.

(iv) (Distributivity with pointwise multiplication) If h is completely multiplicative, then $h(f * g) = (hf) * (hg)$ for any functions f and g.

Remarks. (i) The product of two *completely* multiplicative functions is multiplicative (by the theorem), but not necessarily completely multiplicative. For example, the divisor function $d(n)$ can be expressed as a product $1 * 1$ in which each factor 1 is completely multiplicative, but the divisor function itself is only multiplicative in the restricted sense (i.e., with the coprimality condition). The same applies to the Dirichlet inverse: if f is completely multiplicative, then f^{-1} is multiplicative, but in general not completely multiplicative.

(ii) By Theorem 1.8, any function f with $f(1) \neq 0$ has a Dirichlet inverse. Since a multiplicative function satisfies $f(1) = 1$, any multiplicative function has a Dirichlet inverse.

(iii) Note that the distributivity asserted in property (iv) only holds when the function h is *completely* multiplicative. (In fact, one can show that this property characterizes completely multiplicative functions: If h is any non-zero function for which the identity in (iv) holds for all functions f and g, then h is necessarily completely multiplicative.)

Proof. (i) Let f and g be multiplicative and let $h = f * g$. Given n_1 and n_2 with $(n_1, n_2) = 1$, we need to show that $h(n_1 n_2) = h(n_1)h(n_2)$. To this end we use the fact (see the proof of Theorem 1.7) that each divisor $d|n_1 n_2$ can be factored uniquely as $d = d_1 d_2$ with $d_1|n_1$ and $d_2|n_2$, and that, conversely, given any pair (d_1, d_2) with $d_1|n_1$ and $d_2|n_2$, the product $d = d_1 d_2$ satisfies $d|n_1 n_2$. Hence

$$h(n_1 n_2) = \sum_{d|n_1 n_2} f(d)g(n_1 n_2/d) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1 d_2)g((n_1 n_2)/(d_1 d_2)).$$

Since $(n_1, n_2) = 1$, any divisors $d_1|n_1$ and $d_2|n_2$ satisfy $(d_1, d_2) = 1$ and $(n_1/d_1, n_2/d_2) = 1$. Hence, in the above double sum we can apply the multiplicativity of f and g to obtain

$$\begin{aligned} h(n_1 n_2) &= \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)g(n/d_1)f(d_2)g(n_2/d_2) \\ &= (f * g)(n_1)(f * g)(n_2) = h(n_1)h(n_2), \end{aligned}$$

which is what we had to prove.

(ii) Let f be a multiplicative function and let g be the Dirichlet inverse of f. We prove the multiplicativity property

$$g(n_1 n_2) = g(n_1)g(n_2) \text{ if } (n_1, n_2) = 1 \tag{1.6}$$

by induction on the product $n = n_1 n_2$. If $n_1 n_2 = 1$, then $n_1 = n_2 = 1$, and (1.6) holds trivially. Let $n \geq 2$ be given, and suppose (1.6) holds whenever $n_1 n_2 < n$. Let n_1 and n_2 be given with $n_1 n_2 = n$ and $(n_1, n_2) = 1$. Applying the identity (A_n) above, we obtain, on using the multiplicativity of f and that of g for arguments $< n$,

$$\begin{aligned} 0 &= \sum_{d|n_1 n_2} f(d)g(n_1 n_2/d) \\ &= \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)f(d_2)g(n_1/d_1)g(n_2/d_2) + (g(n_1 n_2) - g(n_1)g(n_2)) \\ &= (f * g)(n_1)(f * g)(n_2) + (g(n_1 n_2) - g(n_1)g(n_2)) \\ &= e(n_1)e(n_2) + (g(n_1 n_2) - g(n_1)g(n_2)), \\ &= g(n_1 n_2) - g(n_1)g(n_2), \end{aligned}$$

since, by our assumption $n = n_1 n_2 \geq 2$, at least one of n_1 and n_2 must be ≥ 2, and so $e(n_1)e(n_2) = 0$. Hence we have $g(n_1 n_2) = g(n_1)g(n_2)$. Thus,

(1.6) holds for pairs (n_1, n_2) of relatively prime integers with $n_1 n_2 = n$, and the induction argument is complete.

(iii) The identity $f * g = h$ implies $g = f^{-1} * h$, where f^{-1} is the Dirichlet inverse of f. Since f and h are multiplicative functions, so is f^{-1} (by (ii)) and $f^{-1} * h$ (by (i)). Hence g is multiplicative as well.

(iv) If h is completely multiplicative, then for any divisor $d|n$ we have $h(n) = h(d)h(n/d)$. Hence, for all n,

$$\begin{aligned} h(f*g)(n) &= h(n) \sum_{d|n} f(d)g(n/d) = \sum_{d|n} h(d)f(d)h(n/d)g(n/d) \\ &= ((hf) * (hg))(n), \end{aligned}$$

proving (iv). □

Application I: Proving identities for multiplicative arithmetic functions. The above results can be used to provide simple proofs of identities for arithmetic functions, using the multiplicativity of the functions involved. To prove an identity of the form $f * g = h$ in the case when f, g, and h are known to be multiplicative functions, one simply shows, by direct calculation, that $(*)$ $(f * g)(p^m) = h(p^m)$ holds for every prime power p^m. Since, by the above theorem, the multiplicativity of f and g implies that of $f * g$, and since multiplicative functions are uniquely determined by their values at prime powers, $(*)$ implies that the identity $(f * g)(n) = h(n)$ holds for all $n \in \mathbb{N}$.

Examples

(1) **Alternate proof of the identity $\sum_{d|n} \mu(d) = e(n)$.** The identity can be written as $\mu * 1 = e$, and since all three functions involved are multiplicative, it suffices to verify that the identity holds on prime powers. Since $e(p^m) = 0$ and $(\mu * 1)(p^m) = \sum_{k=0}^{m} \mu(p^k) = 1 - 1 + 0 - 0 \cdots = 0$, this is indeed the case.

(2) **Proof of $\sum_{d|n} \mu^2(d)/\phi(d) = n/\phi(n)$.** This identity is of the form $f * 1 = g$ with $f = \mu^2/\phi$ and $g = \mathrm{id}\,/\phi$. The functions f and g are both quotients of multiplicative functions and therefore are multiplicative. Hence all three functions in the identity $f * 1 = g$ are multiplicative, and it suffices to verify the identity at prime powers. We have $g(p^m) = p^m/\phi(p^m) = p^m/(p^m - p^{m-1}) = (1 - 1/p)^{-1}$, and $(f * 1)(p^m) = \sum_{k=0}^{m} (\mu^2(p^k)/\phi(p^k)) = 1 + 1/(p-1) = (1 - 1/p)^{-1}$, and

so $g(p^m) = (f * 1)(p^m)$ for every prime power p^m. Thus the identity holds at prime powers, and therefore it holds in general.

(3) **The Dirichlet inverse of λ.** Since $\mu * 1 = e$, the function 1 is the Dirichlet inverse of the Moebius function. To find the Dirichlet inverse of λ, i.e., the unique function f such that $\lambda * f = e$, note first that since λ and e are both multiplicative, f must be multiplicative as well, and it therefore suffices to evaluate f at prime powers. Now, for any prime power p^m,

$$0 = e(p^m) = \sum_{k=0}^{m} f(p^k)\lambda(p^{m-k}) = \sum_{k=0}^{m} f(p^k)(-1)^{m-k},$$

so $f(p^m) = -\sum_{k=0}^{m-1} f(p^k)(-1)^k$. This implies $f(p) = 1$, and by induction $f(p^m) = 0$ for $m \geq 2$. Hence f is the characteristic function of the squarefree numbers, i.e., $\lambda^{-1} = \mu^2$.

Application II: Evaluating Dirichlet products of multiplicative functions. Since the Dirichlet product of multiplicative functions is multiplicative, and since a multiplicative function is determined by its values on prime powers, to evaluate a product $f * g$ with both f and g multiplicative, it suffices to compute the values of $f * g$ at prime powers. By comparing these values to those of familiar arithmetic functions, one can often identify $f * g$ in terms of familiar arithmetic functions.

Examples

(1) **The function $\lambda * 1$.** We have $(\lambda * 1)(p^m) = \sum_{k=0}^{m} \lambda(p^k) = \sum_{k=0}^{m} (-1)^k$, which equals 1 if m is even, and 0 otherwise. However, the latter values are exactly the values at prime powers of the characteristic function of the squares, which is easily seen to be multiplicative. Hence $\lambda * 1$ is equal to the characteristic function of the squares.

(2) **The function $f_k(n) = \sum_{d|n,(d,k)=1} \mu(d)$.** Here k is a fixed positive integer, and the summation runs over those divisors of n that are relatively prime to k. We have $f_k = g_k * 1$, where $g_k(n) = \mu(n)$ if $(n, k) = 1$ and $g_k(n) = 0$ otherwise. It is easily seen that g_k is multiplicative, so f_k is also multiplicative. On prime powers p^m, $g_k(p^m) = -1$ if $m = 1$ and $p \nmid k$ and $g_k(p^m) = 0$ otherwise, so

$f_k(p^m) = \sum_{i=0}^{m} g(p^k) = 1 - 1 = 0$ if $p \nmid k$, and $f_k(p^m) = 1$ otherwise. By the multiplicativity of f_k it follows that f_k is the characteristic function of the set $A_k = \{n \in \mathbb{N} : p|n \Rightarrow p|k\}$.

Application III: Proving the multiplicativity of functions, using known identities. This is, in a sense, the previous application in reverse. Suppose we kow that $f * g = h$ and that f and h are multiplicative. Then, by Theorem 1.10, g must be multiplicative as well.

Examples

(1) **Multiplicativity of ϕ.** Since $\phi * 1 = \mathrm{id}$ (see Theorem 1.5) and the functions 1 and id are (obviously) multiplicative, the function ϕ must be multiplicative as well. This is the promised proof of the multiplicativity of the Euler function (part (ii) of Theorem 1.5).

(2) **Multiplicativity of $d(n)$ and $\sigma(n)$.** Since $d = 1 * 1$, and the function 1 is multiplicative, the function d is multiplicative as well. Similarly, since $\sigma = \mathrm{id} * 1$, and 1 and id are multiplicative, σ is multiplicative.

1.8 Exercises

1.1 Evaluate the function $f(n) = \sum_{d^2|n} \mu(d)$ (where the summation runs over all positive integers d such that $d^2|n$), in the sense of expressing it in terms of familiar arithmetic functions.

1.2 Determine an arithmetic function f such that

$$\frac{1}{\phi(n)} = \sum_{d|n} \frac{1}{d} f\left(\frac{n}{d}\right) \quad (n \in \mathbb{N}).$$

1.3 For each of the following arithmetic functions, "evaluate" the function, or express it in terms of familiar arithmetic functions.

(i) $g_k(n) = \sum_{d|n,(d,k)=1} \mu(d)$, where $k \in \mathbb{N}$ is fixed. (Here the summation runs over all $d \in \mathbb{N}$ that satisfy $d|n$ *and* $(d,k) = 1$.)

(ii) $h_k(n) = \sum_{d|n,k|d} \mu(d)$, where $k \in \mathbb{N}$ is fixed.

1.4 Show that, for every positive integer $n \geq 2$,

$$\sum_{\substack{1 \leq k \leq n-1 \\ (k,n)=1}} k = \frac{n}{2}\phi(n).$$

1.5 Let $f(n) = \sum_{d|n} \mu(d) \log d$. Find a simple expression for $f(n)$ in terms of familiar arithmetic functions.

1.6 Let $f(n) = \#\{(n_1, n_2) \in \mathbb{N}^2 : [n_1, n_2] = n\}$, where $[n_1, n_2]$ is the least common multiple of n_1 and n_2. Show that f is multiplicative and evaluate f at prime powers.

1.7 Let f be a multiplicative function. We know that the Dirichlet inverse f^{-1} is then also multiplicative. Show that f^{-1} is *completely* multiplicative if and only if $f(p^m) = 0$ for all prime powers p^m with $m \geq 2$ (i.e., if and only if f is supported by the squarefree numbers).

1.8 Given an arithmetic function f, a "Dirichlet square root" of f is an arithmetic function g such that $g * g = f$. Prove that the constant function 1 has two Dirichlet square roots, of the form $\pm g$, where g is a multiplicative function, and find the values of g at prime powers.

1.9 Let $f(n) = \phi(n)/n$, and let $\{n_k\}_{k=1}^{\infty}$ be the sequence of values n at which f attains a "record low"; i.e., $n_1 = 1$ and, for $k \geq 2$, n_k is defined as the smallest integer $> n_{k-1}$ with $f(n_k) < f(n)$ for all $n < n_k$. (For example, since the first few values of the sequence $f(n)$ are $1, 1/2, 2/3, 1/2, 4/5, 1/3, \ldots$, we have $n_1 = 1$, $n_2 = 2$, and $n_3 = 6$, and the corresponding values of f at these arguments are 1, 1/2 and 1/3.) Find (with proof) a general formula for n_k and $f(n_k)$.

1.10 Let f be a multiplicative function satisfying $\lim_{p^m \to \infty} f(p^m) = 0$. Show that $\lim_{n \to \infty} f(n) = 0$.

1.11 An arithmetic function f is called periodic if there exists a positive integer k such that $f(n + k) = f(n)$ for every $n \in \mathbb{N}$; the integer k is called a period for f. Show that if f is completely multiplicative and periodic with period k, then the values of f are either 0 or roots of unity. (An root of unity is a complex number z such that $z^n = 1$ for some $n \in \mathbb{N}$.)

Chapter 2

Arithmetic functions II: Asymptotic estimates

The values of most common arithmetic functions $f(n)$, such as the divisor function $d(n)$ or the Moebius function $\mu(n)$, depend heavily on the arithmetic nature of the argument n. As a result, such functions exhibit a seemingly chaotic behavior when plotted or tabulated as functions of n, and it does not make much sense to seek an "asymptotic formula" for $f(n)$.

However, it turns out that most natural arithmetic functions are very well behaved *on average*, in the sense that the arithmetic means $M_f(x) = (1/x)\sum_{n\le x} f(n)$, or, equivalently, the "summatory functions" $S_f(x) = \sum_{n\le x} f(n)$, behave smoothly as $x \to \infty$ and can often be estimated very accurately. In this chapter we discuss the principal methods to derive such estimates. Aside from the intrinsic interest of studying the behavior of $M_f(x)$ or $S_f(x)$, these quantities arise naturally in a variety of contexts, and having good estimates available is crucial for a number of applications. Here are some examples, all of which will be discussed in detail later in this chapter.

(1) The number of Farey fractions of order Q, i.e., the number of rationals in the interval $(0, 1)$ whose denominator in lowest terms is $\le Q$, is equal to $S_\phi(Q)$, where $S_\phi(x) = \sum_{n\le x} \phi(n)$ is the summatory function of the Euler phi function.

(2) The "probability" that two randomly chosen positive integers are coprime is equal to the limit $\lim_{x\to\infty} 2S_\phi(x)/x^2$, which turns to be $6/\pi^2$.

(3) The "probability" that a randomly chosen positive integer is squarefree

is equal to the "mean value" of the function $\mu^2(n)(= |\mu(n)|)$, i.e., the limit $\lim_{x\to\infty} M_{\mu^2}(x)$, which turns out to be $6/\pi^2$.

(4) More generally, if $f_A(n)$ is the characteristic function of a set $A \subset \mathbb{N}$, then the mean value $\lim_{x\to\infty} M_{f_A}(x)$ of f_A, if it exists, can be interpreted as the "density" of the set A, or the "probability" that a randomly chosen positive integer belongs to A.

(5) The Prime Number Theorem is equivalent to the relation $\lim_{x\to\infty} M_\Lambda(x) = 1$, which can be interpreted as saying that the function $\Lambda(n)$ is 1 on average. It is also equivalent to the relation $\lim_{x\to\infty} M_\mu(x) = 0$, which says essentially that a squarefree number is equally likely to have an even and an odd number of prime factors.

Notational conventions. Unless otherwise specified, x denotes a real number, and by $\sum_{n\le x}$ we mean a summation over all *positive* integers n that are less than or equal to x. (In those rare cases where we want to include the term $n = 0$ in the summation, we will indicate this explicitly by writing $\sum_{0\le n\le x}$ or $\sum_{n=0}^{[x]}$.)

Given an arithmetic function f, we let $S_f(x) = \sum_{n\le x} f(n)$ denote the associated summatory function, and $M_f(x) = S_f(x)/x$ the associated finite mean values. Note that if x is a positive integer, then $M_f(x)$ is just the arithmetic mean of the first $[x]$ values of f.

2.1 Big oh and small oh notations, asymptotic equivalence

2.1.1 Basic definitions

A very convenient set of notations in asymptotic analysis are the so-called "O" ("Big oh") and "o" ("small oh") notations, and their variants. The basic definitions are as follows, where $f(x)$ and $g(x)$ are functions defined for all sufficiently large x.

(1) **"Big Oh" estimate:** "$f(x) = O(g(x))$" means that there exist constants x_0 and c such that $|f(x)| \le c|g(x)|$ for all $x \ge x_0$.

(2) **"Small Oh" estimate:** "$f(x) = o(g(x))$" means that $g(x) \ne 0$ for sufficiently large x and $\lim_{x\to\infty} f(x)/g(x) = 0$.

(3) **Asymptotic equivalence:** "$f(x) \sim g(x)$" means that $g(x) \neq 0$ for sufficiently large x and $\lim_{x\to\infty} f(x)/g(x) = 1$.

(4) **Vinogradov's $\ll$ notation:** "$f(x) \ll g(x)$" is equivalent to "$f(x) = O(g(x))$"; we also write $f(x) \gg g(x)$ if $g(x) \ll f(x)$.

(5) **Order of magnitude estimate:** "$f(x) \asymp g(x)$" means that both $f(x) \ll g(x)$ and $f(x) \ll g(x)$ hold; this is easily seen to be equivalent to the existence of positive constants c_1 and c_2 and a constant x_0 such that $c_1|g(x)| \leq |f(x)| \leq c_2|g(x)|$ holds for $x \geq x_0$. If $f(x) \asymp g(x)$, we say that f and g have **the same order of magnitude**.

An **asymptotic formula for** $f(x)$ means a relation of the form $f(x) \sim g(x)$. An **asymptotic estimate for** $f(x)$ is any estimate of the form $f(x) = g(x)+O(R(x))$ (which is to be interpreted as "$f(x)-g(x) = O(R(x)$"), where $g(x)$ is a main term and $O(R(x))$ an error term.

Note that an asymptotic formula $f(x) \sim g(x)$ is only meaningful if the approximating function $g(x)$ is, in some sense, "simpler" than the function $f(x)$ one seeks to approximate. Similarly, an asymptotic estimate $f(x) = g(x)+O(R(x))$ is only meaningful if the error term, $R(x)$, is of smaller order than the main term $g(x)$ in the approximation to $f(x)$, in the sense that $R(x)$ satisfies $R(x) = o(g(x))$. (If $R(x)$ were of the same, or larger, order than $g(x)$, then the above estimate would be equivalent to $f(x) = O(R(x))$, and there would be no point in leaving $g(x)$ in this estimate.)

2.1.2 Extensions and remarks

There exists several extensions and variants of the basic above notations defined above:

More general ranges and limits. "$f(x) = O(g(x))$ $(0 \leq x \leq 1)$" means that the estimate holds in the range $0 \leq x \leq 1$, rather than a range of the form $x \geq x_0$. Similarly, "$f(x) = o(g(x))$ $(x \to 0)$" means that the limit in the definition of the "oh" notation is taken when $x \to 0$ rather than $x \to \infty$. By convention, if no explicit range is given, the range is understood to be of the form $x \geq x_0$, for some x_0. Similarly, the limit implicit in a o-estimate is understood to be the limit as $x \to \infty$, unless a different limit is explicitly given.

Dependence on parameters. If f or g depend on some parameter λ, then the notation "$f(x) = O_\lambda(g(x))$", or, equivalently, "$f(x) \ll_\lambda g(x)$", indicates that the constants x_0 and c implicit in the estimate may depend on λ. If the constants can be chosen independently of λ, for λ in some range, then the estimate is said to hold **uniformly** in that range. Dependence on several parameters is indicated in an analogous way, as in "$f(x) \ll_{\lambda,\alpha} g(x)$".

Oh and oh expressions in equations. A term $O(g(x))$ in an equation stands for a function $R(x)$ satisfying the estimate $R(x) = O(g(x))$. For example, the notation "$f(x) = x(1 + O(1/\log x))$" means that there exist constants x_0 and c and a function $\delta(x)$ defined for $x \geq x_0$ and satisfying $|\delta(x)| \leq c/\log x$ for $x \geq x_0$, such that $f(x) = x(1 + \delta(x))$ for $x \geq x_0$.

"Big oh" versus "small oh". "Big oh" estimates provide more information than "small oh" estimates or asymptotic formulas, since they give explicit bounds for the error terms involved. An o-estimate, or an asymptotic formula, only shows that a certain function tends to zero, but does not provide any information for the rate at which this function tends to zero. For example, the asymptotic relation $f(x) \sim g(x)$, or equivalently, the o-estimate $f(x) = g(x) + o(g(x))$, means that the ratio $(g(x) - f(x))/g(x)$ tends to zero, whereas a corresponding O-estimate, such as $f(x) = g(x) + O(\epsilon(x)g(x))$, with an explicit function $\epsilon(x)$ (e.g., $\epsilon(x) = 1/\log x$), provides additional information on the speed of convergence.

O-estimates are also easier to work with and to manipulate than o-estimates. For example, O's can be "pulled out" of integrals or sums provided the functions involved are nonnegative, whereas such manipulations are in general not allowed with o's.

For the above reasons, O-estimates are much more useful than o-estimates, and one should therefore try to state and prove results in terms of O-estimates. It is very rare that one can prove a o-estimate, without getting an explicit bound for the o-term, and hence a more precise O-estimate, by the same argument.

2.1.3 Examples

Examples from analysis

(1) $x^\alpha = O_{\alpha,c}(e^{cx})$ for any fixed real numbers α and $c > 0$.

(2) $\exp(x^\alpha) \sim \exp((x+1)^\alpha)$ if $\alpha < 1$.

(3) $\log x = O_\epsilon(x^\epsilon)$ for any fixed $\epsilon > 0$.

(4) $\log(1+x) = O(x)$ for $|x| \le 1/2$ (and, more generally, for $|x| \le c$, for any constant $c < 1$).

(5) $\cos x = 1 + O(x^2)$ for $|x| \le 1$ (in fact, for all real x).

(6) $1/(1+x) = 1 + O(x)$ for $|x| \le 1/2$ (say).

(7) Let $0 < \alpha < 1$ be fixed. Then, for any constants $A > 0$ and $\epsilon > 0$,

$$x^\epsilon \ll_{\epsilon,\alpha} \exp\left(-(\log x)^\alpha\right) \ll_{A,\alpha} (\log x)^{-A}).$$

The proofs of such estimates are usually straightforward exercises at the calculus level. To illustrate some typical arguments, we give the proofs of (1), (2), and (5):

Proof of (1). Let α and $c > 0$ be given. We need to show that there exist constants C and x_0 such that $x^\alpha \le Ce^{cx}$ for $x \ge x_0$. Setting $f(x) = x^\alpha e^{-cx}$, this is equivalent to showing that $f(x)$ is bounded for sufficiently large x. This, however, follows immediately on noting that (i) $f(x)$ tends to zero as $x \to \infty$ (which can be seen by l'Hopital's rule) and (ii) $f(x)$ is continuous on the positive real axis, and hence must attain a maximal value on the interval $[1, \infty)$. An alternative argument, which yields explicit values for the constants C and x_0 runs as follows:

If $\alpha \le 0$, then for $x \ge 1$ we have $f(x) = x^\alpha e^{-cx} \le 1$, so the desired bound holds with constants $C = x_0 = 1$. Assume therefore that $0 < \alpha < 1$. We have $\log f(x) = \alpha \log x - cx$ and hence $f'(x)/f(x) = (\log f(x))' = \alpha/x - c$. Hence $f'(x) \le 0$ for $x \ge \alpha/c$, and setting $x_0 = \alpha/c$ and $C = x_0^\alpha e^{-\alpha}$ it follows that $f(x) \le f(x_0) = x_0^\alpha e^{-cx_0} = C$ for $x \ge x_0$. □

Proof of (2). Let $f(x) = \exp(x^\alpha)$. We need to show that $\lim_{x\to\infty} f(x)/f(x+1) = 1$. Now, $f(x)/f(x+1) = \exp\{x^\alpha - (x+1)^\alpha\}$, so the desired relation is equivalent to $x^\alpha - (x+1)^\alpha \to 0$ as $x \to \infty$. The latter relation holds since

$$|x^\alpha - (x+1)^\alpha| \le \max_{x \le y \le x+1} \alpha y^{\alpha-1}$$

by the mean value theorem of calculus, and since the expression on the right here tends to zero as $x \to \infty$, as $\alpha < 1$. □

Proof of (5). In the range $|x| \leq 1$, the estimate $\cos x - 1 = O(x^2)$ with 1 as O-constant follows immediately from the mean value theorem (or, what amounts to the same argument, Taylor's series for $\cos x$ truncated after the first term and with an explicit error term):

$$|\cos x - 1| = |\cos 0 - \cos x| \leq |x| \max_{0 \leq |y| \leq |x|} |\sin y| \leq x^2,$$

where in the last step we used the fact that $|\sin y|$ is increasing and bounded by $|y|$ on the interval $[-1, 1]$. To extend the range for this estimate to all of $\mathbb{R}$, we only need to observe that, since $|\cos x| \leq 1$ for all x we have $|\cos x - 1| \leq 2$ for all x, and hence $|\cos x - 1| \leq 2x^2$ for $|x| \geq 1$. Thus, the desired estimate holds for all x with O-constant 2. □

Examples from number theory

(1) The prime number theorem (PNT) is the statement that $\pi(x) \sim x/\log x$, or, equivalently, $\pi(x) = x/\log x + o(x/\log x))$. Here $\pi(x)$ is the number of primes not exceeding x.

(2) A sharper form of the PNT asserts that $\pi(x) = x/\log x + O(x/(\log x)^2)$. Factoring out the main term $x/\log x$, this estimate can also be written as $\pi(x) = (x/\log x)(1 + O(1/\log x))$, which shows that $O(1/\log x)$ is the *relative error* in the approximation of $\pi(x)$ by $x/\log x$.

(3) A still sharper form involves the approximation $\mathrm{Li}(x) = \int_2^x (1/\log t)dt$. The currently best known estimate for $\pi(x)$ is of the form $\pi(x) = \mathrm{Li}(x) + O_\alpha(x \exp(-(\log x)^\alpha))$, where α is any fixed real number $< 3/5$. By Example (7) above the error term here is of smaller order than $x(\log x)^{-A}$ for any fixed constant A, but of larger order than $x^{1-\epsilon}$, for any fixed $\epsilon > 0$.

(4) The Riemann Hypothesis is equivalent to the statement that $\pi(x) = \mathrm{Li}(x) + O_\epsilon(x^{1/2+\epsilon})$ for any fixed $\epsilon > 0$.

Additional examples and remarks

The following examples and remarks illustrate common uses of the O- and o-notations. The proofs are immediate consequences of the definitions.

(1) A commonly seen O-estimate is $f(x) = O(1)$. This simply means that $f(x)$ is bounded for sufficiently large x (or for all x in a given range). Similarly $f(x) = o(1)$ means that $f(x)$ tends to 0 as $x \to \infty$.

(2) If C is a positive constant, then the estimate $f(x) = O(Cg(x))$ is equivalent to $f(x) = O(g(x))$. In particular, the estimate $f(x) = O(C)$ is equivalent to $f(x) = O(1)$. The same holds for o-estimates.

(3) O-estimates are transitive, in the sense that if $f(x) = O(g(x))$ and $g(x) = O(h(x))$, then $f(x) = O(h(x))$.

(4) As an application of this transitivity and the basic estimates above we have, for example, $\log(1+O(f(x))) = O(f(x))$ and $1/(1+O(f(x))) = 1 + O(f(x))$ whenever $f(x) \to 0$ as $x \to \infty$. (The latter condition ensures that the function represented by the term $O(f(x))$ is bounded by $\le 1/2$ for sufficiently large x, so the estimates $\log(1+y) = O(y)$ and $(1+y)^{-1} = 1 + O(y)$ are applicable with y being the function represented by $O(f(x))$.)

(5) If $f(x) = g(x) + O(1)$, then $e^{f(x)} \asymp e^{g(x)}$, and vice versa.

(6) If $f(x) = g(x) + o(1)$, then $e^{f(x)} \sim e^{g(x)}$, and vice versa.

(7) "O's" can be pulled out of sums or integrals *provided the function inside the O-term is nonnegative.* For example, if $F(x) = \int_0^x f(y)dy$ and $f(y) = O(g(y))$ for $y \ge 0$, where g is a nonnegative function, then $F(x) = O\left(\int_0^x g(y)dy\right)$. (This does not hold without the nonnegativity condition, nor does an analogous result hold for o-estimates; for counterexamples see the exercises.)

(8) According to our convention, an asymptotic estimate for a function of x without an explicitly given range is understood to hold for $x \ge x_0$ for a suitable x_0. This is convenient as many estimates (e.g., $\log\log x = O(\sqrt{\log x})$) do not hold, or do not make sense, for small values of x, and the convention allows one to just ignore those issues. However, there are applications in which it is desirable to have an estimate involving a simple explicit range for x, such as $x \ge 1$, instead of an unspecified range like $x \ge x_0$ with a "sufficiently large" x_0. This can often be accomplished in two steps as follows: First establish the desired estimate for $x \ge x_0$, with a certain x_0. Then use direct (and usually trivial) arguments to show that the estimate also holds for $1 \le x \le x_0$. For example, one form of the PNT states that $(*)$

$\pi(x) = \mathrm{Li}(x) + O(x(\log x)^{-2})$. Suppose we have established $(*)$ for $x \geq x_0$. To show that $(*)$ in fact holds for $x \geq 2$, we can argue as follows: In the range $2 \leq x \leq x_0$ the functions $\pi(x)$ and $\mathrm{Li}(x)$ are bounded from above, say $|\pi(x)|, |\mathrm{Li}(x)| \leq A$ for $2 \leq x \leq x_0$ and some constant A (depending on x_0). On the other hand, the function in the error term, $x(\log x)^{-2}$, is bounded from below by a positive constant, say $\delta > 0$, in this range. (For example, we can take $\delta = 2(\log x_0)^{-2}$.) Hence, for $2 \leq x \leq x_0$ we have

$$|\pi(x) - \mathrm{Li}(x)| \leq 2A \leq \frac{2A}{\delta} x(\log x)^{-2} \quad (2 \leq x \leq x_0),$$

so $(*)$ holds for $2 \leq x \leq x_0$ with $c = 2A/\delta$ as O-constant.

2.1.4 The logarithmic integral

The *logarithmic integral* is the function $\mathrm{Li}(x)$ defined by

$$\mathrm{Li}(x) = \int_2^x (\log t)^{-1} dt \quad (x \geq 2).$$

This integral is important in number theory as it represents the best known approximation to the prime counting function $\pi(x)$. The integral cannot be evaluated *exactly* (in terms of elementary functions), but the following theorem gives (a sequence of) asymptotic estimates for the integral in terms of elementary functions.

Theorem 2.1 (The logarithmic integral). *For any fixed positive integer k we have*

$$\mathrm{Li}(x) = \frac{x}{\log x} \left(\sum_{i=0}^{k-1} \frac{i!}{(\log x)^i} + O_k\left(\frac{1}{(\log x)^k} \right) \right) \quad (x \geq 2).$$

In particular, we have $\mathrm{Li}(x) = x/\log x + O(x/(\log x)^2)$ *for* $x \geq 2$.

To prove the result we require a crude estimate for a generalized version of the logarithmic integral, namely

$$\mathrm{Li}_k(x) = \int_2^x (\log t)^{-k} dt \quad (x \geq 2),$$

where k is a positive integer (so that $\mathrm{Li}_1(x) = \mathrm{Li}(x)$). This result is of independent interest, and its proof is a good illustration of the method of splitting the range of integration.

Lemma 2.2. *For any fixed positive integer k we have*

$$\mathrm{Li}_k(x) \ll_k \frac{x}{(\log x)^k} \quad (x \geq 2).$$

Proof. First note that the bound holds trivially in any range of the form $2 \leq x \leq x_0$ (with the O-constant depending on x_0). We therefore may assume that $x \geq 4$. In this case we have $2 \leq \sqrt{x} \leq x$, so that we may split the range $2 \leq t \leq x$ into the two subranges $2 \leq t < \sqrt{x}$ and $\sqrt{x} \leq t \leq x$. In the first subrange the integrand is bounded by $1/(\log 2)^k$, so the integral over this range is $\leq (\log 2)^{-k}(\sqrt{x} - 2) \ll_k \sqrt{x}$, which is of the desired order of magnitude.

In the remaining range $\sqrt{x} \leq t \leq x$, the integrand is bounded by $\leq (\log \sqrt{x})^{-k} = 2^k (\log x)^{-k}$, so the integral over this range is at most $2^k (\log x)^{-k}(x - \sqrt{x}) \ll_k x(\log x)^{-k}$, which again is of the desired order of magnitude. □

Remark. The choice of $\sqrt{x}$ as the splitting point is sufficient to obtain the asserted upper bound for $\mathrm{Li}_k(x)$, but it is not optimal and choosing a larger division point allows one to derive a more accurate estimate for $\mathrm{Li}_k(x)$ (which, however, is still inferior to what can be obtained with the integration by parts method that we will use to prove Theorem 2.1). For example, splitting the integral at $x(\log x)^{-k-1}$, the contribution of lower subrange is $\ll_k x(\log x)^{-k-1}$, whereas in the upper subrange the integrand can be approximated as follows:

$$(\log t)^{-k} = (\log x + \log(t/x))^{-k} = (\log x)^{-k} \left(1 + O_k\left(\frac{\log\log x}{\log x}\right)\right).$$

This leads to the estimate

$$\mathrm{Li}_k(x) = \frac{x}{(\log x)^k} \left(1 + O_k\left(\frac{\log\log x}{\log x}\right)\right).$$

Proof of Theorem 2.1. Integration by parts shows that, for $i = 1, 2, \ldots$,

$$\begin{aligned} \mathrm{Li}_i(x) &= \frac{x}{(\log x)^i} - \frac{2}{(\log 2)^i} - \int_2^x t \frac{-i}{(\log t)^{i+1} t} dt \\ &= \frac{x}{(\log x)^i} - \frac{2}{(\log 2)^i} + i\,\mathrm{Li}_{i+1}(x). \end{aligned}$$

Applying this identity successively for $i = 1, 2, \ldots, k$ (or, alternatively, using induction on k) gives

$$\mathrm{Li}(x) = \mathrm{Li}_1(x) = O_k(1) + \sum_{i=1}^{k} \frac{(i-1)!x}{(\log x)^i} + k!\,\mathrm{Li}_{k+1}(x).$$

(Here the term $O_k(1)$ absorbs the constant terms $2(\log 2)^{-i}$ that arise when using the above estimate for each $i = 1, 2, \ldots, k$.) Since $\mathrm{Li}_{k+1}(x) \ll_k x(\log x)^{-k-1}$ by Lemma 2.2, the asserted estimate follows. □

Remark. Note that, because of the factor $i!$, the series in the main term diverges if one lets $k \to \infty$. The resulting infinite series $\sum_{i=0}^{\infty} i!(\log x)^{-i}$ is an example of a so-called "asymptotic series", a series that diverges everywhere, but which, when truncated at some level k, behaves like an ordinary convergent series, in the sense that the error introduced by truncating the series at the kth term has an order of magnitude equal to that of the next term in the series.

2.2 Sums of smooth functions: Euler's summation formula

2.2.1 Statement of the formula

The simplest types of sums $\sum_{n \le x} f(n)$ are those in which f is a "smooth" function that is defined for real arguments x. Sums of this type are of interest in their own right (for example, Stirling's formula for $n!$ is equivalent to an estimate for a sum of the above type with $f(n) = \log n$—see Theorem 2.6 and Corollary 2.7 below), but they also occur in the process of estimating sums of arithmetic functions like the divisor function or the Euler phi function (see the following sections).

The basic idea for handling such sums is to approximate the sum by a corresponding integral and investigate the error made in the process. The following important result, known as Euler's summation formula, gives an exact formula for the difference between such a sum and the corresponding integral.

Theorem 2.3 (Euler's summation formula). *Let $0 < y \le x$, and suppose $f(t)$ is a function defined on the interval $[y, x]$ and having a continuous derivative there. Then*

$$\sum_{y < n \le x} f(n) = \int_y^x f(t)dt + \int_y^x \{t\} f'(t)dt - \{x\}f(x) + \{y\}f(y),$$

where $\{t\}$ denotes the fractional part of t, i.e., $\{t\} = t - [t]$.

In most applications, one needs to estimate a sum of the form $\sum_{n \le x} f(n)$, taken over all positive integers $n \le x$. In this case, Euler's summation formula reduces to the following result:

Corollary 2.4 (Euler's summation formula, special case). *Let $x \geq 1$ and suppose that $f(t)$ is defined on $[1, x]$ and has a continuous derivative on this interval. Then we have*

$$\sum_{n \leq x} f(n) = \int_1^x f(t)dt + \int_1^x \{t\}f'(t)dt - \{x\}f(x) + f(1).$$

Proof. We apply Euler's summation formula with $y = 1$. The integrals on the right-hand side are then of the desired form, as is the term $\{x\}f(x)$, while the term $\{y\}f(y)$ vanishes. On the other hand, the sum on the left with $y = 1$ is equal to the sum over all positive integers $n \leq x$ minus the term $f(1)$. Adding this term on both sides of Euler's summation formula gives the identity stated in the corollary. □

Proof of Theorem 2.3. Letting $F(x) = [x] = x - \{x\}$, we can write the given sum as a *Stieltjes integral* $\sum_{y<n\leq x} f(n) = \int_y^x f(t)dF(t)dt$. Writing $dF(t) = dt - d\{t\}$, the integral splits into $\int_y^x f(t)dt - \int_y^x f(t)d\{t\}$. The first of these latter two integrals is the desired main term, while the second can be transformed as follows using integration by parts:

$$\int_y^x f(t)d\{t\} = f(x)\{x\} - f(y)\{y\} - \int_y^x f'(t)\{t\}dt.$$

Combining these formulas gives the desired identity. □

Remark. The above proof is quite simple and intuitive, and motivates the particular form of the Euler summation formula. However, it is less elementary in that it depends on a concept beyond the calculus level, namely the Stieltjes integral. In Section 2.3.1 we will give an independent, more elementary, proof; in fact, we will prove a more general result (the partial summation formula), of which Euler's summation formula is a corollary.

2.2.2 Partial sums of the harmonic series

Euler's summation formula has numerous applications in number theory and analysis. We will give here three such applications; the first is to the partial sums of the harmonic series.

Theorem 2.5 (Partial sums of the harmonic series). *We have*

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right) \quad (x \geq 1),$$

where $\gamma = \lim_{x\to\infty}(\sum_{n\le x} 1/n - \log x) = 0.5772\ldots$ *is a constant, the so-called Euler constant.*

Remark. The error term $O(1/x)$ here is best-possible, since the left-hand side has a jump of size $1/x$ whenever x crosses an integer, while the main term on the right is continuous in x.

Proof. Let $S(x) = \sum_{n\le x} 1/n$. By Euler's summation formula (in the version given by Corollary 2.4) we have, for $x \ge 1$,

$$\sum_{n\le x} = \int_1^x \frac{1}{t}dt + \int_1^x \{t\}\frac{-1}{t^2}dt + \frac{\{x\}}{x} + 1 = \log x - I(x) + 1 + O\left(\frac{1}{x}\right),$$

where $I(x) = \int_1^x \{t\}t^{-2}dt$. To obtain the desired estimate, it suffices to show that $I(x) = \gamma - 1 + O(1/x)$ for $x \ge 1$. To estimate the integral $I(x)$, we employ the following trick: We extend the integration in the integral to infinity and estimate the tail of the integral. Since the integrand is bounded by $1/t^2$, the integral converges absolutely when extended to infinity, and therefore equals a finite constant, say I, and we have

$$I(x) = I - \int_x^\infty \frac{\{t\}}{t^2}dt = I + O\left(\int_x^\infty \frac{1}{t^2}dt\right) = I + O\left(\frac{1}{x}\right) \quad (x \ge 1).$$

We have thus shown that $S(x) = \log x + 1 - I + O(1/x)$ for $x \ge 1$. In particular, this implies that $S(x) - \log x$ converges to $1 - I$ as $x \to \infty$. Since, by definition, $\gamma = \lim_{x\to\infty}(S(x) - \log x)$, we have $1 - I = \gamma$, and thus obtain the desired formula. □

2.2.3 Partial sums of the logarithmic function and Stirling's formula

Our second application of Euler's summation formula is a proof of the so-called Stirling formula, which gives an asymptotic estimate for $N!$, where N is a (large) integer. This formula will be an easy consequence of the following estimate for the logarithm of $N!$, $\log N! = \sum_{n\le N} \log n$, which is a sum to which Euler's summation formula can be applied.

Theorem 2.6 (Partial sums of the logarithmic function). *We have*

$$\sum_{n\le N} \log n = N(\log N - 1) + \frac{1}{2}\log N + c + O\left(\frac{1}{N}\right) \quad (N \in \mathbb{N}),$$

where c is a constant.

Proof. Let $S(N) = \sum_{n \le N} \log n$. Applying Euler's summation formula (again in the special case provided by Corollary 2.4), and noting that $\{N\} = 0$ since N is an integer, we obtain

$$S(N) = I_1(N) + I_2(N)$$

with

$$I_1(N) = \int_1^N (\log t) dt = t(\log t - 1)\Big|_1^N = N \log N - N + 1$$

and

$$I_2(N) = \int_1^N \frac{\{t\}}{t} dt = \int_1^N \frac{1/2}{t} dt + \int_1^N \frac{\rho(t)}{t} dt = \frac{1}{2} \log N + I_3(N),$$

where $\rho(t) = \{t\} - 1/2$ is the "row of teeth" function and $I_3(N) = \int_1^N (\rho(t)/t) dt$. Combining these formulas gives

$$S(N) = N \log N - N + \frac{1}{2} \log N + 1 + I_3(N).$$

Thus, to obtain the desired estimate, it suffices to show that $I_3(N) = c' + O(1/N)$, for some constant c'.

We begin with an integration by parts to get

$$I_3(N) = \frac{R(t)}{t}\Big|_1^N + I_4(N),$$

where

$$R(t) = \int_1^t \rho(t) dt, \quad I_4(x) = \int_1^x \frac{R(t)}{t^2} dt.$$

Since $\rho(t)$ is periodic with period 1, $|\rho(t)| \le 1/2$ for all t, and $\int_k^{k+1} \rho(t) = 0$ for any integer k, we have $R(t) = 0$ whenever t is an integer, and $|R(t)| \le 1/2$ for all t. Hence the terms $R(t)/t$ vanish at $t = 1$ and $t = N$, so we have $I_3(N) = I_4(N)$. Now, the integral $I_4(N)$ converges as $x \to \infty$, since its integrand is bounded by $|R(t)|t^{-2} \le (1/2)t^{-2}$, and we therefore thave

$$I_4(N) = I - \int_N^\infty \frac{R(t)}{t^2} dt = I - O\left(\int_N^\infty \frac{1}{t^2} dt \right) = I + O\left(\frac{1}{N} \right),$$

where

$$I = \int_1^\infty \frac{R(t)}{t^2} dt.$$

(Note here again the "trick" of extending a convergent integral to infinity and estimating the tail.) Hence we have $I_3(N) = I_4(N) = I + O(1/N)$, as we wanted to show. □

We now use this estimate to prove (modulo the evaluation of a constant) Stirling's formula for $n!$.

