ELEMENTARY AND ANALYTIC NUMBER THEORY

W W L CHEN

(c) W W L Chen, 1981.

This work is available free, in the hope that it will be useful.

Any part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, with or without permission from the author.

Chapter 1

ARITHMETIC FUNCTIONS

1.1. Introduction

By an arithmetic function, we mean a function of the form $f: \mathbb{N} \to \mathbb{C}$. We say that an arithmetic function $f: \mathbb{N} \to \mathbb{C}$ is multiplicative if f(mn) = f(m)f(n) whenever $m, n \in \mathbb{N}$ and (m, n) = 1.

EXAMPLE. The function $U: \mathbb{N} \to \mathbb{C}$, defined by U(n) = 1 for every $n \in \mathbb{N}$, is an arithmetic function. Furthermore, it is multiplicative.

THEOREM 1.1. Suppose that the function $f: \mathbb{N} \to \mathbb{C}$ is multiplicative. Then the function $g: \mathbb{N} \to \mathbb{C}$, defined by

$$g(n) = \sum_{m|n} f(m)$$

for every $n \in \mathbb{N}$, is multiplicative.

Here the summation $\sum_{m|n}$ denotes a sum over all positive divisors m of n.

PROOF OF THEOREM 1.1. Suppose that $a, b \in \mathbb{N}$ and (a, b) = 1. If u is a positive divisor of a and v is a positive divisor of b, then clearly uv is a positive divisor of ab. On the other hand, it is well-known that every positive divisor m of ab can be expressed uniquely in the form m = uv, where u is a positive divisor of a and v is a positive divisor of a. It follows that

$$g(ab) = \sum_{m|ab} f(m) = \sum_{u|a} \sum_{v|b} f(uv) = \sum_{u|a} \sum_{v|b} f(u)f(v)$$
$$= \left(\sum_{u|a} f(u)\right) \left(\sum_{v|b} f(v)\right) = g(a)g(b).$$

[†] This chapter was first used in lectures given by the author at Imperial College, University of London, in 1981.

1.2. The Divisor Function

We define the divisor function $d: \mathbb{N} \to \mathbb{C}$ by writing

$$d(n) = \sum_{m|n} 1 \tag{1}$$

for every $n \in \mathbb{N}$. Here the sum is taken over all positive divisors m of n. In other words, the value d(n) denotes the number of positive divisors of the natural number n. On the other hand, we define the function $\sigma : \mathbb{N} \to \mathbb{C}$ by writing

$$\sigma(n) = \sum_{m|n} m \tag{2}$$

for every $n \in \mathbb{N}$. Clearly, the value $\sigma(n)$ denotes the sum of all the positive divisors of the natural number n.

THEOREM 1.2. Suppose that $n \in \mathbb{N}$ and that $n = p_1^{u_1} \dots p_r^{u_r}$ is the canonical decomposition of n. Then

$$d(n) = (1 + u_1) \dots (1 + u_r)$$
 and $\sigma(n) = \frac{p_1^{u_1+1} - 1}{p_1 - 1} \dots \frac{p_r^{u_r+1} - 1}{p_r - 1}$.

PROOF. Every positive divisor m of n is of the form $m=p_1^{v_1}\dots p_r^{v_r}$, where for every $j=1,\dots,r$, the integer v_j satisfies $0 \le v_j \le u_j$. It follows from (1) that d(n) is the number of choices for the r-tuple (v_1,\dots,v_r) . Hence

$$d(n) = \sum_{v_1=0}^{u_1} \dots \sum_{v_r=0}^{u_r} 1 = (1+u_1) \dots (1+u_r).$$

On the other hand, it follows from (2) that

$$\sigma(n) = \sum_{v_1=0}^{u_1} \dots \sum_{v_r=0}^{u_r} p_1^{v_1} \dots p_r^{v_r} = \left(\sum_{v_1=0}^{u_1} p_1^{v_1}\right) \dots \left(\sum_{v_r=0}^{u_r} p_r^{v_r}\right).$$

Note now that for every j = 1, ..., r, we have

$$\sum_{v_j=0}^{u_j} p_j^{v_j} = 1 + p_j + p_j^2 + \ldots + p_j^{u_j} = \frac{p_j^{u_j+1} - 1}{p_j - 1}.$$

The second result follows. ♣

The result below is a simple deduction from Theorem 1.2.