Corollary 2.7 (Stirling's formula). *If n is a positive integer, then*

$$n! = C\sqrt{n}n^n e^{-n}\left(1 + O\left(\frac{1}{n}\right)\right),$$

where C is a constant.

Remark. One can show that the constant C is equal to $\sqrt{2\pi}$, and Stirling's formula is usually stated with this explicit value of the constant. However, proving this is far from easy, and since the value of the constant is not important for our applications, we will not pursue this here. The argument roughly goes as follows: Consider the sum $\sum_{k=0}^{n}\binom{n}{k}$. On the one hand, this sum is exactly equal to 2^n. On the other hand, by expressing the binomial coefficients in terms of factorials and estimating the factorials by Stirling's formula one can obtain an estimate for this sum involving the Stirling constant C. Comparing the two evaluations one obtains $C = \sqrt{2\pi}$.

Proof. Since $n! = \exp\{\sum_{k\le n}\log k\}$, we have, by the theorem,

$$n! = \exp\left\{n\log n - n + \frac{1}{2}\log n + c + O\left(\frac{1}{n}\right)\right\},$$

which reduces to the right-hand side in the estimate of the corollary, with constant $C = e^c$. □

The estimate of Theorem 2.6 applies only to sums $\sum_{n\le x}\log n$ when x is a positive integer; this is the case of interest in the application to Stirling's formula. In numbertheoretic applications one needs estimates for these sums that are valid for all (large) *real* x. The following corollary provides such an estimate, at the cost of a weaker error term.

Corollary 2.8. *We have*

$$\sum_{n\le x}\log n = x(\log x - 1) + O(\log x) \quad (x \ge 2).$$

Proof. We apply the estimate of the theorem with $N = [x]$. The left-hand side remains unchanged when replacing x by N. On the other hand, the main term on the right, $x(\log x - 1)$, has derivative $\log x$. so it changes by an amount of order at most $O(\log x)$ if x is replaced by $[x]$. Since the error

term $O(1/x)$ on the right is also of this order of magnitude, the asserted estimate follows. (Note here the restriction $x \geq 2$; in the larger range $x \geq 1$ this estimate would not be valid, since the error term $O(\log x)$ is 0 at $x = 1$, whereas the main terms on the left and right are clearly not equal when $x = 1$.) □

2.2.4 Integral representation of the Riemann zeta function

The Riemann zeta function is defined for complex arguments s with $\operatorname{Re} s > 1$ by the series

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

As an application of Euler's summation formula, we now derive an integral represention for this function. This representation will be crucial in deriving deeper analytic properties of the zeta function.

Theorem 2.9 (Integral representation of the zeta function). *For* $\operatorname{Re} s > 1$ *we have*

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \{x\} x^{-s-1} dx. \tag{2.1}$$

Proof. Fix s with $\operatorname{Re} s > 1$, and let $S(x) = \sum_{n \leq x} n^{-s}$. Applying Euler's summation formula in the form of Corollary 2.4 with $f(x) = x^{-s}$, we get, for any $x \geq 1$,

$$S(x) = I_1(x) + I_2(x) - \{x\}x^{-s} + 1,$$

where

$$I_1(x) = \int_1^x y^{-s} dy = \frac{1 - x^{1-s}}{s-1} = \frac{1}{s-1} + O_s(x^{1-\operatorname{Re} s})$$

and

$$\begin{aligned} I_2(x) &= \int_1^x \{y\}(-s)y^{-s-1} dy \\ &= -s\int_1^{\infty} \{y\} y^{-s-1} dy + O_s\left(\int_x^{\infty} y^{-\operatorname{Re} s - 1} dy\right) \\ &= -s\int_1^{\infty} \{y\} y^{-s-1} dy + O_s(x^{-\operatorname{Re} s}). \end{aligned}$$

Letting $x \to \infty$, the O-terms in the estimates for $I_1(x)$ and $I_2(x)$, as well as the term $\{x\}x^{-s}$, tend to zero, and we conclude

$$\begin{aligned}\zeta(s) &= \lim_{x\to\infty} S(x) = \frac{1}{s-1} + 1 - s\int_1^\infty \{y\}y^{-s-1}dy \\ &= \frac{s}{s-1} - s\int_1^\infty \{y\}y^{-s-1}dy,\end{aligned}$$

which is the asserted identity. □

2.3 Removing a smooth weight function from a sum: Summation by parts

2.3.1 The summation by parts formula

Summation by parts (also called partial summation or Abel summation) is the analogue for sums of integration by parts. Given a sum of the form $\sum_{n\le x} a(n)f(n)$, where $a(n)$ is an arithmetic function with summatory function $A(x) = \sum_{n\le x} a(n)$ and $f(n)$ is a "smooth" weight, the summation by parts formula allows one to "remove" the weight $f(n)$ from the above sum and reduce the evaluation or estimation of the sum to that of an integral over $A(t)$. The general formula is as follows:

Theorem 2.10 (Summation by parts formula). *Let $a : \mathbb{N} \to \mathbb{C}$ be an arithmetic function, let $0 < y < x$ be real numbers and $f : [y, x] \to \mathbb{C}$ be a function with continuous derivative on $[y, x]$. Then we have*

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt, \tag{2.2}$$

where $A(t) = \sum_{n\le t} a(n)$.

This formula is easy to remember since it has the same form as the formula for integration by parts, if one thinks of $A(x)$ as the "integral" of $a(n)$.

In nearly all applications, the sums to be estimated are sums of the form $\sum_{n\le x} a(n)f(n)$, where n ranges over all positive integers $\le x$. We record the formula in this special case separately.

Corollary 2.11 (Summation by parts formula, special case). *Let $a : \mathbb{N} \to \mathbb{C}$ be an arithmetic function, let $x \geq 1$ be a real number and $f : [1, x] \to \mathbb{C}$ a function with continuous derivative on $[1, x]$. Then we have*

$$\sum_{n \leq x} a(n) f(n) = A(x) f(x) - \int_1^x A(t) f'(t) dt. \tag{2.3}$$

Proof. Applying the theorem with $y = 1$ and adding the term $a(1)f(1) = A(1)f(1)$ on both sides of (2.2) gives (2.3). □

In the case when $a(n) \equiv 1$ the sum on the left of (2.2) is of the same form as the sum estimated by Euler's summation formula (Theorem 2.3), which states that, under the same conditions on f, one has

$$\sum_{y < n \leq x} f(n) = \int_y^x f(t) dt + \int_y^x \{t\} f'(t) dt - \{x\} f(x) + \{y\} f(y).$$

In fact, as we now show, this formula can be derived from the partial summation formula.

Alternate proof of Euler's summation formula (Theorem 2.3). Applying the partial summation formula with $a(n) \equiv 1$ and $A(t) = \sum_{n \leq t} 1 = [t]$, we obtain

$$\begin{aligned} \sum_{y < n \leq x} f(n) &= [x] f(x) - [y] f(y) - \int_y^x [t] f'(t) dt \\ &= x f(x) - y f(y) - \int_y^x t f'(t) dt \\ &\qquad - \{x\} f(x) + \{y\} f(y) + \int_y^x \{t\} f'(t) dt. \end{aligned}$$

By an integration by parts, the first integral on the right-hand side equals $x f(x) - y f(y) - \int_y^x f(t) dt$, so the above reduces to

$$\sum_{y < n \leq x} f(n) = \int_y^x f(t) dt - \{x\} f(x) + \{y\} f(y) + \int_y^x \{t\} f'(t) dt,$$

which is the desired formula. □

Proof of Theorem 2.10. Let $0 < y < x$, a, and f be given as in the theorem. and let I denote the integral on the right of (2.2). Setting $\chi(n,t) = 1$ if $n \le t$ and $\chi(n,t) = 0$ otherwise, we have

$$\begin{aligned} I &= \int_y^x \sum_{n\le x} a(n)\chi(n,t)f'(t)dt = \sum_{n\le x} a(n) \int_y^x \chi(n,t)f'(t)dt \\ &= \sum_{n\le x} a(n) \int_{\max(n,y)}^x f'(t)dt, \end{aligned}$$

where the interchanging of integration and summation is justified since the sum involves only finitely many terms. Since f' is continuous on $[y,x]$, the inner integrals can be evaluated by the fundamental theorem of calculus, and we obtain

$$\begin{aligned} I &= \sum_{n\le x} a(n)(f(x) - f(\max(n,y)) \\ &= \sum_{n\le x} a(n)f(x) - \sum_{n\le y} a(n)f(y) - \sum_{y<n\le x} a(n)f(n) \\ &= A(x)f(x) - A(y)f(y) - \sum_{y<n\le x} a(n)f(n). \end{aligned}$$

Hence,

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - I,$$

which is the desired formula. □

Partial summation is an extremely useful tool that has numerous applications in number theory and analysis. In the following subsections we give three such applications. We will encounter a number of other applications in later chapters.

2.3.2 Kronecker's Lemma

As a first, and simple, illustration of the use of the partial summation formula we prove the following result, known as "Kronecker's Lemma", which is of independent interest and has a number of applications in its own right, in particular, in probability theory and analysis.

Theorem 2.12 (Kronecker's Lemma). *Let $f : \mathbb{N} \to \mathbb{C}$ be an arithmetic function. If s is a complex number with $\operatorname{Re} s > 0$ such that*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{converges,} \tag{2.4}$$

then

$$\lim_{x\to\infty} \frac{1}{x^s} \sum_{n\le x} f(n) = 0. \tag{2.5}$$

In particular, the convergence of $\sum_{n=1}^{\infty} f(n)/n$ implies that f has mean value zero in the sense that $\lim_{x\to\infty}(1/x)\sum_{n\le x} f(n) = 0$.

Remarks. Kronecker's lemma is often stated only in the special case mentioned at the end of the above theorem (i.e., the case $s = 1$), and for most applications it is used in this form. We have stated a slightly more general version involving "weights" n^{-s} instead of n^{-1}, as we will need this version later. In fact, the result holds in greater generality, with the function x^{-s} replaced by a general "weight function" $w(x)$ in both (2.4) and (2.5).

Proof. Fix a function $f(n)$ and $s \in \mathbb{C}$ with $\operatorname{Re} s > 0$ as in the theorem, and set

$$S(x) = \sum_{n\le x} f(n), \quad T(x) = \sum_{n\le x} \frac{f(n)}{n^s}.$$

The hypothesis (2.4) means that $T(x)$ converges to a finite limit T as $x \to \infty$, and the desired conclusion (2.5) is equivalent to $\lim_{x\to\infty} S(x)/x^s = 0$.

Let $\epsilon > 0$ be given. Since $\lim_{x\to\infty} T(x) = T$, there exists $x_0 = x_0(\epsilon) \ge 1$ such that

$$|T(x) - T| \le \epsilon \quad (x \ge x_0). \tag{2.6}$$

Let $x \ge x_0$. Applying the summation by parts formula with $f(n)/n^s$ and n^s in place of $a(n)$ and $f(n)$, respectively, we obtain

$$\begin{aligned} S(x) &= \sum_{n\le x} \frac{f(n)}{n^s} \cdot n^s = T(x)x^s - \int_1^x T(t)st^{s-1}dt \\ &= \int_0^x T(x)st^{s-1}dt - \int_1^x T(t)st^{s-1}dt. \end{aligned}$$

Defining $T(t)$ to be 0 if $t \leq 1$, we can combine the last two integrals to a single integral over the interval $[0, x]$ and obtain

$$\begin{aligned} |S(x)| &= \left| \int_0^x (T(x) - T(t)) s t^{s-1} dt \right| \\ &\leq \int_0^x |T(x) - T(t)||s| t^{\operatorname{Re} s - 1} dt. \end{aligned}$$

To estimate the latter intergral, we split the interval of integration into the two subintervals $[0, x_0)$ and $[x_0, x]$, and bound the integrand separately in these two intervals. For $x_0 \leq t \leq x$ we have, by (2.6),

$$|T(t) - T(x)| \leq |T(t) - T| + |T - T(x)| \leq 2\epsilon,$$

while for $0 \leq t \leq x_0$ we use the trivial bound

$$\begin{aligned} |T(t) - T(x)| &\leq |T(t)| + |T| + |T - T(x)| \\ &\leq \sum_{n \leq x_0} \left| \frac{f(n)}{n^s} \right| + |T| + \epsilon = M, \end{aligned}$$

say, with $M = M(\epsilon)$ a constant depending on ϵ, but not on x. It follows that

$$\begin{aligned} |S(x)| &\leq \epsilon \int_{x_0}^x |s| t^{\operatorname{Re} s - 1} dt + M \int_0^{x_0} |s| t^{\operatorname{Re} s - 1} dt \\ &\leq \frac{|s|}{\operatorname{Re} s} \left(\epsilon \left(x^{\operatorname{Re} s} - {x_0}^{\operatorname{Re} s} \right) + M x_0^{\operatorname{Re} s} \right) \end{aligned}$$

and hence

$$\left| \frac{S(x)}{x^s} \right| \leq \frac{|s|}{\operatorname{Re} s} \left(\epsilon + \frac{M x_0^{\operatorname{Re} s}}{x^{\operatorname{Re} s}} \right).$$

Since, by hypothesis, $\operatorname{Re} s > 0$, the last term on the right tends to zero as $x \to \infty$, so we obtain $\limsup_{x \to \infty} |S(x)/x^s| \leq \epsilon |s| / \operatorname{Re} s$. Since $\epsilon > 0$ was arbitrary, we conclude that $\lim_{x \to \infty} S(x)/x^s = 0$, as desired. □

2.3.3 Relation between different notions of mean values of arithmetic functions

We next use partial summation to study the relation between two different types of "mean values", or averages, of an arithmetic function f: the *ordinary (or asymptotic) mean value*

$$M(f) = \lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} f(n), \tag{2.7}$$

and the *logarithmic mean value*

$$L(f) = \lim_{x\to\infty} \frac{1}{\log x} \sum_{n\le x} \frac{f(n)}{n}, \tag{2.8}$$

The asymptotic mean value is (a limit of) an ordinary average, or arithmetic mean, of the values $f(n)$, while the logarithmic mean value can be regarded as a weighted average of these values, with the weights being $1/n$. Thus, to convert between these two mean values it is natural to use partial summation to remove or re-instate the weights $1/n$. The application of partial summation in this way is very common, and it is also quite instructive as it illustrates both a siutation in which this approach is successful, and a situation in which the method fails.

In one direction (namely, going from $M(f)$ to $L(f)$), the method works well, and we have the following result.

Theorem 2.13. *Let f be an arithmetic function, and suppose that the ordinary mean value $M(f)$ exists. Then the logarithmic mean value $L(f)$ exists as well, and is equal to $M(f)$.*

Proof. Suppose f has mean value $M(f) = A$. Let $S(x) = \sum_{n\le x} f(n)$ and $T(x) = \sum_{n\le x} f(n)/n$. By the assumption $M(f) = A$, we have $\lim_{x\to\infty} S(x)/x = A$, and we need to show that $\lim_{x\to\infty} T(x)/\log x = A$.

To obtain an estimate for $T(x)$, we apply the partial summation formula with $a(n) = f(n)$, $A(x) = S(x)$, and with the function $f(x) = 1/x$ as the weight function to be removed from the sum. We obtain

$$T(x) = \frac{S(x)}{x} + \int_1^x \frac{S(t)}{t^2} dt = \frac{S(x)}{x} + I(x), \tag{2.9}$$

say. Upon dividing by $\log x$, the first term, $S(x)/(x\log x)$, tends to zero, since, by hypothesis, $S(x)/x$ converges, and hence is bounded. To show that the limit $L(f) = \lim_{x\to\infty} T(x)/\log x$ exists and is equal to A, it remains therefore to show that the integral $I(x)$ satisfies

$$\lim_{x\to\infty} \frac{I(x)}{\log x} = A. \tag{2.10}$$

Let $\epsilon > 0$ be given. By our assumption $\lim_{t\to\infty} S(t)/t = A$, there exists $t_0 = t_0(\epsilon) \ge 1$ such that $|S(t)/t - A| \le \epsilon$ for $t \ge t_0$. Moreover, for $1 \le t \le t_0$ we have

$$\left|\frac{S(t)}{t} - A\right| \le \frac{1}{t}\sum_{n\le t_0} |f(n)| + |A| \le \sum_{n\le t_0} |f(n)| + |A| = K_0,$$

say, where $K_0 = K_0(\epsilon)$ is a constant depending on ϵ. Hence, for $x \geq t_0$ we have

$$\begin{aligned} |I(x) - A\log x| &= \left| \int_1^x \frac{S(t)/t - A}{t} dt \right| \\ &\leq \int_1^{t_0} \frac{K_0}{t} dt + \int_{t_0}^x \frac{\epsilon}{t} dt \\ &\leq K_0 \log t_0 + \epsilon \log(x/t_0) \\ &\leq K_0 \log t_0 + \epsilon \log x. \end{aligned}$$

Since ϵ was arbitrary, it follows that

$$\limsup_{x\to\infty} \frac{|I(x) - A\log x|}{\log x} = 0,$$

which is equivalent to (2.10). □

In the other direction (going from $L(f)$ to $M(f)$) the method fails; indeed, the converse of Theorem 2.13 is false:

Theorem 2.14. *There exist arithmetic functions f such that $L(f)$ exists, but $M(f)$ does not exist.*

Proof. Define a function f by $f(n) = n$ if $n = 2^k$ for some nonnegative integer k, and $f(n) = 0$ otherwise. This function does not have an ordinary mean value since the average $(1/x)\sum_{n\leq x} f(n)$, as a function of x, has a jump of size 1 at all powers of 2, and hence does not converge as $x \to \infty$. However, f has a logarithmic mean value (namely $1/\log 2$), since

$$\begin{aligned} \frac{1}{\log x} \sum_{n\leq x} \frac{f(n)}{n} &= \frac{1}{\log x} \sum_{2^k \leq x} \frac{2^k}{2^k} \\ &= \frac{1}{\log x} \left(\left[\frac{\log x}{\log 2} \right] + 1 \right) = \frac{1}{\log 2} + O\left(\frac{1}{\log x} \right). \end{aligned}$$

□

For an arithmetic function to have an asymptotic mean value is therefore a stronger condition than having a logarithmic mean value, and the existence of an asymptotic mean value is usually much harder to prove than the existence of a logarithmic mean value. For example, it is relatively easy to prove (as we will see in the next chapter) that the von Mangoldt function $\Lambda(n)$ has logarithmic mean value 1, and the Moebius function $\mu(n)$ has logarithmic mean value 0. By contrast, the existence of an ordinary asymptotic mean value for Λ or μ is equivalent to the prime number theorem and much more difficult to establish.

Failure of partial summation. It is tempting to try to use partial summation in an attempt to show that the existence of $L(f)$ implies that of $M(f)$. Of course, since this implication is not true, such an approach is bound to fail, but it is instructive to see what exactly goes wrong if one tries to apply partial summation in the "converse" direction. Thus, assume that $L(f)$ exists and is equal to A. In an attempt to show that $M(f)$ exists as well and is equal to A, one would start with the sum $S(x) = \sum_{n\le x}(f(n)/n)n$, and then "remove" the factor n by partial summation. Applying partial summation as in (2.9), but with the roles of $S(x)$ and $T(x)$ interchanged, gives the identity

$$S(x) = xT(x) - \int_1^x T(t)dt,$$

so to show that $M(f) = A$ we would need to show

$$\frac{S(x)}{x} = T(x) - (1/x)\int_1^x T(t)dt \to A \quad (x \to \infty). \tag{2.11}$$

However, the assumption that f has logarithmic mean value A is equivalent to the estimate $T(x) = A\log x + o(\log x)$, and substituting this estimate into (2.11) introduces an error term $o(\log x)$ that prevents one from drawing any conclusions about the convergence of $S(x)/x$ in (2.11). To obtain (2.11) would require a much stronger estimate for $T(x)$, in which the error term is $o(1)$ instead of $o(\log x)$.

The reason why (2.11) is so ineffective is because the right-hand side is a difference of two large terms of nearly the same size, both of which are much larger than the left-hand side. By contrast, the right-hand side of (2.9) is a sum of two expressions, each of the same (or smaller) order of magnitude than the function on the left.

The logarithmic mean value as an average version of the asymptotic mean value. Further insight into the relation between the asymptotic and logarithmic mean values is provided by rewriting the identity (2.9) in terms of the functions

$$\mu(t) = m(e^t), \quad \lambda(t) = l(e^t),$$

where

$$m(x) = \frac{1}{x}\sum_{n\le x} f(n), \quad \lambda(x) = \frac{1}{\log x}\sum_{n\le x}\frac{f(n)}{n}$$

are the finite asymptotic, resp. logarithmic, mean values. Assuming that $m(x) = o(\log x)$ (a very mild assumption that holds, for example, if the function f is bounded), (2.9) becomes

$$\lambda(t) = o(1) + \frac{1}{t}\int_0^t \mu(s)ds.$$

Thus, the convergence of $\lambda(t)$ (i.e., the existence of a logarithmic mean value) is equivalent to the convergence of $\overline{\mu}(t) = (1/t)\int_0^t \mu(s)ds$, i.e., the convergence of a certain average of $\mu(s)$, the ordinary (finite) mean value. It is obvious that if a function $\mu(t)$ converges, then so does its average $\overline{\mu}(t)$, and it is also easy to construct functions $\mu(t)$ for which the converse does not hold. Interpreting $M(f)$ as the limit of a function $\mu(t)$, and $L(f)$ as the limit of the corresponding average function $\overline{\mu}(t)$, it is then clear that the existence of $M(f)$ implies that of $L(f)$, but not vice versa.

2.3.4 Dirichlet series and summatory functions

As a final illustration of the use of partial summation, we prove an integral representation for the so-called Dirichlet series of an arithmetic function.

Given an arithmetic function f, the *Dirichlet series of* f is the (formal) infinite series

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

where s is any complex number. The following result gives a representation of this series as a certain integral involving the partial sums $S(x) = \sum_{n\le x} f(n)$.

Theorem 2.15 (Mellin transform representation of Dirichlet series). *Let f be an arithmetic function, let $S_f(x) = \sum_{n\le x} f(n)$ be the associated summatory function, and let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ be the "Dirichlet series" associated with f, whenever the series converges.*

(i) For any complex number s with $\operatorname{Re} s > 0$ such that $F(s)$ converges we have

$$F(s) = s\int_1^{\infty} \frac{S_f(x)}{x^{s+1}}dx, \tag{2.12}$$

(ii) If $S_f(x) = O(x^{\alpha})$ for some $\alpha \ge 0$, then $F(s)$ converges for all complex numbers s with $\operatorname{Re} s > \alpha$, and (2.12) holds for all such s.

The identity (2.12) can be interpreted in terms of so-called Mellin transforms. Given a function $\phi(x)$ defined on the positive real axis, the *Mellin transform* of ϕ is the function $\hat{\phi}$ defined by

$$\hat{\phi}(s) = \int_0^\infty \phi(s) x^{-s} dx,$$

provided the integral exists. In this terminology (2.12) says that $F(s)/s$ is the Mellin transform of the function $S_f(x)/x$ (with the convention that $S_f(x) = 0$ if $x < 1$).

Proof. (i) Suppose that $F(s)$ converges for some s with $\operatorname{Re} s > 0$. We want to apply partial summation to remove the factor n^{-s} in the summands of $F(s)$ in order express $F(s)$ in terms of the partial sums $S_f(x)$. Since $F(s)$ is an infinite series, we cannot apply the partial summation formula directly to $F(s)$. However, we can apply it to the partial sums $F_N(s) = \sum_{n=1}^N f(n) n^{-s}$ and obtain, for any positive integer N,

$$F_N(s) = \frac{S_f(N)}{N^s} + s \int_1^N \frac{S_f(x)}{x^{s+1}} dx. \tag{2.13}$$

Now let $N \to \infty$ on both sides of this identity. Since, by assumption, the series $F(s)$ converges, the partial sums $F_N(s)$ on the left tend to $F(s)$. Also, by Kronecker's Lemma (Theorem 2.12), the convergence of $F(s)$, along with the hypothesis $\operatorname{Re} s > 0$, implies that the first term on the right, $S_f(N)/N^s$, tends to zero. Hence the integral on the right-hand side converges as N tends to infinity, and we obtain (2.12).

(ii) Suppose that $S_f(x) = O(x^\alpha)$ for some $\alpha > 0$, let s be a complex number with $\operatorname{Re} s > \alpha$, and set $\delta = \operatorname{Re} s - \alpha > 0$. We again apply (2.13), first for fixed finite $N \in \mathbb{N}$, and then let $N \to \infty$. First note that, by our assumptions on $S_f(x)$ and s, the term $S_f(N)N^{-s}$ is of order $O(N^{\alpha - \operatorname{Re} s}) = O(N^{-\delta})$ and hence tends to zero as $N \to \infty$. Also, the integrand $S_f(x)x^{-s-1}$ in the integral on the right of (2.13) is of order $O(x^{-1-\delta})$, so this integral is absolutely convergent when extended to infinity. Letting $N \to \infty$, we conclude that the limit $\lim_{N\to\infty} F_N(s)$ exists and is equal to $s\int_1^\infty S_f(x)x^{-s-1}dx$. But this means that $F(s)$ converges and the identity (2.12) holds. □

2.4 Approximating an arithmetic function by a simpler arithmetic function: The convolution method

2.4.1 Description of the method

Among the various methods for estimating sums of arithmetic functions, one of the most widely applicable is the "convolution method" presented in this section. The basic idea of is as follows. Given an arithmetic function f whose partial sums $F(x) = \sum_{n\le x} f(n)$ we want to estimate, we try to express f as a convolution $f = f_0 * g$, where f_0 is a function that approximates f (in a suitable sense) and which is well-behaved in the sense that good estimates for the partial sums $F_0(x) = \sum_{n\le x} f_0(n)$ are available, and where g is a "perturbation" that is small (again in a suitable sense). Writing $f(n) = \sum_{d|n} g(d) f_0(n/d)$, we have

$$
\begin{aligned}
(2.14) \qquad F(x) = \sum_{n\le x} f(n) &= \sum_{n\le x} \sum_{d|n} g(d) f_0(n/d) = \sum_{d\le x} g(d) \sum_{\substack{n\le x \\ d|n}} f_0(n/d) \\
&= \sum_{d\le x} g(d) \sum_{n'\le x/d} f_0(n') = \sum_{d\le x} g(d) F_0(x/d).
\end{aligned}
$$

Substituting known estimates for $F_0(y)$ then yields an estimate for $F(x) = \sum_{n\le x} f(n)$.

We call this method the convolution method, since the idea of writing an unknown function as a convolution of a known function with a perturbation factor is key to the method.

In practice, the approximating function f_0 is usually a very simple and well-behaved function, such as the function 1, or the identity function $f(n) = n$, though other choices are possible, too. In most applications the function f is multiplicative, and an appropriate approximation is usually easily obtained by taking for f_0 a simple multiplicative function whose values on primes are similar (or equal) to the corresponding values of f.

The following examples illustrate typical situations in which the method can be successfully applied, along with appropriate choices of the approximating function. We will carry out the argument in detail for two of these cases.

Examples

(1) $f(n) = \phi(n)$: f is multiplicative with $f(p) = p - 1$ for all primes p. Thus, a natural approximation to f is provided by the identity function id, which at a prime p has value p. The identity $\phi * 1 = \mathrm{id}$ proved earlier implies $\phi = \mathrm{id} * \mu$, so we have $\phi = f_0 * g$ with $f_0 = \mathrm{id}$ and $g = \mu$. The estimation of $\sum_{n \le x} \phi(n)$ will be carried out in detail in Theorem 2.16 below.

(2) $f(n) = \sigma(n)$: This case is very similar to the previous example. The function $\sigma(n)$ is multiplicative with values $\sigma(p) = p + 1$ at primes, and choosing id as the approximating function f_0 leads to an estimate for $\sum_{lex} \sigma(n)$ of the same quality as the estimate for $\sum_{n \le x} \phi(n)$ given in Theorem 2.16.

(3) $f(n) = \phi(n)/n$: f is multiplicative with $f(p) = 1 - 1/p$ for all primes p, so $f_0 = 1$ is a natural choice for an approximating function. The corresponding perturbation factor is $g = \mu/\mathrm{id}$ which can be seen as follows: Starting from the identity $\phi = (\mathrm{id} * \mu)$, we obtain $f = \phi/\mathrm{id} = (\mathrm{id} * \mu)/\mathrm{id}$. Since the function $1/\mathrm{id}$ is completely multiplicative, it "distributes" over the Dirichlet product (see Theorem 1.10), so $f = (\mathrm{id} * \mu)/\mathrm{id} = 1 * \mu/\mathrm{id}$.

(4) $f(n) = \mu^2(n)$: f is multiplicative with values 1 at all primes p, so $f_0 = 1$ serves as the obvious approximating function. See Theorem 2.18 below for a detailed argument in this case.

(5) $f(n) = \lambda(n)$: Suppose we have information on the behavior of $M(x) = \sum_{n \le x} \mu(n)$, such as the relation $M(x) = o(x)$ (a result which, as we will see in the next chapter, is equivalent to the prime number theorem), or the relation $M(x) = O_\epsilon(x^{1/2+\epsilon})$ for $\epsilon > 0$ (which is equivalent to the Riemann Hypothesis). Applying the convolution method with $f = \lambda$ and $f_0 = \mu$ then allows one to show that estimates of the same type hold for $\lambda(n)$.

(6) $f(n) = 2^{\omega(n)}$: Since $\omega(n)$, the number of distinct prime divisors of n, is an additive function, the function $f = 2^\omega$ is multiplicative. At primes f has the same values as the divisor function. This suggests to apply the convolution method with the divisor function as the approximating function, and to try to derive estimates for the partial sums of f from estimates for the partial sums of the divisor function provided by Dirichlet's theorem (see Theorem 2.20 in the following section). This

approach works, and it yields an estimate for $\sum_{n\le x} 2^{\omega(n)}$ of nearly the same quality as Dirichlet's estimate for $\sum_{n\le x} d(n)$.

2.4.2 Partial sums of the Euler phi function

We will prove the following estimate.

Theorem 2.16. *We have*

$$\sum_{n\le x} \phi(n) = \frac{3}{\pi^2}x^2 + O(x\log x) \quad (x \ge 2). \tag{2.15}$$

Before proving this result, we present some interesting applications and interpretations of the result.

Number of Farey fractions of given order. Let Q be a positive integer. The **Farey fractions of order** Q are the rational numbers in the interval $(0, 1]$ with denominator (in reduced form) at most Q. From the definition of $\phi(n)$ it is clear that $\phi(n)$ represents the number of rational numbers in the interval $(0, 1]$ that in reduced form have denominator n. The sum $\sum_{n\le Q} \phi(n)$ is therefore equal to the number of rationals in the interval $(0, 1]$ with denominators $\le Q$, i.e., the number of Farey fractions of order Q. The theorem shows that this number is equal to $(3/\pi^2)Q^2 + O(Q\log Q)$.

Lattice points visible from the origin. A second application of the theorem is obtained by interpreting the pairs (n, m), with $1 \le m \le n$ and $(m, n) = 1$ as lattice points in the plane. The number of such pairs is equal to the sum $\sum_{n\le x} \phi(n)$ estimated in the theorem. It is easy to see that the condition $(m, n) = 1$ holds if and only if the point (m, n) is visible from the origin, in the sense that the line segment joining this point with the origin does not pass through another lattice point. The theorem therefore gives an estimate for the number of lattice points in the triangular region $0 < n \le x$, $0 < m \le n$, that are visible from the origin. By a simple symmetry argument, it follows that the total number of lattice points in the first quadrant that are visible from the origin and have coordinates at most x is $(6/\pi^2)x^2 + O(x\log x)$.

Probability that two random integers are coprime. Defining this probability as the limit

$$\lim_{N\to\infty} \frac{1}{N^2}\#\{(n,m) : 1 \le n,m \le N, (n,m) = 1\},$$

we see from the previous application that this limit exists and is equal to $6/\pi^2$.

Proof of Theorem 2.16. We apply the identity (2.14) with $f = \phi$ and $f_0 = \mathrm{id}$ as the approximating function. As noted above, the identity $\mathrm{id} = \phi * 1$ implies $\phi = \mathrm{id} * \mu$, so we have $g = \mu$. Moreover, the summatory function of $f_0 (= \mathrm{id})$ equals

$$F_0(x) = \sum_{n\le x} n = \frac{1}{2}[x]([x]+1) = \frac{1}{2}x^2 + O(x).$$

Substituting this estimate into (2.14) gives

$$\begin{aligned}\sum_{n\le x}\phi(n) &= \sum_{d\le x}\mu(d)\left(\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right)\\ &= \frac{1}{2}x^2\sum_{d\le x}\frac{\mu(d)}{d^2} + O\left(x\sum_{d\le x}\frac{1}{d}\right)\\ &= \frac{1}{2}x^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + O\left(x^2\sum_{d>x}\frac{1}{d^2}\right) + O\left(x\sum_{d\le x}\frac{1}{d}\right).\end{aligned}$$

(Note here that for the estimation of $\sum_{d\le x}\mu(d)d^{-2}$ in the last step we used the "trick" of extending the sum to infinity and estimating the tail of the infinite series. This is a very useful device that can be applied to any finite sum that becomes convergent, and hence equal to a constant, when the summation is extended to infinity.) Since $\sum_{d>x} d^{-2} \ll 1/x$ (e.g., by Euler's summation formula, or, simpler, by noting the sum is $\le \int_{x-1}^{\infty} t^{-2}dt = (x-1)^{-1}$) and $\sum_{d\le x} 1/d \ll \log x$ for $x \ge 2$, the two error terms are of order $O(x)$ and $O(x\log x)$, respectively, while the main term is Cx^2, with $C = (1/2)\sum_{d=1}^{\infty}\mu(d)/d^2$.

To complete the proof, it remains to show that the constant C is equal to $3/\pi^2$. This follows from the following lemma. □

Lemma 2.17. *We have* $\sum_{n=1}^{\infty}\mu(n)n^{-2} = 6/\pi^2$.

Proof. By the Moebius identity $e(n) = \sum_{d|n} \mu(d)$ we have

$$\begin{aligned} 1 &= \sum_{n=1}^{\infty} \frac{e(n)}{n^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{d|n} \mu(d) \\ &= \sum_{d=1}^{\infty} \sum_{m=1}^{\infty} \frac{\mu(d)}{(dm)^2} \\ &= \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \sum_{m=1}^{\infty} \frac{1}{m^2}. \end{aligned}$$

Hence

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

By Theorem A.1 of the Appendix, the sum $\sum_{n=1}^{\infty} n^{-2}$ is equal to $\pi^2/6$. The result now follows. □

2.4.3 The number of squarefree integers below x

Since $\mu^2(n)$ is the characteristic function of the squarefree integers, the summatory function of μ^2 is the counting function for the squarefree integers. The following theorem gives an estimate for this function.

Theorem 2.18. *We have*

$$\sum_{n \le x} \mu^2(n) = \frac{6}{\pi^2} x + O(\sqrt{x}) \quad (x \ge 1). \tag{2.16}$$

Thus, the "probability" that a random integer is squarefree is $6/\pi^2 = 0.6079\ldots$.

Proof. Since the function μ^2 is multiplicative and equal to 1 at primes, it is natural to apply the convolution method with $f_0 = 1$ as approximating function. Writing $\mu^2 = f_0 * g = 1 * g$, we have $g = \mu^2 * \mu$ by Moebius inversion.

We begin by explicitly evaluating the function g. Since μ^2 and μ are multiplicative functions, so is the function g, and its value at a prime power p^m is given by

$$g(p^m) = \sum_{k=0}^{m} \mu^2(p^k)\mu(p^{m-k}) = \mu(p^m) + \mu(p^{m-1}) = \begin{cases} 0 & \text{if } m = 1, \\ -1 & \text{if } m = 2, \\ 0 & \text{if } m \ge 3. \end{cases}$$

It follows that $g(n) = 0$ unless $n = m^2$ where m is squarefree, and in this case $g(n) = \mu(m)$. In fact, since $\mu(m) = 0$ if m is not squarefree, we have $g(m^2) = \mu(m)$ for all positive integers m, and $g(n) = 0$ if n is not a square.

The identity (2.14) with g defined as above and $F_0(x) = \sum_{n\le x} 1 = [x]$ then gives

$$\begin{aligned}\sum_{n\le x}\mu^2(n) &= \sum_{d\le x} g(d)[x/d] = \sum_{m\le\sqrt{x}} \mu(m)\left(\frac{x}{m^2}+O(1)\right)\\ &= x\sum_{m\le\sqrt{x}}\frac{\mu(m)}{m^2} + O\left(\sum_{m\le\sqrt{x}}|\mu(m)|\right)\\ &= x\sum_{m=1}^{\infty}\frac{\mu(m)}{m^2} + O\left(x\sum_{m>\sqrt{x}}\frac{1}{m^2}\right) + O(\sqrt{x}).\end{aligned}$$

(Note again the trick of extending a convergent sum to an infinite series and estimating the tail.) The coefficient of x in the main term is $\sum_{m=1}^{\infty}\mu(m)/m^2 = 6/\pi^2$ by Lemma 2.17, the second of the two error terms is of the desired order of magnitude $O(\sqrt{x})$, and in view of the estimate $\sum_{n>y} 1/n^2 \ll 1/y$ the same holds for the first error term. The asserted estimate therefore follows. □

2.4.4 Wintner's mean value theorem

Given an arithmetic function f, we say that f has a **mean value** if the limit

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x} f(n)$$

exists (and is finite), and we denote the limit by $M(f)$, if it exists. The concept of a mean value is a useful one, as many results in number theory can be phrased in terms of existence of a mean value. For example, as we will show in the next chapter, the prime number theorem is equivalent to the assertions $M(\Lambda) = 1$ and $M(\mu) = 0$; Theorem 2.18 above implies $M(\mu^2) = 6/\pi^2$; and a similar argument shows that $M(\phi/\,\mathrm{id}) = 6/\pi^2$.

As a first illustration of the convolution method, we prove a result due to A. Wintner, that gives a general sufficient condition for the existence of a mean value. Note that this theorem does not require the function f to be multiplicative.

Theorem 2.19 (Wintner's mean value theorem). *Suppose $f = 1 * g$, where $\sum_{n=1}^{\infty} |g(n)|/n < \infty$. Then f has a mean value given by $M(f) = \sum_{n=1}^{\infty} g(n)/n$.*

As an illustration of this result, we consider again the function $f = \mu^2$. We have $f = 1 * g$, where the function $g = \mu^2 * \mu$ is given by $g(n) = \mu(m)$ if $n = m^2$ and $g(n) = 0$ if n is not a square, as shown in the proof of Theorem 2.18. Hence the series $\sum_{n=1}^{\infty} g(n)/n$ equals $\sum_{m=1}^{\infty} \mu(m)/m^2$, which converges absolutely, with sum $6/\pi^2$. Wintner's theorem therefore applies and shows that μ^2 has mean value $6/\pi^2$, as we had obtained in Theorem 2.18. (Of course, a direct application of the convolution method, as in the proof of Theorem 2.18, may yield more precise estimates with explicit error terms in any given case. The main advantage of Wintner's mean value theorem lies in its generality.)

Proof. Applying again the identity (2.14) with $f_0 = 1$, $F_0(x) = [x]$, we obtain

$$\begin{aligned}\frac{1}{x}\sum_{n\le x} f(n) &= \frac{1}{x}\sum_{d\le x} g(d)[x/d] \\ &= \sum_{d=1}^{\infty}\frac{g(d)}{d} + O\left(\sum_{d>x}\frac{|g(d)|}{d}\right) + O\left(\frac{1}{x}\sum_{d\le x}|g(d)|\right).\end{aligned}$$

As $x \to \infty$, the first of the two error terms tends to zero, by convergence of the series $\sum_{d=1}^{\infty} |g(d)|/d$. The same is true for the second error term, in view of Kronecker's Lemma (Theorem 2.12) and the hypothesis that $\sum_{d=1}^{\infty} |g(d)|/d$ converges. Hence, as $x \to \infty$, the left-hand side converges to the sum $\sum_{d=1}^{\infty} g(d)/d$, i.e., $M(f)$ exists and is equal to the value of this sum. □

2.5 A special technique: The Dirichlet hyperbola method

2.5.1 Sums of the divisor function

In this section we consider a rather special technique, the "Dirichlet hyperbola method," invented by Dirichlet to estimate the partial sums of the divisor function. Dirichlet's result is as follows:

Theorem 2.20 (Dirichlet). *We have*

$$\sum_{n\le x} d(n) = x\log x + (2\gamma-1)x + O(\sqrt{x}) \quad (x\ge 1),$$

where γ is Euler's constant (see Theorem 2.5).

Proof. Let $D(x) = \sum_{n\le x} d(n)$. Writing $d(n) = \sum_{ab=n} 1$, where a and b run over positive integers with product n, we obtain

$$D(x) = \sum_{n\le x}\sum_{ab=n} 1 = \sum_{\substack{a,b\le x\\ ab\le x}} 1.$$

Note that, in the latter sum, the condition $ab\le x$ forces at least one of a and b to be $\le\sqrt{x}$. The key idea now is to split this sum into $\sum_1 + \sum_2 - \sum_3$, where

$$\sum\nolimits_1 = \sum_{a\le\sqrt{x}}\sum_{b\le x/a}, \quad \sum\nolimits_2 = \sum_{b\le\sqrt{x}}\sum_{a\le x/b}, \quad \sum\nolimits_3 = \sum_{a\le\sqrt{x}}\sum_{b\le\sqrt{x}}.$$

The last sum, $\sum_3$, here compensates for the overlap, i.e., those terms (a,b) that are counted in both $\sum_1$ and $\sum_2$.

The last sum is trivial to estimate. We have

$$\sum\nolimits_3 = \left(\sum_{a\le\sqrt{x}} 1\right)\left(\sum_{b\le\sqrt{x}} 1\right) = [\sqrt{x}]^2 = (\sqrt{x}+O(1))^2 = x + O(\sqrt{x}).$$

Also, $\sum_2 = \sum_1$, so it remains to estimate $\sum_1$.

This is rather straightforward, using the estimate for the partial sums of the harmonic series (Theorem 2.5). We have

$$\begin{aligned}\sum\nolimits_1 &= \sum_{a\le\sqrt{x}}\left[\frac{x}{a}\right] = x\sum_{a\le\sqrt{x}}\frac{1}{a} + O\left(\sum_{a\le\sqrt{x}} 1\right)\\ &= x\left(\log\sqrt{x}+\gamma+O\left(\frac{1}{\sqrt{x}}\right)\right)+O(\sqrt{x})\\ &= \frac{1}{2}x\log x + \gamma x + O(\sqrt{x}).\end{aligned}$$

Hence

$$\sum\nolimits_1 + \sum\nolimits_2 - \sum\nolimits_3 = x\log x + (2\gamma-1)x + O(\sqrt{x}),$$

which is the desired estimate. □

2.5.2 Extensions and remarks

Geometric interpretation. The argument in this proof has the following simple geometric interpretation, which explains why it is called the "hyperbola method." The sum $D(x)$ is equal to the number of pairs (a, b) of positive integers with $ab \le x$, i.e., the number of lattice points in the first quadrant (not counting points on the coordinate axes) that are to the left of the hyperbola $ab = x$. The sums $\sum_1$ and $\sum_2$ count those points which, in addition, fall into the infinite strips defined by $0 < a \le \sqrt{x}$, and $0 < b \le \sqrt{y}$, respectively, whereas $\sum_3$ counts points that fall into the intersection of these two strips. It is geometrically obvious that $\sum_1 + \sum_2 - \sum_3$ is equal to $D(x)$, the total number of lattice points located in the first quadrant and to the left of the hyperbola $ab = x$.

The hyperbola method for general functions. The method underlying the proof of Dirichlet's theorem can be generalized as follows. Consider a sum $F(x) = \sum_{n \le x} f(n)$, and suppose f can be represented as a convolution $f = g * h$. Letting $G(x)$ and $H(x)$ denote the partial sums of the functions $g(n)$ and $h(n)$, respectively, we can try to obtain a good estimate for $F(x)$ by writing $F(x) = \sum_1 + \sum_2 - \sum_3$ with

$$\sum\nolimits_1 = \sum_{a \le \sqrt{x}} g(a)H(x/a), \quad \sum\nolimits_2 = \sum_{b \le \sqrt{x}} h(a)G(x/b),$$
$$\sum\nolimits_3 = G(\sqrt{x})H(\sqrt{x}),$$

and estimating each of these sums individually. This can lead to better estimates than more straightforward approaches (such as writing $F(x) = \sum_{a \le x} g(a)H(x/a)$), provided good estimates for the functions $H(x)$ and $G(x)$ are available. The Dirichlet divisor problem is an ideal case, since here the functions g and h are identically 1, and $H(x) = G(x) = [x]$ for all $x \ge 1$. In practice, the usefulness of this method is limited to a few very special situations, which are similar to that of the Dirichlet divisor problem, and in most cases the method does not provide any advantage over simpler approaches. In particular, the convolution method discussed in the previous section has a much wider range of applicability, and for most problems this should be the first method to try.

Maximal order of the divisor function. Dirichlet's theorem gives an estimate for the "average order" of the divisor function, but the divisor func-

tion can take on values that are significantly smaller or significantly larger than this average. Regarding lower bounds, we have $d(n) = 2$ whenever n is prime, and this bound is obviously best possible. The problem of obtaining a similarly optimal upper bound is harder. It is easy to prove that $d(n)$ grows at a rate slower than any power of n, in the sense that, for any given $\epsilon > 0$ and all sufficiently large n, we have $d(n) \le n^{\epsilon}$. This can be improved to $d(n) \le \exp\{(1+\epsilon)(\log 2)(\log n)/(\log\log n)\}$, for any $\epsilon > 0$ and $n \ge n_0(\epsilon)$, a bound that is best-possible, in the sense that, if $1+\epsilon$ is replaced by $1-\epsilon$, it becomes false.

The Dirichlet divisor problem. Let $\Delta(x)$ denote the error term in Dirichlet's theorem, i.e., $\Delta(x) = \sum_{n\le x} d(n) - x\log x - (2\gamma - 1)x$. Thus $\Delta(x) = O(\sqrt{x})$ by Dirichlet's theorem. The problem of estimating $\Delta(x)$ is known as the Dirichlet divisor problem and attained considerable notoriety. The problem is of interest, partly because it is a difficult problem that is still largely unsolved, but mainly because in trying to approach this problem one is led to other deep problems (involving so-called "exponential sums") which have connections with other problems in number theory, including the Riemann Hypothesis. Thus, significant progress on this problem will likely have ramifications on a host of other problems. Most of the known results are estimates of the form $(*)$ $\Delta(x) = O(x^{\theta})$ with a certain constant θ. Dirichlet's theorem shows that one can take $\theta = 1/2$. In the other direction, G.H. Hardy proved in the early part of the 20th century that the estimate does not hold with a value of θ that is less than $1/4$. It is conjectured that $1/4$ is, in fact, the "correct" exponent, but this is still open. Nearly 100 years ago, G.F. Voronoii proved that one can take $\theta = 1/3 = 0.333\ldots$, but despite enormous efforts by many authors not much progress has been made: the current record for θ is near 0.31.

2.6 Exercises

2.1 For $x \geq e$ define $I(x) = \int_e^x \log\log t\, dt$. Obtain an estimate for $I(x)$ to within an error term $O(x/\log^2 x)$.

2.2 Let $f(x)$ and $g(x)$ be positive, continuous functions on $[0, \infty)$, and set $F(x) = \int_0^x f(y)dy$, $G(x) = \int_0^x g(y)dy$.

(i) Show (by a counterexample) that the relation

$$f(x) = o(g(x)) \quad (x \to \infty) \tag{1}$$

does *not* imply

$$F(x) = o(G(x)) \quad (x \to \infty). \tag{2}$$

(ii) Find an appropriate *general* condition on $g(x)$ under which the implication (1) $\Rightarrow$ (2) becomes true.

Remark: It is trivial to show that, if "o" is replaced by "O" in (1) and (2), then the implication holds. In other words, one can "pull out" a O-sign from an integral (provided the integrand is positive).

2.3 Show that if $f(x)$ satisfies $f(x) = x^2 + O(x)$, and f is differentiable *with nondecreasing derivative* $f'(x)$ for sufficiently large x, then $f'(x) = 2x + O(\sqrt{x})$.

Remark. While O-estimates can be integrated provided the range of integration is contained in the range of validity of the estimate, in general such estimates cannot be differentiated. The above problem illustrates a situation where, under certain additional conditions (namely, the monoticity of the derivative), differentiation of a O-estimate is allowed.

2.4 Let n be an integer ≥ 2 and p a positive real number. A useful estimate is

$$\left(\sum_{i=1}^n a_i\right)^p \asymp_{n,p} \sum_{i=1}^n a_i^p \quad (a_1, a_2, \ldots, a_n > 0).$$

Prove this estimate with explicit and *best-possible* values for the implied constants. In other words, determine the largest value of $c_1 = c_1(n,p)$ and the smallest value of $c_2 = c_2(n,p)$ such that

$$c_1 \sum_{i=1}^n a_i^p \leq \left(\sum_{i=1}^n a_i\right)^p \leq c_2 \sum_{i=1}^n a_i^p \quad (a_1, a_2, \ldots, a_n > 0).$$

2.5 Obtain an estimate for the sum $\sum_{n\le x}(\log n)/n$ with error term $O((\log x)/x)$.

2.6 Given a positive integer k, let $S_k(x) = \sum_{n\le x}(\log n - \log x)^k$. Estimate $S_k(x)$ to within an error $O_k((\log x)^k)$. Deduce that, for each k, the limit $\lambda_k = \lim_{x\to\infty}(1/x)S_k(x)$ exists (as a finite number), and obtain an explicit evaluation of the constant λ_k.

2.7 Given an arithmetic function f define a mean value $H(f)$ by

$$H(f) = \lim_{x\to\infty} \frac{1}{x\log x}\sum_{n\le x} f(n)\log n,$$

if the limit exists. Show that $H(f)$ exists if and only if the ordinary mean value $M(f) = \lim_{x\to\infty}(1/x)\sum_{n\le x} f(n)$ exists.

2.8 Given an arithmetic function $a(n)$, $n = 1, 2, \ldots$, and a real number $\alpha > -1$ define a mean value $M_\alpha(a)$ by

$$M_\alpha(a) = \lim_{x\to\infty} \frac{1+\alpha}{x^{1+\alpha}}\sum_{n\le x} n^\alpha a(n),$$

provided the limit exist. (In particular, $M_0(a) = M(a)$ is the usual asymptotic mean value of a.) Prove, using a rigorous $\epsilon - x_0$ argument, that the mean value $M_\alpha(a)$ exists if and only if the ordinary mean value $M(a) = M_0(a)$ exists. (As a consequence, if one of the mean values $M_\alpha(a)$, $\alpha > -1$, exists, then all of these mean values exist.)

2.9 Say that an arithmetic function f has an *analytic mean value* A if the Dirichlet series $F(s) = \sum_{n=1}^\infty f(n)n^{-s}$ satisfies

$$F(s) = \frac{A}{s-1} + o\left(\frac{1}{s-1}\right) \quad (s\to 1+). \tag{0}$$

Show that if f has a logarithmic mean value $L(f) = A$, then f also has an analytic mean value, and the two mean values are equal.

2.10 Let f be an arithmetic function having a non-zero mean value $M(f) = A$, and let α be a fixed real number. Obtain an asymptotic formula for the sums $\sum_{n\le x} f(n)n^{i\alpha}$.

2.11 Say that an arithmetic function f has a *strong logarithmic mean value* A, and write $L^*(f) = A$, if f satisfies an estimate of the form

$$\sum_{n\le x} \frac{f(n)}{n} = A\log x + B + o(1) \quad (x\to\infty)$$

for some constants A and B. This is obviously a stronger condition than the existence of a logarithmic mean value which would correspond to an estimate of the above form with $o(\log x)$ in place of $B + o(1)$.

(i) Show that, in contrast to the (ordinary) logarithmic mean value, this stronger condition is sufficient to imply the existence of the asymptotic mean value. That is, show that if f has a strong logarithmic mean value A in the above sense, then the ordinary mean value $M(f)$ also exists and is equal to A.

(ii) Is the converse true, i.e., does the existence of $M(f)$ imply that of a strong logarithmic mean value?

2.12 Let $\lambda > 1$ and $t \neq 0$ be fixed real numbers, and $S_{t,\lambda}(x) = \sum_{x<n\le\lambda x} n^{-1-it}$. Obtain an estimate for $S_{t,\lambda}(x)$ as $x\to\infty$ with error term $O_{t,\lambda}(1/x)$. Deduce from this estimate that for any non-zero t and any $\lambda > 1$, the limit $\lim_{x\to\infty} |S_{t,\lambda}(x)|$ exists, and that, for given $t \neq 0$ and *suitable* choices of λ, this limit is non-zero. (Thus, by Cauchy's criterion, the series $\sum_{n=1}^{\infty} n^{-1-it}$ diverges for every real $t \neq 0$.)

2.13 Obtain an asymptotic estimate with error term $O(x^{1/3})$ for the number of squarefull integers $\le x$, i.e., for the quantity

$$S(x) = \#\{n \le x : p|n \Rightarrow p^2|n\}.$$

2.14 For any positive integer n define its squarefree kernel $k(n)$ by $k(n) = \prod_{p|n} p$. Obtain an estimate for $\sum_{n\le x} k(n)/n$ with error term $O(\sqrt{x})$.

2.15 Obtain an estimate, of similar quality as Dirichlet's estimate for $\sum_{n\le x} d(n)$, for the sum $\sum_{n\le x} 2^{\omega(n)}$.

2.16 Obtain an estimate, similar to the estimate for $\sum_{n\le x} 1/n$ proved in Theorem 2.5, for the sum $\sum_{n\le x} 1/\phi(n)$. (Hint: Convolution method.)

2.17 Let $q_1 = 1, q_2 = 2, q_3 = 3, q_4 = 5 \ldots$ denote the sequence of squarefree numbers.

(i) Obtain an asymptotic estimate with error term $O(\sqrt{n})$ for q_n.

(ii) Show that there are arbitrarily large gaps in the sequence $\{q_n\}$, i.e., $\limsup_{n\to\infty}(q_{n+1} - q_n) = \infty$. (Hint: Chinese Remainder Theorem.)

(iii) Prove the stronger bound

$$\limsup_{n\to\infty} \frac{q_{n+1} - q_n}{\log n / \log\log n} \geq \frac{1}{2}.$$

(iv)* (Harder) Prove that (iii) holds with $1/2$ replaced by the constant $\pi^2/12$, i.e., that the limsup above is at least $\pi^2/12$.

2.18 Show that, $\phi(n) \geq n/4$ holds for at least $1/3$ of all positive integers n (in the sense that if A is the set of such n, then $\liminf_{x\to\infty}(1/x)\#\{n \leq x : n \in A\} \geq 1/3$). (Hint: use the fact that (1) $\sum_{n\leq x} \phi(n) \sim (3/\pi^2)x^2$ (which was proved in Theorem 2.16) or (2) $\sum_{n\leq x} \phi(n)/n \sim (6/\pi^2)x$ (an easy consequence of Wintner's theorem, or of (1), by partial summation).)

2.19 Let $f = 1 * g$. Wintner's theorem (Theorem 2.19) shows that if the series

$$\sum_{n=1}^{\infty} \frac{g(n)}{n} \tag{1}$$

converges *absolutely*, then the mean value $M(f)$ of f exists and is equal to the sum of the series (1).

(i) Show that the conclusion of Wintner's theorem remains valid if the series (1) converges only conditionally and if, in addition,

$$\limsup_{x\to\infty} \frac{1}{x} \sum_{n\leq x} |g(n)| < \infty. \tag{2}$$

(ii) Show that condition (2) cannot be dropped; i.e., construct an example of a function g for which the series (1) converges, but the function $f = 1 * g$ does not have a mean value.

2.20 Using the Dirichlet hyperbola method (or some other method), obtain an estimate for the sum $\sum_{n\leq x} d(n)/n$ with an error term $O((\log x)/\sqrt{x})$.

Chapter 3

Distribution of primes I: Elementary results

The Prime Number Theorem (PNT), in its most basic form, is the asymptotic relation $\pi(x) \sim x/\log x$ for the prime counting function $\pi(x)$, the number $\pi(x)$ of primes $\leq x$. This result had been conjectured by Legendre and (in a more precise form) by Gauss, based on examining tables of primes. However, neither succeeded in proving the PNT (and it certainly wasn't for lack of trying!). It was only much later, near the end of the 19th century, that a proof of the PNT was given, independently by J. Hadamard and C. de la Vallee Poussin, via a new, analytic, approach that was not available to Gauss and his contemporaries. We will give a proof of the PNT, in a strong form with an explicit error term, in a later chapter.

In this chapter we establish a number of elementary results on the distribution of primes that are much easier to prove than the PNT and which, for the most part, have been known long before the PNT was proved. These results are of interest in their own right, and they have many applications.

3.1 Chebyshev type estimates

Getting upper and lower bounds for the prime counting function $\pi(x)$ is surprisingly difficult. Euclid's result that there are infinitely many primes shows that $\pi(x)$ tends to infinity, but the standard proofs of the infinitude of prime are indirect and do not give an explicit lower bound for $\pi(x)$, or give only a very weak bound. For example, Euclid's argument shows that the n-th prime p_n satisfies the bound $p_n \leq p_1 \dots p_{n-1} + 1$. By induction, this implies that $p_n \leq e^{e^{n-1}}$ for all n, from which one can deduce the bound

$\pi(x) \geq \log\log x$ for sufficiently large x. This bound is far from the true order of $\pi(x)$, but it is essentially the best one derive from Euclid's argument.

Euler's proof of the infinitude of primes proceeds by showing that $\sum_{p\leq x} 1/p \geq \log\log x - c$ for some constant c and sufficiently large x. Although this gives the correct order for the partials sum of the reciprocals of primes (as we will see below, the estimate is accurate to within an error $O(1)$), one cannot deduce from this a lower bound for $\pi(x)$ of comparable quality. In fact, one can show (see the exercises) that the most one can deduce from the above bound for $\sum_{p\leq x} 1/p$ is a lower bound of the form $\pi(x) \gg \log x$. While this is better than the bound obtained from Euclid's argument, it is still far from the true order of magnitude.

In the other direction, getting non-trivial upper bounds for $\pi(x)$ is not easy either. Even showing that $\pi(x) = o(x)$, i.e., that the primes have density zero among all integers, is by no means easy, when proceeding "from scratch". (Try to prove this bound without resorting to any of the results, techniques, and tricks you have learned so far.)

In light of these difficulties in getting even relatively weak nontrivial bounds for $\pi(x)$ it is remarkable that, in the middle of the 19th century, the Russian mathematician P.L. Chebyshev was able to determine the precise order of magnitude of the prime counting function $\pi(x)$, by showing that there exist positive constants c_1 and c_2 such that

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}$$

for all sufficiently large x. In fact, Chebyshev proved such an inequality with constants $c_1 = 0.92\ldots$ and $c_2 = 1.10\ldots$. This enabled him to conclude that, for sufficiently large x (and, in fact, for all $x \geq 1$) there exists a prime p with $x < p \leq 2x$, an assertion known as **Bertrand's postulate**.

In establishing these bounds, Chebyshev introduced the auxiliary functions

$$\theta(x) = \sum_{p\leq x} \log p, \quad \psi(x) = \sum_{n\leq x} \Lambda(n),$$

which proved to be extremely useful in subsequent work. Converting results on $\pi(x)$ to results on $\psi(x)$ or $\theta(x)$, or vice versa, is easy (see Theorem 3.2 below), and we will state most of our results for all three of these functions and use whichever version is most convenient for the proof.

Theorem 3.1 (Chebyshev estimates). *For $x \geq 2$ we have*

(i) $$\psi(x) \asymp x,$$

(ii) $$\theta(x) \asymp x,$$

(iii) $$\pi(x) \asymp \frac{x}{\log x}.$$

Proof. We will establish (i), and then deduce (ii) and (iii) from (i).

To prove (i), we need to show that there exist positive constants c_1 and c_2 such that

$$c_1 x \leq \psi(x) \leq c_2 x \tag{3.1}$$

holds for all $x \geq 2$.

We begin by noting that it suffices to establish (3.1) for $x \geq x_0$, for a suitable $x_0 \geq 2$. Indeed, suppose there exists a constant $x_0 \geq 2$ such that (3.1) holds for $x \geq x_0$. Since for $2 \leq x \leq x_0$ we have, trivially, $\psi(x)/x \leq \psi(x_0)/2$ and $\psi(x)/x \geq \psi(2)/x_0 = \log 2/x_0$, it then follows that (3.1) holds for all $x \geq 2$ with constants $c_1' = \min(c_1, \log 2/x_0)$ and $c_2' = \max(c_2, \psi(x_0)/2)$ in place of c_1 and c_2.

In what follows, we may therefore assume that x is sufficiently large. (Recall our convention that O-estimates without explicit range are understood to hold for $x \geq x_0$ with a sufficiently large x_0.)

Define

$$S(x) = \sum_{n \leq x} \log n, \quad D(x) = S(x) - 2S(x/2).$$

To prove (3.1) we will evaluate $D(x)$ in two different ways. On the one hand, using the asymptotic estimate for $S(x)$ established earlier (see Corollary 2.8), we have

$$\begin{aligned} D(x) &= x(\log x - 1) + O(\log x) - 2(x/2)(\log(x/2) - 1) + O(\log(x/2)) \\ &= (\log 2)x + O(\log x). \end{aligned}$$

Since $1/2 < \log 2 < 1$, this implies

$$x/2 \leq D(x) \leq x \quad (x \geq x_0) \tag{3.2}$$

with a suitable x_0.

On the other hand, using the identity $\log n = (\Lambda * 1)(n) = \sum_{d|n} \Lambda(d)$ and interchanging summations, we have

$$S(x) = \sum_{d \leq x} \Lambda(d) \sum_{\substack{n \leq x \\ d|n}} 1 = \sum_{d \leq x} \Lambda(d)[x/d] \quad (x \geq 1), \tag{3.3}$$

where $[t]$ denotes the greatest integer function. Applying (3.3) to $S(x)$ and $S(x/2)$, we get

$$D(x) = S(x) - 2S(x/2) = \sum_{d \le x} \Lambda(d) f(x/d) \quad (x \ge 2), \tag{3.4}$$

where $f(t) = [t] - 2[t/2]$. (Note that in the evaluation of $S(x/2)$ the summation range $d \le x/2$ can be extended to $d \le x$, since the terms with $x/2 < d \le x$ do not contribute to the sum due to the factor $[x/2d]$.) By the elementary inequalities $[s] \le s$ and $[s] > s - 1$, valid for any real number s, we have

$$f(t) \begin{cases} < t - 2(t/2 - 1) = 2, \\ > t - 1 - 2(t/2) = -1. \end{cases}$$

Since the function $f(t) = [t] - 2[t/2]$ is integer-valued, it follows that

$$f(t) \begin{cases} = 1 & \text{if } 1 \le t < 2, \\ \in \{0, 1\} & \text{if } t \ge 2. \end{cases}$$

Hence (3.4) implies

$$D(x) \begin{cases} \le \sum_{d \le x} \Lambda(d) = \psi(x) \\ \ge \sum_{x/2 < d \le x} \Lambda(d) = \psi(x) - \psi(x/2) \end{cases} \qquad (x \ge 2). \tag{3.5}$$

Combining (3.2) and (3.5), we obtain

$$\psi(x) \ge D(x) \ge x/2 \quad (x \ge x_0), \tag{3.6}$$

and

$$\psi(x) \le D(x) + \psi(x/2) \le x + \psi(x/2) \quad (x \ge x_0). \tag{3.7}$$

The first of these inequalities immediately gives the lower bound in (3.1) (with $c_1 = 1/2$). To obtain a corresponding upper bound, we note that iteration of (3.7) yields

$$\psi(x) \le \sum_{i=0}^{k-1} x 2^{-i} + \psi(x 2^{-k}),$$

for any positive integer k such that $x 2^{-k+1} \ge x_0$. Choosing k as the maximal such integer, we have $2^{-k+1} x \ge x_0 > 2^{-k} x$ and thus $\psi(x 2^{-k}) \le \psi(x_0)$, and hence obtain

$$\psi(x) \le \sum_{i=0}^{k-1} x 2^{-i} + \psi(x_0) \le 2x + \psi(x_0),$$

which gives the upper bound in (3.1) for $x \geq x_0$ with a sufficiently large constant c_2 (in fact, we could take $c_2 = 2 + \epsilon$, for $x \geq x_0(\epsilon)$, for any fixed $\epsilon > 0$ with a suitable $x_0(\epsilon)$).

This completes the proof of (i).

To deduce (ii), we note that

$$\psi(x) - \theta(x) = \sum_{p^m \leq x} \log p - \sum_{p \leq x} \log p \tag{3.8}$$
$$= \sum_{p \leq \sqrt{x}} \log p \sum_{2 \leq m \leq \log x / \log p} 1$$
$$\leq \sum_{p \leq \sqrt{x}} (\log p) \left[\frac{\log x}{\log p} \right] \leq \sqrt{x} \log x,$$

so that

$$\theta(x) \begin{cases} \leq \psi(x), \\ \geq \psi(x) - \sqrt{x} \log x. \end{cases}$$

Hence the upper bound in (3.1) remains valid for $\theta(x)$, with the same values of c_2 and x_0, and the lower bound holds for $\theta(x)$ with constant $c_1/2$ (for example) instead of c_1, upon increasing the value of x_0 if necessary.

The lower bound in (iii) follows immediately from that in (ii), since $\pi(x) \geq (1/\log x) \sum_{p \leq x} \log p = \theta(x)/\log x$. The upper bound follows from the inequality

$$\pi(x) \leq \pi(\sqrt{x}) + \frac{1}{\sqrt{\log x}} \sum_{\sqrt{x} < p \leq x} \log p \leq \sqrt{x} + \frac{2}{\log x} \theta(x)$$

and the upper bound in (ii). □

Alternate proofs of Theorem 3.1. The proof given here rests on the convolution identity $\Lambda * 1 = \log$, which relates the "unknown" function Λ to two extremely well-behaved functions, namely 1 and log. Given this relation, it is natural to try to use it to derive information on the average behavior of the function $\Lambda(n)$ from the very precise information that is available on the behavior of the functions 1 and $\log n$. The particular way this identity is used in the proof of the theorem may seem contrived. Unfortunately, more natural approaches don't work, and one has to resort to some sort of "trickery" to get any useful information out of the above identity. For example, it is tempting to try to simply invert the relation $\Lambda * 1 = \log$ to express Λ as $\Lambda = \mu * \log$, interpret Λ as a "perturbation" as the function log and proceed

as in the convolution method described in Section 2.4. Unfortunately, the error terms in this approach are too large to be of any use.

There exist alternate proofs of Theorem 3.1, but none is particularly motivated or natural, and all involve some sort of "trick". For example, a commonly seen argument, which may be a bit shorter than the one given here, but has more the character of pulling something out of the air, is based on an analysis of the middle binomial coefficient $\binom{2n}{n}$: On the one hand, writing this coefficient as a fraction $(n+1)(n+2)\cdots(2n)/n!$ and noting that every prime p with $n < p \le 2n$ divides the numerator, but not the denominator, we see that $\binom{2n}{n}$ is divisible by the product $\prod_{n<p\le 2n} p$. On the other hand, the binomial theorem gives the bound

$$\binom{2n}{n} \le \sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n}.$$

Hence $\prod_{n<p\le 2n} p \le 2^{2n}$, and taking logarithms, we conclude

$$\theta(2n) - \theta(n) = \sum_{n<p\le 2n} \log p \le (2\log 2)n,$$

for any positive integer n. By iterating this inequality, one gets $\theta(2^k) \le (2\log 2)2^k$ for any positive integer k, and then $\theta(x) \le (4\log 2)x$ for any real number $x \ge 2$. This proves the upper bound in (ii) with constant $4\log 2$. The lower bound in (ii) can be proved by a similar argument, based on an analysis of the prime factorization of $\binom{2n}{n}$, and the lower bound

$$\binom{2n}{n} \ge \frac{1}{2n+1} \sum_{k=0}^{2n} \binom{2n}{k} = \frac{2^{2n}}{2n+1}.$$

The constants in Chebyshev's estimates. An inspection of the above argument shows that it yields (3.1) with any constants c_1 and c_2 satisfying $c_1 < \log 2 = 0.69\ldots$ and $c_2 > 2\log 2 = 1.38\ldots$, for sufficiently large x. Chebyshev used a more complicated version of this argument, in which the linear combination $S(x) - 2S(x/2)$ is replaced by $S(x) - S(x/2) - S(x/3) - S(x/5) + S(x/30)$, to obtain $c_1 = 0.92\ldots$ and $c_2 = 1.10\ldots$ as constants in (3.1). For most applications, the values of these constants are not important. However, since the PNT had not been proved at the time Chebyshev proved his estimates, there was a strong motivation

to obtain constants as close to 1 as possible. It is natural to ask if, by considering more general linear combinations of the functions $S(x/k)$, one can further improve these constants. This is indeed the case; in fact, Diamond and Erdös showed that it is possible to obtain constants c_1 and c_2 arbitrarily close to 1, by using Chebyshev's approach with a suitable linear combination of the function $S(x)$. Now, the assertion that (3.1) holds with constants c_1 and c_2 arbitrarily close to 1, clearly implies the PNT in the form $\psi(x) \sim x$, so it would seem that Chebyshev's method in fact yields a proof of the PNT. However, this is not the case, since in proving that c_1 and c_2 can be taken arbitrarily close to 1, Diamond and Erdös had to use the PNT.

Theorem 3.2 (Relation between π, ψ, and θ). *For $x \geq 2$ we have*

(i) $$\theta(x) = \psi(x) + O(\sqrt{x}),$$

(ii) $$\pi(x) = \frac{\psi(x)}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Proof. A slightly weaker version of (i), with error term $O(\sqrt{x}\log x)$ instead of $O(\sqrt{x})$, was established in (3.8) above. To obtain (i) as stated, we use again the identity (3.8) for $\psi(x)-\theta(x)$, but instead of estimating the right-hand side trivially, we apply Chebyshev's bound (which we couldn't use while proving Theorem 3.1). This gives for $\psi(x) - \theta(x)$ the bound $\leq \pi(\sqrt{x})\log x \ll (\sqrt{x}/\log\sqrt{x})\log x \ll \sqrt{x}$.

To obtain (ii), we write

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

and "eliminate" the factor $1/\log p$ by partial summation:

$$\pi(x) = \frac{\theta(x)}{x} - \int_2^x \theta(t)\left(-\frac{1}{t(\log t)^2}\right)dt = \frac{\theta(x)}{x} + \int_2^x \frac{\theta(t)}{t(\log t)^2}dt.$$

Since $\theta(t) \ll t$ by Chebyshev's estimate, the last integral is of order

$$\begin{aligned} &\ll \int_2^x \frac{1}{(\log t)^2}dt \leq \int_2^{\sqrt{x}} \frac{1}{(\log 2)^2} + \int_{\sqrt{x}}^x \frac{1}{(\log\sqrt{x})^2}dt \\ &\ll \sqrt{x} + \frac{x}{(\log\sqrt{x})^2} \ll \frac{x}{(\log x)^2}, \end{aligned}$$

so we have

$$\pi(x) = \frac{\theta(x)}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

In view of (i), we may replace $\theta(x)$ by $\psi(x)$ on the right-hand side, and thus obtain (ii). □

Corollary 3.3 (Equivalent formulations of PNT). *The following relations are equivalent:*

(i) $$\pi(x) \sim \frac{x}{\log x} \quad (x \to \infty),$$

(ii) $$\theta(x) \sim x \quad (x \to \infty),$$

(iii) $$\psi(x) \sim x \quad (x \to \infty).$$

Proof. By the previous theorem, the functions $\psi(x)$, $\theta(x)$, and $\pi(x)\log x$ differ by an error term that is of order $O(x/\log x)$ (at worst), and hence are of smaller order (by a factor $1/\log x$) than the main terms in the asserted relations. □

3.2 Mertens type estimates

A second class of estimates below the level of the PNT are estimates for certain weighted sums over primes, such as the sum of reciprocals of primes up to x. These estimates seem surprisingly strong as the error terms involved are by at least a logarithmic factor smaller than the main term, yet they are not strong enough to imply the PNT.

Theorem 3.4 (Mertens' estimates). *We have*

(i) $$\sum_{n \le x} \frac{\Lambda(n)}{n} = \log x + O(1),$$

(ii) $$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1),$$

(iii) $$\sum_{p \le x} \frac{1}{p} = \log\log x + A + O\left(\frac{1}{\log x}\right),$$

(iv) $$\prod_{p \le x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right),$$

where A is a constant and γ is Euler's constant.

Before proving this result, we make some remarks and derive two corollaries.

Estimate (iv) is usually referred to as **Mertens' formula**. We will prove this result here with an unspecified constant in place of $e^{-\gamma}$; the proof that this constant is equal to $e^{-\gamma}$ requires additional tools and will be deferred until the next chapter. It is easy to show that the product on the left-hand side of (iv) is equal to the density of positive integers that have no prime factor $\leq x$, i.e., $\lim_{y\to\infty}(1/y)\#\{n \leq y : p|n \Rightarrow p > x\}$. (For example, this follows by applying Wintner's mean value theorem (Theorem 2.11) to the characteristic function of the integers with no prime factor $\leq x$.) Mertens' formula shows that this density, i.e., the "probability" that an integer has no prime factors $\leq x$, tends to zero as $x \to \infty$ at a rate proportional to $1/\log x$.

An equivalent formulation of (iv), obtained by taking the reciprocal on each side, is

$$\text{(iv')} \qquad \prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1} = e^{\gamma}(\log x)\left(1+O\left(\frac{1}{\log x}\right)\right).$$

This version has the following interesting interpretation:

Let $P(x)$ denote the product on the left of (iv'). Expanding each of the factors $(1-1/p)^{-1}$ into a geometric series and multiplying out all terms in this product, one obtains a sum over terms $(*)$ $\prod_{p\leq x} p^{-\alpha_p}$, where the exponents α_p run over all non-negative integers. Now, $(*)$ is the reciprocal of a positive integer n all of whose prime factors are $\leq x$, and by the fundamental theorem of arithmetic each such reciprocal $1/n$ has exactly one representation in the form $(*)$. Hence, letting $A_x = \{n \in \mathbb{N} : p|n \Rightarrow p \leq x\}$ denote the set of such integers n, we have $P(x) = \sum_{n\in A_x} 1/n$. Now A_x clearly contains every positive integer $n \leq x$, so we have the lower bound $P(x) \geq \sum_{n\leq x} 1/n$, which is asymptotic to $\log x$. The estimate (iv') shows that $P(x)$ is (asymptotically) by a factor e^{γ} larger than this trivial lower bound. The difference between the actual estimate and the trivial bound, $(e^{\gamma}-1)\log x$, can be interpreted as a measure of how many integers from A_x were missed by only counting integers $n \leq x$.

The estimates (i)–(iii) can be viewed as average versions of the PNT, expressed in terms of $\psi(x)$, $\theta(x)$, and $\pi(x)$, respectively. For example, (i) implies that the *logarithmic mean value* of the von Mangoldt function $\Lambda(n)$ exists and is equal to 1. The existence of the *ordinary (asymptotic) mean value* of $\Lambda(n)$ would imply (in fact, is equivalent to) the PNT. However, as we have seen in Theorems 2.13 and 2.14, the existence of an asymptotic mean value is a strictly stronger assertion than the existence of a logarithmic mean value, so the PNT does not follow from these estimates.

The following corollary makes the interpretation of Mertens' estimates as average versions of the PNT more explicit.

Corollary 3.5. *We have*

$$\int_1^x \frac{\psi(t)/t}{t} dt = \log x + O(1). \tag{3.9}$$

Proof. By partial summation and Chebyshev's estimate (Theorem 3.1), the left-hand side of (i) in Theorem 3.4 equals

$$\frac{\psi(x)}{x} + \int_1^x \frac{\psi(t)}{t^2} dt = O(1) + \int_1^x \frac{\psi(t)/t}{t} dt,$$

so (i) implies the estimate of the corollary. □

A simple consequence of this estimate is the following result, which says that the proportionality constant in the PNT, if it exists (i.e., if $\psi(x) \sim cx$ for *some* constant c), must be equal to 1.

Corollary 3.6. *Let A_* and A^* denote, respectively, the* lim inf*, and the* lim sup*, of $\psi(x)/x$. Then $A_* \le 1 \le A^*$. Moreover, if the limit $A = \lim_{x\to\infty} \psi(x)/x$ exists, then $A = 1$.*

Proof. The second assertion clearly follows from the first. To prove the first assertion, suppose, for example, that A^* is strictly less than 1. Then there exist $\epsilon > 0$ and $x_0 \ge 2$ such that $\psi(x) \le (1-\epsilon)x$ for $x \ge x_0$. Hence, for $x \ge x_0$, the left-hand side of (3.9) is

$$\le \int_1^{x_0} \frac{\psi(t)/t}{t} dt + (1-\epsilon) \int_{x_0}^x \frac{1}{t} dt \le \psi(x_0) \int_1^\infty \frac{1}{t^2} dt + (1-\epsilon) \log x,$$

which contradicts (3.9) if x is sufficiently large. Hence $A^* \ge 1$, and a similar argument shows $A_* \le 1$. □

Proof of Theorem 3.4. To prove (i) we begin, as in the proof of Chebyshev's estimate for $\psi(x)$, with two evaluations for $S(x) = \sum_{n\le x} \log n$. On the one hand, by Corollary 2.7, we have $S(x) = x \log x + O(x)$. On the other hand, (3.3) and Chebyshev's estimate imply

$$\begin{aligned} S(x) &= \sum_{d\le x} \Lambda(d)[x/d] = x \sum_{n\le x} \frac{\Lambda(d)}{d} + O\left(\sum_{d\le x} \Lambda(d)\right) \\ &= x \sum_{n\le x} \frac{\Lambda(d)}{d} + O(x). \end{aligned}$$

Setting the last expression equal to $x \log x + O(x)$ and dividing by x, we obtain (i).

The estimate (ii) follows from (i) on noting that the difference between the sums in (i) and (ii) equals

$$\sum_{\substack{p^m \le x \\ m \ge 2}} \frac{\log p}{p^m},$$

which can be bounded by

$$\le \sum_p \log p \sum_{m=2}^{\infty} \frac{1}{p^m} \le 2 \sum_p \frac{\log p}{p^2} < \infty.$$

Hence the sums in (i) and (ii) differ by a term of order $O(1)$, and so (ii) follows from (i).

We now deduce (iii) from (ii). To this end we write the summand $1/p$ as $((\log p)/p)(1/\log p)$ and apply partial summation to "remove" the factor $1/\log p$. Defining $L(t)$ and $R(t)$ by

$$L(t) = \sum_{p \le t} \frac{\log p}{p} = \log t + R(t)$$

(so that $R(t) = O(1)$ by (ii)), we obtain

$$\begin{aligned} \sum_{p \le x} \frac{1}{p} &= \frac{L(x)}{\log x} - \int_2^x L(t) \frac{-1}{t(\log t)^2} dt \\ &= 1 + \frac{R(x)}{\log x} + \int_2^x \frac{1}{t \log t} dt + \int_2^x \frac{R(t)}{t(\log t)^2} dt \\ &= 1 + O\left(\frac{1}{\log x}\right) + \log\log x - \log\log 2 + I(x), \end{aligned}$$

where $I(x) = \int_2^x R(t)/(t \log^2 t) dt$. To obtain the desired estimate (iii), it suffices to show that, for some constant C,

$$I(x) = C + O\left(\frac{1}{\log x}\right). \tag{3.10}$$

To prove this, note that, since $R(t) = O(1)$ and the integral $\int_2^\infty (t \log^2 t)^{-1} dt$ converges, the infinite integral $I(\infty) = \int_2^\infty R(t)/(t \log^2 t) dt$ converges. Setting $C = I(\infty)$, we have

$$I(x) = C - \int_x^\infty \frac{R(t)}{t(\log t)^2} dt = C + O\left(\int_x^\infty \frac{1}{t(\log t)^2} dt\right) = C + O\left(\frac{1}{\log x}\right),$$

which proves (3.10).

It remains to prove (iv). We will establish (iv) with *some* positive constant B in place of $e^{-\gamma}$, but defer the proof that this constant equals $e^{-\gamma}$ (which is, in fact, the most difficult part of the proof of Theorem 3.4), to a later chapter.

Taking logarithms, (iv) becomes

$$\sum_{p\le x} \log\left(1-\frac{1}{p}\right) = -\gamma - \log\log x + \log\left(1+O\left(\frac{1}{\log x}\right)\right).$$

Since, for $|y| \le 1/2$, $|\log(1+y)| \asymp |y|$, this estimate is equivalent to

$$-\sum_{p\le x} \log\left(1-\frac{1}{p}\right) = C + \log\log x + O\left(\frac{1}{\log x}\right), \tag{3.11}$$

with $C = -\gamma$. We will show that the latter estimate holds, with a suitable constant C.

Using the expansion $-\log(1-x) = \sum_{n\ge1} x^n/n$ ($|x|<1$), we have

$$-\sum_{p\le x} \log\left(1-\frac{1}{p}\right) = \sum_{p\le x}\frac{1}{p} + \sum_{p\le x} r_p,$$

with $r_p = \sum_{m=2}^{\infty} 1/(mp^m)$. Since $|r_p| \le (1/2)\sum_{m=2}^{\infty} p^{-m} \le p^{-2}$, the series $\sum_p r_p$ is absolutely convergent, with sum R, say, and we have

$$\sum_{p\le x} r_p = R - \sum_{p>x} r_p = R + O\left(\sum_{p>x}\frac{1}{p^2}\right) = R + O\left(\frac{1}{x}\right).$$

Hence the difference between the left-hand sides of (iii) and (3.11) is $R + O(1/x)$. Therefore (3.11) follows from (iii).

□

3.3 Elementary consequences of the PNT

The following result gives some elementary consequences of the PNT.

Theorem 3.7 (Elementary consequences of the PNT). *The PNT implies:*

(i) The nth prime p_n satisfies $p_n \sim n\log n$ as $n\to\infty$.

(ii) The function $\omega(n)$, the number of distinct prime factors of n, has maximal order $(\log n)/(\log\log n)$, i.e., it satisfies

$$\limsup_{n\to\infty} \frac{\omega(n)}{(\log n)/(\log\log n)} = 1.$$

(iii) For every $\epsilon > 0$ there exists $x_0 = x_0(\epsilon) \geq 2$ such that for all $x \geq x_0$ there exists a prime p with $x < p \leq (1+\epsilon)x$.

(iv) The set of rational numbers p/q with p and q prime is dense on the positive real axis.

(v) Given any finite string $a_1 \dots a_n$ of digits $\{0, 1, \dots, 9\}$ with $a_1 \neq 0$, there exists a prime number whose decimal expansion begins with this string.

Proof. (i) Since $p_n \to \infty$ as $n \to \infty$, the PNT gives

$$n = \pi(p_n) \sim \frac{p_n}{\log p_n} \quad (n \to \infty). \tag{3.12}$$

This implies that, for any fixed $\epsilon > 0$ and all sufficiently large n, we have $p_n^{1-\epsilon} \leq n \leq p_n$, and hence $(1-\epsilon)\log p_n \leq \log n \leq \log p_n$. The latter relation shows that $\log p_n \sim \log n$ as $n \to \infty$, and substituting this asymptotic formula into (3.12) yields $n \sim p_n/\log n$, which is equivalent to the desired relation $p_n \sim n \log n$.

(ii) First note that, given any positive integer k, the least positive integer n with $\omega(n) = k$ is $n_k = p_1 \dots p_k$, where p_i denotes the i-th prime. Since $\log n/\log\log n$ is a monotone increasing function for sufficiently large n, it suffices to consider integers n from the sequence $\{n_k\}$ in the limsup in (ii). We then need to show that

$$\limsup_{k\to\infty} \frac{k}{(\log n_k)/(\log\log n_k)} = 1. \tag{3.13}$$

The PNT and the asymptotic formula for p_k proved in part (i) implies

$$\log n_k = \sum_{i=1}^{k} \log p_i = \theta(p_k) \sim p_k \sim k \log k \quad (k \to \infty)$$

and

$$\begin{aligned} \log\log n_k &= \log((1+o(1))k\log k) = \log k + \log\log k + \log(1+o(1)) \\ &= (1+o(1))\log k. \end{aligned}$$

Substituting these estimates on the left side of (3.13) gives the desired relation.

(iii) By the PNT we have, for any fixed $\epsilon > 0$,

$$\frac{\pi((1+\epsilon)x)}{\pi(x)} \sim \frac{(1+\epsilon)x/\log((1+\epsilon)x)}{x/\log x} = (1+\epsilon)\frac{\log x}{\log(1+\epsilon)+\log x},$$

and thus $\lim_{x\to\infty} \pi((1+\epsilon)x)/\pi(x) = 1+\epsilon$. This implies $\pi((1+\epsilon)x) > \pi(x)$ for any $\epsilon > 0$ and $x \geq x_0(\epsilon)$, which is equivalent to the assertion in (iii).

(iv) Given a positive real number α and $\epsilon > 0$, we need to show that there exist primes p and q with $|p/q - \alpha| \leq \epsilon$, or equivalently $(*)$ $\alpha q - \epsilon q \leq p \leq \alpha q + \epsilon q$. To this end, set $\epsilon' = \epsilon/\alpha$, and let q be any prime such that $\alpha q \geq x_0$, where $x_0 = x_0(\epsilon')$ is defined as in the previous proof relative to ϵ'. Thus, for $x \geq x_0$, there exists a prime p with $x < p \leq (1+\epsilon')x$. Taking $x = \alpha q$, we conclude that there exists a prime p with $\alpha q < p \leq (1+\epsilon')\alpha q = \alpha q + \epsilon q$, as desired.

(v) Given a string of digits $a_1 \ldots a_r$, with $a_1 \neq 0$, let $A = a_1 \ldots a_r$ denote the integer formed by these digits. Since $a_1 \neq 0$, A is a positive integer. Now observe that a positive integer n begins with the string $a_1 \ldots a_r$ if and only if, for some integer $k \geq 0$, $(*)$ $10^k A \leq n < 10^k(A+1)$. Applying the result of (iii) with some $\epsilon < 1/A$ (say, $\epsilon = 1/(A+1)$), we see that the interval $(*)$ contains a prime for sufficiently large k. □

3.4 The PNT and averages of the Moebius function

As we have seen above, the PNT is "equivalent" to each of the relations $\psi(x) \sim x$ and $\theta(x) \sim x$, in the sense that deducing one statement from the other, and vice versa, is substantially easier than proving either of these statements. (One should be aware that this type of "equivalence" is an imprecise, and to some extent subjective, notion, but in the context of the prime number theorem this informal usage of the term "equivalent" has become standard. Of course, from a purely logical point of view, all true statements are equivalent to each other.)

There exist many other prime number sums or products for which an asymptotic estimation is equivalent, in the same sense, to the PNT. These equivalences are usually neither particularly deep or unexpected, and are easily established.

In this section we prove the equivalence of the PNT to a rather different type of result, namely that the Moebius function has mean value zero. In contrast to the above-mentioned equivalences, the connection between the PNT and the mean value of the Moebius function lies much deeper and is more difficult to establish (though still easier than a proof of the PNT). The precise statement is the following.

Theorem 3.8 (Relation between PNT and the Moebius function). *The PNT is equivalent to the relation*

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \mu(n) = 0, \tag{3.14}$$

i.e., the assertion that the mean value $M(\mu)$ of the Moebius function exists and is equal to 0*.*

The proof of this result will be given in the second part of this section. We first make some remarks and establish several auxiliary results.