THEOREM 1.3. The arithmetic functions $d: \mathbb{N} \to \mathbb{C}$ and $\sigma: \mathbb{N} \to \mathbb{C}$ are both multiplicative.

Natural numbers $n \in \mathbb{N}$ where $\sigma(n) = 2n$ are of particular interest, and are known as perfect numbers. A perfect number is therefore a natural number which is equal to the sum of its own proper divisors; in other words, the sum of all its positive divisors other than itself.

EXAMPLE. It is easy to see that 6 = 1 + 2 + 3 and 28 = 1 + 2 + 4 + 7 + 14 are perfect numbers.

It is not known whether any odd perfect number exists. However, we can classify the even perfect numbers.

THEOREM 1.4. (Euclid-Euler) Suppose that $m \in \mathbb{N}$. If $2^m - 1$ is a prime, then the number $2^{m-1}(2^m - 1)$ is an even perfect number. Furthermore, there are no other even perfect numbers.

PROOF. Suppose that $n = 2^{m-1}(2^m - 1)$, and $2^m - 1$ is prime. Clearly

$$(2^{m-1}, 2^m - 1) = 1.$$

It follows from Theorems 1.2 and 1.3 that

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = \frac{2^m - 1}{2 - 1}2^m = 2n,$$

so that n is a perfect number, clearly even since $m \geq 2$.

Suppose now that $n \in \mathbb{N}$ is an even perfect number. Then we can write $n = 2^{m-1}u$, where $m \in \mathbb{N}$ and m > 1, and where $u \in \mathbb{N}$ is odd. By Theorem 1.2, we have

$$2^{m}u = \sigma(n) = \sigma(2^{m-1})\sigma(u) = (2^{m} - 1)\sigma(u),$$

so that

$$\sigma(u) = \frac{2^m u}{2^m - 1} = u + \frac{u}{2^m - 1}. (3)$$

Note that $\sigma(u)$ and u are integers and $\sigma(u) > u$. Hence $u/(2^m - 1) \in \mathbb{N}$ and is a divisor of u. Since m>1, we have $2^m-1>1$, and so $u/(2^m-1)\neq u$. It now follows from (3) that $\sigma(u)$ is equal to the sum of two of its positive divisors. But $\sigma(u)$ is equal to the sum of all its positive divisors. Hence u must have exactly two positive divisors, so that u is prime. Furthermore, we must have $u/(2^m-1)=1$, so that $u = 2^m - 1$.

We are interested in the behaviour of d(n) and $\sigma(n)$ as $n \to \infty$. If $n \in \mathbb{N}$ is a prime, then clearly d(n) = 2. Also, the magnitude of d(n) is sometimes greater than that of any power of $\log n$. More precisely, we have the following result.

THEOREM 1.5. For any fixed real number c > 0, the inequality $d(n) \ll (\log n)^c$ as $n \to \infty$ does not hold.

PROOF. The idea of the proof is to consider integers which are divisible by many different primes. Suppose that c>0 is given and fixed. Let $\ell\in\mathbb{N}\cup\{0\}$ satisfy $\ell\leq c<\ell+1$. For every $j=1,2,3,\ldots$ let p_j denote the j-th positive prime in increasing order of magnitude, and consider the integer

$$n = (p_1 \dots p_{\ell+1})^m.$$

Then in view of Theorem 1.2, we have

$$d(n) = (m+1)^{\ell+1} > \left(\frac{\log n}{\log(p_1 \dots p_{\ell+1})}\right)^{\ell+1} > K(c)(\log n)^{\ell+1} > K(c)(\log n)^c, \tag{4}$$

where the positive constant

$$K(c) = \left(\frac{1}{\log(p_1 \dots p_{\ell+1})}\right)^{\ell+1}$$

depends only on c. The result follows on noting that the inequality (4) holds for every $m \in \mathbb{N}$.

On the other hand, the order of magnitude of d(n) cannot be too large either.