Primes and the Moebius function. What is so surprising about this result is that there does not seem to be any obvious connection between the distribution of primes (which is described by the PNT), and the distribution of the values of the Moebius function (which is described by the result that $M(\mu) = 0$). If one restricts to squarefree numbers, then the Moebius function encodes the *parity* of the number of prime factors of an integer. The assertion that $M(\mu) = 0$ can then be interpreted as saying that the two parities, even and odd, occur with the same asymptotic frequency. More precisely, this may be formulated as follows: Let $Q(x)$ denote the number of squarefree positive integers $\le x$, and $Q_+(x)$, resp. $Q_-(x)$, the number of squarefree positive integers $\le x$ with an even, resp. odd, number of prime factors. Then $\sum_{n\le x} \mu(n) = Q_+(x) - Q_-(x)$, so the relation $M(\mu) = 0$ is equivalent to

$$Q_-(x) = Q_+(x) + o(x) = (1/2)Q(x) + o(x) \sim \frac{3}{\pi^2}x \quad (x \to \infty),$$

in view of the asymptotic relation $Q(x) \sim (6/\pi^2)x$. The equivalence between the PNT and the relation $M(\mu) = 0$ therefore means that an asymptotic formula for the function $\pi(x)$, which counts positive integers $\le x$ with *exactly one* prime factor, is equivalent to an asymptotic formula for the function $Q_-(x)$, which counts positive integers $\le x$ with *an odd number* of prime

factors. That those two counting functions should be so closely related is anything but obvious.

Next, we prove a simple, and surprisingly easy-to-prove, bound for "logarithmic" averages of the Moebius function. This result may be regarded as a Moebius function analogue of Mertens' estimates for "logarithmic" prime number sums given in Theorem 3.4.

Lemma 3.9 (Mertens' type estimate for the Moebius function). *For any $x \geq 1$,*

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1.$$

Proof. Note first that, without loss of generality, we can assume that $x = N$, where N is a positive integer. We then evaluate the sum $S(N) = \sum_{n \leq N} e(n)$, where e is the convolution identity, defined by $e(n) = 1$ if $n = 1$ and $e(n) = 0$ otherwise, in two different ways. On the one hand, by the definition of $e(n)$, we have $S(N) = 1$; on the other hand, writing $e(n) = \sum_{d|n} \mu(d)$ and interchanging summations, we obtain

$$S(N) = \sum_{d \leq N} \mu(d)[N/d] = N \sum_{d \leq N} \frac{\mu(d)}{d} - \sum_{d \leq N} \mu(d)\{N/d\},$$

where $\{t\}$ denotes the fractional part of t. We now bound the latter sum. Since N is an integer, we have $\{N/d\} = 0$ when $d = N$. Thus we can restrict the summation to those terms for which $1 \leq d \leq N-1$, and using the trivial bound $|\mu(d)\{N/d\}| \leq 1$ for these terms, we see that this sum is bounded by $N - 1$. Hence,

$$\left| N \sum_{d \leq N} \frac{\mu(d)}{d} \right| \leq (N-1) + |S(N)| = (N-1) + 1 = N,$$

which gives the asserted bound for $x = N$. □

Corollary 3.10 (Logarithmic mean value of the Moebius function). *The Moebius function has logarithmic mean value $L(\mu) = 0$. Moreover, if the ordinary mean value $M(\mu)$ exists, it must be equal to 0.*

Proof. The first statement follows immediately from the definition of the logarithmic mean value and Theorem 3.9. The second statement follows from the first and the general result (Theorem 2.13) that if the ordinary mean value $M(f)$ of an arithmetic function f exists, then the logarithmic mean value $L(f)$ exists as well, and the two mean values are equal. □

Our second auxiliary result is a general result relating the ordinary mean value of an arithmetic function to a mean value involving logarithmic weights. Its proof is a simple exercise in partial summation and is omitted here.

Lemma 3.11. *Given an arithmetic function f, define a mean value $H(f)$ by*

$$H(f) = \lim_{x\to\infty} \frac{1}{x\log x} \sum_{n\le x} f(n)\log n,$$

if the limit exists. Then $H(f)$ exists if and only if the ordinary mean value $M(f)$ exits.

We are now ready to prove the main result of this section.

Proof of 3.8. The proof of this result is longer and more complex than any of the proofs we have encountered so far. Yet it is still easier than a proof of the PNT itself. Its proof requires much of the arsenal of tools and tricks we have assembled so far: convolution identities between arithmetic functions, partial summation, convolution arguments, the Dirichlet hyperbola method, and an estimate for sums of the divisor functions.

We will use the fact that the PNT is equivalent to the relation

$$\psi(x) \sim x \quad (x\to\infty). \tag{3.15}$$

We will also use the result of Lemma 3.11 above, according to which (3.14) is equivalent to

$$\lim_{x\to\infty} \frac{1}{x\log x} \sum_{n\le x} \mu(n)\log n = 0. \tag{3.16}$$

To prove Theorem 3.8 it is therefore enough to show the implications (i) (3.15) $\Rightarrow$ (3.16) and (ii) (3.14) $\Rightarrow$ (3.15).

(i) Proof of (3.15) $\Rightarrow$ (3.16): This is the easier direction. The proof rests on the following identity which is a variant of the identity $\log = 1 * \Lambda$.

Lemma 3.12. *We have*

$$\mu(n)\log n = -(\mu * \Lambda)(n) \quad (n\in\mathbb{N}). \tag{3.17}$$

Proof. Suppose first that n is squarefree. In this case we have, for any divisor d of n, $\mu(n) = \mu(d)\mu(n/d)$ (since any such divisor d must be squarefree and relatively prime to its complementary divisor n/d) and $\mu(d)\Lambda(d) = -\Lambda(d)$

(since for squarefree d, $\Lambda(d)$ is zero unless d is a prime, in which case $\mu(d) = -1$). Thus, multiplying the identity $\log n = \sum_{d|n} \Lambda(n/d)$ by $\mu(n)$, we obtain

$$\mu(n) \log n = \sum_{d|n} \mu(d)\mu(n/d)\Lambda(n/d) = -\sum_{d|n} \mu(d)\Lambda(n/d),$$

which proves (3.17) for squarefree n. If n is not squarefree, the left-hand side of (3.17) is zero, so it suffices to show that $(\mu * \Lambda)(n) = 0$ for non-squarefree n. Now $(\mu * \Lambda)(n) = \sum_{p^m|n} (\log p)\mu(n/p^m)$. If n is divisible by the squares of at least two primes, then none of the numbers n/p^m occurring in this sum is squarefree, so the sum vanishes. On the other hand, if n is divisible by exactly one square of a prime, then n is of the form $n = p_0^{m_0} n_0$ with $m_0 \geq 2$ and n_0 squarefree, $(n_0, p_0) = 1$, and the above sum reduces to $(\log p_0)\mu(n_0) + (\log p_0)\mu(n_0 p_0)$, which is again zero since $\mu(n_0 p_0) = \mu(n_0)\mu(p_0) = -\mu(n_0)$. This completes the proof of the lemma. □

Now, suppose (3.15) holds, and set

$$H(x) = \sum_{n \leq x} \mu(n) \log n.$$

We need to show that, given $\epsilon > 0$, we have $|H(x)| \leq \epsilon x \log x$ for all sufficiently large x. From the identity (3.17) we have

$$\begin{aligned} H(x) &= -\sum_{n \leq x} \sum_{d|n} \mu(d)\Lambda(n/d) \\ &= -\sum_{d \leq x} \mu(d) \sum_{m \leq x/d} \Lambda(m) = -\sum_{d \leq x} \mu(d)\psi(x/d). \end{aligned}$$

Let $\epsilon > 0$ be given. By the hypothesis (3.15) there exists $x_0 = x_0(\epsilon) \geq 1$ such that, for $x \geq x_0$, $|\psi(x) - x| \leq \epsilon x$. Moreover, we have trivially $|\Psi(x)| \leq \sum_{n \leq x} \log n \leq x \log x$ for all $x \geq 1$. Applying the first bound with x/d in place of x for $d \leq x/x_0$, and the second (trivial) bound for $x/x_0 < d \leq x$,

we obtain, for $x \geq x_0$,

$$
\begin{aligned}
|H(x)| &\leq \left| \sum_{d \leq x/x_0} \mu(d) \frac{x}{d} \right| + \sum_{d \leq x/x_0} |\mu(d)| \left| \psi\left(\frac{x}{d}\right) - \frac{x}{d} \right| \\
&\qquad + \sum_{x/x_0 < d \leq x} |\mu(d)| \left| \psi\left(\frac{x}{d}\right) \right| \\
&\leq \left| \sum_{d \leq x/x_0} \mu(d) \frac{x}{d} \right| + \sum_{d \leq x/x_0} |\mu(d)| \epsilon \frac{x}{d} \\
&\qquad + \sum_{x/x_0 < d \leq x} |\mu(d)| \frac{x}{d} \log(x/d) \\
&= \left| \sum\nolimits_1 \right| + \sum\nolimits_2 + \sum\nolimits_3,
\end{aligned} \tag{3.18}
$$

say. Of the three sums here, the first is bounded by

$$
\left| \sum\nolimits_1 \right| = x \left| \sum_{d \leq x/x_0} \frac{\mu(d)}{d} \right| \leq x
$$

by Lemma 3.9. The second sum is bounded by

$$
\sum\nolimits_2 \leq \epsilon x \sum_{d \leq x/x_0} \frac{1}{d} = \epsilon x (\log(x/x_0) + O(1)) \leq \epsilon x (\log x + O(1)),
$$

by Theorem 2.5. The third sum satisfies

$$
\sum\nolimits_3 \leq (\log x_0) x_0 \sum_{d \leq x} 1 \leq (\log x_0) x_0 x,
$$

and hence is of order $O_\epsilon(x)$ (with the O-constant depending on ϵ via x_0). Collecting these estimates, we obtain

$$
|H(x)| \leq \epsilon x \log x + O_\epsilon(x) \quad (x \geq x_0),
$$

which implies

$$
\limsup_{x \to \infty} \frac{|H(x)|}{x \log x} \leq \epsilon.
$$

Since ϵ was arbitrary, the limsup must be zero, i.e., (3.16) holds.

(ii) Proof of (3.14) $\Rightarrow$ (3.15): The proof rests on the identity $\Lambda = \log * \mu$, which follows from $\log = 1 * \Lambda$ by Moebius inversion. However, a

direct application of this identity is not successful: Namely, writing $\Lambda(n) = \sum_{d|n}(\log d)\mu(n/d)$ and inverting the order of summation as usual yields

$$\psi(x) = \sum_{n\le x}\Lambda(n) = \sum_{d\le x}(\log d)\sum_{n\le x/d}\mu(n).$$

Assuming a bound of the form $\epsilon x/d$ for the (absolute value of) the inner sum would yield a bound $\le \epsilon\sum_{d\le x}(\log d)(x/d)$, which has order of magnitude $\epsilon x(\log x)^2$ and thus would not even yield a Chebyshev type bound for $\psi(x)$. Even assuming stronger bounds on $\sum_{n\le x}\mu(n)$ (e.g., bounds of the form $O(x/\log^A x)$ for some constant A) would at best yield Chebyshev's bound $\psi(x) \ll x$ in this approach.

To get around these difficulties, we take the unusual (and surprising) step of approximating a smooth function, namely $\log n$, by an arithmetic function that is anything but smooth, but which has nice arithmetic properties. The approximation we choose is the function $f(n) = d(n) - 2\gamma$, where $d = 1*1$ is the divisor function and γ is Euler's constant. This choice is motivated by the fact that the summatory function of $f(n)$ approximates the summatory function of $\log n$ very well. Indeed, on the one hand, Theorem 2.20 gives

$$\begin{aligned}\sum_{n\le x} f(n) &= \sum_{n\le x} d(n) - 2\gamma\sum_{n\le x} 1\\ &= x(\log x + 2\gamma - 1) + O(\sqrt{x}) - 2\gamma x + O(1)\\ &= x(\log x - 1) + O(\sqrt{x}),\end{aligned}$$

while, on the other hand, by Corollary 2.8,

$$\sum_{n\le x}\log n = x(\log x - 1) + O(\log x).$$

Thus, if we define the "remainder function" $r(n)$ by

$$\log = f + r = (1*1) - 2\gamma + r,$$

we have

$$\sum_{n\le x} r(n) = \sum_{n\le x}\log n - \sum_{n\le x} f(n) = O(\sqrt{x}) \quad (x \ge 1). \tag{3.19}$$

Replacing the function log by $f + r = (1*1) - 2\gamma\cdot 1 + r$ in the identity $\Lambda = \mu * \log$, we obtain, using the algebraic properties of the Dirichlet convolution,

$$\begin{aligned}\Lambda &= \mu * (1*1 - 2\gamma\cdot 1 + r)\\ &= (\mu*1)*1 - 2\gamma(\mu*1) + \mu*r = 1 - 2\gamma e + \mu*r,\end{aligned}$$

where e is the usual convolution identity. It follows that

$$\psi(x) = \sum_{n\le x} 1 - 2\gamma + \sum_{n\le x}(\mu * r)(n) = x + O(1) + E(x), \tag{3.20}$$

where

$$E(x) = \sum_{n\le x}(\mu * r)(n).$$

Thus, in order to obtain (3.15), it remains to show that the term $E(x)$ is of order $o(x)$ as $x \to \infty$.

It is instructive to compare the latter sum $E(x)$ with the sum $\psi(x) = \sum_{n\le x}(\mu * \log)(n)$ we started out with. Both of these sums are convolution sums involving the Moebius function. The difference is that, in the sum $E(x)$, the function $\log n$ has been replaced by the function $r(n)$, which, by (3.19), is much smaller on average than the function $\log n$. This makes a crucial difference in our ability to successfully estimate the sum. Indeed, writing

$$E(x) = \sum_{d\le x}\mu(d)\sum_{n\le x/d} r(n)$$

and bounding the inner sum by (3.19) would give the bound

$$E(x) \ll \sum_{d\le x}\sqrt{x/d} = \sqrt{x}\sum_{d\le x}\frac{1}{\sqrt{d}} \ll x,$$

which is by a factor $(\log x)^2$ better than what a similar argument with the function $\log n$ instead of $r(n)$ would have given and strong enough to yield Chebyshev's bound for $\psi(x)$.

Thus, it remains to improve the above bound from $O(x)$ to $o(x)$, by exploiting our assumption (3.14) (which was not used in deriving the above bound). To this end, we use a general version of the Dirichlet hyperbola method: We fix y with $1 \le y \le x$ and split the sum $E(x)$ into

$$E(x) = \sum_{n\le x}\sum_{d|n} r(d)\mu(n/d) = \sum_{dm\le x} r(d)\mu(m) = \sum\nolimits_1 + \sum\nolimits_2 - \sum\nolimits_3, \tag{3.21}$$

where

$$\sum\nolimits_1 = \sum_{d\le y} r(d)M(x/d),\ \ \sum\nolimits_2 = \sum_{m\le x/y}\mu(m)R(x/m),\ \ \sum\nolimits_3 = R(y)M(x/y),$$

with

$$M(x) = \sum_{n\le x}\mu(n), \quad R(x) = \sum_{n\le x} r(n).$$

We proceed to estimate the three sums arising in the decomposition (3.21). Let $\epsilon > 0$ be given. Then, by our assumption (3.14), there exists $x_0 = x_0(\epsilon)$ such that $|M(x)| \le \epsilon x$ for $x \ge x_0$. Moreover, by (3.19), there exists a constant c such that $|R(x)| \le c\sqrt{x}$ for all $x \ge 1$. Applying these bounds we obtain, for $x \ge x_0 y$,

$$\left|\sum\nolimits_3\right| \le c\sqrt{y}\epsilon(x/y) \le c\epsilon x,$$

and

$$\left|\sum\nolimits_2\right| \le \sum_{m\le x/y} |\mu(m)| c\sqrt{x/m} \le c\sqrt{x} \sum_{m\le x/y} \frac{1}{\sqrt{m}} \le \frac{2cx}{\sqrt{y}},$$

where the latter estimate follows (for example) from Euler's summation formula in the form

$$\begin{aligned}\sum_{n\le t} \frac{1}{\sqrt{n}} &= 1 + \int_1^t \frac{1}{\sqrt{s}} ds - \frac{\{t\}}{\sqrt{t}} - \int_1^t \frac{\{s\}}{s^2} ds \\ &\le 1 + \int_1^t t^{-1/2} dt \le 2\sqrt{t} \quad (t \ge 2).\end{aligned}$$

Finally, we have

$$\left|\sum\nolimits_1\right| \le \sum_{d\le y} |r(d)| \epsilon(x/d) \le C(y)\epsilon x,$$

where

$$C(y) = \sum_{d\le y} \frac{|r(d)|}{d}$$

is a constant depending only on y.

Substituting the above bounds into (3.21), we obtain

$$|E(x)| \le x\left(c\epsilon + C(y)\epsilon + \frac{2c}{\sqrt{y}}\right).$$

It follows that

$$\limsup_{x\to\infty} \frac{|E(x)|}{x} \le \epsilon(c + C(y)) + \frac{2c}{\sqrt{y}},$$

for any fixed $\epsilon > 0$ and $y \ge 1$. Since $\epsilon > 0$ was arbitrary, the above limsup is bounded by $\le 2c/\sqrt{y}$, and since y can be chosen arbitrarily large, it must be equal to 0. Hence $\lim_{x\to\infty} E(x)/x = 0$, which is what we set out to prove. (Note that, for this argument to work it was essential that the constant c did not depend on ϵ or y, and that the constant $C(y)$ did not depend on ϵ.) □

3.5 Exercises

3.1 Using Bertrand's postulate that for any $x \geq 1$ there exists a prime in the interval $(x, 2x]$, show that every integer $n \geq 7$ can be written in the form $n = \sum_{i=1}^{k} p_i$ with *distinct* primes p_i.

3.2 Let $P(x) = \prod_{p \leq x} p$. Show that the PNT is equivalent to the relation $P(x)^{1/x} \to e$ as $x \to \infty$.

3.3 Let $L(n) = [1, 2, \ldots, n]$, where $[\ldots]$ denotes the least common multiple. Show that the limit $\lim_{n\to\infty} L(n)^{1/n}$ exists if and only if the PNT holds.

3.4 Let a_n be a nonincreasing sequence of positive numbers. Show that $\sum_p a_p$ converges if and only if $\sum_{n=2}^{\infty} a_n / \log n$ converges.

3.5 For positive integers k define the generalized von Mangoldt functions Λ_k by the identity $\sum_{d|n} \Lambda_k(d) = (\log n)^k$ (which for $k = 1$ reduces to the familiar identity for the ordinary von Mangoldt function $\Lambda(n)$). Show that $\Lambda_k(n) = 0$ if n has more than k distinct prime factors.

3.6 Call a positive integer n round if it has no prime factors greater than $\sqrt{n}$. Let $R(x)$ denote the number of round integers $\leq x$. Estimate $R(x)$ to within an error $O(x/\log x)$. (Hint: Estimate first the slightly different counting function

$$R_0(x) = \#\{n \leq x : p|n \Rightarrow p \leq \sqrt{x}\},$$

and then show that the difference between $R(x)$ and $R_0(x)$ is of order $O(x/\log x)$ and thus negligible.)

3.7 Let α be a fixed non-zero real number, and let $S_\alpha(x) = \sum_{p \leq x} p^{-1-i\alpha}$. Use the prime number theorem in the form $\pi(x) = x/\log x + O(x/\log^2 x)$ to derive an estimate for $S_\alpha(x)$ with error term $O_\alpha(1/\log x)$.

3.8 Without using the PNT (you may use Chebyshev's estimates or Mertens' estimates), obtain an asymptotic estimate for the partial sums

$$S(x) = \sum_{p \leq x} \frac{1}{p \log p}$$

(with as good an error term as you can get using only results at the level of Chebyshev or Mertens).

3.9 Let $Q(x) = \prod_{p \le x}(1 + 1/p)$. Obtain an estimate for $Q(x)$ with relative error $O(1/\log x)$. Express the constant arising in this estimate in terms of well-known mathematical constants. (Hint: Relate $Q(x)$ to the product $P(x) = \prod_{p \le x}(1 - 1/p)$ estimated by Mertens' formula.)

3.10 (i) Show that the estimate (a stronger version of one of Mertens' estimates)

$$\sum_{n \le x} \frac{\Lambda(n)}{n} = \log x + C + o(1), \tag{1}$$

where C is a constant, implies the PNT.

(ii) (Harder) Show that the converse also holds, i.e., the PNT implies (1).

3.11 Show that

$$\sum_{n \le x} \mu^2(n) = \frac{6}{\pi^2} x + o(\sqrt{x}) \quad (x \to \infty).$$

(With error term $O(\sqrt{x})$ this was proved in Theorem 2.18, quite easily and without using the PNT. To improve this error term to $o(\sqrt{x})$ requires an appeal to the PNT and a more careful treatment of the term that gave rise to the $O(\sqrt{x})$ error.)

3.12 Euler's proof of the infinitude of primes shows that $(*)$ $\sum_{p \le x} 1/p \ge \log\log x - C$, for some constant C and all sufficiently large x. This is a remarkably good lower bound for the sum of reciprocals of primes (it is off by only a term $O(1)$), so it is of some interest to see what this bound implies for $\pi(x)$. The answer is, surprisingly little, as the following problems show.

(i) Deduce from $(*)$, *without using any other information about the primes*, that there exists $\delta > 0$ such that $\pi(x) > \delta \log x$ for all sufficiently large x. In other words, show that if A is any sequence of positive integers satisfying

$$\sum_{a \le x, a \in A} \frac{1}{a} \ge \log\log x - C \tag{1}$$

for some constant C and all sufficiently large x, then there exists a constant $\delta > 0$ such that the counting function $A(x) = \#\{a \in A, a \le x\}$ satisfies

$$A(x) \ge \delta \log x \tag{2}$$

for all sufficiently large x.

(ii) (Harder) Show that this result is nearly best possible, in the sense that it becomes false if the function $\log x$ on the right-hand side of (2) is replaced by a power $(\log x)^\alpha$ with an exponent α greater than 1. In other words, given $\epsilon > 0$, construct a sequence A of positive integers, satisfying (1) above, but for which the counting function $A(x) = \#\{a \in A, a \le x\}$ satisfies

$$\liminf_{x\to\infty} A(x)(\log x)^{-1-\epsilon} = 0. \tag{3}$$

Chapter 4

Arithmetic functions III: Dirichlet series and Euler products

4.1 Introduction

Given an arithmetic function $f(n)$, the series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \tag{4.1}$$

is called the *Dirichlet series* associated with f. A Dirichlet series can be regarded as a purely formal infinite series (i.e., ignoring questions about convergence), or as a function of the complex variable s, defined in the region in which the series converges. The variable s is usually written as

$$s = \sigma + it, \quad \sigma = \operatorname{Re} s, \quad t = \operatorname{Im} s. \tag{4.2}$$

Dirichlet series serve as a type of generating functions for arithmetic functions, adapted to the multiplicative structure of the integers, and they play a role similar to that of ordinary generating functions in combinatorics. For example, just as ordinary generating functions can be used to prove combinatorial identities, Dirichlet series can be applied to discover and prove identities among arithmetic functions.

On a more sophisticated level, the analytic properties of a Dirichlet series, regarded as a function of the complex variable s, can be exploited to obtain information on the behavior of partial sums $\sum_{n \le x} f(n)$ of arithmetic

functions. This is how Hadamard and de la Vallée Poussin obtained the first proof of the Prime Number Theorem. In fact, most analytic proofs of the Prime Number Theorem (including the one we shall give in the following chapter) proceed by relating the partial sums $\sum_{n\le x}\Lambda(n)$ to a complex integral involving the Dirichlet series $\sum_{n=1}^{\infty}\Lambda(n)n^{-s}$, and evaluating that integral by analytic techniques.

The most famous Dirichlet series is the *Riemann zeta function* $\zeta(s)$, defined as the Dirichlet series associated with the constant function 1, i.e.,

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\quad(\sigma>1), \tag{4.3}$$

where σ is the real part of s, as defined in (4.2).

4.2 Algebraic properties of Dirichlet series

We begin by proving two important elementary results which show that Dirichlet series "respect" the multiplicative structure of the integers. It is because of these results that Dirichlet series, rather than ordinary generating functions, are the ideal tool to study the behavior of arithmetic functions.

The first result shows that the Dirichlet series of a convolution product of arithmetic functions is the (ordinary) product of the associated Dirichlet series. It is analogous to the well-known (and easy to prove) fact that, given two functions $f(n)$ and $g(n)$, the product of their *ordinary* generating functions $\sum_{n=0}^{\infty}f(n)z^n$ and $\sum_{n=0}^{\infty}g(n)z^n$ is the generating function for the function $h(n)=\sum_{k=0}^{n}f(k)g(n-k)$, the *additive* convolution of f and g.

Theorem 4.1 (Dirichlet series of convolution products). *Let f and g be arithmetic functions with associated Dirichlet series $F(s)$ and $G(s)$. Let $h=f*g$ be the Dirichlet convolution of f and g, and $H(s)$ the associated Dirichlet series. If $F(s)$ and $G(s)$ converge absolutely at some point s, then so does $H(s)$, and we have $H(s)=F(s)G(s)$.*

Proof. We have

$$\begin{aligned}F(s)G(s)&=\sum_{k=1}^{\infty}\sum_{m=1}^{\infty}\frac{f(k)g(m)}{k^s m^s}\\&=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{km=n}f(k)g(m)=\sum_{n=1}^{\infty}\frac{(f*g)(n)}{n^s},\end{aligned}$$

where the rearranging of terms in the double sum is justified by the absolute convergence of the series $F(s)$ and $G(s)$. This shows that $F(s)G(s) = H(s)$; the absolute convergence of the series $H(s) = \sum_{n=1}^{\infty} h(n)n^{-s}$ follows from that of $F(s)$ and $G(s)$ in view of the inequality

$$\begin{aligned}\sum_{n=1}^{\infty}\left|\frac{h(n)}{n^s}\right| &\le \sum_{n=1}^{\infty}\frac{1}{|n^s|}\sum_{km=n}|f(k)|\cdot|g(m)| \\ &= \left(\sum_{k=1}^{\infty}\left|\frac{f(k)}{k^s}\right|\right)\left(\sum_{m=1}^{\infty}\left|\frac{g(m)}{m^s}\right|\right).\end{aligned}$$

□

Remark. The hypothesis that the Dirichlet series $F(s)$ and $G(s)$ converge *absolutely* is essential here, since one has to be able to rearrange the terms in the double series obtained by multiplying the series $F(s)$ and $G(s)$. Without this hypothesis, the conclusion of the theorem need not hold.

Corollary 4.2 (Dirichlet series of convolution inverses). *Let f be an arithmetic function with associated Dirichlet series $F(s)$, and g the convolution inverse of f (so that $f * g = e$), and let $G(s)$ be the Dirichlet series associated with g. Then we have $G(s) = 1/F(s)$ at any point s at which both $F(s)$ and $G(s)$ converge absolutely.*

Proof. Since the function e has Dirichlet series $\sum_{n=1}^{\infty} e(n)n^{-s} = 1$, the result follows immediately from the theorem. □

Remark. The absolute convergence of $F(s)$ does not imply that of the Dirichlet series associated with the Dirichlet inverse of f. For example, the function defined by $f(1) = 1$, $f(2) = -1$, and $f(n) = 0$ for $n \ge 3$ has Dirichlet series $F(s) = 1 - 2^{-s}$, which converges everywhere. However, the Dirichlet series of the Dirichlet inverse of f is $1/F(s) = (1 - 2^{-s})^{-1} = \sum_{k=0}^{\infty} 2^{-ks}$, which converges absolutely in $\sigma > 0$, but not in the half-plane $\sigma \le 0$.

The theorem and its corollary can be used, in conjunction with known convolution identities, to evaluate the Dirichlet series of many familiar arithmetic functions, as is illustrated by the following examples.

Examples of Dirichlet series

(1) **Unit function.** The Dirichlet series for $e(n)$, the convolution unit, is $\sum_{n=1}^{\infty} e(n)n^{-s} = 1$.

(2) **Moebius function.** Since μ is the convolution inverse of the function 1 and the associated Dirichlet series $\sum_{n=1}^{\infty} \mu(n)n^{-s}$ and $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ both converge absolutely in $\sigma > 1$, we have $\sum_{n=1}^{\infty} \mu(n)n^{-s} = 1/\zeta(s)$ for $\sigma > 1$. In particular, setting $s = 2$, we obtain the relation $\sum_{n=1}^{\infty} \mu(n)n^{-2} = 1/\zeta(2) = 6/\pi^2$, which we had derived earlier.

(3) **Characteristic function of the squares.** Let $s(n)$ denote the characteristic function of the squares. Then the associated Dirichlet series is given by $\sum_{n=1}^{\infty} s(n)n^{-s} = \sum_{m=1}^{\infty}(m^2)^{-s} = \zeta(2s)$, which converges absolutely in $\sigma > 1/2$.

(4) **Logarithm.** Termwise differentiation of the series $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ gives the series $-\sum_{n=1}^{\infty}(\log n)n^{-s}$. Since $\zeta(s)$ converges absolutely and uniformly in any range of the form $\sigma \geq 1+\epsilon$ with $\epsilon > 0$ (which follows, for example, by applying the Weierstrass M-test since the terms of the series are bounded by $n^{-1-\epsilon}$ in that range and $\sum_{n=1}^{\infty} n^{-1-\epsilon}$ converges), termwise differentiation is justified in the range $\sigma > 1$, and we therefore have $\zeta'(s) = -\sum_{n=1}^{\infty}(\log n)n^{-s}$. Hence the Dirichlet series for the function $\log n$ is $-\zeta'(s)$ and converges absolutely in $\sigma > 1$.

(5) **Identity function.** The Dirichlet series associated with the identity function is $\sum_{n=1}^{\infty} \mathrm{id}(n)n^{-s} = \sum_{n=1}^{\infty} n^{-(s-1)} = \zeta(s-1)$, which converges absolutely in $\sigma > 2$.

(6) **Euler phi function.** By the identity $\phi = \mathrm{id} * \mu$ and the formulas for the Dirichlet series for id and μ obtained above, the Dirichlet series for $\phi(n)$ is $\sum_{n=1}^{\infty} \phi(n)n^{-s} = \zeta(s-1)/\zeta(s)$ and converges absolutely for $\sigma > 2$.

(7) **Divisor function.** Since $d = 1 * 1$, the Dirichlet series for the divisor function is $\sum_{n=1}^{\infty} d(n)n^{-s} = \zeta(s)^2$ and converges absolutely in $\sigma > 1$.

(8) **Characteristic function of the squarefree numbers.** The function μ^2 satisfies the identity $\mu^2 * s = 1$, where s is the characteristic function of the squares, whose Dirichlet series was evaluated above as $\zeta(2s)$. Hence the Dirichlet series associated with μ^2, i.e., $F(s) = \sum_{n=1}^{\infty} \mu^2(n)n^{-s}$, satisfies $F(s)\zeta(2s) = \zeta(s)$, where all series converge absolutely in $\sigma > 1$. It follows that $F(s) = \zeta(s)/\zeta(2s)$ for $\sigma > 1$.

(9) **Von Mangoldt function.** Since $\Lambda * 1 = \log$ and the function log has Dirichlet series $-\zeta'(s)$ (see above), we have $\sum_{n=1}^{\infty} \Lambda(n)n^{-s}\zeta(s) =$

$-\zeta'(s)$, and so $\sum_{n=1}^{\infty} \Lambda(n)n^{-s} = -\zeta'(s)/\zeta(s)$, with all series involved converging absolutely in $\sigma > 1$. Thus, the Dirichlet series for the von Mangoldt function $\Lambda(n)$ is (up to a minus sign) equal to the logarithmic derivative of the zeta function. This relation plays a crucial role in the analytic proof of the prime number theorem, and since any zero of $\zeta(s)$ generates a singularity of the function $\sum_{n=1}^{\infty} \Lambda(n)n^{-s} = -\zeta'(s)/\zeta(s)$, it clearly shows the influence of the location of zeta zeros on the distribution of prime numbers.

The second important result of this section gives a representation of the Dirichlet series of a *multiplicative* function as an infinite product over primes, called "Euler product". Given a Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$, the **Euler product** for $F(s)$ is the infinite product

$$\prod_p \left(1 + \sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}}\right). \tag{4.4}$$

(For the definition of convergence and absolute convergence of infinite products, and some basic results about such products, see Section A.2 in the Appendix.)

Theorem 4.3 (Euler product identity). *Let f be a multiplicative arithmetic function with Dirichlet series F, and let s be a complex number.*

(i) If $F(s)$ converges absolutely at some point s, then the infinite product (4.4) *converges absolutely and is equal to $F(s)$.*

(ii) The Dirichlet series $F(s)$ converges absolutely if and only if

$$\sum_{p^m} \left|\frac{f(p^m)}{p^{ms}}\right| < \infty. \tag{4.5}$$

Proof. (i) The absolute convergence of the infinite product follows from the bound

$$\sum_p \left|\sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}}\right| \le \sum_p \sum_{m=1}^{\infty} \left|\frac{f(p^m)}{p^{ms}}\right| \le \sum_{n=1}^{\infty} \left|\frac{f(n)}{n^s}\right| < \infty,$$

and a general convergence criterion for infinite products (Lemma A.3 in the Appendix). It therefore remains to show that the product is equal to $F(s)$, i.e., that $\lim_{N\to\infty} P_N(s) = F(s)$, where

$$P_N(s) = \prod_{p\le N} \left(1 + \sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}}\right).$$

Let $N \geq 2$ be given, and let $p_1, \ldots, p_k$ denote the primes $\leq N$. Upon multiplying out $P_N(s)$ (note that the term 1 in each factor can be written as $f(p^m)/p^{ms}$ with $m = 0$) and using the multiplicativity of f, we obtain

$$\begin{aligned} P_N(s) &= \sum_{m_1=0}^{\infty} \cdots \sum_{m_k=0}^{\infty} \frac{f(p_1^{m_1}) \cdots f(p_k^{m_k})}{p_1^{m_1 s} \cdots p_k^{m_k s}} \\ &= \sum_{m_1=0}^{\infty} \cdots \sum_{m_k=0}^{\infty} \frac{f(p_1^{m_1} \cdots p_k^{m_k})}{(p_1^{m_1} \cdots p_k^{m_k})^s}. \end{aligned}$$

The integers $p_1^{m_1} \ldots p_k^{m_k}$ occurring in this sum are positive integers composed only of prime factors $p \leq N$, i.e., elements of the set

$$A_N = \{n \in \mathbb{N} : p|n \Rightarrow p \leq N\}.$$

Moreover, by the Fundamental Theorem of Arithmetic theorem, each element of A_N has a *unique* factorization as $p_1^{m_1} \ldots p_k^{m_k}$ with $m_i \in \mathbb{N} \cup \{0\}$, and thus occurs exactly once in the above sum. Hence we have $P_N(s) = \sum_{n \in A_N} f(n) n^{-s}$. Since A_N contains all integers $\leq N$, it follows that

$$|P_N(s) - F(s)| = \left| \sum_{n \notin A_N} \frac{f(n)}{n^s} \right| \leq \sum_{n > N} \left| \frac{f(n)}{n^s} \right|,$$

which tends to zero as $N \to \infty$, in view of the absolute convergence of the series $\sum_{n=1}^{\infty} f(n) n^{-s}$. Hence $\lim_{N \to \infty} P_N(s) = F(s)$.

(ii) Since the series in (4.5) is a subseries of $\sum_{n=1}^{\infty} |f(n) n^{-s}|$, the absolute convergence of $F(s)$ implies (4.5). Conversely, if (4.5) holds, then, by Lemma A.3, the infinite product

$$\prod_p \left(1 + \sum_{m=1}^{\infty} \left| \frac{f(p^m)}{p^{ms}} \right| \right)$$

converges (absolutely). Moreover, if $P_N^*(s)$ denotes the same product, but restricted to primes $p \leq N$, then, as in the proof of part (i), we have

$$P_N^*(s) = \sum_{n \in A_N} \left| \frac{f(n)}{n^s} \right| \geq \sum_{n \leq N} \left| \frac{f(n)}{n^s} \right|.$$

Since $P_N^*(s)$ converges as $N \to \infty$, the partial sums on the right are bounded as $N \to \infty$. Thus, $F(s)$ converges absolutely. □

Remarks. As in the case of the previous theorem, the result is not valid without assuming *absolute* convergence of the Dirichlet series $F(s)$.

The theorem is usually only stated in the form (i); however, for most applications the condition stated in (ii) is easier to verify than the absolute convergence of $F(s)$.

Examples of Euler products

(1) **Riemann zeta function.** The most famous Euler product is that of the Riemann zeta function, the Dirichlet series of the arithmetic function 1:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{1}{p^{ms}}\right) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \quad (\sigma > 1).$$

Euler's proof of the infinitude of primes was based on this identity. In fact, if one could take $s = 1$ in this identity one would immediately obtain the infinitude of primes since in that case the series on the left is divergent, forcing the product on the right to have infinitely many factors. However, since the identity is only valid in $\sigma > 1$, a slightly more complicated argument is needed, by applying the identity with real $s = \sigma > 1$ and investigating the behavior of the left and right sides as $s \to 1+$. If there were only finitely many primes, then the product on the right would involve only finitely many factors, and hence would converge to the finite product $\prod_p (1 - 1/p)^{-1}$ as $s \to 1+$. On the other hand, for every N, the series on the left (with $s = \sigma > 1$) is $\geq \sum_{n \leq N} n^{-\sigma}$, which converges to $\sum_{n \leq N} n^{-1}$ as $s \to 1+$. Hence the limit of the left-hand side, as $s \to 1+$, is $\geq \sum_{n \leq N} n^{-1}$ for every fixed N and, since $\sum_{n \leq N} n^{-1} \to \infty$ as $N \to \infty$, this limit must be infinite. This contradiction proves the infinitude of primes.

(2) **Moebius function.** The Dirichlet series for the Moebius function has Euler product

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right),$$

a representation that is valid in the half-plane $\sigma > 1$. This can be seen directly, by the definition of the Euler product. Alternatively, one can argue as follows: Since the Moebius function is the Dirichlet inverse

of the arithmetic function 1, its Dirichlet series is the reciprocal of the Riemann zeta function. Hence, by Lemma A.4, its Euler product consists of factors that are reciprocals of the factors of the Euler product of the zeta function.

(3) **Completely multiplicative functions.** The functions 1 and μ considered above are examples of completely multiplicative functions and their inverses. The Euler products of arbitrary completely multiplicative functions and their inverses have the same general shape. Indeed, let f be a completely multiplicative function with Dirichlet series $F(s)$, and let g be the Dirichlet inverse of f, with Dirichlet series $G(s)$. Then, formally, we have the identities

$$F(s) = \prod_p \left(\sum_{m=0}^{\infty} \frac{f(p)^m}{p^{ms}} \right) = \prod_p \left(1 - \frac{f(p)}{p^s} \right)^{-1},$$

and

$$G(s) = \frac{1}{F(s)} = \prod_p \left(1 - \frac{f(p)}{p^s} \right).$$

These representations are valid provided the associated Dirichlet series converge absolutely, a condition that can be checked, for example, using the criterion of part (ii) of Theorem 4.3. For example, if $|f(p)| \leq 1$ for all primes p, then both $F(s)$ and $G(s)$ converge absolutely in $\sigma > 1$, and so the Euler product representations are valid in $\sigma > 1$ as well.

(4) **Characteristic function of integers relatively prime to a given set of primes.** Given a finite or infinite set of primes $\mathcal{P}$, let $f_{\mathcal{P}}$ denote the characteristic function of the positive integers that do not have a prime divisor belonging to the set $\mathcal{P}$. Thus $f_{\mathcal{P}}$ is the completely multiplicative function defined by $f_{\mathcal{P}} = 1$ if $p \notin \mathcal{P}$ and $f_{\mathcal{P}} = 0$ if $p \in \mathcal{P}$. Then the Dirichlet series $F_{\mathcal{P}}$ of $f_{\mathcal{P}}$ is given by the Euler product

$$F_{\mathcal{P}}(s) = \prod_{p \notin \mathcal{P}} \left(1 - \frac{1}{p^s} \right)^{-1} = \zeta(s) \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s} \right),$$

and this representation is valid in $\sigma > 1$.

(5) **Characteristic function of k-free integers.** Given an integer $k \geq 2$, fet $f_k(n)$ denote the characteristic function of the "k-free" integers, i.e., integers which are not divisible by the k-th power of a prime. The

function f_k is obviously multiplicative, and since it is bounded by 1, its Dirichlet series $F_k(s)$ converges absolutely in the half-plane $\sigma > 1$ and there has Euler product

$$F_k(s) = \prod_p \left(\sum_{m=0}^{k-1} \frac{1}{p^{ms}} \right) = \prod_p \frac{1 - p^{-ks}}{1 - p^{-s}} = \frac{\zeta(s)}{\zeta(ks)}.$$

(6) **Euler phi function.** Since $\phi(p^m) = p^m - p^{m-1}$ for $m \geq 1$, we have, formally,

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} &= \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{p^m - p^{m-1}}{p^{ms}} \right) \\ &= \prod_p \left(1 + \frac{1 - p^{-1}}{p^{s-1}(1 - p^{-s+1})} \right) = \prod_p \frac{1 - p^{-s}}{1 - p^{-s+1}}. \end{aligned}$$

Since $\phi(n) \leq n$, the Dirichlet series for ϕ converges absolutely in the half-plane $\sigma > 2$, so the above Euler product representation is valid in this half-plane. Moreover, the last expression above can be recognized as the product of the Euler product representations for the Dirichlet series $\zeta(s-1)$ and $1/\zeta(s)$. Thus, the Dirichlet series for $\phi(n)$ is equal to $\zeta(s-1)/\zeta(s)$, a result we had obtained earlier using the identity $\phi = \mathrm{id} * \mu$.

4.3 Analytic properties of Dirichlet series

We begin by proving two results describing the regions in the complex plane in which a Dirichlet series converges, absolutely or conditionally.

In the case of an ordinary power series $\sum_{n=0}^{\infty} a_n z^n$, it is well-known that there exists a "disk of convergence" $|z| < R$ such that the series converges absolutely $|z| < R$, and diverges when $|z| > R$. The number R, called "radius of convergence", can be any positive real number, or 0 (in which case the series diverges for all $z \neq 0$), or ∞ (in which case the series converges everywhere). For values z on the circle $|z| = R$, the series may converge or diverge.

For Dirichlet series, a similar result is true, with the disk of convergence replaced by a half-plane of convergence of the form $\sigma > \sigma_0$. However, in contrast to the situation for power series, where the regions for convergence

and absolute convergence are identical (except possibly for the boundaries), for Dirichlet series there may be a nontrivial region in the form of a vertical strip in which the series converges, but does not converge absolutely.