THEOREM 1.6. For any fixed real number $\epsilon > 0$, we have $d(n) \ll_{\epsilon} n^{\epsilon}$ as $n \to \infty$.

PROOF. For every natural number n > 1, let $n = p_1^{u_1} \dots p_r^{u_r}$ be its canonical decomposition. It follows from Theorem 1.2 that

$$\frac{d(n)}{n^{\epsilon}} = \frac{(1+u_1)}{p_1^{\epsilon u_1}} \dots \frac{(1+u_r)}{p_r^{\epsilon u_r}}.$$

We may assume without loss of generality that $\epsilon < 1$. If $2 \le p_j < 2^{1/\epsilon}$, then

$$p_j^{\epsilon u_j} \ge 2^{\epsilon u_j} = e^{\epsilon u_j \log 2} > 1 + \epsilon u_j \log 2 > (1 + u_j) \epsilon \log 2,$$

so that

$$\frac{(1+u_j)}{p_i^{\epsilon u_j}} < \frac{1}{\epsilon \log 2}.$$

On the other hand, if $p_j \geq 2^{1/\epsilon}$, then $p_i^{\epsilon} \geq 2$, and so

$$\frac{(1+u_j)}{p_j^{\epsilon u_j}} \le \frac{1+u_j}{2^{u_j}} \le 1.$$

It follows that

$$\frac{d(n)}{n^{\epsilon}} < \prod_{p < 2^{1/\epsilon}} \frac{1}{\epsilon \log 2},$$

a positive constant depending only on ϵ .

We see from Theorems 1.5 and 1.6 and the fact that d(n) = 2 infinitely often that the magnitude of d(n) fluctuates a great deal as $n \to \infty$. It may then be more fruitful to average the function d(n) over a range of values n, and consider, for positive real numbers $X \in \mathbb{R}$, the value of the average

$$\frac{1}{X} \sum_{n \le X} d(n).$$

THEOREM 1.7. (Dirichlet) As $X \to \infty$, we have

$$\sum_{n < X} d(n) = X \log X + (2\gamma - 1)X + O(X^{1/2}).$$

Here γ is Euler's constant and is defined by

$$\gamma = \lim_{Y \to \infty} \left(\sum_{n \le Y} \frac{1}{n} - \log Y \right) = 0.5772156649\dots$$

REMARK. It is an open problem in mathematics to determine whether Euler's constant γ is rational or irrational.

The proof of Theorem 1.7 depends on the following intermediate result.

THEOREM 1.8. As $Y \to \infty$, we have

$$\sum_{n \le Y} \frac{1}{n} = \log Y + \gamma + O\left(\frac{1}{Y}\right).$$

PROOF. As $Y \to \infty$, we have

$$\begin{split} \sum_{n \le Y} \frac{1}{n} &= \sum_{n \le Y} \left(\frac{1}{Y} + \int_{n}^{Y} \frac{1}{u^{2}} \, \mathrm{d}u \right) = \frac{[Y]}{Y} + \sum_{n \le Y} \int_{n}^{Y} \frac{1}{u^{2}} \, \mathrm{d}u \\ &= \frac{[Y]}{Y} + \int_{1}^{Y} \frac{1}{u^{2}} \left(\sum_{n \le u} 1 \right) \, \mathrm{d}u = \frac{[Y]}{Y} + \int_{1}^{Y} \frac{[u]}{u^{2}} \, \mathrm{d}u \\ &= \frac{[Y]}{Y} + \int_{1}^{Y} \frac{1}{u} \, \mathrm{d}u - \int_{1}^{Y} \frac{u - [u]}{u^{2}} \, \mathrm{d}u \\ &= \log Y + 1 + O\left(\frac{1}{Y}\right) - \int_{1}^{\infty} \frac{u - [u]}{u^{2}} \, \mathrm{d}u + \int_{Y}^{\infty} \frac{u - [u]}{u^{2}} \, \mathrm{d}u \\ &= \log Y + \left(1 - \int_{1}^{\infty} \frac{u - [u]}{u^{2}} \, \mathrm{d}u \right) + O\left(\frac{1}{Y}\right). \end{split}$$