Theorem 4.4 (Absolute convergence of Dirichlet series). *For every Dirichlet series there exists a number $\sigma_a \in \mathbb{R} \cup \{\pm\infty\}$, called the* abscissa of absolute convergence*, such that for all s with $\sigma > \sigma_a$ the series converges absolutely, and for all s with $\sigma < \sigma_a$, the series does not converge absolutely.*

Proof. Given a Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$, let A be the set of complex numbers s at which $F(s)$ converges absolutely. If the set A is empty, the conclusion of the theorem holds with $\sigma_a = \infty$. Otherwise, set $\sigma_a = \inf\{\operatorname{Re} s : s \in A\} \in \mathbb{R} \cup \{-\infty\}$. By the definition of σ_a, the series $F(s)$ does not converge absolutely if $\sigma < \sigma_a$. On the other hand, if $s = \sigma + it$ and $s' = \sigma' + it'$ with $\sigma' \geq \sigma$, then

$$\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^{s'}} \right| = \sum_{n=1}^{\infty} \frac{|f(n)|}{n^{\sigma'}} \leq \sum_{n=1}^{\infty} \frac{|f(n)|}{n^{\sigma}} = \sum_{n=1}^{\infty} \left| \frac{f(n)}{n^{s}} \right|.$$

Hence, if $F(s)$ converges absolutely at some point s, then it also converges absolutely at any point s' with $\operatorname{Re} s' \geq \operatorname{Re} s$. Since, by the definition of σ_a, there exist points s with σ arbitrarily close to σ_a at which the Dirichlet series $F(s)$ converges absolutely, it follows that the series converges absolutely at *every* point s with $\sigma > \sigma_a$. This completes the proof of the theorem. □

Remark. In the case when $\sigma = \sigma_a$, the series may or may not converge absolutely. For example, the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ has abscissa of absolute convergence $\sigma_a = 1$, but it does not converge absolutely when $\sigma = 1$. On the other hand, the Dirichlet series corresponding to the arithmetic function $f(n) = 1/\log^2(2n)$ has the same abscissa of convergence 1, but also converges absolutely at $\sigma = 1$.

Establishing an analogous result for *conditional* convergence is harder. The key step is contained in the following theorem.

Proposition 4.5. *Suppose the Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converges at some point $s = s_0 = \sigma_0 + it_0$. Then the series converges at every point s with $\sigma > \sigma_0$. Moreover, the convergence is uniform in every compact region contained in the half-plane $\sigma > \sigma_0$.*

Proof. Suppose $F(s)$ converges at s_0, and let s be a point with $\sigma > \sigma_0$. Set $\delta = \sigma - \sigma_0$ (so that $\delta > 0$) and let

$$S(x, y) = \sum_{x < n \leq y} \frac{f(n)}{n^s}, \quad S_0(x, y) = \sum_{x < n \leq y} \frac{f(n)}{n^{s_0}} \quad (y > x \geq 1).$$

We will establish the convergence of the series $F(s)$ by showing that it satisfies Cauchy's criterion.

Let $\epsilon > 0$ be given. By Cauchy's criterion, applied to the series $F(s_0) = \sum_{n=1}^{\infty} f(n)n^{-s_0}$ (which, by hypothesis, converges) there exists $x_0 = x_0(\epsilon) \geq 1$ such that

$$|S_0(x,y)| \leq \epsilon \quad (y > x \geq x_0). \tag{4.6}$$

We now relate the sums $S(x,y)$ to the sums $S_0(x,y)$ by writing the summands as $f(n)n^{-s_0} \cdot n^{s_0-s}$, and "removing" the factor n^{s_0-s} by partial summation. Given $y > x \geq x_0$, we have

$$\begin{aligned} S(x,y) &= \sum_{x<n\leq y} \frac{f(n)}{n^{s_0}} \cdot n^{s_0-s} \\ &= S_0(x,y)y^{s_0-s} - \int_x^y S_0(x,u)(s_0-s)u^{s_0-s-1}du. \end{aligned}$$

Since, by (4.6), $|S_0(x,u)| \leq \epsilon$ for $u \geq x(\geq x_0)$, and $|u^{s_0-s}| = u^{\sigma_0-\sigma} = u^{-\delta}$ with $\delta > 0$, we obtain

$$\begin{aligned} |S(x,y)| &\leq \epsilon y^{-\delta} + \epsilon|s-s_0| \int_x^y u^{-\delta-1}du \\ &\leq \epsilon\left(1 + |s-s_0| \int_1^{\infty} u^{-\delta-1}du\right) \\ &= \epsilon\left(1 + \frac{|s-s_0|}{\delta}\right) = C\epsilon \quad (y > x \geq x_0(\epsilon)), \end{aligned}$$

where $C = C(s,s_0) = 1 + |s-s_0|/\delta$ is independent of x and y. Since ϵ was arbitrary, this shows that the series $F(s)$ satisfies Cauchy's criterion and hence converges.

To prove that the convergence is uniform on compact subsets of the half plane $\sigma > \sigma_0$, note that in any compact subset K of the half-plane $\sigma > \sigma_0$, the quantity $\delta = \sigma - \sigma_0$ is bounded from below and $|s-s_0|$ is bounded from above. Hence, the constant $C = C(s,s_0) = |s-s_0|/\delta$ defined above is bounded by a constant $C_0 = C_0(K)$ depending only on the subset K, but not on s, and the Cauchy criterion therefore holds uniformly in K. □

The following result describes the region of convergence of a Dirichlet series and is the analog of Theorem 4.4 for conditional convergence.

Theorem 4.6 (Convergence of Dirichlet series). *For every Dirichlet series there exists a number $\sigma_c \in \mathbb{R} \cup \{\pm\infty\}$, called the* abscissa of convergence*, such that the series converges in the half-plane $\sigma > \sigma_c$ (the "half-plane of convergence"), and diverges in the half-plane $\sigma < \sigma_c$. The convergence is uniform on compact subsets of the half-plane of convergence. Moreover, the abscissa of convergence σ_c and the abscissa of absolute convergence σ_a satisfy $\sigma_a - 1 \leq \sigma_c \leq \sigma_a$.*

Remarks. As in the case of Theorem 4.4, at points s on the line $\sigma = \sigma_c$, the series may converge or diverge.

The inequalities $\sigma_a - 1 \leq \sigma_c \leq \sigma_a$ are best-possible, in the sense that equality can occur in both cases, as illustrated by the following examples.

(i) If $f(n)$ is nonnegative, then, at any point s *on the real line* the associated Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converges if and only if it converges absolutely. Since, by the theorem, convergence (and absolute convergence) occurs on half-planes, this implies that the half-planes of convergence and absolute convergence are identical. Hence we have $\sigma_c = \sigma_a$ whenever $f(n)$ is nonnegative.

(ii) The Dirichlet series $F(s) = \sum_{n=1}^{\infty}(-1)^n n^{-s}$ is an example for which $\sigma_c = \sigma_a - 1$. Indeed, $F(s)$ converges at any *real* s with $s > 0$ (since it is an alternating series with decreasing terms at such points), and diverges for $\sigma \leq 0$ (since for $\sigma \leq 0$ the terms of the series do not converge to zero), so we have $\sigma_c = 0$. However, since $\sum_{n=1}^{\infty} |(-1)^n n^{-s}| = \sum_{n=1}^{\infty} n^{-\sigma}$, the series converges absolutely if and only if $\sigma > 1$, so that $\sigma_a = 1$.

Proof. If the series $F(s)$ diverges everywhere, the result holds with $\sigma_c = \infty$. Suppose therefore that the series converges at at least one point, let D be the set of all points s at which the series converges, and define $\sigma_c = \inf\{\operatorname{Re} s : s \in D\} \in \mathbb{R} \cup \{-\infty\}$. Then, by the definition of σ_c, $F(s)$ diverges at any point s with $\sigma < \sigma_c$. On the other hand, there exist points $s_0 = \sigma_0 + it_0$ with σ_0 arbitrarily close to σ_c such that the series converges at s_0. By Proposition 4.5 it follows that, given such a point s_0, the series $F(s)$ converges at every point s with $\sigma > \sigma_0$, and the convergence is uniform in compact subsets of $\sigma > \sigma_0$. Since σ_0 can be taken arbitrarily close to σ_c, it follows that $F(s)$ converges in the half-plane $\sigma > \sigma_c$, and that the convergence is uniform on compact subsets of this half-plane.

To obtain the last assertion of the theorem, note first that the inequality $\sigma_c \leq \sigma_a$ holds trivially since absolute convergence implies convergence. Moreover, if $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converges at some point $s = s_0 = \sigma_0 + it_0$, then $f(n)n^{-s_0}$ tends to zero as $n \to \infty$, so that, in

particular, $|f(n)n^{-s_0}| \leq 1$ for $n \geq n_0$, say. Hence, for $n \geq n_0$ and any s we have $|f(n)n^{-s}| \leq n^{-(\sigma-\sigma_0)}$, and since the series $\sum_{n=1}^{\infty} n^{-(\sigma-\sigma_0)}$ converges whenever $\sigma > \sigma_0 + 1$, it follows that $F(s)$ converges absolutely in $\sigma > \sigma_0 + 1$. Since σ_0 can be taken arbitrarily close to σ_c, this implies that $\sigma_a \leq \sigma_c + 1$. □

We are now ready to prove the most important result about Dirichlet series, namely that Dirichlet series are analytic functions of s in their half-plane of convergence. It is this result that allows one to apply the powerful apparatus of complex analysis to the study of arithmetic functions.

Theorem 4.7 (Analytic properties of Dirichlet series). *A Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ represents an analytic function of s in its half-plane of convergence $\sigma > \sigma_c$. Moreover, in the half-plane of convergence, the Dirichlet series can be differentiated termwise, that is, we have $F'(s) = -\sum_{n=1}^{\infty} f(n)(\log n)n^{-s}$, and the latter series also converges in this half-plane.*

Proof. Let $F_N(s) = \sum_{n=1}^{N} f(n)n^{-s}$ denote the partial sums of $F(s)$. Since each term $f(n)n^{-s} = f(n)e^{-s(\log n)}$ is an entire function of s, the functions $F_N(s)$ are entire. By Theorem 4.6, as $N \to \infty$, $F_N(s)$ converges to $F(s)$, uniformly on compact subsets of the half-plane $\sigma > \sigma_c$. By Weierstrass' theorem on uniformly convergent sequences of analytic functions, it follows that $F(s)$ is analytic in every compact subset of the half-plane $\sigma > \sigma_c$, and hence in the entire half-plane. This proves the first assertion of the theorem. The second assertion regarding termwise differentiation follows since the finite partial sums $F_N(s)$ can be termwise differentiated with derivative $F_N'(s) = \sum_{n=1}^{N} f(n)(-\log n)n^{-s}$, and since, by another application of Weierstrass' theorem, the derivatives $F_N'(s)$ converge to $F'(s)$ in the half-plane $\sigma > \sigma_c$. □

Remark. Note that the analyticity of $F(s)$ holds in the half-plane of convergence $\sigma > \sigma_c$, not just in the (smaller) half-plane $\sigma > \sigma_a$ in which the series converges *absolutely*.

The next theorem is a simple, but very useful result, which shows that an arithmetic function is uniquely determined by its Dirichlet series.

Theorem 4.8 (Uniqueness theorem for Dirichlet series). *Suppose $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ and $G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$ are Dirichlet series with finite abscissa of convergence that satisfy $F(s) = G(s)$ for all s with σ sufficiently large. Then $f(n) = g(n)$ for all n.*

Proof. Set $h(n) = f(n) - g(n)$ and let $H(s) = F(s) - G(s)$ be the Dirichlet series for h. By the hypotheses of the theorem there exists σ_0 such that $H(s)$ converges absolutely in the half-plane $\sigma \geq \sigma_0$, and is identically 0 in this half-plane. We need to show that $h(n) = 0$ for all n. To get a contradiction, suppose h is not identically 0, and let n_0 be the smallest positive integer n such that $h(n) \neq 0$. Then $H(s) = h(n_0)n_0^{-s} + H_1(s)$, where $H_1(s) = \sum_{n=n_0+1}^{\infty} h(n)n^{-s}$. Since $H(s) = 0$ for $\sigma \geq \sigma_0$, it follows that, for any $\sigma \geq \sigma_0$, $h(n_0)n_0^{-\sigma} = -H_1(\sigma)$, and hence

$$|h(n_0)| \leq |H_1(\sigma)|n_0^{\sigma} \leq \sum_{n=n_0+1}^{\infty} |h(n)|\frac{n_0^{\sigma}}{n^{\sigma}}.$$

Setting $\sigma = \sigma_0 + \lambda$ with $\lambda \geq 0$, we have, for $n \geq n_0 + 1$,

$$\frac{n_0^{\sigma}}{n^{\sigma}} = \left(\frac{n_0}{n}\right)^{\lambda}\left(\frac{n_0^{\sigma_0}}{n^{\sigma_0}}\right) \leq \left(\frac{n_0}{n_0+1}\right)^{\lambda}\left(\frac{n_0^{\sigma_0}}{n^{\sigma_0}}\right),$$

so that

$$|h(n_0)| \leq n_0^{\sigma_0}\left(\frac{n_0}{n_0+1}\right)^{\lambda} \sum_{n=n_0+1}^{\infty} \frac{|h(n)|}{n^{\sigma_0}} = C_0\left(\frac{n_0}{n_0+1}\right)^{\lambda},$$

where $C_0 = n_0^{\sigma_0}\sum_{n=n_0+1}^{\infty} |h(n)|n^{-\sigma_0}$ is a (finite) constant, independent of λ, by the absolute convergence of $H(\sigma_0)$. Letting $\lambda \to \infty$, the right-hand side tends to zero, contradicting our hypothesis that $h(n_0) \neq 0$. □

Corollary 4.9 (Computing convolution inverses via Dirichlet series). *Let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ be a Dirichlet series with finite abscissa of convergence, and suppose that $1/F(s) = G(s)$, where $G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$ is a Dirichlet series with finite abscissa of convergence. Then g is the convolution inverse of f.*

Proof. Let $h = f * g$, and let $H(s)$ be the Dirichlet series for h. By the hypotheses of the corollary and Theorems 4.4 and 4.6, the series $F(s)$ and $G(s)$ converge absolutely in a half-plane $\sigma \geq \sigma_0$. By Theorem 4.1 it then follows that $H(s)$ also converges absolutely in the same half-plane and is equal to $F(s)G(s)$ there. On the other hand, since $G(s) = 1/F(s)$, we have $H(s) = 1 = \sum_{n=1}^{\infty} e(n)n^{-s}$. By the uniqueness theorem it follows that $h(n) = e(n)$ for all n, i.e., we have $h = f * g = e$. □

Application: Proving identities for arithmetic functions via Dirichlet series. The uniqueness theorem and its corollary provide a new method for obtaining identities among arithmetic functions and computing convolution inverses. In order to prove an identity of the form $f(n) \equiv g(n)$, it suffices to show that the corresponding Dirichlet series converge and are equal for sufficiently large σ. In practice, this is usually carried out by algebraically manipulating the Dirichlet series for $f(n)$ to obtain another Dirichlet series and then "reading off" the coefficients of the latter Dirichlet series, to conclude that these coefficients must be equal to those in the original Dirichlet series. In most cases, the functions involved are multiplicative, so that the Dirichlet series can be written as Euler products, and it is the individual factors in the Euler product that are manipulated. We illustrate this technique with the following examples.

Examples

(1) **Alternate proof of the identity $\phi = \mu * \mathrm{id}$.** Using only the multiplicativity of ϕ and the definition of ϕ at prime powers, we have shown above that the Dirichlet series of ϕ is equal to $\zeta(s-1)/\zeta(s)$. Since $\zeta(s-1)$ and $1/\zeta(s)$ are, respectively, the Dirichlet series of the functions id and μ, $\zeta(s-1)/\zeta(s)$ is the Dirichlet series of the convolution product $\mathrm{id} * \mu$. Since both of these series converge absolutely for $\sigma > 2$, we can apply the uniqueness theorem for Dirichlet series to conclude that $\phi = \mathrm{id} * \mu$.

(2) **Computing "square roots" of completely multiplicative functions.** Given a completely multiplicative function f, we want to find a function g such that $g * g = f$. To this end note that if g satisfies $g * g = f$, then the corresponding Dirichlet series $G(s)$ must satisfy $G(s)^2 = F(s)$, provided $G(s)$ converges absolutely. Thus, we seek a function whose Dirichlet series is the square root of the Dirichlet series for f. Now, since f is completely multiplicative, its Dirichlet series has an Euler product with factors of the form $(1 - f(p)p^{-s})^{-1}$. Taking the square root of this expression and using the binomial series $(1+x)^{-1/2} = \sum_{n=0}^{\infty} \binom{-1/2}{n} x^n$ gives

$$\left(1 - \frac{f(p)}{p^s}\right)^{-1/2} = 1 + \sum_{m=1}^{\infty} \binom{-1/2}{m} \frac{(-1)^m f(p)^m}{p^{ms}}.$$

The latter series can be identified as the p-th factor of the Euler product of the multiplicative function g defined by $g(p^m) =$

$(-f(p))^m\binom{-1/2}{m}$. Let $G(s)$ be the Dirichlet series for g. Then $G(s)^2 = F(s)$, and the uniqueness theorem yields $g * g = f$ provided both series $G(s)$ and $F(s)$ have finite abscissa of convergence. The bound $|\binom{-1/2}{m}| = |(-1)^m\binom{2m}{m}| \leq 2^{2m}$ shows that this convergence condition is satisfied if, for example, the values $f(p)$ are uniformly bounded.

(3) **Computing convolution inverses.** A direct computation of convolution inverses requires solving an infinite system of linear equations, but Dirichlet series often allow a quick computation of an inverse. As an application of Corollary 4.9, consider the function f defined by $f(1) = 1$, $f(2) = -1$, and $f(n) = 0$ for $n \geq 3$. This function has Dirichlet series $F(s) = 1 - 2^{-s}$, which is an entire function of s. The reciprocal of $F(s)$ is given by $1/F(s) = (1 - 2^{-s})^{-1} = \sum_{k=0}^{\infty} 2^{-ks}$. Writing this series in the form $G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$, and reading off the coefficients $g(n)$, we see that $1/F(s)$ is the Dirichlet series of the function g defined by $g(n) = 1$ if $n = 2^k$ for some nonnegative integer k, and $g(n) = 0$ otherwise. The series $G(s)$ converges absolutely for $\sigma > 0$. Hence, Corollary 4.9 is applicable and shows that g is the convolution inverse of f.

(4) **Evaluating functions via Dirichlet series.** Another type of application is illustrated by the following example. Let $f_k(n)$ denote the characteristic function of k-free integers. In order to estimate the partial sums $\sum_{n\leq x} f_k(n)$ (i.e., the number of k-free positive integers $\leq x$), a natural approach is to use the convolution method with the function 1 as the approximating function. This requires computing the "perturbation factor" g_k defined by $f_k = 1 * g_k$. If F_k and G_k denote the Dirichlet series of f_k and g_k, respectively, then $G_k(s) = F_k(s)/\zeta(s)$. In the previous section, we computed $F_k(s)$ as $F_k(s) = \zeta(s)/\zeta(ks)$, so

$$G_k(s) = \frac{1}{\zeta(ks)} = \prod_p \left(1 - \frac{1}{p^{ks}}\right).$$

The latter product is the Euler product of the Dirichlet series for the multiplicative function g_k^* defined by $g_k^*(p^m) = -1$ if $m = k$ and $g_k^*(p^m) = 0$ otherwise, i.e., $g_k^*(n) = \mu(n^{1/k})$ if n is a k-th power, and $g_k^*(n) = 0$ otherwise. Since all series involved converge absolutely for $\sigma > 1$, the uniqueness theorem applies, and we conclude that the coefficients of the latter series and those of $G_k(s)$ must be equal, i.e., we have $g_k \equiv g_k^*$.

(5) **Wintner's theorem for multiplicative functions.** In the terminology and notation of Dirichlet series, Wintner's theorem (Theorem 2.19) states that if $f = 1 * g$ and if the Dirichlet series $G(s)$ of g converges absolutely at $s = 1$, then the mean value $M(f)$ exists and is equal to $G(1)$. This result holds for arbitrary arithmetic functions f and g satisfying the above conditions, but if these functions are multiplicative, then one can express the mean value $M(f)$ as an Euler product, and one can check the condition that the Dirichlet series $G(s)$ converges absolutely at $s = 1$ by the criterion of Theorem 4.3: Applying Theorem 4.3 to the function $g = f * \mu$, noting that $g(p^m) = f(p^m) - f(p^{m-1})$ for every prime power p^m, and using the fact that if f is multiplicative, then so is $g = f * \mu$, we obtain the following version of Wintner's theorem for multiplicative functions:

Suppose f is multiplicative and satisfies

$$\sum_{p^m} \frac{|f(p^m) - f(p^{m-1})|}{p^m} < \infty.$$

Then the mean value $M(f)$ exists and is given by

$$\begin{aligned} M(f) &= \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{f(p^m) - f(p^{m-1}}{p^m}\right) \\ &= \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \sum_{m=1}^{\infty} \frac{f(p^m)}{p^m}\right). \end{aligned}$$

4.4 Dirichlet series and summatory functions

4.4.1 Mellin transform representation of Dirichlet series

As we have seen in Chapter 2, to investigate the behavior of arithmetic functions one usually considers the associated summatory functions

$$M(f, x) = \sum_{n \le x} f(n), \tag{4.7}$$

or weighted versions of those sums, such as the "logarithmic" sums

$$L(f, x) = \sum_{n \le x} \frac{f(n)}{n}. \tag{4.8}$$

In contrast to the individual values $f(n)$, which for most natural arithmetic functions oscillate wildly and show no discernable pattern when $n \to \infty$, the summatory functions $M(f,x)$ and $L(f,x)$ are usually well-behaved and can be estimated in a satisfactory manner. Most results and problems on arithmetic functions can be expressed in terms of these summatory functions. For example, as we have seen in Chapter 2, Mertens' estimates show that $L(\Lambda,x) = \log x + O(1)$ and the PNT is equivalent to the asymptotic formula $M(\Lambda,x) \sim x$.

It is therefore natural to try to express the Dirichlet series $F(s)$ of an arithmetic function f in terms of the summatory functions $M(f,x)$ and vice versa, to exploit this to translate between properties of the analytic function $F(s)$ those of the arithmetic quantity $M(f,x)$.

In one direction, namely going from $M(f,x)$ to $F(s)$, this is rather easy. The key result is the following theorem which expresses $F(s)$ as an integral over $M(f,x)$ and is a restatement (in a slightly different notation) of Theorem 2.15. The converse direction is considerably more difficult, and will be considered in a separate section.

Theorem 4.10 (Mellin transform representation of Dirichlet series). *Let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ be a Dirichlet series with finite abscissa of convergence σ_c, and let $M(f,x)$ and $L(f,x)$ be given by* (4.7) *and* (4.8)*, respectively. Then we have*

$$F(s) = s\int_1^{\infty} M(f,x)x^{-s-1}dx \quad (\sigma > \max(0,\sigma_c)), \tag{4.9}$$

$$F(s) = (s-1)\int_1^{\infty} L(f,x)x^{-s}dx \quad (\sigma > \max(1,\sigma_c)). \tag{4.10}$$

Proof. We first show that the second relation follows from the first, applied to the function $\tilde{f}(n) = f(n)/n$, with $\tilde{s} = s-1$ in place of s, and $\tilde{F}(s) = \sum_{n=1}^{\infty} \tilde{f}(n)n^{-s}$ in place of $F(s)$. To this end, observe first that $L(f,x) = M(\tilde{f},x)$, so the right-hand side of (4.10) becomes the right-hand side of (4.9) with $\tilde{f}$ in place of f and $\tilde{s} = s-1$ in place of s. Moreover, we have $F(s) = \tilde{F}(s-1) = \tilde{F}(\tilde{s})$, so the left-hand sides of these relations are also equal under these substitutions. Finally, since $\tilde{F}(s) = F(s+1)$, the abscissa of convergence $\tilde{\sigma}_c$ of $\tilde{F}$ is equal to $\sigma_c - 1$, so the condition $\tilde{\sigma} > \max(0,\tilde{\sigma}_c)$ in (4.9) translates into $\sigma - 1 > \max(0,\sigma_c - 1)$, or, equivalently, $\sigma > \max(1,\sigma_c)$, which is the condition in (4.10).

The first relation, (4.9), was already proved in Theorem 2.15 of Chapter 2, as an application of partial summation. We give here an alternate argument: Let f and $F(s)$ be given as in the theorem, and fix s with

$\sigma > \min(0, \sigma_c)$, so that the Dirichlet series $F(s)$ converges at s. Write

$$M(f,x) = \sum_{n=1}^{\infty} \chi(n,x) f(n),$$

where

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

Then, for every $X \ge 1$,

$$\begin{aligned} s\int_1^X M(f,x)x^{-s-1}dx &= s\int_1^X \sum_{n=1}^{\infty} \chi(x,n) f(n) x^{-s-1} dx \\ &= s\int_1^X \sum_{n\le X} \chi(x,n) f(n) x^{-s-1} dx \\ &= s\sum_{n\le X} f(n) \int_1^X \chi(x,n) x^{-s-1} dx \\ &= s\sum_{n\le X} f(n) \int_n^X x^{-s-1} dx \\ &= s\sum_{n\le X} f(n) \frac{1}{s}\left(\frac{1}{n^s} - \frac{1}{X^s}\right) \\ &= \sum_{n\le X} \frac{f(n)}{n^s} - \frac{1}{X^s} M(f,X). \end{aligned}$$

Now let $X \to \infty$. Then, by the convergence of $F(s)$, the first term on the right tends to $F(s)$. Moreover, Kronecker's Lemma (Theorem 2.12) implies that the second term tends to 0. Hence we conclude

$$\lim_{X\to\infty} s\int_1^X M(f,x)x^{-s-1}dx = F(s),$$

which proves (4.9). □

Despite its rather elementary nature and easy proof, this result has a number of interesting and important applications, as we will illustrate in the following subsections.

4.4.2 Analytic continuation of the Riemann zeta function

As a first application of Theorem 4.10, we give an integral representation for the Riemann zeta function that is valid in the half-plane $\sigma > 0$ and provides an analytic continuation of $\zeta(s)$ to this half-plane.

Theorem 4.11 (Integral representation and analytic continuation of the zeta function). *The Riemann zeta function, defined for $\sigma > 1$ by the series*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \tag{4.11}$$

has an analytic continuation to a function defined on the half-plane $\sigma > 0$ and analytic in this half-plane with the exception of a simple pole at $s = 1$ with residue 1, given by

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \{x\}x^{-s-1}dx \quad (\sigma > 0). \tag{4.12}$$

Remark. Strictly speaking, we should use a different symbol, say $\tilde{\zeta}(s)$, for the analytic continuation defined by (4.12). However, to avoid awkward notations, it has become standard practice to denote the analytic continuation of a Dirichlet series by the same symbol as the series itself, and we will usually follow this practice. That said, one should be aware that the validity of the series representation in general does not extend to the region in which the Dirichlet series is analytic (in the sense of having an analytic continuation there). For example, the Dirichlet series representation (4.11) of the zeta function diverges at every point in the half-plane $\sigma < \sigma_c = 1$ (and even at every point on the line $\sigma = 1$, as one can show by Euler's summation), and thus is not even well defined outside the half-plane $\sigma > 1$. By contrast, the representation (4.12) is well-defined in the larger half-plane $\sigma > 0$ and represents an analytic function there.

Proof. Applying Theorem 4.10 with $f \equiv 1$, $F(s) = \zeta(s)$, $\sigma_c = 1$, and $M(f, x) = [x]$, we obtain

$$\zeta(s) = s\int_1^{\infty} [x]x^{-s-1}dx \quad (\sigma > 1).$$

Setting $[x] = x - \{x\}$, where $\{x\}$ is the fractional part of x, we can write the last integral as

$$\int_1^{\infty} x^{-s}dx - \int_1^{\infty} \{x\}x^{-s-1}dx = \frac{1}{s-1} - \int_1^{\infty} \{x\}x^{-s-1}dx,$$

and thus obtain the representation (4.12) in the half-plane $\sigma > 1$. Now note that, given $\epsilon > 0$, the integral in (4.12) is bounded, for any s with $\sigma \geq \epsilon$, by

$$\left| \int_1^\infty \{x\} x^{-s-1} dx \right| \leq \int_1^\infty x^{-\sigma-1} dx \leq \int_1^\infty x^{-\epsilon-1} dx = \frac{1}{\epsilon}.$$

Hence this integral converges absolutely and uniformly in the half-plane $\sigma \geq \epsilon$ and therefore represents an analytic function of s in the half-plane $\sigma \geq \epsilon$. Since $\epsilon > 0$ can be taken arbitrarily small, this function is in fact analytic in the half-plane $\sigma > 0$. It follows that the right-hand side of (4.12) is an analytic function in this half-plane, with the exception of the pole at $s = 1$ with residue 1, coming from the term $s/(s-1)$. This provides the asserted analytic continuation of $\zeta(s)$ to the half-plane $\sigma > 0$. □

As an immediate consequence of the representation (4.12) for $\zeta(s)$, we obtain an estimate for $\zeta(s)$ near the point $s = 1$.

Corollary 4.12 (Estimate for $\zeta(s)$ near $s = 1$). *For $|s-1| \leq 1/2$, $s \neq 1$, we have*

$$\zeta(s) = \frac{1}{s-1} + \gamma + O(|s-1|),$$

where γ is Euler's constant.

Proof. By Theorem 4.11, the function $\zeta(s) - 1/(s-1)$ is analytic in the disk $|s-1| < 1$ and therefore has a power series expansion

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

in this disk. It follows that

$$\zeta(s) - \frac{1}{s-1} = a_0 + O(|s-1|)$$

in the disk $|s-1| \leq 1/2$. Thus it remains to show that the constant a_0 is equal to γ. By (4.12) we have, in the half-plane $\sigma > 0$,

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

Letting $s \to 1$ on the right-hand side, we get

$$a_0 = \lim_{s \to 1} \left(\zeta(s) - \frac{1}{s-1} \right) = 1 - \int_1^\infty \{x\} x^{-2} dx.$$

Now, from the proof of the harmonic sum estimate (Theorem 2.5) we have $\gamma = 1 - \int_1^\infty \{x\} x^{-2} dx$, so we obtain $a_0 = \gamma$ as claimed. □

4.4.3 Lower bounds for error terms in summatory functions

We begin with a general result relating error terms in estimates for the summatory functions $M(f,x)$ to the region of analyticity of the Dirichlet series $F(s)$.

Theorem 4.13 (Error terms in estimates for $M(f,x)$ and analyticity of $F(s)$).

(i) If $M(f,x) = O(x^\theta)$ for some $\theta \geq 0$, then $F(s)$ is analytic in the half-plane $\sigma > \theta$.

(ii) If $M(f,x) = Ax^\alpha + O(x^\theta)$ for some constants A, α and θ with $\alpha > \theta \geq 0$, then $F(s) - As(s-\alpha)^{-1}$ is analytic in the half-plane $\sigma > \theta$.

Proof. First note that since $f(n) = M(f,n) - M(f,n-1)$, the given estimates for $M(f,x)$ imply that $f(n) = O(n^\theta)$ in case (i) and $f(n) = O(n^\alpha)$ in case (ii), so the Dirichlet series $F(s)$ has finite abscissa of convergence, and Theorem 4.10 can therefore be applied in both cases.

(i) If $M(f,x) = O(x^\theta)$, then the integrand in the integral in (4.9) is of order $O(x^{\theta-\sigma-1})$. Hence, for any $\epsilon > 0$, this integral is uniformly convergent in $\sigma \geq \theta + \epsilon$, so it represents a function that is analytic in $\sigma \geq \theta + \epsilon$ for every $\epsilon > 0$, and thus analytic in the half-plane $\sigma > \theta$. Consequently, the function on the right of (4.9), and therefore $F(s)$, is analytic in this half-plane as well.

(ii) If $M(f,x) = Ax^\alpha + O(x^\theta)$, we set $M(f,x) = Ax^\alpha + M_1(f,x)$, and split the integral on the right of (4.9) into a sum of two integrals corresponding to the terms Ax^α and $M_1(f,x)$. Since $M_1(f,x) = O(x^\theta)$, the second of these integrals is analytic in $\sigma > \theta$ by the above argument. The first integral is

$$\int_1^\infty Ax^{\alpha-s-1}dx = \frac{A}{s-\alpha}.$$

Thus,

$$F(s) = \frac{As}{s-\alpha} + F_1(s),$$

where $F_1(s)$ is analytic in $\sigma > \theta$, as claimed. □

Theorem 4.13 can be used, in conjunction with known analytic properties of the zeta function, to obtain *lower* bounds on error terms in the various (equivalent) versions of the PNT.

We illustrate this in the case of the summatory function of the Moebius function, $M(\mu,x) = \sum_{n\leq x} \mu(n)$. The PNT is equivalent to the estimate

$M(\mu, x) = o(x)$, but since $\mu(n)$ takes on the values $0, \pm 1$ in a seemingly random manner, one might expect that the "true" order of $M(\mu, x)$ is much smaller. Indeed, if the values ± 1 on squarefree integers were assigned in a truly random manner, the rate of growth of the summatory function $M(\mu, x)$ would be roughly $\sqrt{x}$, with probability close to 1.

To investigate the consequences of such estimates, suppose that, for some $\theta \geq 0$, we have

$$M(\mu, x) = O_\theta(x^\theta). \tag{4.13}$$

Theorem 4.13 then implies that the Dirichlet series for the Moebius function, namely $\sum_{n=1}^{\infty} \mu(n) n^{-s} = 1/\zeta(s)$, is analytic in the half-plane $\sigma > \theta$. This in turn implies that $\zeta(s)$ is meromorphic in this half-plane and satisfies

$$\zeta(s) \text{ has no zeros in } \sigma > \theta. \tag{4.14}$$

Thus, the quality of estimates for $M(\mu, x)$, and hence the quality of the error term in the PNT, depends on the "zero-free region" of the Riemann zeta function, and specifically the values θ for which (4.14) holds. Unfortunately, very little is known in this regard. The current state of knowledge can be summarized as follows:

- (4.14) holds for $\theta > 1$. (This follows immediately from the Euler product representation for $\zeta(s)$.)
- It is known that $\zeta(s)$ has infinitely many zeros with real part $1/2$, so (4.14) does not hold for any value $\theta < 1/2$. (The proof of this is not easy and beyond the scope of this course.)
- For $\theta = 1/2$, statement (4.14) is the "Riemann Hypothesis", the most famous problem in number theory. It is easily seen that (4.14) holds for $\theta = 1/2$ if and only if it holds for all $\theta > 1/2$.
- It is not known whether there exists *some* θ with $1/2 \leq \theta < 1$ for which (4.14) holds (which would be a weak form of the Riemann Hypothesis).

From these remarks and Theorem 4.13 we have the following result.

Theorem 4.14 (Lower bounds for the error term in the PNT). The estimate (4.13) does not hold for any $\theta < 1/2$. If it holds for $\theta = 1/2 + \epsilon$, for any $\epsilon > 0$, then the Riemann Hypothesis follows.

Remarks. (i) By a similar argument, using part (ii) of Theorem 4.13 and the fact that the Dirichlet series for $\Lambda(n)$ is $-\zeta'(s)/\zeta(s)$, one can relate the error term in the estimate $M(\Lambda, x) = x + o(x)$ to the zerofree region (4.14) and show that an estimate of the form

$$M(\Lambda, x) = x + O_\theta(x^\theta) \tag{4.15}$$

implies (4.14). Since (4.14) known to be false when $\theta < 1/2$, (4.15) does not hold if $\theta < 1/2$. Moreover, if (4.15) holds for $\theta = 1/2 + \epsilon$, for every $\epsilon > 0$, then the Riemann Hypothesis follows.

(ii) The converse of the above statements also holds, though this requires an entirely different argument, which is beyond the scope of this course. Namely, if the Riemann Hypothesis is true, then (4.13) and (4.15) hold for any $\theta > 1/2$, i.e., the error terms in these estimates are essentially (namely, up to a factor x^ϵ) of size $O(\sqrt{x})$. Since such a "squareroot bound" is characteristic of a random sequence of values ± 1, the Riemann Hypothesis can thus be interpreted as saying that the values of the Moebius function behave (essentially) "randomly".

4.4.4 Evaluation of Mertens' constant

As a final application of Theorem 4.10, we now evaluate the constant in Mertens' formula (Theorem 3.4), which we had proved in Chapter 3 in the form

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right) = \frac{e^{-C}}{\log x} \left(1 + O\left(\frac{1}{\log x}\right)\right) \quad (x \ge 2), \tag{4.16}$$

with an unspecified constant C. We will now show this constant is equal to the Euler constant γ, as claimed in Theorem 3.4.

Taking logarithms in (4.16), we see that (4.16) is equivalent to

$$-\log P(x) = \log\log x + C + \left(\frac{1}{\log x}\right) \quad (x \ge 2), \tag{4.17}$$

where

$$P(x) = \prod_{p \le x} \left(1 - \frac{1}{p}\right).$$

Now,

$$\begin{aligned}
-\log P(x) &= -\sum_{p\le x} \log\left(1-\frac{1}{p}\right) \\
&= \sum_{p\le x}\sum_{m=1}^{\infty} \frac{1}{mp^m} \\
&= \sum_{p\le x} \frac{1}{mp^m} + O\left(\sum_{p\le x}\sum_{m>\log x/\log p} \frac{1}{p^m}\right) \\
&= \sum_{p\le x} \frac{1}{mp^m} + O\left(\sum_{p\le x} \frac{1}{x}\right) \\
&= L(f,x) + O\left(\frac{\pi(x)}{x}\right) \\
&= L(f,x) + O\left(\frac{1}{\log x}\right),
\end{aligned}$$

where f is the function defined by

$$f(n) = \begin{cases} \frac{1}{m} & \text{if } n = p^m, \\ 0 & \text{otherwise,} \end{cases}$$

and $L(f,x) = \sum_{n\le x} f(n)/n$ is the "logarithmic" summatory function of f, as defined in Theorem 4.10. Thus, (4.17) is equivalent to

$$L(f,x) = \log\log x + C + \left(\frac{1}{\log x}\right) \quad (x \ge 2). \tag{4.18}$$

We now relate f to the Riemann zeta function. Let s be real and greater than 1. Expanding $\zeta(s)$ into an Euler product and taking logarithms, we obtain

$$\begin{aligned}
\log\zeta(s) = \log\prod_p \left(1-\frac{1}{p^s}\right)^{-1} &= \sum_p \log\left(1-\frac{1}{p^s}\right)^{-1} \\
&= \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}} = F(s),
\end{aligned}$$

where $F(s)$ is the Dirichlet series of $f(n)$. On the other hand, Corollary 4.12

gives

$$\begin{aligned}\log\zeta(s) &= \log\left(\frac{1}{s-1}\,(1+O(s-1))\right)\\ &= \log\frac{1}{s-1}+\log(1+O(s-1))\\ &= \log\frac{1}{s-1}+O(s-1)\quad(1<s<s_0),\end{aligned}$$

for a suitable s_0 with $1<s_0<3/2$. Thus, we have

$$F(s)=\log\frac{1}{s-1}+O(s-1)\quad(1<s<s_0). \tag{4.19}$$

Next, we apply Theorem 4.10 to express $F(s)$ as an integral over $L(f,x)$. Since $0\le f(n)\le 1$, the abscissa of convergence of $F(s)$ is ≤ 1, so the representation given by this theorem is valid in $\sigma>1$. Noting that $L(f,x)=0$ for $x<2$, we obtain, in the half-plane $\sigma>1$,

$$F(s)=(s-1)\int_2^\infty L(f,x)x^{-s}dx.$$

Substituting the estimate (4.18) for $L(f,x)$, we get

$$\begin{aligned}F(s) &= (s-1)\int_2^\infty\left(\log\log x+C+O\left(\frac{1}{\log x}\right)\right)x^{-s}dx\\ &= (s-1)\int_{\log 2}^\infty\left(\log u+C+O\left(\frac{1}{u}\right)\right)e^{-u(s-1)}du\\ &= \int_{(s-1)\log 2}^\infty\left(\log\frac{1}{s-1}+\log v+C+O\left(\frac{s-1}{v}\right)\right)e^{-v}dv.\end{aligned} \tag{4.20}$$

We now restrict s to the interval $1<s<s_0(<3/2)$ and estimate the integral on the right of (4.20). The contribution of the O-term to this integral is bounded by

$$\begin{aligned}&\ll (s-1)\int_{(s-1)\log 2}^\infty\frac{e^{-v}}{v}dv\\ &\le (s-1)\left(\log\frac{1}{(s-1)\log 2}+\int_1^\infty e^{-v}dv\right)\\ &\le (s-1)\left(\log\frac{1}{s-1}+O(1)\right)\ll(s-1)\log\frac{1}{s-1},\end{aligned}$$

since $1 \ll \log 1/(s-1)$ by our assumption $1 < s < s_0 < 3/2$. In the integral over the terms $\log 1/(s-1) + \log v + C$ we replace the lower integration limit by 0, which introduces an error of order

$$\ll \int_0^{(s-1)\log 2} \left(\log \frac{1}{s-1} + |\log v| + |C| \right) dv \ll (s-1) \log \frac{1}{s-1}.$$

With these estimates, (4.20) becomes

$$\begin{aligned} F(s) &= \log \frac{1}{s-1} \int_0^\infty e^{-v} dv + \int_0^\infty (\log v) e^{-v} dv + C \int_0^\infty e^{-v} dv \\ &\quad + O\left((s-1) \log \frac{1}{s-1} \right) \\ &= \log \frac{1}{s-1} + I + C + O\left((s-1) \log \frac{1}{s-1} \right), \end{aligned} \tag{4.21}$$

where

$$I = \int_0^\infty (\log v) e^{-v} dx$$

Equating the estimates (4.21) and (4.19) for $F(s)$ we get

$$\log \frac{1}{s-1} + O(s-1) = \log \frac{1}{s-1} + I + C + O\left((s-1) \log \frac{1}{s-1} \right) \quad (1 < s < s_0).$$

Letting $s \to 1+$, the error terms here tends to zero, and we therefore conclude that

$$C = -I = -\int_0^\infty (\log v) e^{-v} dv.$$

The integral I can be found in many standard tables of integrals (e.g., Gradsheyn and Ryzhik, "Table of integrals, series, and products") and is equal to $-\gamma$. Hence $C = \gamma$, which is what we wanted to show.

4.5 Inversion formulas

In this section, we consider the converse problem of representing the partial sums $M(f, x)$ in terms of the Dirichlet series $F(s)$. This is a more difficult problem than that of expressing $F(s)$ in terms of $M(f, x)$, and the resulting formulas are more complicated, involving complex integrals, usually in truncated form with error terms, because of convergence problems. However, such "inversion formulas" are essential in applications such as the

analytic proof of the prime number theorem, since in those applications analytic information on the generating Dirichlet series of an arithmetic function is available and one needs to translate that information into information on the behavior of the partial sums of the arithmetic function.

Formulas expressing $M(f,x)$, or similar functions, in terms of $F(s)$, are collectively known as "Perron formulas". We prove here two such formulas, one for $M(f,x)$, and the other for an average version of $M(f,x)$, defined by

$$M_1(f,x) = \int_1^x M(f,y)dy = \sum_{n\le x} f(n)(x-n). \tag{4.22}$$

(The second identity here follows by writing $M(f,y) = \sum_{n\le y} f(n)$ and inverting the order of summation and integration.)

The proof of these formulas rests on the evaluation of certain complex integrals, which we state in the following lemma.

Lemma 4.15. *Let $c > 0$, and for $T > 0$ and $y > 0$ set*

$$I(y,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s}ds, \quad I_1(y) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s(s+1)}ds. \tag{4.23}$$

(i) Given $T > 0$ and $y > 0$, $y \neq 1$, we have

$$\begin{cases} |I(y,T) - 1| \le \dfrac{y^c}{\pi T \log y} & \text{if } y > 1, \\ |I(y,T)| \le \dfrac{y^c}{\pi T |\log y|} & \text{if } 0 < y < 1. \end{cases} \tag{4.24}$$

(ii) For all $y > 0$ we have

$$I_1(y) = \begin{cases} \left(1 - \frac{1}{y}\right) & \text{if } y > 1, \\ 0 & \text{if } 0 < y \le 1. \end{cases} \tag{4.25}$$

Proof. (i) Suppose first that $y > 1$; we seek to estimate $|I(y,T) - 1|$. Given $b < 0$, we apply the residue theorem, replacing the path $[c - iT, c + iT]$ by the path consisting of the two horizontal segments $[c - iT, b - iT]$ and $[b + iT, c + iT]$ and the vertical segment $[b - iT, b + iT]$. In doing so, we pick up a residue equal to 1 from the pole of the integrand y^s/s at $s = 0$. It remains to estimate the integral over the new path. On the vertical segment $[b - iT, b + iT]$, the integrand is bounded by $\le |y^s|/|s| \le y^b/|b|$, and so the integral over $[b - iT, b + iT]$ is bounded by $\le 2Ty^b/|b|$. Since $y > 1$, this bound tends to 0 as $b \to -\infty$.