It is a simple exercise to show that

$$1 - \int_{1}^{\infty} \frac{u - [u]}{u^2} \, \mathrm{d}u = \gamma.$$

PROOF OF THEOREM 1.7. As $X \to \infty$, we have

$$\begin{split} \sum_{n \leq X} d(n) &= \sum_{\substack{x,y \\ xy \leq X}} 1 = \sum_{\substack{x \leq X^{1/2} \\ y \leq \frac{X}{x}}} 1 + \sum_{\substack{y \leq X^{1/2} \\ x \leq \frac{X}{y}}} \sum_{1 < x \leq \frac{X}{y}} 1 - \sum_{\substack{x \leq X^{1/2} \\ x \leq \frac{X}{y}}} 1 \\ &= 2 \sum_{\substack{x \leq X^{1/2} \\ x \leq \frac{X}{y}}} \left[\frac{X}{x} \right] - \left[X^{1/2} \right]^2 = 2 \sum_{\substack{x \leq X^{1/2} \\ x \leq X^{1/2}}} \frac{X}{x} + O(X^{1/2}) - (X^{1/2} + O(1))^2 \\ &= 2X \left(\log X^{1/2} + \gamma + O\left(\frac{1}{X^{1/2}}\right) \right) + O(X^{1/2}) - X \\ &= X \log X + (2\gamma - 1)X + O(X^{1/2}). \end{split}$$

We next turn our attention to the study of the behaviour of $\sigma(n)$ as $n \to \infty$. Every number $n \in \mathbb{N}$ has divisors 1 and n, so we must have $\sigma(1) = 1$ and $\sigma(n) > n$ if n > 1. On the other hand, it follows from Theorem 1.6 that for any fixed real number $\epsilon > 0$, we have

$$\sigma(n) \le nd(n) \ll_{\epsilon} n^{1+\epsilon}$$

as $n \to \infty$.

In fact, it is rather easy to prove a slightly stronger result.

THEOREM 1.9. We have $\sigma(n) \ll n \log n$ as $n \to \infty$.

PROOF. As $n \to \infty$, we have

$$\sigma(n) = \sum_{m|n} \frac{n}{m} \le n \sum_{m \le n} \frac{1}{m} \ll n \log n.$$

As in the case of d(n), the magnitude of $\sigma(n)$ fluctuates a great deal as $n \to \infty$. As before, we shall average the function $\sigma(n)$ over a range of values n, and consider some average version of the function. Corresponding to Theorem 1.7, we have the following result.

THEOREM 1.10. As $X \to \infty$, we have

$$\sum_{n \le X} \sigma(n) = \frac{\pi^2}{12} X^2 + O(X \log X).$$

PROOF. As $X \to \infty$, we have

$$\sum_{n \le X} \sigma(n) = \sum_{n \le X} \sum_{m|n} \frac{n}{m} = \sum_{m \le X} \sum_{n \le X} \frac{n}{m} = \sum_{m \le X} \sum_{r \le X/m} r$$

$$= \sum_{m \le X} \frac{1}{2} \left[\frac{X}{m} \right] \left(1 + \left[\frac{X}{m} \right] \right) = \frac{1}{2} \sum_{m \le X} \left(\frac{X}{m} + O(1) \right)^2$$

$$= \frac{X^2}{2} \sum_{m \le X} \frac{1}{m^2} + O\left(X \sum_{m \le X} \frac{1}{m} \right) + O\left(\sum_{m \le X} 1 \right)$$

$$= \frac{X^2}{2} \sum_{m = 1}^{\infty} \frac{1}{m^2} + O\left(X^2 \sum_{m > X} \frac{1}{m^2} \right) + O(X \log X)$$

$$= \frac{\pi^2}{12} X^2 + O(X \log X).$$

1.3. The Möbius Function

We define the Möbius function $\mu: \mathbb{N} \to \mathbb{C}$ by writing

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 \dots p_r, \text{ a product of distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

REMARKS. (i) A natural number which is not divisible by the square of any prime is called a squarefree number. Note that 1 is both a square and a squarefree number. Furthermore, a number $n \in \mathbb{N}$ is squarefree if and only if $\mu(n) = \pm 1$.

(ii) The motivation for the definition of the Möbius function lies rather deep. To understand the definition, one needs to study the Riemann zeta function, an important function in the study of the distribution of primes. For a more detailed discussion, see Chapters 4, 5 and 6. At this point, it suffices to remark that the Möbius function is defined so that if we formally multiply the two series

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{and} \quad \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

then the product is identically equal to 1. Heuristically, note that

$$\left(\sum_{k=1}^{\infty} \frac{1}{k^s}\right) \left(\sum_{m=1}^{\infty} \frac{\mu(m)}{m^s}\right) = \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \sum_{m=1}^{\infty} \frac{\mu(m)}{n^s} = \sum_{n=1}^{\infty} \left(\sum_{m|n} \mu(m)\right) \frac{1}{n^s}.$$

It follows that the product is identically equal to 1 if

$$\sum_{m|n} \mu(m) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

We shall establish this last fact and study some of its consequences over the next four theorems.

THEOREM 1.11. The Möbius function $\mu : \mathbb{N} \to \mathbb{C}$ is multiplicative.

PROOF. Suppose that $a, b \in \mathbb{N}$ and (a, b) = 1. If a or b is not squarefree, then neither is ab, and so $\mu(ab) = 0 = \mu(a)\mu(b)$. On the other hand, if both a and b are squarefree, then since (a,b) = 1, ab must also be squarefree. Furthermore, the number of prime factors of ab must be the sum of the numbers of prime factors of a and of b. \clubsuit

THEOREM 1.12. Suppose that $n \in \mathbb{N}$. Then

$$\sum_{m|n} \mu(m) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Consider the function $f: \mathbb{N} \to \mathbb{C}$ defined by writing

$$f(n) = \sum_{m|n} \mu(m)$$

for every $n \in \mathbb{N}$. It follows from Theorems 1.1 and 1.11 that f is multiplicative. For n = 1, the result is trivial. To complete the proof, it therefore suffices to show that $f(p^k) = 0$ for every prime p and every $k \in \mathbb{N}$. Indeed,

$$f(p^k) = \sum_{m|p^k} \mu(m) = \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^k) = 1 - 1 + 0 + \dots + 0 = 0.$$

Theorem 1.12 plays the central role in the proof of the following two results which are similar in nature.

THEOREM 1.13. (Möbius Inversion Formula) Given any function $f: \mathbb{N} \to \mathbb{C}$, suppose that the function $g: \mathbb{N} \to \mathbb{C}$ is defined by writing

$$g(n) = \sum_{m|n} f(m)$$

for every $n \in \mathbb{N}$. Then for every $n \in \mathbb{N}$, we have

$$f(n) = \sum_{m|n} \mu(m) g\left(\frac{n}{m}\right) = \sum_{m|n} \mu\left(\frac{n}{m}\right) g(m).$$

The second equality is obvious. Also

$$\sum_{m|n} \mu(m)g\left(\frac{n}{m}\right) = \sum_{m|n} \mu(m) \left(\sum_{k|\frac{n}{m}} f(k)\right) = \sum_{\substack{k,m\\km|n}} \mu(m)f(k)$$
$$= \sum_{k|n} f(k) \left(\sum_{m|\frac{n}{k}} \mu(m)\right) = f(n),$$

in view of Theorem 1.12. ♣

THEOREM 1.14. For any function $g: \mathbb{N} \to \mathbb{C}$, if the function $f: \mathbb{N} \to \mathbb{C}$ is defined by writing

$$f(n) = \sum_{m|n} \mu\left(\frac{n}{m}\right) g(m)$$

for every $n \in \mathbb{N}$, then for every $n \in \mathbb{N}$, we have

$$g(n) = \sum_{m|n} f(m) = \sum_{m|n} f\left(\frac{n}{m}\right).$$

The second equality is obvious. Also

$$\sum_{m|n} f\left(\frac{n}{m}\right) = \sum_{m|n} \left(\sum_{k|\frac{n}{m}} \mu\left(\frac{n}{mk}\right) g(k)\right) = \sum_{k|n} g(k) \left(\sum_{m|\frac{n}{k}} \mu\left(\frac{n/k}{m}\right)\right)$$
$$= \sum_{k|n} g(k) \left(\sum_{m|\frac{n}{k}} \mu(m)\right) = g(n),$$