On the two horizontal segments we have $|y^s/s| \le y^\sigma/T$, so the integral over each of these two segments is bounded by

$$\le \frac{1}{2\pi}\int_b^c \frac{y^\sigma}{T}d\sigma \le \frac{1}{2\pi}\int_{-\infty}^c \frac{y^\sigma}{T}d\sigma = \frac{y^c}{2\pi T\log y}.$$

Letting $b \to -\infty$, we conclude that, for $y > 1$, the integral $I(y,T)$ differs from 1 by at most twice the above bound, i.e., an amount $\le (1/\pi)y^c/(T\log y)$, as claimed.

In the case $0 < y < 1$, we apply a similar argument, except that we now move the path of integration to a line $\sigma = a$ to the right of the line $\sigma = c$, with the new path consisting of the horizontal segments $[c - iT, a - iT]$ and $[a + iT, c + iT]$ and the vertical segment $[a - iT, a + iT]$. As before, the contribution of the vertical segment tends to 0 on letting $a \to \infty$, whereas the contribution of each of the horizontal segments is at most $\le (1/2\pi)\int_c^\infty (y^\sigma/T)d\sigma \le y^c/(2\pi T|\log y|)$. This time, however, there is no residue contribution, since the integrand has no poles in the region enclosed by the old and new paths of integration. Hence, for $0 < y < 1$, we have $|I(y,T)| \le y^c/(\pi T\log|y|)$.

(ii) Considering first the integral over a finite line segment $[c-iT, c+iT]$ and treating this integral as that of (i) by shifting the path of integration, we obtain in the case $y > 1$ a contribution coming from the residues of $y^s/(s(s+1))$ at the poles $s = 0$ and $s = -1$, namely $1 - 1/y$, and an error term that tends to 0 as $T \to \infty$. Letting $T \to \infty$, we conclude that $I_1(y) = (1-1/y)$ in the case $y > 1$. If $0 < y < 1$, the same argument applies, but without a residue contribution, so in this case we have $I_1(y) = 0$. Hence (4.25) holds for all $y > 0$ except possibly $y = 1$. To deal with the remaining case $y = 1$, we use a continuity argument: It is easily verified that the left and right-hand sides of (4.25) are continuous functions of $y > 0$. Since both sides are equal for $y > 1$, if follows that the equality persists when $y = 1$. □

We are now ready to state the two main results of this section, which give formulas for $M_1(f,x)$ and $M(f,x)$ as complex integrals over $F(s)$.

Theorem 4.16 (Perron Formula for $M_1(f,x)$). *Let $f(n)$ be an arithmetic function, and suppose that the Dirichlet series $F(s) = \sum_{n=1}^\infty f(n)n^{-s}$ has finite abscissa of absolute convergence σ_a. Let $M_1(f,x)$ be defined by* (4.22) *and* (4.7)*. Then we have, for any $c > \max(0,\sigma_a)$ and any real number $x \ge 1$,*

$$M_1(f,x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(s)\frac{x^{s+1}}{s(s+1)}ds. \tag{4.26}$$

Remark. Since, on the line of integration, $|x^{s+1}| = x^{c+1}$ and $|F(s)| \le \sum_{n=1}^{\infty} |f(n)|n^{-c} < \infty$, the integrand is bounded by $\ll x^{c+1}/|s|^2$. Thus, the integral in (4.26) converges absolutely. By contrast, the formula for $M(f,x)$ (see Theorem 4.17 below) involves an integral over $F(s)x^{s+1}/s$, which is only conditionally convergent.

Proof. Ignoring questions of convergence for the moment, we obtain (4.26) by writing the right-hand side as

$$\begin{aligned}\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \frac{x^{s+1}}{s(s+1)} ds &= \frac{1}{2\pi i} \sum_{n=1}^{\infty} f(n) \int_{c-i\infty}^{c+i\infty} \frac{(x/n)^s x}{s(s+1)} ds \\ &= \sum_{n=1}^{\infty} f(n) x I_1(x/n) = \sum_{n \le x} f(n)(x-n) = M_1(f,x),\end{aligned}$$

using the evaluation of $I_1(y)$ given by Lemma 4.15. To justify the interchanging of the order of integration and summation, we note that

$$\begin{aligned}&\int_{c-i\infty}^{c+i\infty} \sum_{n=1}^{\infty} \frac{|f(n)|}{|n^s|} \left| \frac{x^{s+1}}{s(s+1)} \right| \cdot |ds| \\ &\qquad \le x^{c+1} \sum_{n=1}^{\infty} \frac{|f(n)|}{n^c} \int_{c-i\infty}^{c+i\infty} \frac{x^{c+1}}{|s(s+1)|} |ds| < \infty,\end{aligned}$$

since, by the assumption $c > \max(0, \sigma_a)$, we have $\sum_{n=1}^{\infty} |f(n)|n^{-c} < \infty$ and

$$\int_{c-i\infty}^{c+i\infty} \frac{1}{|s(s+1)|} |ds| \le \int_{c-i\infty}^{c+i\infty} \frac{1}{|s|^2} |ds| = \int_{-\infty}^{\infty} \frac{1}{c^2+t^2} dt < \infty. \qquad \square$$

Theorem 4.17 (Perron Formula for $M(f,x)$). *Let $f(n)$ be an arithmetic function, and suppose that the Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ has finite abscissa of absolute convergence σ_a. Then we have, for any $c > \max(0, \sigma_a)$ and any non-integral value $x > 1$,*

$$M(f,x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} F(s) \frac{x^s}{s} ds, \tag{4.27}$$

where the improper integral $\int_{c-i\infty}^{c+i\infty}$ is to be interpreted as the symmetric limit $\lim_{T\to\infty} \int_{c-iT}^{c+iT}$. Moreover, given $T > 0$, we have

$$M(f,x) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} F(s) \frac{x^s}{s} ds + R(T), \tag{4.28}$$

where

$$|R(T)| \le \frac{x^c}{T} \sum_{n=1}^{\infty} \frac{|f(n)|}{n^c |\log(x/n)|}. \tag{4.29}$$

Remark. The restriction to non-integral values of x in the "infinite" version of Perron's formula (4.27) can be dropped if we replace the function $M(f,x)$ by the interpolation between its left and right limits, namely $M^*(f,x) = (1/2)(M(f,x-)+M(f,x+))$. This can be proved in the same manner using the following evaluation of the integral $I(y,T)$ in the case $y=1$:

$$\begin{aligned} I(1,T) &= \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{1}{s} ds = \frac{1}{2\pi}\int_{-T}^{T} \frac{c-it}{c^2+t^2} dt \\ &= \frac{1}{2\pi}\int_{-T}^{T} \frac{c}{c^2+t^2} dt = \frac{1}{2\pi}\int_{-T/c}^{T/c} \frac{1}{1+u^2} du \\ &= \frac{1}{2\pi}\left(\arctan(T/c) - \arctan(-T/c)\right), \end{aligned}$$

which converges to $(1/2\pi)(\pi/2 - (-\pi/2)) = 1/2$ as $T \to \infty$.

However, in applications the stated version is sufficient, since for any integer N, $M(f,N)$ is equal to $M(f,x)$ for $N < x < N+1$ and one can therefore apply the formula with such a non-integral value of x. Usually one takes x to be of the form $x = N + 1/2$ in order to minimize the effect a small denominator $\log(x/n)$ on the right-hand side of (4.29) can have on the estimate.

Proof. The formula (4.27) follows on letting $T \to \infty$ in (4.28), so it suffices to prove the latter formula. To this end we proceed as in the proof of Theorem 4.16, substituting $F(s) = \sum_{n=1}^{\infty} f(n) n^{-s}$ in the first (main) term on the right-hand side of (4.28), to obtain

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} F(s)\frac{x^s}{s} ds = \sum_{n=1}^{\infty} f(n) I(x/n, T).$$

The interchanging of integration and summation is again permissible, since the range of integration is a compact interval, $[c-iT, c+iT]$, and the series $\sum_{n=1}^{\infty} f(n) n^{-s}$ converges absolutely and uniformly on that interval. Estimating $I(x/n,T)$ by Lemma 4.15, we obtain

$$\sum_{n=1}^{\infty} f(n) I(x/n,T) = \sum_{n \le x} f(n) + E(T) = M(f,x) + E(T),$$

where

$$|E(T)| \le \sum_{n=1}^{\infty} |f(n)| \frac{(x/n)^c}{T|\log(x/n)|} = \frac{x^c}{T} \sum_{n=1}^{\infty} \frac{|f(n)|}{n^\sigma |\log(x/n)|}.$$

Collecting these estimates yields (4.28), with $R(T) = -E(T)$ satisfying (4.29), as required. □

4.6 Exercises

4.1 Let $F(s) = \sum_{m,n=1}^{\infty} [m,n]^{-s}$. Determine the abscissa of convergence σ_c of $F(s)$ and express $F(s)$ in terms of the Riemann zeta function. (Hint: Express $F(s)$ as $\sum_{n=1}^{\infty} f(n) n^{-s}$, where $f(n) = \#\{(a,b) \in \mathbb{N}^2 : [a,b] = n\}$, and represent the latter as an Euler product.)

4.2 Express the Dirichlet series $\sum_{n=1}^{\infty} d(n)^2 n^{-s}$ in terms of the Riemann zeta function. Then use this relation to derive a convolution identity relating the functions $d^2(n)$ and $d_4(n)$ (where $d_k(n) \#\{(a_1, \dots, a_k) \in \mathbb{N}^k : a_1 \dots a_k = n\}$ is the generalized divisor function).

4.3 Evaluate the series $\sum_{(m_1,\dots,m_r)=1} m_1^{-s} \cdots m_r^{-s}$, where the summation is over all tuples $(m_1, \dots, m_r)$ of positive integers that are relatively prime, in terms of the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.

4.4 Let $f(n)$ be the unique positive real-valued arithmetic function that satisfies $\sum_{d|n} f(d) f(n/d) = 1$ for all n. Let $F(s) = \sum_{n=1}^{\infty} f(n) n^{-s}$ be the Dirichlet series of $F(s)$.

(i) Express $F(s)$ for $\sigma > 1$ in terms of the Riemann zeta function.

(ii) Find an explicit formula for $f(p^k)$, where p is prime and $k \geq 1$.

4.5 For each of the following functions $f(n)$ determine the abscissa of convergence σ_c and the abscissa of absolute convergence σ_a of the associated Dirichlet series.

(i) $f(n) = \omega(n)$ (where $\omega(n)$ is the number of distinct prime factors of n)

(ii) $f(n) = e^{2\pi i \alpha n}$, where $\alpha \in \mathbb{R} \setminus \mathbb{Z}$

(iii) $f(n) = n^{i\alpha n}$, where $\alpha \in \mathbb{Z}$

(iv) $f(n) = d_k(n) = \#\{(a_1, \dots, a_k) \in \mathbb{N}^k : a_1 \dots a_k = n\}$ (the generalized divisor function)

(v) $f(n)$ any periodic function with period q and $\sum_{n=1}^{q} f(n) = 0$.

4.6 Let σ_1 and σ_2 be real numbers with $\sigma_1 \leq \sigma_2 \leq \sigma_1 + 1$. Construct an arithmetic function whose Dirichlet series has abscissa of convergence $\sigma_c = \sigma_1$ and abscissa of absolute convergence $\sigma_a = \sigma_2$.

Chapter 5

Distribution of primes II: Proof of the Prime Number Theorem

5.1 Introduction

In this chapter we give an analytic proof of the Prime Number Theorem (PNT) with error term. In its original form, the PNT is the assertion that the number of primes, $\pi(x)$, satisfies

$$\pi(x) \sim \frac{x}{\log x} \quad (x \to \infty), \tag{5.1}$$

but, as we have shown in Chapter 3, the PNT is equivalent to any one of the relations

$$\pi(x) \sim \mathrm{Li}(x) \quad (x \to \infty), \tag{5.2}$$

$$\theta(x) \sim x \quad (x \to \infty), \tag{5.3}$$

$$\psi(x) \sim x \quad (x \to \infty), \tag{5.4}$$

where

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t},$$

and

$$\theta(x) = \sum_{p \le x} \log p, \quad \psi(x) = \sum_{n \le x} \Lambda(n).$$

We will prove the PNT in the form (5.4); more precisely, we will establish the following quantitative form (i.e., one with explicit error term) of this relation.

Theorem 5.1 (Prime number theorem with error term). *We have*

$$\psi(x) = x + O\left(x \exp\left(-c(\log x)^{\alpha}\right)\right) \quad (x \geq 2), \tag{5.5}$$

where c is a positive constant and $\alpha = 1/10$.

To gauge the quality of the error term, we note that, on the one hand,

$$x \exp\left(-c(\log x)^{\alpha}\right) \ll_k \frac{x}{(\log x)^k},$$

for any fixed constant k, while, on the other hand,

$$x \exp\left(-c(\log x)^{\alpha}\right) \gg_{\epsilon} x^{1-\epsilon}$$

for any fixed $\epsilon > 0$. (These estimates hold regardless of the specific value of α, as long as $0 < \alpha < 1$.)

The PNT was proved independently, and essentially simultaneously, by Jacques Hadamard and Charles de la Vallée Poussin at the end of the 19th century. The proofs of Hadamard and de la Vallée Poussin both used an analytic approach that had its roots in the work of Riemann some 50 years earlier.

After the PNT had been proved, the main focus shifted to establishing the PNT with as good an error term as possible. This problem is still wide open, and what we know is very far from what is being conjectured.

Tables 5.1 and 5.2 list the principal milestones in this development, and a more detailed description is given below. We will state all results in terms of the form (5.4) of the PNT, but the error terms in the relations (5.3) and (5.2) are essentially the same as for (5.4). (This is not true for the original form (5.1) of the PNT, since the right-hand side, $x/\log x$, is only a crude approximation to $\pi(x)$ that differs from the "true" size of $\pi(x)$ by a term of order $x/(\log x)^2$; the "correct" approximation for $\pi(x)$ is the logarithmic integral $\mathrm{Li}(x)$.)

Author(s)	**Bound for** $\psi(x) - x$	**Zerofree region** $(t^* = \max(\lvert t\rvert, 3))$	**Remarks**
Chebyshev (1851)	$cx \quad (x \geq x_0)$ $(c \approx 0.1)$		Chebyshev bound
Hadamard, de la Vallée Poussin (1896)	$o(x)$	$\sigma \geq 1$	Prime Number Theorem
De la Vallée Poussin (1899)	$O\left(xe^{-c\sqrt{\log x}}\right)$	$\sigma \geq 1 - \frac{c}{\log t^*}$	"Classical" error term
Littlewood (1922)	$O\left(xe^{-c\sqrt{\log x \log\log x}}\right)$	$\sigma \geq 1 - \frac{c \log\log t^*}{\log t^*}$	
Vinogradov–Korobov (1958)	$O\left(xe^{-c\frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}}\right)$	$\sigma \geq 1 - \frac{c(\log\log t^*)^{-1/3}}{(\log t^*)^{2/3}}$	Current record
	$O_\epsilon(x^{1/2+\epsilon})$, $\epsilon > 0$	$\sigma > 1/2$	Riemann Hypothesis

Table 5.1: The error term in the Prime Number Theorem, I

Author(s)	**Bound for** $\psi(x) - x$	**Remarks**
Erdös–Selberg (1949)	$o(x)$	First elementary proof
Bombieri, Wirsing (1964)	$O_A\left(x(\log x)^{-A}\right)$, any $A > 0$	First elementary proof with error term
Diamond–Steinig (1970)	$O_\alpha\left(xe^{-c(\log x)^\alpha}\right)$, any $\alpha < 1/7$	First elementary proof with exponential error term
Lavrik–Sobirov (1973)	$O_\alpha\left(xe^{-c(\log x)^\alpha}\right)$, any $\alpha < 1/6$	Current confirmed record for error term in elementary proof
	$O\left(xe^{-c\sqrt{\log x}}\right)$	Likely limit of elementary proofs

Table 5.2: The error term in the Prime Number Theorem, II: Elementary proofs

- **The classical error term.** (5.5) with $\alpha = 1/2$ was established by de la Vallée Poussin shortly after his proof of the PNT. This is a stronger result than the one we will prove here (with $\alpha = 1/10$), but to obtain this error term requires considerably more machinery from complex analysis than we have time to develop (such as the theory of entire functions of finite order, Hadamard products, and the theory of the Gamma function). The proof we will give goes back to E. Landau in the early part of the 20th century and has the advantage that it is a relatively "low tech" proof, requiring only a modest amount of

complex analysis.

- **Vinogradov's error term.** The only significant improvement over de la Vallée Poussin's error term is due to I.M. Vinogradov who, some 50 years ago, obtained (5.5) with $\alpha = 3/5 - \epsilon$, for any fixed $\epsilon > 0$ (with the constant c depending on ϵ). Aside from minor improvements, in which the "ϵ" was made precise, Vinogradov's result still represents the current record in the error term of the PNT.

- **Error terms obtained by elementary methods.** The first "elementary" proof of the PNT was given by Erdős and Selberg in the 1940s. (Here "elementary" is to be interpreted in a technical sense—an elementary proof is one that avoids the use of tools from complex analysis. "Elementary" in this context is not synonymous with "simple"; in fact, the restriction to "elementary" methods comes at the expense of rendering the proof much longer, more complicated, and less transparent.)

  Other elementary proofs have since been given, but the early elementary proofs did not give explicit error terms, and most elementary approaches to the PNT yield only very weak error terms. It wasn't until the 1970s when Diamond and Steinig obtained a form of the PNT by elementary methods that involved an exponential error term as in (5.5), though only with an exponent $\alpha = 1/7 - \epsilon$, which is smaller than the exponents $\alpha = 1/2$ and $\alpha = 3/5 - \epsilon$ in the results of de la Vallée Poussin and Vinogradov. The current record for the value of α in elementary error terms is only slightly larger, namely $\alpha = 1/6 - \epsilon$. This still falls far short of the "classical" exponent $\alpha = 1/2$. Obtaining the value $\alpha = 1/2$ by elementary means would be a major achievement, and there are reasons to believe that this value represents the limit of what can possibly be achieved by elementary methods.

- **The conjectured error term.** Assuming primes behave, in some appropriate sense, randomly, one might expect the error term in (5.5) to be of size about the square root of the main term. Thus, a natural conjecture would be that $\psi(x) = x + O_\epsilon(x^{1/2+\epsilon})$ for every fixed $\epsilon > 0$. As we will see, this conjecture is equivalent to the Riemann Hypothesis. Moreover, if true, it is best-possible; i.e., the exponent $1/2$ here cannot be replaced by a smaller exponent. An indication of how far we are from proving such a result is the fact, noted above, that the error term in (5.5) is greater than $x^{1-\epsilon}$, for any fixed $\epsilon > 0$.

The proof of Theorem 5.1 will take up most of the remainder of this chapter. We now give a brief outline of the argument.

Our starting point is Perron's formula in the form given by Theorem 4.16 for the function $f(n) = \Lambda(n)$. Since $\Lambda(n)$ has Dirichlet series $-\zeta'(s)/\zeta(s)$, this formula gives

$$\psi_1(f,x) = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^{s+1}}{s(s+1)}ds$$

for any $a > 1$, where

$$\psi_1(x) = \int_0^x \psi(y)dy.$$

We apply this formula initially with a value of a depending on x and slightly larger than 1 (namely, $a = 1 + 1/\log x$), and then move part of the line of integration to the left of the line $\sigma = 1$. Since $\zeta(s)$ has a pole at $s = 1$, the integrand has a pole at the same point, and passing over this pole we pick up a contribution $x^2/2$ from the residue of the integrand at $s = 1$. This contribution will be the main term in the estimate for $\psi_1(x)$. The error term will come from bounding the integral over the shifted path of integration. In order to obtain good estimates for the integrand, we need to, on the one hand, move as far to the left of $\sigma = 1$ as possible (so that $|x^s| = x^\sigma$ is small compared to x). On the other hand, since any zero of $\zeta(s)$ gives rise to a pole of $\zeta'(s)/\zeta(s)$, we can only move within a region that we know to be "zero-free", and in which we have good upper bounds for $|\zeta'(s)|$ and $1/|\zeta(s)|$. The region in which we can establish such bounds consists of points s bounded on the left by a curve of the form $\sigma = 1 - c(\log t)^{-9}$, which approaches the line $\sigma = 1$ asymptotically as $|t| \to \infty$. (Of course, if we knew RH, and had corresponding bounds for $|\zeta'(s)|$ and $1/|\zeta(s)|$, we could work in the larger region $\sigma > 1/2$.)

The establishment of a zero-free region and the proof of appropriate bounds for $1/\zeta$ and ζ' within this region will take up the bulk of the proof of Theorem 5.1. Once we have such bounds, the estimation of the complex integral is relatively easy, leading to a formula of the form $\psi_1(x) = x^2/2 + R(x)$ with an error term that is essentially (except for an extra factor x and a different value of the constant) that in (5.5) with $\alpha = 1/10$. An additional argument is then needed to translate this estimate into a similar one for $\psi(x)$.

Notation and conventions. Many of our estimates will involve constants. We will label these constants consecutively by $c_1, c_2, \ldots$ or $A_1, A_2, \ldots$.

Unless otherwise indicated, all constants are positive and absolute; i.e., they do not depending on any parameters and could, in principle, be given numerical values.

5.2 The Riemann zeta function, I: basic properties

Recall that for $\sigma > 1$ the Riemann zeta function is defined by

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

i.e., $\zeta(s)$ is the Dirichlet series for the arithmetic function 1. We begin by collecting some elementary properties of this function, most of which have been established earlier.

Theorem 5.2 (Basic properties of the zeta function).

(i) $\zeta(s)$ *is analytic in* $\sigma > 1$ *and there has the Dirichlet series representation* $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.

(ii) $\zeta(s)$ *has an analytic continuation to a function defined on the half-plane* $\sigma > 0$ *and analytic in this half-plane with the exception of a simple pole at* $s = 1$ *with residue* 1. *The analytic continuation is also denoted by* $\zeta(s)$ *and has the integral representation*

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \{x\} x^{-s-1} dx \quad (\sigma > 0). \tag{5.6}$$

(iii) $\zeta(s)$ *has an Euler product representation* $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ *in* $\sigma > 1$.

(iv) $\zeta(s)$ *has no zeros in the half-plane* $\sigma > 1$.

Proof. (i), (ii), and (iii) were established in Theorems 4.11 and 4.3; (iv) follows immediately from the Euler product representation, since the Euler product is absolutely convergent, and none of its factors is zero, in the half-plane $\sigma > 1$. (In general, an absolutely convergent infinite product can only be 0 if one of its factors is 0.) □

5.3 The Riemann zeta function, II: upper bounds

In this section we establish upper bounds for $\zeta(s)$ and $\zeta'(s)$ in a region that extends slightly to the left of the line $\sigma = 1$ into the critical strip. Recall that c_i and A_i denote positive constants.

Theorem 5.3 (Upper bounds for $\zeta(s)$ and $\zeta'(s)$).

(i) $$|\zeta(s)| \le 4\frac{|t|^{1-\sigma_0}}{1-\sigma_0} \quad (|t| \ge 2,\ 1/2 \le \sigma_0 < 1, \sigma \ge \sigma_0)$$

(ii) $$|\zeta(s)| \le A_1 \log|t| \quad (|t| \ge 2,\ \sigma \ge 1 - \frac{1}{4\log|t|})$$

(iii) $$|\zeta'(s)| \le A_2 \log^2|t| \quad (|t| \ge 2,\ \sigma \ge 1 - \frac{1}{12\log|t|})$$

To prove this result, we need three lemmas.

Lemma 5.4.

$$\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} - \frac{N^{1-s}}{1-s} - s\int_N^\infty \{u\}u^{-s-1}du \quad (N \in \mathbb{N}, \sigma > 0). \tag{5.7}$$

Proof. The argument is modification of that used to establish the integral representation (5.6). Given a positive integer N, we apply the Mellin transform representation (Theorem 4.10) to the Dirichlet series

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

This is the Dirichlet series corresponding to the function f defined by $f(n) = 1$ if $n > N$ and $f(n) = 0$ if $n \le N$, whose partial sums are given by $M(f,x) = [x] - N$ if $x \ge N$ and $M(f,x) = 0$ otherwise. Hence Theorem 4.10 gives, for $\sigma > 1$,

$$\begin{aligned} F(s) &= s\int_1^\infty M(f,x)x^{-s-1}dx = s\int_N^\infty ([x]-N)x^{-s-1}dx \\ &= s\int_N^\infty x^{-s}dx - sN\int_N^\infty x^{-s-1}dx - s\int_N^\infty \{x\}x^{-s-1}dx \\ &= -\frac{sN^{1-s}}{1-s} - N^{1-s} - s\int_N^\infty \{x\}x^{-s-1}dx \\ &= -\frac{N^{1-s}}{1-s} - s\int_N^\infty \{x\}x^{-s-1}dx. \end{aligned}$$

Since $\zeta(s) = F(s) + \sum_{n=1}^{N} n^{-s}$, this yields the desired relation (5.7) in the range $\sigma > 1$. Since both sides of this relation are analytic in $\sigma > 0$ except for a simple pole at $s = 1$ with residue 1 (note that the integral $\int_N^\infty \{x\}x^{-s-1}dx$ is uniformly convergent, and hence analytic, in any half-plane $\sigma \geq \epsilon$, $\epsilon > 0$), the relation remains valid in the larger half-plane $\sigma > 0$, as asserted. □

Lemma 5.5.

$$|\zeta(s)| \leq \sum_{n=1}^{N} \frac{1}{n^\sigma} + \frac{N^{1-\sigma}}{|t|} + \frac{|s|}{\sigma} N^{-\sigma} \quad (N \in \mathbb{N}, \sigma > 0, t \neq 0). \tag{5.8}$$

Proof. This follows immediately from the previous lemma, on noting that each of the three terms on the right-hand side of (5.7) is bounded, in absolute value, by the corresponding term on the right of (5.8). For the first two terms, this is obvious, and for the third term this follows from the inequality

$$\left| s \int_N^\infty \{u\} u^{-s-1} du \right| \leq |s| \int_N^\infty u^{-\sigma-1} du = \frac{|s| N^{-\sigma}}{|\sigma|}. \qquad \square$$

Lemma 5.6.

$$|\zeta(s)| \leq \frac{N^{1-\sigma_0}}{1-\sigma_0} + \frac{N^{1-\sigma_0}}{|t|} + \left(1 + \frac{|t|}{\sigma_0}\right) N^{-\sigma_0} \tag{5.9}$$
$$(N \in \mathbb{N}, 1/2 < \sigma_0 < 1, \sigma \geq \sigma_0 > 0, t \neq 0).$$

Proof. We show that the three terms on the right of (5.8) are bounded by the corresponding terms in (5.9). Using the hypotheses $\sigma \geq \sigma_0$ and $\sigma_0 < 1$ and the inequality $n^{-\sigma} \leq \int_{n-1}^{n} x^{-\sigma} dx$, we see that the first term on the right of (5.8) is at most

$$\sum_{n=1}^{N} \frac{1}{n^{\sigma_0}} \leq 1 + \int_1^N x^{-\sigma_0} dx = 1 + \frac{N^{1-\sigma_0} - 1}{1-\sigma_0} \leq \frac{N^{1-\sigma_0}}{1-\sigma_0},$$

as desired. Since $\sigma \geq \sigma_0$, the second term is trivially bounded by the corresponding term in (5.9). The same holds for the third term, in view of the bound $|s|/\sigma \leq (\sigma + |t|)/\sigma \leq 1 + |t|/\sigma_0$. Hence (5.9) follows from (5.8). □

Proof of Theorem 5.3. (i) We apply Lemma 5.6 with $N = [|t|]$, where $[x]$ denotes the greatest integer $\leq x$. Since, by hypothesis, $0 < \sigma_0 < 1$, we then have $N^{1-\sigma_0} \leq |t|^{1-\sigma_0}$, so the lemma gives

$$|\zeta(s)| \leq \frac{|t|^{1-\sigma_0}}{1-\sigma_0} \left(1 + \frac{1-\sigma_0}{|t|} + \frac{1-\sigma_0}{[|t|]} + \frac{(1-\sigma_0)|t|}{\sigma_0 [|t|]}\right). \tag{5.10}$$

Since $|t| \geq 2$ we have $(1-\sigma_0)/|t| \leq (1-\sigma_0)/[|t|] \leq 1/2$. Moreover, the inequalities $[|t|] \geq |t|/2$ and $1/2 \leq \sigma_0 < 1$ give $(1-\sigma_0)|t|/(\sigma_0[|t|]) \leq 2$. Hence the expression in parentheses on the right of (5.10) is at most $1 + 1/2 + 1/2 + 2 = 4$, and we obtain (i).

(ii) We set $\sigma_0 = 1 - 1/(4\log|t|)$. Since $|t| \geq 2$, we have $4\log|t| \geq \log 16 > 2$ and so $1/2 < \sigma_0 < 1$. Hence we can apply the estimate of part (i) with this value of σ_0 and obtain

$$|\zeta(s)| \leq 4\frac{|t|^{1-\sigma_0}}{1-\sigma_0} = \frac{4e^{1/4}}{1/(4\log|t|)} = 16e^{1/4}\log|t|,$$

which is the desired bound with constant $A_1 = 16e^{1/4}$.

(iii) First note that, for $\sigma \geq 2$, the Dirichlet series representation of $\zeta'(s)$ implies $|\zeta'(s)| \leq \sum_{n=1}^{\infty}(\log n)n^{-2}$, so the asserted bound holds trivially in the half-plane $\sigma \geq 2$. Also, the analyticity of $\zeta(s)$ in the region $\{s : \operatorname{Re} s > 0, s \neq 1\}$ implies that $|\zeta'(s)|$ is uniformly bounded in any compact rectangle contained in this region. Hence the asserted bound also holds in the range $2 \leq |t| \leq 3$, $\sigma \geq 1/2$. It therefore remains to show that this bound holds (with a suitable choice of the constant A_2) when $|t| \geq 3$.

Let now s be given in the range $\sigma \geq 1 - 1/(12\log|t|)$, $|t| \geq 3$, and set $\delta = 1/(12\log|t|)$. Note that, since $|t| \geq 3 \geq e$, we have $\sigma > 1 - 1/12$, and $0 < \delta < 1/12$, so the disk $\{s' \in \mathbb{C} : |s'-s| \leq \delta\}$ is contained in the region of analyticity of $\zeta(s)$. We can therefore express $\zeta'(s)$ by Cauchy's theorem to get

$$|\zeta'(s)| = \left|\frac{1}{2\pi i}\oint_{|s'-s|=\delta}\frac{\zeta(s')}{(s'-s)^2}ds\right| \leq \frac{1}{\delta}\max_{|s'-s|=\delta}|\zeta(s')|. \tag{5.11}$$

To estimate the right-hand side of (5.11), we will show that for $|s'-s| \leq \delta$, $\zeta(s')$ is bounded by a constant multiple of $\log|t|$. We will do so by verifying that all s' in this range fall into the range of validity of the upper bound for $\zeta(s')$ established in part (ii).

Let $s' = \sigma' + it'$ with $|s'-s| \leq \delta$ be given. By our hypotheses $|t| \geq 3$ and $\sigma \geq 1 - \delta$ we have

$$|t'| \geq |t| - \delta \geq |t| - 1/12 > 2$$

and

$$|t'| \leq |t| + \delta \leq |t| + 1/12 \leq \frac{13}{12}|t| \leq |t|^{3/2}.$$

Hence

$$\sigma' \geq \sigma - \delta \geq 1 - \frac{1}{6\log|t|} \geq 1 - \frac{1}{6\log|t'|^{2/3}} = 1 - \frac{1}{4\log|t'|}.$$

Thus the point s' lies in the range in which the bound (ii) is valid, and we therefore obtain

$$|\zeta(s')| \le A_1 \log|t'| \le (3/2)A_1 \log|t| \quad (|s'-s| = \delta).$$

Substituting this estimate in (5.11), we obtain

$$|\zeta'(s)| \le \frac{1}{\delta}(3/2)A_1 \log|t| = 18A_1(\log|t|)^2,$$

which is the desired estimate. □

5.4 The Riemann zeta function, III: lower bounds and zerofree region

The next result gives a zero-free region for $\zeta(s)$ to the left of the line $\sigma = 1$ of "width" a constant multiple of $(\log|t|)^{-9}$, and a lower bound for $\zeta(s)$ in this region. This result is the most important ingredient in the proof of the PNT; the value $\alpha = 1/10$ in the estimate (5.5) is directly related to the exponent 9 appearing in the definition of the region. De la Vallée Poussin's error term ($\alpha = 1/2$) is a consequence of a similar estimate, but in a wider region, with the exponent 1 instead of 9, and Vinogradov's value $\alpha = 3/5-\epsilon$ corresponds to an exponent $2/3+\epsilon$ in the zero-free region.

Theorem 5.7 (Zero-free region and upper bound for $1/\zeta(s)$).

(i) *$\zeta(s)$ has no zeros in the closed half-plane $\sigma \ge 1$.*

(ii) *There exist constants $c_1 > 0$ and $A_3 > 0$ such that $\zeta(s)$ has no zeros in the region*

$$\sigma > 1 - c_1, \quad |t| \le 2,$$

and in this region satisfies

$$\left|\frac{1}{\zeta(s)}\right| \le A_3.$$

(iii) *There exist constants $c_2 > 0$ and $A_4 > 0$ such that $\zeta(s)$ has no zeros in the region*

$$\sigma \ge 1 - \frac{c_2}{(\log|t|)^9}, \quad |t| \ge 2,$$

and in this region satisfies

$$\left|\frac{1}{\zeta(s)}\right| \le A_4(\log|t|)^7.$$

The key ingredient in the proof is the following elementary inequality.

Lemma 5.8 (3-4-1 Lemma). *For any real number θ we have*

$$3 + 4\cos\theta + \cos(2\theta) \geq 0.$$

Proof. We have

$$\begin{aligned} 0 \leq (1+\cos\theta)^2 &= 1 + 2\cos\theta + \cos^2\theta = 1 + 2\cos\theta + (1/2)(1+\cos(2\theta)) \\ &= (1/2)(3 + 4\cos\theta + \cos(2\theta)). \end{aligned}$$

□

We use this lemma to deduce a lower bound for a certain product of powers of the zeta function.

Lemma 5.9 (3-4-1 inequality for $\zeta(s)$). *We have*

$$\left|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)\right| \geq 1 \quad (\sigma > 1, t \in \mathbb{R}).$$

Proof. Note that for $\operatorname{Re} s > 1$,

$$\begin{aligned} \log|\zeta(s)| &= \log\left|\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}\right| = -\operatorname{Re}\sum_p \log\left(1 - \frac{1}{p^s}\right) \\ &= \operatorname{Re}\sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}} = \sum_p \sum_{m\geq 1} \frac{\cos(t\log p^m)}{mp^{m\sigma}}, \end{aligned}$$

where, as usual, $\sigma = \operatorname{Re} s$ and $t = \operatorname{Im} s$, and log denotes the principal branch of the logarithm. Applying this relation with σ, $\sigma + it$, and $\sigma + 2it$ in place of s, we obtain

$$\begin{aligned} &\log\left|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)\right| \\ &\quad = 3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+it)| + \log|\zeta(\sigma+2it)| \\ &\quad = \sum_p \sum_{m\geq 1} \frac{P(t\log p^m)}{mp^{m\sigma}}, \end{aligned}$$

where

$$P(\theta) = 3 + 4\cos\theta + \cos(2\theta)$$

is the trigonometric polynomial of Lemma 5.8. Since, by that lemma, $P(\theta)$ is nonnegative, all terms in the double series on the right are nonnegative, so the left-hand side is nonnegative as well. This implies the asserted inequality. □

Proof of Theorem 5.7. (i) By Theorem 5.2 $\zeta(s)$ has no zeros in the *open* half-plane $\sigma > 1$, so it remains to exclude the possibility of a zero on the line $\sigma = 1$. We argue by contradiction and suppose that $\zeta(1 + it_0) = 0$ for some real number t_0. Recall that, by Theorem 5.2, $\zeta(s)$ is analytic in the half-plane $\sigma > 0$, except for a simple pole at $s = 1$. Since ζ has a pole at $s = 1$, it cannot have a zero there, so we necessarily have $t_0 \neq 0$.

With a view towards applying Lemma 5.9, we consider the behavior of the three functions $\zeta(\sigma)$, $\zeta(\sigma + it_0)$, and $\zeta(\sigma + 2it_0)$ as $\sigma \to 1+$. Since $\zeta(s)$ has a pole at 1, $\zeta(\sigma)(\sigma - 1)$ is bounded as $\sigma \to 1+$. Furthermore, our assumption that $\zeta(1 + it_0) = 0$ implies, by the analyticity of $\zeta(s)$, that the expression

$$\frac{\zeta(\sigma + it_0)}{\sigma - 1} = \frac{\zeta(\sigma + it_0) - \zeta(1 + it_0)}{(\sigma + it_0) - (1 + it_0)}$$

also stays bounded as $\sigma \to 1+$. Finally, the analyticity of $\zeta(s)$ at $1 + 2it_0$ implies that $\zeta(\sigma+2it_0)$ converges to $\zeta(1+2it_0)$ as $\sigma \to 1+$, and, in particular, stays bounded. It follows that the function

$$\begin{aligned} &\left|\zeta(\sigma)^3\zeta(\sigma + it_0)^4\zeta(\sigma + 2it_0)\right| \\ &\qquad = (\sigma - 1)\ \left|\zeta(\sigma)(\sigma - 1)\right|^3 \cdot \left|\frac{\zeta(\sigma + it_0)}{\sigma - 1}\right|^4 \cdot \left|\zeta(\sigma + 2it_0)\right| \end{aligned}$$

is of order $O(\sigma-1)$ as $\sigma \to 1+$ and hence tends to 0. On the other hand, by Lemma 5.9, this function is bounded from below by 1, so we have arrived at a contradiction. Hence $\zeta(s)$ cannot have a zero on the line $\sigma = 1$.

(ii) First note that in the half-plane $\sigma \geq 2$ the asserted bound holds trivially: indeed, in this half-plane we have

$$|\zeta(s) \geq 1 - \sum_{n\geq 2} \frac{1}{n^2} = 1 - \left(\frac{\pi^2}{6} - 1\right) > 0$$

and thus

$$\left|\frac{1}{\zeta(s)}\right| \leq (2 - \pi^2/6)^{-1} \quad (\sigma \geq 2). \tag{5.12}$$

It remains therefore to show that $1/\zeta(s)$ is uniformly bounded in the compact rectangle

$$1 - c_1 \leq \sigma \leq 2, \quad |t| \leq 2, \tag{5.13}$$

with a sufficiently small positive constant c_1.

Now, by part (i), $\zeta(s)$ has no zeros in the closed half-plane $\sigma \geq 1$, so $1/\zeta(s)$ is analytic in this half-plane and therefore bounded in any compact region contained in this half-plane. In particular, $1/\zeta(s)$ is bounded in the rectangle $1 \leq \sigma \leq 2$, $|t| \leq 2$. By compactness, it follows that $1/\zeta(s)$ remains bounded in any sufficiently small neighborhood of this rectangle, and, in particular, in a rectangle of the form (5.13).

(iii) For $\sigma \geq 2$ the bound follows from (5.12), so we may restrict to the case when $\sigma \leq 2$. To obtain the desired bound for $1/\zeta(s)$ we will use again Lemma 5.9, in conjunction with the upper bounds for $\zeta(s)$ and $\zeta'(s)$ established in Theorem 5.3.

We fix a constant A that will be chosen later and let t be given with $|t| \geq 2$. We consider first the range

$$1 + A(\log|t|)^{-9} \leq \sigma \leq 2. \tag{5.14}$$

By Lemma 5.9 we have, for $\sigma > 1$,

$$|\zeta(\sigma + it)| \geq \frac{1}{\zeta(\sigma)^{3/4}} \cdot \frac{1}{|\zeta(\sigma + 2it)|^{1/4}}. \tag{5.15}$$

Since $\zeta(s)$ has a simple pole at $s = 1$, there exists an absolute constant c_3 such that

$$\zeta(\sigma) \leq c_3(\sigma - 1)^{-1}$$

for $1 < \sigma \leq 2$. Moreover, by Theorem 5.3(ii) we have

$$|\zeta(\sigma + 2it)| \leq A_1 \log|2t| \leq 2A_1 \log|t|,$$

where in the last step we have used the trivial inequality $\log(2|t|) \leq \log|t|^2 = 2\log|t|$, which is valid since $|t| \geq 2$. Inserting these bounds into (5.15) and now restricting to the narrower range (5.14), we obtain

$$\begin{aligned} |\zeta(\sigma + it)| &\geq c_3^{-3/4}(2A_1)^{-1/4}(\sigma - 1)^{3/4}(\log|t|)^{-1/4} \\ &\geq c_4 A^{3/4}(\log|t|)^{-7}, \end{aligned} \tag{5.16}$$

where $c_4 = c_3^{-3/4}(2A_1)^{-1/4}$ is an absolute constant.

This proves the asserted bound in the range (5.14), for any choice of the constant A. To complete the proof, we show that, if A is chosen sufficiently small, then a bound of the same type holds in the range

$$1 - A(\log|t|)^{-9} \leq \sigma \leq 1 + A(\log|t|)^{-9}. \tag{5.17}$$

Write

$$\sigma_1 = \sigma_1(A,t) = 1 - A(\log|t|)^{-9},$$
$$\sigma_2 = \sigma_2(A,t) = 1 + A(\log|t|)^{-9},$$

and note that for $\sigma_1 \le \sigma \le \sigma_2$ we have

$$\begin{aligned}|\zeta(\sigma+it)| &= \left|\zeta(\sigma_2+it) - \int_\sigma^{\sigma_2} \zeta'(u+it)du\right| \\ &\ge |\zeta(\sigma_2+it)| - (\sigma_2-\sigma_1)\max_{\sigma_1\le u\le\sigma_2}|\zeta'(u+it)|.\end{aligned}$$

Since $\sigma_2 + it$ falls in the range (5.14), the first term on the right can be estimated by (5.16). Moreover, by Theorem 5.3, we have $|\zeta'(s)| \le A_2(\log|t|)^2$ provided σ satisfies $\sigma \ge 1 - (12\log|t|)^{-1}$. If the constant A is sufficiently small, the range (5.17) is contained in the latter range, and so the above bound for $|\zeta'(s)|$ is valid in this range. We therefore obtain

$$\begin{aligned}|\zeta(\sigma+it)| &\ge c_4 A^{3/4}(\log|t|)^{-7} - 2A(\log|t|)^{-9}A_2(\log|t|)^2 \\ &= A^{3/4}(c_4 - 2A^{1/4}A_2)(\log|t|)^{-7}.\end{aligned}$$

Choosing now A to be a small enough absolute constant, the coefficient of $(\log|t|)^{-7}$ in this bound becomes positive, and we obtain $|\zeta(\sigma+it)| \ge c_5(\log|t|)^{-7}$, with an absolute positive constant c_5. This gives the estimate asserted in (iii) with $c_2 = A$ and $A_4 = 1/c_5$. □

For later use, we record an easy consequence of the estimates of Theorems 5.7 and 5.3.

Theorem 5.10 (Upper bounds for $\zeta'(s)/\zeta(s)$). *There exist absolute positive constants $0 < c_6 < 1/2$ and A_5 such that for all s in the range*

$$\sigma \ge 1 - \frac{c_6}{(\log|t|)^9}, \quad |t| \ge 2, \tag{5.18}$$

we have

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \le A_5(\log|t|)^9,$$

and for all s in the range

$$\sigma \ge 1 - c_6, \quad |t| \le 2, \quad s \ne 1, \tag{5.19}$$

we have

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \le A_5 \max\left(1, \frac{1}{|\sigma-1|}\right).$$

Proof. The first estimate follows by combining the bounds (iii) of Theorems 5.7 and 5.3, and noting that the ranges of validity of these latter estimates, namely $\sigma \geq 1 - c_2(\log|t|)^{-9}$ and $\sigma \geq 1 - 1/(12\log|t|)$, both contain the range (5.18), provided $|t| \geq 2$ and the constant c_6 is chosen sufficiently small.

The second estimate is a consequence of the analytic properties of $\zeta(s)$: Since $1/\zeta(s)$ is analytic in $\sigma \geq 1$ and $\zeta(s)$ is analytic in $\sigma > 0$ except for a simple pole at $s = 1$, the logarithmic derivative $\zeta'(s)/\zeta(s)$ is analytic in $\sigma \geq 1$, except for a simple pole at $s = 1$. Hence $(s-1)\zeta'(s)/\zeta(s)$ is analytic in $\sigma \geq 1$. By compactness the analyticity extends to a region of the form $\sigma \geq 1 - c_6$, $|t| \leq 2$, provided c_6 is a sufficiently small constant. It follows that this function is bounded in the compact region $1 - c_6 \leq \sigma \leq 2$, $|t| \leq 2$, so that we have $|\zeta'(s)/\zeta(s)| \ll 1/|s-1| \leq 1/|\sigma - 1|$ in this region. Since for $\sigma \geq 2$, $\zeta'(s)/\zeta(s) = -\sum_{n\geq 1} \Lambda(n) n^{-s}$ is trivially bounded by $\sum_{n\geq 1} \Lambda(n) n^{-2} < \infty$, we obtain the second estimate of the theorem, by adjusting the constant A_5 if necessary. □

5.5 Proof of the Prime Number Theorem

We are now ready to prove the prime number theorem in the form given by Theorem 5.1. We break the proof into several steps:

Application of Perron's formula. We let

$$\psi_1(x) = \int_0^x \psi(y)dy = \sum_{n\leq x} \Lambda(n)(x-n),$$

and apply Perron's formula in the version given by Theorem 4.16 with $f(n) = \Lambda(n)$. The corresponding Dirichlet series is $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s} = -\zeta'(s)/\zeta(s)$, which converges absolutely in $\sigma > 1$. Hence Perron's formula gives, for any $a > 1$ and any $x \geq 2$,

$$\psi_1(x) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)}\right) \frac{x^{s+1}}{s(s+1)} ds. \tag{5.20}$$

We fix $x \geq e$, let $e \leq T \leq x$ be a parameter that will be chosen later (as a function of x), and we set

$$a = 1 + \frac{1}{\log x}, \quad b = 1 - \frac{c_6}{(\log T)^9},$$

where c_6 is the constant of Theorem 5.10. Note that, since $c_6 < 1/2$ and $e \le T \le x$, we have

$$1 < a \le 2, \quad \frac{1}{2} < 1 - c_6 < b < 1. \tag{5.21}$$

Shifting the path of integration. The path of integration in (5.20) is a vertical line located within the half-plane $\sigma > 1$. We move the portion $|t| \le T$ of this path to the left of the line $\sigma = 1$, replacing it by a rectangular path joining the points $b \pm iT$ and $a \pm iT$. Thus, the new path of integration is of the form $L = \bigcup_{i=1}^{5} L_i$, with

$$\begin{aligned} L_1 &= (a - i\infty, a - iT], \\ L_2 &= [a - iT, b - iT], \\ L_3 &= [b - iT, b + iT], \\ L_4 &= [b + iT, a + iT], \\ L_5 &= [a + iT, a + i\infty). \end{aligned}$$

With this change of the path of integration we have

$$\psi_1(x) = M + \frac{1}{2\pi i} \sum_{j=1}^{5} I_j, \tag{5.22}$$

where M, the main term, is the contribution of the residues at singularities of the integrand in the region enclosed by the two paths and I_j denotes the integral over the path L_j.

The main term. The region enclosed by the original and the modified paths of integration is the rectangle with vertices

$$a \pm iT = 1 + \frac{1}{\log x} \pm iT, \quad b \pm iT = 1 - \frac{c_6}{(\log T)^9} \pm iT,$$

which falls within the zero-free region of $\zeta(s)$ given by Theorem 5.7. Thus, the integrand function has only one singularity in this region, namely that generated by the pole of $\zeta(s)$ at $s = 1$. Since this pole is simple, it follows that $-\zeta'(s)/\zeta(s)$ has a simple pole with residue 1 at $s = 1$, so the residue of the integrand function at this point is

$$\operatorname{Res}\left(-\frac{\zeta'(s)}{\zeta(s)} \cdot \frac{x^{s+1}}{s(s+1)}, s = 1\right) = \frac{1}{2}x^2.$$

Hence we have

$$M = \frac{1}{2}x^2. \tag{5.23}$$

This will be the main term of our estimate for $\psi_1(x)$. It remains to estimate the contribution of the integrals I_j. Here and in the remainder of this section, the constants implied in the $\ll$ notation are absolute and, in particular, independent of the value of T (which will only be chosen at the end of the proof).

Estimates of I_1 and I_5. These are the integrals along the vertical segments $(a - i\infty, a - iT]$ and $[a + iT, a + i\infty)$. On these segments we have $\sigma = a = 1 + 1/\log x$ and $|t| \geq T$. Thus,

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leq \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^a} = -\frac{\zeta'(a)}{\zeta(a)} \ll \frac{1}{a-1} = \log x,$$

and

$$\left|\frac{x^{s+1}}{s(s+1)}\right| = \frac{x^{a+1}}{|s||s+1|} \leq \frac{x^{a+1}}{t^2} = \frac{ex^2}{t^2}.$$

Hence we obtain the bounds

$$I_{1,5} \ll \int_T^{\infty} (\log x)\frac{x^2}{t^2}dt \ll \frac{x^2 \log x}{T}. \tag{5.24}$$

Estimates of I_2 and I_4. These are the integrals along the horizontal segments $[a - iT, b - iT]$ and $[b + iT, a + iT]$. By Theorem 5.10 we have on these paths

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \ll (\log T)^9$$

and

$$\left|\frac{x^{s+1}}{s(s+1)}\right| \leq \frac{x^{a+1}}{|s||s+1|} \ll \frac{x^2}{T^2}.$$

Hence

$$I_{2,4} \ll \int_a^b (\log T)^9 \frac{x^2}{T^2}d\sigma \ll \frac{x^2(\log T)^9}{T^2}. \tag{5.25}$$

Estimate of I_3. The remaining integral I_3 is the integral over the vertical segment $[b-iT, b+iT]$. By Theorem 5.10 and our choice $b = 1-c_6(\log T)^{-9}$, we have on this segment

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \ll \max\left((\log T)^9, (1-b)^{-1}\right) \ll (\log T)^9.$$

Since

$$\left|\frac{x^{s+1}}{s(s+1)}\right| = \frac{x^{b+1}}{|s||s+1|} \ll x^{b+1}\min(1, t^{-2}),$$

we obtain the bound

$$I_3 \ll \int_{-T}^{T} x^{b+1}(\log T)^9 \min(1, t^{-2})dt \ll x^{b+1}(\log T)^9. \tag{5.26}$$

Estimation of $\psi_1(x)$. Substituting the estimates (5.23)–(5.26) into (5.22), we obtain

$$\psi_1(x) = \frac{1}{2}x^2 + R(x, T)$$

with

$$\begin{aligned} R(x,T) &\ll \sum_{j=1}^{5} |I_j| \ll x^2\left(\frac{\log x}{T} + \frac{(\log T)^9}{T^2} + x^{b-1}(\log T)^9\right) \\ &\ll x^2\left(\frac{\log x}{T} + (\log T)^9 \exp\left(-c_6\frac{\log x}{(\log T)^9}\right)\right), \end{aligned}$$

where in the last step we used the assumption $T \le x$, which implies that the term $(\log T)^9 T^{-2}$ is of smaller order than the term $(\log x)T^{-1}$ and hence can be dropped. We now choose T as

$$T = \exp\left((\log x)^{1/10}\right).$$

Since $x \ge e$, this choice satisfies our initial requirement on T, namely $e \le T \le x$, and we obtain

$$\begin{aligned} R(x,T) &\ll x^2\left((\log x)\exp\left(-(\log x)^{1/10}\right) + (\log x)^{9/10}\exp\left(-c_6(\log x)^{1/10}\right)\right) \\ &\ll x^2\exp\left(-c_7(\log x)^{1/10}\right), \end{aligned}$$

with a suitable positive constant c_7. (In fact, any constant less than c_6 will do.) Hence we have

$$\psi_1(x) = \frac{1}{2}x^2 + O\left(x^2\exp\left(-c_7(\log x)^{1/10}\right)\right) \quad (x \ge e). \tag{5.27}$$

Transition to $\psi(x)$. As the final step in the proof of the prime number theorem, we need to derive an estimate for $\psi(x)$ from the above estimate for $\psi_1(x)$. Recall that the two functions are related by $\psi_1(x) = \int_0^\psi (y)dy$. While from an estimate for a function one can easily derive a corresponding estimate for the integral of this function, a similar derivation in the other direction is in general not possible. However, in this case we are able to do so by exploiting the fact that the function $\psi(x) = \sum_{n\le x} \Lambda(n)$ is nondecreasing.

We fix $x \ge 6$ and a number $0 < \delta < 1/2$ (to be chosen later as a suitable function of x) and note that, by the monotonicity of $\psi(x)$, we have

$$\psi_1(x) - \psi_1(x(1-\delta)) = \int_{x(1-\delta)}^{x} \psi(y)dy \le \delta x\psi(x).$$

Since $x \ge x(1-\delta) \ge x/2 \ge 3 \ge e$ by our assumptions $x \ge 6$ and $\delta < 1/2$, we can apply (5.27) to each of the two terms on the left and obtain

$$\begin{aligned} \delta x\psi(x) &\ge \frac{1}{2}x^2 + O(x^2\Delta) - \frac{1}{2}x^2(1-\delta)^2 + O(x^2\Delta') \\ &= \delta x + O(x^2(\delta^2 + \Delta + \Delta')), \end{aligned} \tag{5.28}$$

where

$$\Delta = \exp\left(-c_7(\log x)^{1/10}\right), \quad \Delta' = \exp\left(-c_7(\log x(1-\delta))^{1/10}\right)$$

denote the *relative* error terms in (5.27), applied to x and $x' = x(1-\delta)$, respectively. Since $x(1-\delta) \ge x/2 \ge \sqrt{x}$, we have

$$(\log x(1-\delta))^{1/10} \ge (\log\sqrt{x})^{1/10} \ge (1/2)(\log x)^{1/10},$$

and hence $\Delta' \le \Delta^{1/2} \le 1$. With this inequality, (5.28) yields

$$\psi(x) \le x + O(x(\delta + \sqrt{\Delta}/\delta)).$$

Defining now δ by

$$\delta = \min(1/2, \Delta^{1/4}),$$

we obtain

$$\psi(x) \ge x + O(x\delta) = x + O\left(\exp\left(-c_8(\log x)^{1/10}\right)\right) \tag{5.29}$$

with $c_8 = c_7/4$.

A similar, but slightly simpler, argument starting from the inequality

$$\psi_1(x(1+\delta)) - \psi_1(x) \ge \delta x\psi(x).$$

shows that (5.29) also holds with the inequality sign reversed. Thus we have obtained the estimate

$$\psi(x) = x + O\left(\exp\left(-c_8(\log x)^{1/10}\right)\right)$$

in the range $x \geq 6$. Since the same estimate holds trivially for $2 \leq x \leq 6$, this completes the proof of the prime number theorem in the form (5.5) stated at the beginning of this section.

5.6 Consequences and remarks

Consequences of the PNT with error term. Using partial summation one can easily derive from the prime number theorem with the error term established here estimates for other prime number sums with comparable error terms. We collect the most important of these estimates in the following theorem.

Theorem 5.11 (Consequences of the PNT). *For $x \geq 2$ we have*

(i) $$\theta(x) = x + O(xR(x)),$$

(ii) $$\pi(x) = \mathrm{Li}(x) + O(xR(x)),$$

(iii) $$\sum_{p \leq x} \frac{\log p}{p} = \log x + C_1 + O(R(x)),$$

(iv) $$\sum_{p \leq x} \frac{1}{p} = \log\log x + C_2 + O(R(x)),$$

(v) $$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1 + O(R(x))\right),$$

where $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$, the C_i are absolute constants, and $R(x)$ is an error term of the same type as in Theorem 5.1, except possibly for the value of the constant in the exponent, i.e., $R(x) = \exp(-c(\log x)^{1/10})$, with c a positive constant (not necessarily the same as in Theorem 5.1).

Proof. Estimate (i) follows from the $\psi(x)$ version of the PNT (i.e., Theorem 5.1) and the estimate

$$\begin{aligned} 0 \leq \psi(x) - \theta(x) &= \sum_{p \leq \sqrt{x}} \sum_{m=2}^{[(\log x)/(\log p)]} \log p \\ &\leq \sum_{p \leq \sqrt{x}} \log p \frac{\log x}{\log p} = \pi(\sqrt{x}) \log x \ll \sqrt{x} \ll xR(x). \end{aligned}$$

Estimates (ii)–(iv) can be deduced from (i) by a routine application of partial summation. We omit the details, and only note that the process typically results in a small loss in the constant in the exponent in $R(x)$. This is because one has to apply the PNT with values $y \le x$ in place of x and use estimates such as

$$\exp\{-c(\log y)^\alpha\} \le \exp\{-c2^{-\alpha}(\log x)^\alpha\} \quad (\sqrt{x} \le y \le x),$$

to bound error terms at y in terms of error terms at x.

The estimate (v) is a sharper version of Mertens' formula. Except for the value of the constant, this estimate follows from (iv), on noting that

$$\begin{aligned} -\sum_{p\le x} \log\left(1-\frac{1}{p}\right) - \sum_{p\le x}\frac{1}{p} &= \sum_{p\le x}\sum_{m=2}^{\infty}\frac{1}{mp^m} \\ &= \sum_{p}\sum_{m=2}^{\infty}\frac{1}{mp^m} + O\left(\sum_{p>x}\frac{1}{p^2}\right) = C + O\left(\frac{1}{x}\right), \end{aligned}$$

where C is a constant. That the constant on the right of (v) must be equal to $e^{-\gamma}$ follows from Mertens' formula (Theorem 3.4(iv)). □

It is important to note that an analogous sharpening does not hold for the original form $\pi(x) \sim x/\log x$ of the prime number theorem. In fact, combining the estimate (ii) of Theorem 5.11 with the asymptotic estimate for the logarithmic integral $\mathrm{Li}(x)$ given in Theorem 2.1 shows that $\pi(x)$ differs from $x/\log x$ by a term that is asymptotic to $x/\log^2 x$; more precisely, we have:

Corollary 5.12. *For any fixed positive integer k we have*

$$\pi(x) = \sum_{i=1}^{k}\frac{(i-1)!x}{(\log x)^i} + O_k\left(\frac{x}{(\log x)^{k+1}}\right) \quad (x \ge 2). \tag{5.30}$$

Estimates for the Moebius function. As we have seen in Chapter 3, the PNT in its asymptotic form $\psi(x) \sim x$ is equivalent to the asymptotic relation $M(\mu, x) = \sum_{n\le x}\mu(n) = o(x)$. It is reasonable to expect that a sharper form of the PNT would translate to a corresponding sharpening of the estimate for $M(\mu, x)$. This is indeed the case, and we have:

Theorem 5.13 (Moebius sum estimate). *For $x \ge 2$, we have*

$$\sum_{n\le x}\mu(n) \ll xR(x),$$

where $R(x)$ is defined as in Theorem 5.11.

This result can be proved by essentially repeating the proof of the last section, with the function $-\zeta'(s)/\zeta(s)$, the Dirichlet series for $\Lambda(n)$, replaced by $1/\zeta(s)$, the Dirichlet series for $\mu(n)$. The argument goes through without problems with this modification, and, indeed, is simpler in some respects. The main difference is that the function $1/\zeta(s)$, unlike $\zeta'(s)/\zeta(s)$, is analytic at $s = 1$, so no main term appears when estimating the corresponding Perron integral. We omit the details.

Zero-free regions of the zeta function and the error term in the prime number theorem. The proof of the prime number theorem given here depended crucially on the existence of a zero-free region for the zeta function and bounds for $\zeta(s)$ and $1/\zeta(s)$ within this region. It is easy to see that a larger zero-free region, along with corresponding zeta bounds in this region, would lead to a better error term. In turns out that, in some sense, the converse also holds: a smaller error term in the prime number theorem implies the existence of a larger zero-free region for the zeta function. Indeed, there are results that go in both directions and give equivalences between zero-free regions and error terms. We state, without proof, one simple result of this type and derive several consequences from it.

Theorem 5.14. *Let $0 < \theta < 1$. Then the following are equivalent:*

(i) The Riemann zeta function has no zeros in the half-plane $\sigma > \theta$.

(ii) The prime number theorem holds in the form

$$\psi(x) = x + O_\epsilon(x^{\theta+\epsilon}) \quad (x \geq 2)$$

for every fixed $\epsilon > 0$.

The Riemann Hypothesis is the statement that $\zeta(s)$ has no zeros in the half-plane $\sigma > 1/2$. Taking $\theta = 1/2$ in the above result, we therefore obtain the following equivalence to the Riemann Hypothesis.

Corollary 5.15. *The Riemann Hypothesis holds if and only if, for every $\epsilon > 0$,*

$$\psi(x) = x + O_\epsilon(x^{1/2+\epsilon}) \quad (x \geq 2).$$

Since it is known that the Riemann zeta function has infinitely many zeros on the line $\sigma = 1/2$, condition (i) in Theorem 5.14 cannot hold with $\theta < 1/2$. By the equivalence of (i) and (ii) it follows that the same is true for condition (ii); that is, we have:

Corollary 5.16. *Given any $\epsilon > 0$, the estimate*

$$\psi(x) = x + O(x^{1/2-\epsilon}) \quad (x \geq 2)$$

does not hold.

5.7 Further results

The results on the Riemann zeta function and the PNT that we have proved in this chapter represent only a small part of what is known in this connection. The Riemann zeta function is one of the most thoroughly studied "special" functions in mathematics, and entire books have been devoted to this function. Even though the most famous problem about this function, the Riemann Hypothesis, remains open, there exists a well-developed theory of the Riemann zeta function, and its connection to the PNT. In this section, we present, without proof, some of the major known results, as well as some of the main conjectures in this area.

The functional equation and analytic continuation. A fundamental property of the zeta function that is key to any deeper study of this function is the functional equation it satisfies:

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos(\pi s/2)\zeta(s). \tag{5.31}$$

Here $\Gamma(s)$ is the so-called Gamma function, a meromorphic function that interpolates factorials in the sense that $\Gamma(n) = (n-1)!$ when n is a positive integer. The Gamma function is analytic in the half-plane $\sigma > 0$ and there has integral representation $\Gamma(s) = \int_0^\infty e^{-x}x^{s-1}dx$.

The functional equation relates values of $\zeta(s)$ to values $\zeta(1-s)$. The vertical line $\sigma = 1/2$ acts as an axis of symmetry for this functional equation, in that if s lies in the half-plane to the right of this line, then $1-s$ falls in the half-plane to the left of this line.

By Theorem 4.11, $\zeta(s)$ has an analytic continuation to the half-plane $\sigma > 0$. Similar arguments could be used to obtain a continuation to $\sigma > -1$, and, by induction, to $\sigma > -n$, for any positive integer n. However, the functional equation (5.31) provides an analytic continuation to the entire complex plane in a single step. To see this, note that function on the right of the equation is analytic in $\sigma > 0$ (the pole of $\zeta(s)$ at $s = 1$ is cancelled out by a zero of $\cos(\pi s/2)$ at the same point). Hence the same must be true for the function on the left. But this means that $\zeta(1-s)$ has an analytic continuation to the half-plane $\sigma > 0$, or, equivalently, that $\zeta(s)$ has an analytic continuation to the half-plane $\sigma < 1$.

Analytic properties of the Riemann zeta function. The key analytic properties (both known and conjectured) of the Riemann zeta function (henceforth considered as a meromorphic function on the entire complex plane), are the following:

- **Poles:** $\zeta(s)$ has a single pole at $s = 1$, with residue 1, and is analytic elsewhere.
- **Trivial zeros:** $\zeta(s)$ has simple zeros at the points $s = -2n$, $n = 1, 2, \ldots$. These are called **trivial zeros**, as they are completely understood and have no bearing on the distribution of primes.
- **Nontrivial zeros:** All other zeros of $\zeta(s)$ are located in the **critical strip** $0 < \sigma < 1$. These zeros, commonly denoted by $\rho = \beta + i\gamma$, are closely related to the error term in the prime number theorem. They are symmetric with respect to both the **critical line** $\sigma = 1/2$, and the real axis. It is known that there are infinitely many nontrivial zeros, and good estimates are available for the number of such zeros up to a given height T, but their horizontal distribution within the strip $0 < \sigma < 1$ remains largely a mystery.
- **The Riemann Hypothesis:** The Riemann Hypothesis (RH) is the assertion that all nontrivial zeros lie exactly on the critical line $\sigma = 1/2$. This has been numerically verified for the first several billion nontrivial zeros (when ordered by increasing imaginary part). The closest theoretical approximation to the Riemann Hypothesis are zero-free regions of the form $\sigma > 1 - c(\log|t|)^{-\alpha}$, $|t| \geq 2$, for suitable exponents of α, the current record being Vinogradov's value of $\alpha = 2/3 + \epsilon$.
- **The Lindelöf Hypothesis:** Another well-known conjecture, though not quite as famous as RH, is the Lindelöf Hypothesis (LH), which states that the bound $\zeta(1/2 + it) \ll_\epsilon |t|^\epsilon$ holds for every fixed $\epsilon > 0$ and $|t| \geq 1$. It is easy to show that a bound of this type holds with exponent $1/2$; the current record for the exponent is approximately 0.16. It is known that LH follows from RH, though the proof of this implication is not easy.

Approximation of $\zeta(s)$ by partial sums. One of the more remarkable results on the zeta function is that, even though the series representation $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is only valid in $\sigma > 1$ (in fact, the series does not even

converge when $\sigma \le 1$), an *approximate* version of this representation remains valid to the left of the line $\sigma = 1$. Here is a typical result of this nature:

Theorem 5.17 (Approximate formula for $\zeta(s)$). *For $1/2 \le \sigma \le 2$ and $|t| \ge 2$ we have*

$$\zeta(s) = \sum_{n \le |t|} \frac{1}{n^s} + O\left(|t|^{-\sigma}\right).$$

This estimate can be deduced from the identity (5.7). In fact, applying this identity with $N = [|t| + 1]$ gives, under the conditions $1/2 \le \sigma \le 2$ and $|t| \ge 2$ and assuming (without loss of generality) that $|t|$ is not an integer,

$$\left|\zeta(s) - \sum_{n \le |t|} \frac{1}{n^s}\right| \ll \frac{[|t|+1]^{1-\sigma}}{|1-s|} + |s| \left|\int_{[|t|+1]}^{\infty} \{u\} u^{-s-1} du\right|,$$

The first term on the right is of the desired order $\ll |t|^{-\sigma}$. Using the trivial bound $|\{u\}u^{-s-1}| \le u^{-\sigma-1}$ in the integral would give for the second term the bound $|s||t|^{-\sigma}/\sigma \ll |t|^{1-\sigma}$. This is too weak, but a more careful estimate of the integral, using integration by parts and the estimate $\int_0^x \{u\} du = (1/2)x + O(1)$, shows that this term is also of order $\ll |t|^{-\sigma}$.

Explicit formulae. The proof of the prime number theorem given in the last section clearly showed the significance of the zeros of the zeta function in obtaining sharp versions of the prime number theorem. However, the effect of possible zeros in this proof was rather indirect: A zero of the zeta function leads to a singularity in the Dirichlet $-\zeta'(s)/\zeta(s)$, thus creating an obstacle to moving the path of integration further to the left. Since the quality of the error term depends largely on how far to the left one can move the path of integration, the presence of zeros with real part close to 1 puts limits on the error terms one can obtain with this argument.

There are results, known as **explicit formulae**, that make the connection between prime number estimates much more explicit. We state two of these formulae in the following theorems.

Theorem 5.18 (Explicit formula for $\psi_1(x)$). *We have, for $x \ge 1$,*

$$\psi_1(x) = \frac{x^2}{2} - \sum_{\rho} \frac{x^{\rho+1}}{\rho(\rho+1)} - \frac{\zeta'(0)}{\zeta(0)} x + \frac{\zeta'(-1)}{\zeta(-1)} - \sum_{n=1}^{\infty} \frac{x^{1-2n}}{(2n)(2n-1)}, \tag{5.32}$$

where ρ runs through all nontrivial zeros of $\zeta(s)$.

Theorem 5.19 (Explicit formula for $\psi(x)$). *We have, for $x \geq 2$ and any $2 \leq T \leq x$*

$$\psi(x) = x - \sum_{|\gamma| \leq T} \frac{x^\rho}{\rho} + O\left(\frac{x \log^2 x}{T}\right), \tag{5.33}$$

where $\rho = \beta + i\gamma$ runs through all nontrivial zeros of $\zeta(s)$ of height $|\gamma| \leq T$.

It is known that

$$\sum_\rho \frac{1}{|\rho|^2} < \infty, \tag{5.34}$$

while

$$\sum_\rho \frac{1}{|\rho|} = \infty, \tag{5.35}$$

so the series over ρ in the first explicit formula (for $\psi_1(x)$) converges absolutely, but not that in the second formula (for $\psi(x)$). Hence the need for working with a truncated version of this series in the latter case.

Explicit formulas can be used to translate results or conjectures on zeros of the zeta function to estimates for the prime counting functions $\psi(x)$ or $\psi_1(x)$. We illustrate this with two corollaries.

Corollary 5.20. *Assuming the Riemann Hypothesis, we have*

$$\psi_1(x) = \frac{x^2}{2} + O(x^{3/2}).$$

Proof. This follows immediately from (5.32) and (5.34) on noting that, under the Riemann Hypothesis, $|x^\rho| = x^{\operatorname{Re}\rho} = x^{1/2}$ for all nontrivial zeros ρ. □

The second corollary shows the effect of a single hypothetical zero that violates the Riemann Hypothesis. We first note that, due to the symmetry of the (nontrivial) zeros of the zeta function, zeros off the line $\sigma = 1/2$ come in quadruples: If $\rho = \beta + i\gamma$ is a zero of the zeta function with $1/2 < \beta \leq 1$, then so are $\beta - i\gamma$ and $1 - \beta \pm i\gamma$. Thus, it suffices consider zeros $\rho = \beta + i\gamma$ in the quadrant $\beta \geq 1/2$ and $\gamma \geq 0$.

Corollary 5.21. *Suppose that there exists exactly one zero $\rho = \beta + i\gamma$ of the zeta function with $1/2 < \beta \leq 1$, $\gamma \geq 0$, so that all zeros except $\beta \pm i\gamma$ and $1 - \beta \pm i\gamma$ have real part $1/2$. Then*

$$\psi_1(x) = \frac{x^2}{2} + cx^{1+\beta}\cos(\gamma \log x) + O(x^{3/2}),$$

where c is a constant depending on ρ.

Proof. As before, the contribution of the zeros satisfying the Riemann Hypothesis to the sum over ρ in (5.32) is of order $O(x^{3/2})$, and the same holds for the contribution of the zeros $1-\beta\pm i\gamma$ since $1-\beta < 1/2$. Thus, the only remaining terms in this sum are those corresponding to $\rho = \beta \pm i\gamma$. Their contribution is

$$\frac{x^{1+\beta+i\gamma}}{(\beta+i\gamma)(\beta+1+i\gamma)} + \frac{x^{1+\beta-i\gamma}}{(\beta-i\gamma)(\beta+1-i\gamma)},$$

and a simple calculation shows that this term is of the form $cx^{1+\beta}\cos(\gamma \log x)$. □

Thus, under the hypothesis of the corollary, $\psi_1(x)$ oscillates around the main term $x^2/2$ with an amplitude $cx^{1+\beta}$. In particular, a zero *on* the line $\sigma = 1$, i.e., with $\beta = 1$, would result in an oscillatory term of the form $cx^2\cos(\gamma \log x)$ in the estimate for $\psi_1(x)$, and thus contradict the PNT (though not Chebyshev's estimate, if the constant c is smaller than 1).

5.8 Exercises

5.1 Show that, if x is sufficiently large, then the interval $[2, x]$ contains more primes than the interval $(x, 2x]$.

5.2 Define $A(x)$ by $\pi(x) = x/(\log x - A(x))$. Show that $A(x) = 1 + O(1/\log x)$ for $x \geq 2$.

Remark. This result is of historical interest for the following reason: While the function $x/\log x$ is asymptotically equal to $\pi(x)$ by the prime number theorem, examination of numerical data suggests that the function $x/\log x$ is not a particularly good approximation to $\pi(x)$. Therefore, in the early (pre-PNT) history of prime number theory several other functions were suggested as suitable approximations to $\pi(x)$. In particular, Legendre proposed the function $x/(\log x - 1.08366)$ (The particular value of the constant 1.08366 was presumably obtained by some kind of regression analysis on the data.) On the other hand, Gauss suggested that $x/(\log x - 1)$ was a better match to $\pi(x)$. The problem settles this dispute, showing that Gauss had it right.

5.3 Let $f(n) = \Lambda(n) - 1$. Show that the Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converges for every s on the line $\sigma = 1$, and obtain an estimate for the rate of convergence, i.e., the difference $F(s) - \sum_{n \leq x} f(n)n^{-s}$, when $s = 1 + it$ for some fixed t. (The estimate may depend on t, but try to get as good an error term as possible assuming the PNT with exponential error term.)

5.4 Let $0 < \alpha < 1$ be fixed. Show that if

$$\theta(x) = x + O\left(x \exp\{-c(\log x)^{\alpha}\}\right) \quad (x \geq 2) \tag{1}$$

with some positive constant c, then

$$\pi(x) = \mathrm{Li}(x) + O\left(x \exp\{-c'(\log x)^{\alpha}\}\right) \quad (x \geq 2) \tag{2}$$

with some (other) positive constant c' (but the same value of the exponent α).

5.5 Let $M(x) = \sum_{n \leq x} \mu(n)$. Using complex integration as in the proof of the PNT, show that $M(x) = O(x \exp(-c(\log x)^{\alpha}))$, where $\alpha = 1/10$ and c is a positive constant.

5.6 Evaluate the integral

$$I_k(y) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s^k} ds,$$

where k is an integer ≥ 2, and y and c are positive real numbers. Then use this evaluation to derive a Perron type formula for the integral

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(s)\frac{x^s}{s^k} ds,$$

where $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ is a Dirichlet series, stating any conditions that are needed for this formula to be valid.

5.7 Let $F(s) = \sum_p p^{-s}$, where the summation runs over all primes. Show that $F(s) = \log\zeta(s) + G(s)$, where log denotes the principal branch of the logarithm, and $G(s)$ is analytic in the half-plane $\sigma > 1/2$. Deduce from this that the function $F(s)$ does *not* have a meromorphic continuation to the left of the line $\sigma = 1$.

Chapter 6

Primes in arithmetic progressions: Dirichlet's Theorem

6.1 Introduction

The main goal of this chapter is a proof of Dirichlet's theorem on the existence of primes in arithmetic progressions, a result that predates the prime number theorem by about 50 years, and which has had an equally profound impact on the development of analytic number theory. In its original version this result is the following.

Theorem 6.1 (Dirichlet's Theorem). *Given any positive integers q and a with $(a,q)=1$, there exist infinitely many primes congruent to a modulo q. In other words, each of the arithmetic progressions*

$$\{qn+a: \quad n=0,1,2,\dots\}, \quad q,a\in\mathbb{N},\ (a,q)=1, \tag{6.1}$$

contains infinitely many primes.

The above form of Dirichlet's theorem is the analog of Euclid's theorem on the infinitude of primes. Our proof will in fact give a stronger result, namely an analog of Mertens' estimate for primes in arithmetic progressions.

Theorem 6.2 (Dirichlet's Theorem, quantitative version). *Given any positive integers q and a with $(a,q)=1$, we have*

$$\sum_{\substack{p\le x\\ p\equiv a \bmod q}} \frac{1}{p} = \frac{1}{\phi(q)}\log\log x + O_q(1) \quad (x\ge 3). \tag{6.2}$$

This is still short of an analog of the PNT for primes in arithmetic progressions, which would be an asymptotic formula for the counting functions $\pi(x;q,a) = \#\{p \le x : p \equiv a \bmod q\}$. Such estimates are indeed known, but the proofs are rather technical, so we will not present them here. (Essentially, one has to combine Dirichlet's method for the proof of Theorem 6.1 with the analytic argument we used in the previous chapter to prove the PNT with error term.)

We note that the condition $(a,q) = 1$ in Dirichlet's theorem is necessary, for if $(a,q) = d > 1$, then any integer congruent to a modulo q is divisible by d, and hence there can be at most one prime in the residue class a modulo q. Thus, for given q, all but finitely many exceptional primes fall into one of the residue classes a mod q, with $(a,q) = 1$. By the definition of the Euler phi function, there are $\phi(q)$ such residue classes, and if we assume that the primes are distributed approximately equally among these residue classes, then a given class a modulo q, with $(a,q) = 1$, can be expected to contain a proportion $1/\phi(q)$ of all primes. Thus, the factor $1/\phi(q)$ in (6.2) is indeed the "correct" factor here.

A natural attempt to prove Dirichlet's theorem would be to try to mimick Euclid's proof of the infinitude of primes. In certain special cases, this does indeed succeed. For example, to show that there are infinitely many primes congruent to 3 modulo 4, assume there are only finitely many, say $p_1, \ldots, p_n$, and consider the number $N = p_1^2 \ldots p_n^2 + 2$. Since $p_i^2 \equiv 3^2 \equiv 1 \bmod 4$ for each i, N must be congruent to 3 modulo 4. Now note that, since N is odd, all its prime factors are odd, and so congruent to either 1 or 3 modulo 4. Moreover, N must be divisible by at least one prime congruent to 3 modulo 4, and hence by one of the primes p_i, since otherwise N would be a product of primes congruent to 1 modulo 4 and thus itself congruent to 1 modulo 4. But this is impossible, since then p_i would divide both N and $N-2$, and hence also $N - (N-2) = 2$.

Similar, though more complicated, elementary arguments can be given for some other special arithmetic progressions, but the general case of Dirichlet's theorem cannot be proved by these methods.

As was the case with the PNT, the breakthrough that led to a proof of Dirichlet's theorem in its full generality came with the introduction of analytic tools. The key tools that Dirichlet introduced and which are now named after him, are the *Dirichlet characters* and *Dirichlet L-functions*. Dirichlet characters are certain arithmetic functions that are used to extract terms belonging to a given arithmetic progression from a summation. Dirichlet L-functions are the Dirichlet series associated with these functions. The analytic properties of these Dirichlet series, and in particular the loca-

tion of their zeros, play a key role in the argument. In fact, the most difficult part of the proof consists in showing that the single point $s = 1$ is not a zero for a Dirichlet L-function.

6.2 Dirichlet characters

The basic definition of a character is as follows.

Definition (Dirichlet characters). Let q be a positive integer. A **Dirichlet character modulo** q is an arithmetic function χ with the following properties:

(i) χ is periodic modulo q, i.e., $\chi(n+q) = \chi(n)$ for all $n \in \mathbb{N}$.

(ii) χ is completely multiplicative, i.e., $\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in \mathbb{N}$ and $\chi(1) = 1$.

(iii) $\chi(n) \neq 0$ if and only if $(n, q) = 1$.

The arithmetic function $\chi_0 = \chi_{0,q}$ defined by $\chi_0(n) = 1$ if $(n, q) = 1$ and $\chi_0(n) = 0$ otherwise (i.e., the characteristic function of the integers coprime with q) is called the **principal character modulo** q.

Remarks. (i) That the principal character χ_0 is, in fact, a Dirichlet character can be seen as follows: condition (i) follows from the relation $(n, q) = (n + q, q)$, (ii) follows from the fact that $(nm, q) = 1$ holds if and only if $(n, q) = 1$ and $(m, q) = 1$, and (iii) holds by the definition of χ_0.

(ii) The notation χ_0 has become the standard notation for the principal character. In using this notation, one must keep in mind that χ_0 depends on q, even though this is not explicitly indicated in the notation.

(iii) In analogy with the residue class notation "$a \bmod q$", the notation "$\chi \bmod q$" is used to indicate that χ is a Dirichlet character modulo q. In a summation condition this notation denotes a sum over all characters χ modulo q.

Examples

(1) **Characters modulo 1.** The constant function 1 clearly satisfies the conditions of the above definition with $q = 1$. Moreover, since any character modulo 1 must be periodic modulo 1 and equal to 1 at 1, $\chi \equiv 1$ is the only Dirichlet character modulo 1. Note that this character is the principal character modulo 1.

(2) **Characters modulo 2.** The coprimality condition forces any character modulo 2 to be 0 at even integers, and the periodicity condition along with the requirement $\chi(1) = 1$ then forces $\chi(n)$ to be equal to 1 at odd integers. Thus, as in the case $q = 1$, there is only one character modulo 2, namely the principal character χ_0 defined by $\chi_0(n) = 1$ if $(n, 2) = 1$ and $\chi_0(n) = 0$ otherwise.

(3) **Characters modulo 3.** We have again the principal character $\chi_0(n)$, defined by $\chi_0(n) = 1$ if $(n, 3) = 1$ and $\chi_0(n) = 0$ otherwise. We will show that there is exactly one other character modulo 3.

Suppose χ is a character modulo 3. Then properties (i)–(iii) force $\chi(1) = 1$, $\chi(3) = 0$, and $\chi(2)^2 = \chi(4) = \chi(1) = 1$, so that $\chi(2) = \pm 1$. If $\chi(2) = 1$, then χ is equal to χ_0 since both functions are periodic modulo 3 and have the same values at $n = 1, 2, 3$. If $\chi(2) = -1$, then $\chi = \chi_1$, where χ_1 is the unique periodic function modulo 3 defined by $\chi_1(1) = 1$, $\chi_1(2) = -1$, and $\chi_1(3) = 0$. Clearly χ_1 satisfies properties (i) and (iii). The complete multiplicativity is not immediately obvious, but can be seen as follows:

Define a completely multiplicative function f by $f(3) = 0$, $f(p) = -1$ if $p \equiv -1 \bmod 3$ and $f(p) = 1$ if $p \equiv 1 \bmod 3$. Then $f(n) = \chi_1(n)$ for $n = 1, 2, 3$, so to show that $f = \chi_1$ (and hence that χ_1 is completely multiplicative) it suffices to show that f is periodic with period 3.

To this end, note first that if $n \equiv 0 \bmod 3$, then $f(n) = 0$. Otherwise $n \equiv \pm 1 \bmod 3$, and in this case n can be written as $n = \prod_{i \in I} p_i \prod_{j \in J} p_j$, where the products over $i \in I$ and $j \in J$ are finite (possibly empty), and the primes p_i, $i \in I$, and p_j, $j \in J$, are congruent to 1, resp. -1, modulo 3. We then have $f(n) = \prod_{i \in I} f(p_i) \prod_{j \in J} f(p_j) = (-1)^{|J|}$. On the other hand, since $p_i \equiv 1 \bmod 3$ and $p_j \equiv -1 \bmod 3$, we have $n \equiv (-1)^{|J|} \bmod 3$. Hence, if $|J|$ is even, then $n \equiv 1 \bmod 3$, and $f(n) = 1 = f(1)$, and if $|J|$ is odd, then $n \equiv 2 \bmod 3$, and $f(n) = -1 = f(2)$. Thus, f is periodic with period 3, as we wanted to show.

(4) **Legendre symbols as characters.** Let q be an odd prime, and let $\chi(n) = \left(\frac{n}{q}\right)$ denote the Legendre symbol modulo q, defined as 0 if $(n, q) > 1$, 1 if $(n, q) = 1$ and $n \equiv x^2 \bmod q$ has a solution (i.e., if n is a quadratic residue modulo q), and -1 otherwise (i.e., if n is a quadratic non-residue modulo q). Then $\chi(n)$ is a character modulo q. Indeed, properties (i) (periodicity) and (iii) (coprimality) follow immediately

from the definition of the Legendre symbol, while (ii) (complete multiplicativity) amounts to the identity $\left(\frac{nm}{q}\right) = \left(\frac{n}{q}\right)\left(\frac{m}{q}\right)$, which is a known result from elementary number theory.

A character χ derived from a Legendre symbol in this way takes on only the values $0, \pm 1$, and thus satisfies $\chi^2 = \chi_0$, but $\chi \neq \chi_0$. Characters with the latter two properties are called **quadratic characters**. Note that a character taking on only real values (such a character is called **real character**) necessarily has all its values in $\{0, \pm 1\}$, and so is either a principal character or a quadratic character.

We will later describe a systematic method for constructing all Dirichlet characters to a given modulus q.

We next deduce some simple consequences from the definition of a character.

Theorem 6.3 (Elementary properties of Dirichlet characters). *Let q be a positive integer.*

(i) The values of a Dirichlet character χ modulo q are either 0, or $\phi(q)$-th roots of unity; i.e., for all n, we have either $\chi(n) = 0$ or $\chi(n) = e^{2\pi i\nu/\phi(q)}$ for some $\nu \in \mathbb{N}$.

(ii) The characters modulo q form a group with respect to pointwise multiplication, defined by $(\chi_1\chi_2)(n) = \chi_1(n)\chi_2(n)$. The principal character χ_0 is the neutral element of this group, and the inverse of a character χ is given by the character $\overline{\chi}$ defined by $\overline{\chi}(n) = \overline{\chi(n)}$.

Proof. (i) If $\chi(n) \neq 0$, then $(n, q) = 1$. By Euler's generalization of Fermat's Little Theorem we then have $n^{\phi(q)} \equiv 1 \bmod q$. By the complete multiplicativity and periodicity of χ this implies $\chi(n)^{\phi(q)} = \chi\left(n^{\phi(q)}\right) = \chi(1) = 1$, as claimed.

(ii) The group properties follow immediately from the definition of a character. □

In order to derive further information on the properties of the group of characters, we need a well-known result from algebra, which we state here without proof.

Lemma 6.4 (Basis theorem for finite abelian groups). *Every finite abelian group is a direct product of cyclic groups. That is, for every finite abelian group G there exist elements $g_1, \dots, g_r \in G$ of respective orders $h_1, \dots, h_r$, such that every element $g \in G$ has a unique representation $g = \prod_{i=1}^{r} g_i^{\nu_i}$ with $0 \leq \nu_i < h_i$. Moreover, we have $\prod_{i=1}^{r} h_i = |G|$.*

We note that in case the group is trivial, i.e., consists of only the identity element, the result remains valid with an empty set as "basis" if the product representation $g = \prod_i g_i^{\nu_i}$ is interpreted as the empty product whose value is the identity element.

If we specialize the group G in Lemma 6.4 as the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$ of reduced residue classes modulo q, this result becomes:

Lemma 6.5 (Basis theorem for reduced residue classes modulo q). *Let q be a positive integer. Then there are positive integers $g_1, \ldots, g_r$, all relatively prime to q and of respective orders $h_1, \ldots, h_r$ modulo q (i.e., h_i is the least positive integer h such that $g_i^h \equiv 1 \bmod q$), with the following property: For every integer n with $(n, q) = 1$ there exist unique integers ν_i with $0 \le \nu_i < h_i$, such that $n \equiv \prod_{i=1}^r g_i^{\nu_i} \bmod q$. Moreover, we have $\prod_{i=1}^r h_i = \phi(q)$.*

Examples

(1) If $q = p^m$ is a prime power, with p an *odd* prime, then, by a result from elementary number theory, there exists a *primitive root* g modulo p^m, i.e., an element g that generates the multiplicative group modulo p^m. Thus, this group is itself cyclic, and the basis theorem therefore holds with $r = 1$ and $g_1 = g$. (For powers of 2 the situation is slightly more complicated, as the corresponding residue class groups are in general not cyclic.)

(2) Let $q = 15 = 3 \cdot 5$. We claim that $(g_1, g_2) = (2, 11)$ is a basis. It is easily checked that the orders of g_1 and g_2 are $h_1 = 4$ and $h_2 = 2$, respectively. Note also that $h_1 h_2 = 4 \cdot 2 = \phi(5)\phi(3) = \phi(15)$, in agreement with the theorem. A simple case-by-case check then shows that the congruence classes $2^{\nu_1} 11^{\nu_2}$ with $0 \le \nu_1 < 4$ and $0 \le \nu_2 < 2$ cover every residue class $a \bmod q$ with $(a, 15) = 1$ exactly once.

Our main application of the basis theorem is given in the following lemma.

Lemma 6.6 (Number of characters modulo q). *Let q be a positive integer. Then exist exactly $\phi(q)$ Dirichlet characters modulo q. Moreover, for any integer a with $(a, q) = 1$ and $a \not\equiv 1 \bmod q$ there exists a character χ with $\chi(a) \neq 1$.*

Proof. Let $g_1, \ldots, g_r$ and $h_1, \ldots, h_r$ be as in Lemma 6.5, and set $\omega_j = e^{2\pi i/h_j}$. Thus ω_j^ν, $\nu = 0, 1, \ldots, h_j$, are distinct h_j-th roots of unity. We claim that there is a one-to-one correspondence between the tuples

$$\nu = (\nu_1, \ldots, \nu_r), \quad 0 \le \nu_i < h_i, \tag{6.3}$$

and the characters modulo q.

To show this, suppose first that χ is a character modulo q. Then $\chi(n) = 0$ for $(n, q) > 1$, by the definition of a character. On the other hand, if $(n, q) = 1$, then, by the basis theorem, we have $n \equiv \prod_{i=1}^r g_i^{\mu_i} \bmod q$ with a unique tuple $\mu = (\mu_1, \ldots, \mu_r)$ with $0 \le \mu_i < h_i$. The periodicity and complete multiplicativity properties of a character then imply

$$\chi(n) = \chi\left(\prod_{i=1}^r g_i^{\mu_i}\right) = \prod_{i=1}^r \chi(g_i)^{\mu_i}, \text{ if } n \equiv \prod_{i=1}^r g_i^{\mu_i} \bmod q. \tag{6.4}$$

Thus, χ is uniquely specified by its values on the generators g_i. Moreover, since g_i has order h_i, we have

$$\chi(g_i)^{h_i} = \chi(g_i^{h_i}) = \chi(1) = 1,$$

so $\chi(g_i)$ must be an h_i-th root of unity; i.e., setting $\omega_j = \exp(2\pi i/h_j)$, we have

$$\chi(g_i) = \omega_i^{\nu_i} \quad (i = 1, \ldots, r), \tag{6.5}$$

for a unique tuple $\nu = (\nu_1, \ldots, \nu_r)$ of the form (6.3). Thus, every character χ modulo q gives rise to a unique tuple ν of the above form.

Conversely, given a tuple ν of this form, we define an arithmetic function $\chi = \chi_\nu$ by setting $\chi(n) = 0$ if $(n, q) > 1$ and defining $\chi(n)$ via (6.4) and (6.5) otherwise. By construction, this function $\chi(n)$ is periodic modulo q and satisfies $\chi(n) \ne 0$ if and only if $(n, q) = 1$, and one can verify that χ is also completely multiplicative. Thus χ is indeed a Dirichlet character modulo q.

We have thus shown that the characters modulo q are in one-to-one correspondence with tuples ν of the form (6.3). Since by Lemma 6.5 there are $h_1 \ldots h_r = \phi(q)$ such tuples, it follows that there are $\phi(q)$ characters modulo q. This establishes the first part of the Lemma 6.6.

For the proof of the second part, let an integer a be given with $(a, q) = 1$ and $a \not\equiv 1 \bmod q$. By the basis theorem, we have $a \equiv \prod_{i=1}^r g_i^{\mu_i} \bmod q$ with suitable exponents μ_i of the form (6.3). Since $a \not\equiv 1 \bmod q$, at least one

of the exponents μ_i must be non-zero. Without loss of generality, suppose that $\mu_1 \neq 0$. Define a character χ by setting $\chi(g_1) = \omega_1$ and $\chi(g_i) = 1$ for $i = 2, \ldots, r$. Then

$$\chi(a) = \chi(g_i^{\mu_1}) = \chi(g_i)^{\mu_1} = \exp\left\{\frac{2\pi i \mu_1}{h_1}\right\} \neq 1,$$

since $0 < \mu_1 < h_1$. □

Example: Characters modulo 15

We illustrate the construction of characters in the case of the modulus $q = 15$ considered in the example following Lemma 6.5. There we had obtained $g_1 = 2$ and $g_2 = 11$ as generators with respective orders $h_1 = 4$ and $h_2 = 2$. The corresponding roots of unity ω_i in (6.5) are $\omega_1 = e^{2\pi i/4} = i$ and $\omega_2 = e^{2\pi i/2} = -1$. Thus there are 8 characters χ_{ν_1,ν_2} modulo 15, corresponding to the pairs (ν_1, ν_2) with $0 \leq \nu_1 < 4$ and $0 \leq \nu_2 < 2$, and defined by setting $\chi_{\nu_1,\nu_2}(2) = i^{\nu_1}$ and $\chi_{\nu_1,\nu_2}(11) = (-1)^{\nu_2}$. The corresponding values of $\chi_{\nu_1,\nu_2}(a)$ at all integers $1 \leq a \leq q$ with $(a, 15) = 1$ can be calculated by representing a in the form $a \equiv 2^{\mu_1}11^{\mu_2} \bmod 15$ with $0 \leq \mu_1 < 4$, $0 \leq \mu_2 < 2$, and then using the formula $\chi(a) = \chi(2^{\mu_1}11^{\mu_2}) = \chi(2)^{\mu_1}\chi(11)^{\mu_2}$. The result is given in Table 6.1:

(μ_1, μ_2)	$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$
a	1	2	4	8	11	7	14	13
$\chi_{0,0}(a)$	1	1	1	1	1	1	1	1
$\chi_{0,1}(a)$	1	1	1	1	-1	-1	-1	-1
$\chi_{1,0}(a)$	1	i	-1	$-i$	1	i	-1	$-i$
$\chi_{1,1}(a)$	1	i	-1	$-i$	-1	$-i$	1	i
$\chi_{2,0}(a)$	1	-1	1	-1	1	-1	1	-1
$\chi_{2,1}(a)$	1	-1	1	-1	-1	1	-1	1
$\chi_{3,0}(a)$	1	$-i$	-1	i	1	$-i$	-1	i
$\chi_{3,1}(a)$	1	$-i$	-1	i	-1	i	1	$-i$

Table 6.1: Table of all Dirichlet characters modulo 15. The integers a in the second row are the values of $2^{\mu_1}11^{\mu_2}$ modulo 15.

The main result of this section is the following.

Theorem 6.7 (Orthogonality relations for Dirichlet characters). *Let q be a positive integer.*

(i) For any Dirichlet character χ modulo q we have

$$\sum_{a=1}^{q} \chi(a) = \begin{cases} \phi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$$

where χ_0 is the principal character modulo q.

(ii) For any integer $a \in \mathbb{N}$ we have

$$\sum_{\chi \bmod q} \chi(a) = \begin{cases} \phi(q) & \text{if } a \equiv 1 \bmod q, \\ 0 & \text{otherwise,} \end{cases}$$

where the summation runs over all Dirichlet characters modulo q.

(iii) For any Dirichlet characters χ_1, χ_2 modulo q we have

$$\sum_{a=1}^{q} \chi_1(a)\overline{\chi_2(a)} = \begin{cases} \phi(q) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise.} \end{cases}$$

(iv) For any integers $a_1, a_2 \in \mathbb{N}$ we have

$$\sum_{\chi \bmod q} \chi(a_1)\overline{\chi(a_2)} = \begin{cases} \phi(q) & \text{if } a_1 \equiv a_2 \bmod q \text{ and } (a_1, q) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where the summation runs over all Dirichlet characters modulo q.

Proof. (i) Let S denote the sum on the left. If $\chi = \chi_0$, then $\chi(a) = 1$ if $(a, q) = 1$, and $\chi(a) = 0$ otherwise, so $S = \phi(q)$.

Suppose now that $\chi \neq \chi_0$. Then there exists a number a_1 with $(a_1, q) = 1$ such that $\chi(a_1) \neq 1$. Note that, since $\chi(a) = 0$ if $(a, q) > 1$, the sum in (i) may be restricted to terms with $(a, q) = 1$, $1 \leq a \leq q$. Also, observe that, if a runs through these values, then so does $b = aa_1$, after reducing modulo q. Therefore,

$$\chi(a_1)S = \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \chi(a_1)\chi(a) = \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \chi(a_1 a) = \sum_{\substack{1 \leq b \leq q \\ (b,q)=1}} \chi(b) = S.$$

Since $\chi(a_1) \neq 1$, this implies $S = 0$. This completes the proof of part (i).

(ii) Let S denote the sum on the left. If $(a, q) > 1$, then all terms in this sum are 0, so $S = 0$. If $(a, q) = 1$ and $a \equiv 1 \bmod q$, then $\chi(a) = \chi(1) = 1$ for all characters χ modulo q, and since by Lemma 6.6 there exist exactly $\phi(q)$ such characters, we have $S = \phi(q)$ in this case.

Now suppose that $(a, q) = 1$ and $a \not\equiv 1 \bmod q$. By Lemma 6.6, there exists a character χ_1 modulo q with $\chi_1(a) \neq 1$. Since the characters modulo q form a group, if χ runs through all characters modulo q, then so does $\chi_1\chi$. We therefore have

$$\chi_1(a)S = \sum_{\chi \bmod q} \chi_1(a)\chi(a) = \sum_{\chi \bmod q} (\chi_1\chi)(a) = \sum_{\psi \bmod q} \psi(a) = S,$$

where in the last sum ψ runs through all characters modulo q. Since $\chi_1(a) \neq 1$, this implies $S = 0$, as desired.

(iii) This follows by applying (i) with the character $\chi = \chi_1\overline{\chi_2}$ and noting that $\chi = \chi_0$ if and only if $\chi_1 = \chi_2$.

(iv) We may assume that $(a_1, q) = (a_2, q) = 1$ since otherwise the sum is 0 and the result holds trivially. Therefore, a_2 has a multiplicative inverse $\overline{a_2}$ modulo q. We now apply (ii) with $a = a_1\overline{a_2}$. Noting that

$$\chi(a_2)\chi(a) = \chi(a_2a) = \chi(a_2a_1\overline{a_2}) = \chi(a_1)$$

and hence

$$\chi(a) = \frac{\chi(a_1)}{\chi(a_2)} = \chi(a_1)\overline{\chi(a_2)},$$

and that $a = a_1\overline{a_2} \equiv 1 \bmod q$ if and only $a_1 \equiv a_2 \bmod q$, we obtain the desired relation. □

The last part, (iv), is by far the most important, and it is key to Dirichlet's argument. This identity allows one to extract terms satisfying a given congruence from a sum. We will apply it with a_2 a fixed congruence class $a \bmod q$ and with a_1 running through primes p, in order to extract those primes that fall into the congruence class $a \bmod q$. This identity alone is often referred to as the orthogonality relation for Dirichlet characters.

We record one simple, but useful consequence of part (i) of the above theorem.

Corollary 6.8 (Summatory function of characters). *Let q be a positive integer and χ a character modulo q.*

(i) If χ is not the principal character χ_0 modulo q, then

$$\left|\sum_{n\le x}\chi(n)\right| \le \phi(q) \quad (x \ge 1).$$

(ii) If $\chi = \chi_0$, then

$$\left|\sum_{n\le x}\chi(n) - \frac{\phi(q)}{q}x\right| \le 2\phi(q) \quad (x \ge 1).$$

Proof. Since χ is periodic modulo q, we have, for any $x \ge 1$,

$$\sum_{n\le x}\chi(n) = [x/q]S + R,$$

where

$$S = \sum_{a=1}^{q}\chi(a), \quad |R| \le \sum_{a=1}^{q}|\chi(n)|.$$

Clearly, $|R| \le \phi(q)$, and by part (i) of Theorem 6.7 we have $S = 0$ if $\chi \ne \chi_0$, and $S = \phi(q)$ if $\chi = \chi_0$. The asserted bounds follow from these remarks. □

6.3 Dirichlet L-functions

Given a Dirichlet character χ, its Dirichlet series, i.e., the function

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}, \tag{6.6}$$

is called the *Dirichlet L-function*, or *Dirichlet L-series*, associated with the character χ.

The analytic behavior of Dirichlet L-functions plays a crucial role in the proof of Dirichlet's theorem. The following theorem collects the main analytic properties of L-functions that we will need for the proof of Dirichlet's theorem. The key property, upon which the success of the argument hinges, is the last one, which asserts that L-functions do not have a zero at the point $s = 1$. This is also the most difficult property to establish, and we therefore defer its proof to a later section.

Theorem 6.9 (Analytic properties of L-functions). *Let χ be a Dirichlet character modulo q, and let $L(s,\chi)$ denote the associated Dirichlet L-function, defined by* (6.6).

(i) If $\chi \neq \chi_0$, where χ_0 is the principal character modulo q, then $L(s,\chi)$ is analytic in the half-plane $\sigma > 0$.

(ii) If $\chi = \chi_0$, then $L(s,\chi)$ has a simple pole at $s = 1$ with residue $\phi(q)/q$, and is analytic at all other points in the half-plane $\sigma > 0$.

(iii) If $\chi \neq \chi_0$, then $L(1,\chi) \neq 0$.

Proof. As mentioned above, we defer the proof of (iii) to a later section, and only prove (i) and (ii) in this section.

By Corollary 6.8 the summatory function $M(\chi,x) = \sum_{n\le x}\chi(n)$ satisfies, for $x \ge 1$,

$$M(\chi,x) = \begin{cases} O_q(1) & \text{if } \chi \neq \chi_0, \\ \dfrac{\phi(q)}{q}x + O_q(1) & \text{if } \chi = \chi_0, \end{cases} \tag{6.7}$$

where the O-constant depends only on q. Parts (i) and (ii) then follow as special cases of Theorem 4.13.

Alternatively, one can obtain (i) and (ii) as follows:

If $\chi \neq \chi_0$, then using partial summation and the fact that the partial sums $\sum_{n\le x}\chi(n)$ are bounded in this case, one can easily see that the Dirichlet series (6.6) converges in the half-plane $\sigma > 0$. Since a Dirichlet series represents an analytic function in its half-plane of convergence, this shows that $L(s,\chi)$ is analytic in $\sigma > 0$ when $\chi \neq \chi_0$.

In the case $\chi = \chi_0$ one can argue similarly with the arithmetic function $f(n) = \chi_0(n) - \phi(q)/q$. By (6.7), the partial sums $\sum_{n\le x} f(n)$ are bounded, so the Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converges in the half-plane $\sigma > 0$ and is therefore analytic in this half-plane. On the other hand, writing $\chi_0(n) = f(n) + \phi(q)/q$, we see that $L(s,\chi_0) = F(s) + (\phi(q)/q)\zeta(s)$ for $\sigma > 1$. Since $F(s)$ is analytic in $\sigma > 0$ and $\zeta(s)$ is analytic in $\sigma > 0$ with the exception of a pole at $s = 1$ with residue 1, we conclude that $L(s,\chi_0)$ is analytic in $\sigma > 0$ with the exception of a pole at $s = 1$ with residue $\phi(q)/q$. □

6.4 Proof of Dirichlet's Theorem

In this section we prove Dirichlet's theorem in the quantitative version given in Theorem 6.2, modulo the nonvanishing result for $L(1,\chi)$ stated in part

(iii) of Theorem 6.9. The latter result which will be established in the next section.

We fix positive integers a and q with $(a,q) = 1$, and we define the functions

$$S_{a,q}(x) = \sum_{\substack{p \le x \\ p \equiv a \bmod q}} \frac{1}{p} \quad (x \ge 2),$$

$$F_{a,q}(s) = \sum_{\substack{p \\ p \equiv a \bmod q}} \frac{1}{p^s} \quad (\sigma > 1),$$

$$F_\chi(s) = \sum_p \frac{\chi(p)}{p^s} \quad (\sigma > 1).$$

Note that the Dirichlet series $F_{a,q}(s)$ and $F_\chi(s)$ are absolutely convergent in $\sigma > 1$. We will use these series only in this half-plane.

In the above notation, the estimate of Theorem 6.2 takes the form

$$S_{a,q}(x) = \frac{1}{\phi(q)} \log\log x + O_q(1) \quad (x \ge 3). \tag{6.8}$$

We will establish this estimate by a sequence of steps that reduce the estimation of $S_{a,q}(x)$ in turn to that of the functions $F_{a,q}(s)$, $F_\chi(s)$, $L(s,\chi)$, and ultimately to the non-vanishing of $L(1,\chi)$ for $\chi \ne \chi_0$.

To ease the notation, we will not explicitly indicate the dependence of error terms on q. *Through the remainder of the proof, all O-constants are allowed to depend on q.*

Reduction to $F_{a,q}(s)$. We first show that (6.8) follows from

$$F_{a,q}(\sigma) = \frac{1}{\phi(q)} \log \frac{1}{\sigma - 1} + O(1) \quad (\sigma > 1). \tag{6.9}$$

To see this, let $x \ge 3$ and take $\sigma = \sigma_x = 1 + 1/\log x$ in (6.9). Then the main term on the right of (6.9) is equal to the main term on the right of (6.8), and the error term in (6.9) is of the desired order $O(1)$. Thus, it suffices to show that the left-hand sides of these relations, i.e., $S_{a,q}(x)$ and $F_{a,q}(\sigma_x)$, differ by at most $O(1)$.

To show this, we write

$$S_{a,q}(x) - F_{a,q}(\sigma_x) = \sum_{\substack{p \le x \\ p \equiv a \bmod q}} \frac{1 - p^{1-\sigma_x}}{p} - \sum_{\substack{p > x \\ p \equiv a \bmod q}} \frac{1}{p^{\sigma_x}} \tag{6.10}$$
$$= \sum\nolimits_1 - \sum\nolimits_2,$$

say. Since

$$1 - p^{1-\sigma_x} = 1 - \exp\left\{-\frac{\log p}{\log x}\right\} \ll \frac{\log p}{\log x} \quad (p \le x),$$

we have

$$\sum\nolimits_1 \ll \frac{1}{\log x} \sum_{p \le x} \frac{\log p}{p} \ll 1,$$

by Mertens' estimate. Moreover, by partial summation and Chebyshev's estimate,

$$\begin{aligned} \sum\nolimits_2 &\le \sum_{p > x} \frac{1}{p^{\sigma_x}} = -\frac{\pi(x)}{x^{\sigma_x}} + \sigma_x \int_x^\infty \frac{\pi(u)}{u^{\sigma_x + 1}} du \\ &\ll \frac{1}{\log x} + \int_x^\infty \frac{1}{u^{\sigma_x} \log u} du \\ &\le \frac{1}{\log x} + \frac{x^{1-\sigma_x}}{(\sigma_x - 1)(\log x)} \ll 1. \end{aligned}$$

Thus, both terms on the right-hand side of (6.10) are of order $O(1)$, which is what we wanted to show.

Reduction to $F_\chi(s)$. Next, let $\sigma > 1$, so that the series $F_{a,q}(\sigma)$ and $F_\chi(\sigma)$ are absolutely convergent. By the orthogonality relation for characters (part (iv) of Theorem 6.7) we have

$$F_{a,q}(\sigma) = \sum_p \frac{1}{p^\sigma} \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \chi(p) \tag{6.11}$$
$$= \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^\sigma} = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} F_\chi(\sigma).$$

Reduction to Dirichlet L-functions. Since a Dirichlet character is completely multiplicative and of absolute value at most 1, the associated L-function $L(s,\chi)$ has an Euler product representation in the half-plane $\sigma > 1$, given by

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

Taking logarithms on both sides (using the principal branch of the logarithm) we get, for $\sigma > 1$,

$$\begin{aligned}\log L(s,\chi) &= -\sum_p \log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_p \sum_{m=1}^{\infty} \frac{\chi(p)^m}{mp^{ms}} = F_\chi(s) + R_\chi(s),\end{aligned}$$

where $F_\chi(s) = \sum_p \chi(p)p^{-s}$ is the function defined above and

$$|R_\chi(s)| \le \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^{m\sigma}} \le \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^m} \ll \sum_p \frac{1}{p^2} < \infty.$$

Thus, we have

$$F_\chi(s) = \log L(s,\chi) + O(1) \quad (\sigma > 1). \tag{6.12}$$

Contribution of the principal character. If $\chi = \chi_0$, then, by part (ii) of Theorem 6.9, $L(s,\chi_0)$ has a pole with residue $\phi(q)/q$ at $s = 1$ and is analytic elsewhere in the half-plane $\sigma > 0$. Thus, in $\sigma > 0$ we have

$$L(s,\chi_0) = \frac{\phi(q)}{q}\frac{1}{\sigma - 1} + H(s),$$

where $H(s) = H_{\chi_0}(s)$ is analytic in $\sigma > 0$. In particular, $H(s)$ is bounded in any compact set contained in this half-plane, and hence satisfies

$$|H(\sigma)| \le \frac{\phi(q)}{2q(\sigma - 1)} \quad (1 < \sigma \le \sigma_0) \tag{6.13}$$

with a suitable constant $\sigma_0 > 1$ (depending on q). Thus

$$\begin{aligned}\log L(\sigma,\chi_0) &= \log\left(\frac{\phi(q)/q}{\sigma - 1}\left(1 + H(\sigma)(\sigma - 1)\frac{q}{\phi(q)}\right)\right) \\ &= \log(\phi(q)/q) + \log\frac{1}{\sigma - 1} + \log\left(1 + H(\sigma)(\sigma - 1)\frac{q}{\phi(q)}\right) \\ &= \log\frac{1}{\sigma - 1} + O(1) \quad (1 < \sigma \le \sigma_0),\end{aligned}$$

where in the last step we used (6.13). By (6.12) it follows that

$$F_{\chi_0}(\sigma) = \log \frac{1}{\sigma - 1} + O(1), \tag{6.14}$$

initially only in the range $1 < \sigma \leq \sigma_0$, but in view of the trivial bound

$$|F_{\chi_0}(\sigma)| \leq \sum_p \frac{1}{p^\sigma} \leq \sum_p \frac{1}{p^{\sigma_0}} < \infty \quad (\sigma > \sigma_0),$$

in the full range $\sigma > 1$.

Contribution of the non-principal characters. If $\chi \neq \chi_0$, then, by part (i) of Theorem 6.9, $L(s, \chi)$ is analytic in $\sigma > 0$, and thus, in particular, continuous at $s = 1$. Moreover, by the last part of this result, $L(1, \chi) \neq 0$. Hence, $\log L(s, \chi)$ is analytic and thus continuous in a neighborhood of $s = 1$. In particular, there exists $\sigma_0 > 1$ such that $\log L(\sigma, \chi)$ is bounded in $1 < \sigma \leq \sigma_0$. In view of (6.12), this implies

$$F_\chi(\sigma) = O(1) \quad (\chi \neq \chi_0), \tag{6.15}$$

first for $1 < \sigma \leq \sigma_0$, and then, since as before $F_\chi(\sigma)$ is bounded in $\sigma \geq \sigma_0$, for the full range $\sigma > 1$.

Proof of Dirichlet's theorem. Substituting the estimates (6.14) and (6.15) into (6.11), we obtain

$$\begin{aligned} F_{a,q}(\sigma) &= \frac{1}{\phi(q)} \overline{\chi_0(a)} F_{\chi_0}(\sigma) + O(1) \\ &= \frac{1}{\phi(q)} \log \frac{1}{\sigma - 1} + O(1) \quad (1 < \sigma \leq 2), \end{aligned}$$

since $\chi_0(a) = 1$ by the definition of a principal character and the assumption $(a, q) = 1$. This proves (6.9), and hence the asserted estimate (6.8).

6.5 The non-vanishing of $L(1, \chi)$

We now prove part (iii) of Theorem 6.9, which we restate in the following theorem.

Theorem 6.10 (Non-vanishing of $L(1, \chi)$). *Let q be a positive integer and χ a non-principal character modulo q. Then $L(1, \chi) \neq 0$.*

The proof requires several auxiliary results, which we state as lemmas. The first lemma is reminiscent of the "3-4-1 inequality" of the previous chapter (Lemma 5.9), which was key to obtaining a zero-free region for the zeta function.

Lemma 6.11. *Let*

$$P(s) = P_q(s) = \prod_{\chi \bmod q} L(s, \chi).$$

Then, for $\sigma > 1$,

$$P(\sigma) \geq 1.$$

Proof. Expanding the Dirichlet series $L(s, \chi)$ into Euler products and taking logarithms, we obtain, for $\sigma > 1$,

$$\begin{aligned} \log P(\sigma) &= \sum_{\chi \bmod q} \log L(\sigma, \chi) = \sum_{\chi \bmod q} \sum_{p} \log \left(1 - \frac{\chi(p)}{p^\sigma}\right)^{-1} \\ &= \sum_{\chi \bmod q} \sum_{p} \sum_{m=1}^{\infty} \frac{\chi(p)^m}{p^{m\sigma}} \\ &= \sum_{p} \sum_{m=1}^{\infty} \frac{1}{p^{m\sigma}} \sum_{\chi \bmod q} \chi(p)^m. \end{aligned}$$

Since

$$\sum_{\chi \bmod q} \chi(p)^m = \sum_{\chi \bmod q} \chi(p^m) = \begin{cases} \phi(q) & \text{if } p^m \equiv 1 \bmod q, \\ 0 & \text{else,} \end{cases}$$

by the complete multiplicativity of χ and the orthogonality relation for characters (part (ii) of Theorem 6.7), the right-hand side above is a sum of nonnegative terms, and the assertion of the lemma follows. □

Proof of Theorem 6.10 for complex characters χ. We will use the above lemma to show that $L(1, \chi) \neq 0$ in the case χ is a *complex* character modulo q, i.e., if χ takes on non-real values. The argument is similar to that used in the proof of the non-vanishing of $\zeta(s)$ on the line $\sigma = 1$ (see Theorem 5.7).

We assume that $L(1, \chi_1) = 0$ for some complex character χ_1 modulo q. We shall derive a contradiction from this assumption.

We first note that, since χ_1 is a complex character, the characters χ_1 and $\overline{\chi_1}$ are distinct, and neither character is equal to the principal character

χ_0. Hence, χ_0, χ_1, and $\overline{\chi_1}$ each contribute a factor to the product $P(\sigma)$ in Lemma 6.11. Splitting off these three factors, we obtain, for $\sigma > 1$,

$$P(\sigma) = L(\sigma, \chi_0)L(\sigma, \chi_1)L(\sigma, \overline{\chi_1})Q(\sigma), \tag{6.16}$$

where

$$Q(\sigma) = \prod_{\substack{\chi \bmod q \\ \chi \neq \chi_0, \chi_1, \overline{\chi_1}}} L(\sigma, \chi).$$

We now examine the behavior of each term on the right of (6.16) as $\sigma \to 1+$. First, by part (ii) of Theorem 6.9, $L(s, \chi_0)$ has a simple pole at $s = 1$, so we have $L(\sigma, \chi_0) = O(1/(\sigma - 1))$ as $\sigma \to 1+$. Next, our assumption $L(1, \chi_1) = 0$ and the analyticity of $L(s, \chi_1)$ at $s = 1$ imply $L(\sigma, \chi_1) = O(\sigma - 1)$, and since

$$L(\sigma, \overline{\chi_1}) = \sum_{n=1}^{\infty} \frac{\overline{\chi_1(n)}}{n^\sigma} = \overline{\sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^\sigma}} = \overline{L(\sigma, \chi_1)},$$

we also have $L(\sigma, \overline{\chi_1}) = O(\sigma - 1)$. Finally, by part (i) of Theorem 6.9, $Q(\sigma)$ is bounded as $\sigma \to 1+$.

It follows from these estimates that $P(\sigma) = O(\sigma - 1)$ as $\sigma \to 1+$. This contradicts the bound $P(\sigma) \geq 1$ of Lemma 6.11. Thus $L(1, \chi_1)$ cannot be equal to 0, and the proof of Theorem 6.10 for complex characters is complete. □

The above argument breaks down in the case of a real character χ_1, since then $\overline{\chi_1} = \chi_1$ and in the above factorization of the product $P(\sigma)$ only one L-function corresponding to χ_1 would appear, so the assumption $L(1, \chi_1) = 0$ would only give an estimate $P(\sigma) = O(1)$, which is not enough to obtain a contradiction. To prove the non-vanishing of $L(1, \chi)$ for real characters, a completely different, and more complicated, argument is needed. We prove several auxiliary results first.

Lemma 6.12. *Let χ be a real character and let $f = 1 * \chi$. Then*

$$f(n) \begin{cases} \geq 1 & \text{if } n \text{ is a square,} \\ \geq 0 & \text{otherwise.} \end{cases}$$

Proof. Since χ is multiplicative, so is f. Since χ is a real character modulo q, we have $\chi(p) = \pm 1$ if $p \nmid q$, and $\chi(p) = 0$ if $p|q$. Thus, at prime powers

p^m we have

$$f(p^m) = 1 + \sum_{k=1}^{m} \chi(p)^k = \begin{cases} 1 & \text{if } p|q, \\ m+1 & \text{if } p \nmid q \text{ and } \chi(p) = 1, \\ 0 & \text{if } p \nmid q,\ \chi(p) = -1, \text{ and } m \text{ is odd}, \\ 1 & \text{if } p \nmid q,\ \chi(p) = -1, \text{ and } m \text{ is even} \end{cases}$$

It follows that

$$f(p^m) \begin{cases} \geq 1 & \text{if } m \text{ is even}, \\ \geq 0 & \text{if } m \text{ is odd}. \end{cases}$$

By the multiplicativity of f this yields the assertion of the lemma. □

Lemma 6.13. *We have*

$$\sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right) \quad (x \geq 1),$$

where A is a constant.

Proof. By Euler's summation formula, we have

$$\begin{aligned} \sum_{n \leq x} \frac{1}{\sqrt{n}} &= 1 - \{x\}x^{-1/2} + \int_1^x u^{-1/2} du + \int_1^x \{u\}(-1/2)u^{-3/2} du \\ &= 1 + O\left(\frac{1}{\sqrt{x}}\right) + 2(\sqrt{x} - 1) \\ &\quad - \frac{1}{2}\int_1^\infty \{u\}u^{-3/2} du + O\left(\int_x^\infty u^{-3/2} du\right) \\ &= 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right) \end{aligned}$$

with $A = -1 - (1/2)\int_1^\infty \{u\}u^{-3/2} du$. □

Lemma 6.14. *Let χ be a non-principal character modulo q and s a complex number in the half-plane $\sigma > 0$. Then*

$$\sum_{n \leq x} \frac{\chi(n)}{n^s} = L(s, \chi) + O_{q,s}(x^{-\sigma}) \quad (x \geq 1). \tag{6.17}$$

Proof. Let $M(u) = M(\chi, u) = \sum_{n \le u} \chi(n)$. By partial summation we have, for $y > x$,

$$\sum_{x < n \le y} \frac{\chi(n)}{n^s} = \frac{M(y)}{y^s} - \frac{M(x)}{x^s} + s \int_x^y M(u) u^{-s-1} du.$$

Since χ is non-principal, we have $M(u) = O_q(1)$ by Corollary 6.8, so the right-hand side above is bounded by

$$\ll_q x^{-\sigma} + |s| \int_x^y u^{-\sigma-1} du \ll_{q,s} x^{-\sigma}.$$

Letting $y \to \infty$, the left-hand side tends to $L(s, \chi) - \sum_{n \le x} \chi(n) n^{-s}$, and the result follows. □

Proof of Theorem 6.10 for real characters χ. We fix a real, non-principal character χ modulo q. Throughout the proof, we let constants in O-estimates depend on χ, and hence also on q, without explicitly indicating this dependence.

We let f be defined as in Lemma 6.12 and consider the sum

$$S(x) = \sum_{n \le x} \frac{f(n)}{\sqrt{n}}.$$

On the one hand, by Lemma 6.12 we have

$$S(x) \ge \sum_{m^2 \le x} \frac{f(m^2)}{\sqrt{m^2}} \ge \sum_{m \le \sqrt{x}} \frac{1}{m} \gg \log x \quad (x \ge 2). \tag{6.18}$$

On the other hand, we can estimate $S(x)$ by writing $f(n) = \sum_{d|n} \chi(d) = \sum_{dm=n} \chi(d)$ and splitting up the resulting double sum according to the Dirichlet hyperbola method:

$$S(x) = \sum_{\substack{d,m \le x \\ dm \le x}} \frac{\chi(d) \cdot 1}{\sqrt{d} \cdot \sqrt{m}} = \sum\nolimits_1 + \sum\nolimits_2 - \sum\nolimits_3, \tag{6.19}$$

where

$$\sum\nolimits_1 = \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{m \le x/d} \frac{1}{\sqrt{m}},$$

$$\sum\nolimits_2 = \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}} \sum_{d \le x/m} \frac{\chi(d)}{\sqrt{d}},$$

$$\sum\nolimits_3 = \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}}.$$

The last three sums can be estimated using Lemmas 6.13 and 6.14: We obtain

$$\begin{aligned}
\sum\nolimits_1 &= \sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \left(2\sqrt{x/d} + A + O\left(\frac{1}{\sqrt{x/d}}\right)\right) \\
&= 2\sqrt{x} \sum_{d\le\sqrt{x}} \frac{\chi(d)}{d} + A \sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} + O\left(\sum_{d\le\sqrt{x}} \frac{1}{\sqrt{x}} \right) \\
&= 2\sqrt{x}\left(L(1,\chi) + O\left(\frac{1}{\sqrt{x}}\right)\right) + A\left(L(1/2,\chi) + O\left(\frac{1}{x^{1/4}}\right)\right) + O(1) \\
&= 2\sqrt{x}L(1,\chi) + O(1), \\
\sum\nolimits_2 &= \sum_{m\le\sqrt{x}} \frac{1}{\sqrt{m}} \left(L(1/2,\chi) + O\left(\frac{1}{\sqrt{x/m}}\right)\right) \\
&= L(1/2,\chi)\left(2x^{1/4} + O(1)\right) + O\left(\sum_{m\le\sqrt{x}} \frac{1}{\sqrt{x}} \right) \\
&= L(1/2,\chi)2x^{1/4} + O(1), \\
\sum\nolimits_3 &= \left(L(1/2,\chi) + O\left(\frac{1}{x^{1/4}}\right)\right)\left(2x^{1/4} + O(1)\right) \\
&= L(1/2,\chi)2x^{1/4} + O(1).
\end{aligned}$$

Substituting these estimates into (6.19), we get

$$S(x) = 2\sqrt{x}L(1,\chi) + O(1).$$

If now $L(1,\chi) = 0$, then we would have $S(x) = O(1)$, contradicting (6.18). Hence $L(1,\chi) \neq 0$, and the proof of Theorem 6.10 is complete. □

6.6 Exercises

6.1 Show that if every arithmetic progression a mod q with $(a, q) = 1$ contains at least one prime, then every such progression contains *infinitely* many primes.

6.2 Show that if f is a periodic, completely multiplicative arithmetic function, then f is a Dirichlet character to some modulus q.

6.3 Let χ be a nonprincipal character mod q. Show that for all positive integers $a < b$ we have $\left|\sum_{n=a}^{b} \chi(n)\right| \leq (1/2)\phi(q)$.

6.4 Given a rational number a with $0 < a \leq 1$, define $\zeta(s, a) = \sum_{n=0}^{\infty}(n + a)^{-s}$. Show that any Dirichlet L-function can be expressed in terms of the functions $\zeta(s, a)$, and that, conversely, any such function $\zeta(s, a)$ with rational a can be expressed in terms of Dirichlet L-functions.

6.5 Let a and q be positive integers with $(a, q) = 1$. Express the Dirichlet series $\sum_{n \equiv a \bmod q} \mu(n)n^{-s}$ in the half-plane $\sigma > 1$ in terms of Dirichlet L-functions.

6.6 Given an arithmetic function f, and a real number α, let $f_\alpha(n) = f(n)e^{2\pi i\alpha n}$, and let $F_\alpha(s)$ be the corresponding Dirichlet series. For the case when α is rational and $f = \mu$ or $f = \Lambda$, express $F_\alpha(s)$ in terms of Dirichlet L-functions.

Appendix A

Some results from analysis

A.1 Evaluation of $\sum_{n=1}^{\infty} n^{-2}$

Theorem A.1. $\sum_{n=1}^{\infty} n^{-2} = \pi^2/6$.

Proof. We use the following result from Fourier analysis.

Theorem A.2 (Parseval's Formula). *Let f be a bounded and integrable function on $[0,1]$, and define the Fourier coefficients of f by $a_n = \int_0^1 f(x)e^{2\pi inx}dx$. Then*

$$\int_0^1 |f(x)|^2 = \sum_{n\in\mathbb{Z}} |a_n|^2.$$

This result can be found in most standard texts on Fourier series, and in many texts on Differential Equations (such as the text by Boyce/de Prima). It is usually stated in terms of Fourier sine and cosine coefficients, but the above form is simpler and easier to remember.

We apply Parseval's formula to the function $f(x) = x$ (which, when extended by periodicity to all of $\mathbb{R}$, becomes the fractional parts function $\{x\}$). We have $a_0 = \int_0^1 xdx = 1/2$ and, for $n \neq 0$,

$$a_n = \int_0^1 xe^{2\pi inx}dx = \frac{1}{2\pi in}e^{2\pi inx}x\Big|_0^1 - \frac{1}{2\pi in}\int_0^1 e^{2\pi inx}dx = \frac{1}{2\pi in}.$$

Hence, the right-hand side in Parseval's formula equals

$$\frac{1}{4} + \sum_{n\in\mathbb{Z},n\neq 0} \frac{1}{4\pi^2 n^2} = \frac{1}{4} + \frac{1}{2\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2},$$

whereas the left side is equal to $\int_0^1 x^2 dx = 1/3$. Setting the two expressions equal and solving for $\sum_{n=1}^{\infty} 1/n^2$ gives $\sum_{n=1}^{\infty} 1/n^2 = (1/3 - 1/4)2\pi^2 = \pi^2/6$ as claimed. □

Remark. There are several alternative proofs of this result. One consists of expanding the function defined by $f(x) = x^2$ on $[0, 1)$, and extended to a periodic function with period 1, into a Fourier series: $f(x) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n x}$, with $a_0 = \int_0^1 x^2 dx = 1/3$ and $a_n = -1/(2\pi^2 n^2)$ for $n \neq 0$. In this case, the Fourier series converges (absolutely) for all x. From the general theory of Fourier series its sum equals $f(x)$ at points where $f(x)$ is continuous, and $(1/2)(f(x-)+f(x+))$ at any point x at which f has a jump. We take $x = 0$. The Fourier series at this point equals $1/3+(1/\pi^2)\sum_{n=1}^{\infty} 1/n^2$. On the other hand, we have $(1/2)f(0-) + f(0+)) = (1/2)(1 + 0) = 1/2$. Setting the two expressions equal and solving for $\sum_{n=1}^{\infty} 1/n^2$, we again obtain the evaluation $\pi^2/6$ for this sum.

Yet another approach is to express $\sum_{n=1}^{\infty} 1/n^2 = \zeta(2)$ in terms of $\zeta(-1)$, using the functional equation of the zeta function, and evaluating $\zeta(-1)$. This is the method given at in Apostol's book (see Theorem 12.17).

A.2 Infinite products

Given a sequence $\{a_n\}_{n=1}^{\infty}$ of real or complex numbers, the infinite product

$$\prod_{n=1}^{\infty}(1 + a_n) \tag{A.1}$$

is said to be *convergent* to a (real or complex) limit P, if the partial products $P_n = \prod_{k=1}^{n}(1 + a_k)$ converge to P as $n \to \infty$. The product is said to be *absolutely convergent*, if the product $\prod_{n=1}^{\infty}(1 + |a_n|)$ converges.

It is easy to see that absolute convergence of an infinite product implies convergence. Indeed, defining P_n as above and setting $P_n^* = \prod_{k=1}^{n}(1 + |a_k|)$, we have, for $m > n$,

$$\begin{aligned} |P_m - P_n| &= \prod_{k=1}^{n} |1 + a_k| \left| \prod_{k=n+1}^{m} (1 + a_k) - 1 \right| \\ &\leq \prod_{k=1}^{n}(1 + |a_k|) \left(\prod_{k=n+1}^{m} (1 + |a_k|) - 1 \right) = P_m^* - P_n^*, \end{aligned}$$

so by Cauchy's criterion for the sequence $\{P_n^*\}$, the sequence $\{P_n\}$ satisfies Cauchy's criterion and hence converges.

The following lemma gives a criterion for the absolute convergence of an infinite product.

Lemma A.3. *The product* (A.1) *converges absolutely if and only if*

$$\sum_{n=1}^{\infty} |a_n| < \infty. \tag{A.2}$$

Proof. Let $P_n^* = \prod_{k=1}^{n}(1+|a_k|)$. By definition, the product (A.1) converges absolutely if and only if the sequence $\{P_n^*\}$ converges. Since this sequence is non-decreasing, it converges if and only if it is bounded. If (A.2) holds, then, in view of the inequality $1 + x \le e^x$ (valid for any real x), we have $P_n^* \le \exp\{\sum_{k=1}^{n} |a_k|\} \le e^S$, where S is the value of the infinite series in (A.2), so P_n^* is bounded. Conversely, if P_n^* is bounded, then using the inequality $P_n^* \ge 1 + \sum_{k=1}^{n} |a_k|$ (which follows by multiplying out the factors in P_n^* and discarding terms involving more than one factor $|a_k|$), we see that the series in (A.2) converges. □

The next lemma shows that the reciprocal of a convergent infinite product is the product of the reciprocals.

Lemma A.4. *If the product* (A.1) *converges to a value* $P \neq 0$*, then the product* $(*)$ $\prod_{n=1}^{\infty}(1+a_n)^{-1}$ *converges to* P^{-1}*. If, in addition, the product* (A.1) *is absolutely convergent, then so is the product* $(*)$*.*

Proof. We first note that if the product (A.1) converges to a non-zero limit P, then none of the factors $1+a_k$ can be zero (since if $1+a_k = 0$ then $P_n = 0$ for all $n \ge k$, and so $P = \lim_{n\to\infty} P_n = 0$). Hence, the partial products $P_n^* = \prod_{k=1}^{n}(1+a_k)^{-1}$ are well-defined, and equal to P_n^{-1}, where $P_n = \prod_{k=1}^{n}(1+a_k)$. The convergence of P_n to P therefore implies that of P_n^* to P^{-1}, proving the first assertion of the lemma. If the product (A.1) converges absolutely, then, by Lemma A.3, we have $\sum_{n=1}^{\infty} |a_n| < \infty$ and hence $|a_n| \le 1/2$ for sufficiently large n. Writing $(1 + a_n)^{-1} = 1 + a_n^*$, and using the inequality $|1 + x|^{-1} \le 1 + |x| \sum_{n=0}^{\infty} |x|^n \le 1 + 2|x|$ ($|x| \le 1/2$), we see that for such n, $|a_n^*| \le 2|a_n|$. Hence, the convergence of $\sum_{n=1}^{\infty} |a_n|$ implies that of $\sum_{n=1}^{\infty} |a_n^*|$, and applying the criterion the absolute convergence given in Lemma A.3 we conclude that the product $\prod_{n=1}^{\infty}(1 + a_n^*)$ converges absolutely. □