in view of Theorem 1.12. ♣

REMARK. In number theory, it occurs quite often that in the proof of a theorem, a change of order of summation of the variables is required, as illustrated in the proofs of Theorems 1.13 and 1.14. This process of changing the order of summation does not depend on the summand in question. In both instances, we are concerned with a sum of the form

$$\sum_{m|n} \sum_{k|\frac{n}{m}} A(k,m).$$

This means that for every positive divisor m of n, we first sum the function A over all positive divisors k of n/m to obtain the sum

$$\sum_{k\mid \frac{n}{\overline{m}}} A(k,m),$$

which is a function of m. We then sum this sum over all divisors m of n. Now observe that for every natural number k satisfying $k \mid n/m$ for some positive divisor m of n, we must have $k \mid n$. Consider therefore a particular natural number k satisfying $k \mid n$. We must find all natural numbers m satisfying the original summation conditions, namely $m \mid n$ and $k \mid n/m$. These are precisely those natural numbers m satisfying $m \mid n/k$. We therefore obtain, for every positive divisor k of n, the sum

$$\sum_{m\mid \frac{n}{h}} A(k,m).$$

Summing over all positive divisors k of n, we obtain

$$\sum_{k|n} \sum_{m|\frac{n}{k}} A(k,m).$$

Since we are summing the function A over the same collection of pairs (k, m), and have merely changed the order of summation, we must have

$$\sum_{m|n} \sum_{k|\frac{n}{m}} A(k,m) = \sum_{k|n} \sum_{m|\frac{n}{k}} A(k,m).$$

The Euler Function

We define the Euler function $\phi: \mathbb{N} \to \mathbb{C}$ as follows. For every $n \in \mathbb{N}$, we let $\phi(n)$ denote the number of elements in the set $\{1, 2, ..., n\}$ which are coprime to n.

THEOREM 1.15. For every number $n \in \mathbb{N}$, we have

$$\sum_{m|n} \phi(m) = n.$$

PROOF. We shall partition the set $\{1, 2, ..., n\}$ into d(n) disjoint subsets \mathcal{B}_m , where for every positive divisor m of n,

$$\mathcal{B}_m = \{x : 1 \le x \le n \text{ and } (x, n) = m\}.$$

If $x \in \mathcal{B}_m$, let x = mx'. Then (mx', n) = m if and only if (x', n/m) = 1. Also $1 \le x \le n$ if and only if $1 \le x' \le n/m$. Hence

$$\mathcal{B}'_m = \{x' : 1 \le x' \le n/m \text{ and } (x', n/m) = 1\}$$

has the same number of elements as \mathcal{B}_m . Note now that the number of elements of \mathcal{B}'_m is exactly $\phi(n/m)$. Since every element of the set $\{1, 2, \ldots, n\}$ falls into exactly one of the subsets \mathcal{B}_m , we must have

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

Apply the Möbius inversion formula to the conclusion of Theorem 1.15, we obtain immediately the following result.

THEOREM 1.16. For every number $n \in \mathbb{N}$, we have

$$\phi(n) = \sum_{m|n} \mu(m) \frac{n}{m} = n \sum_{m|n} \frac{\mu(m)}{m}.$$

THEOREM 1.17. The Euler function $\phi : \mathbb{N} \to \mathbb{C}$ is multiplicative.

PROOF. Since the Möbius function μ is multiplicative, it follows that the function $f: \mathbb{N} \to \mathbb{C}$, defined by $f(n) = \mu(n)/n$ for every $n \in \mathbb{N}$, is multiplicative. The result now follows from Theorem 1.1. \clubsuit

THEOREM 1.18. Suppose that $n \in \mathbb{N}$ and n > 1, and that $n = p_1^{u_1} \dots p_r^{u_r}$ is the canonical decomposition of n. Then

$$\phi(n) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j} \right) = \prod_{j=1}^{r} p_j^{u_j - 1} (p_j - 1).$$

PROOF. The second equality is trivial. On the other hand, for every prime p and every $u \in \mathbb{N}$, we have by Theorem 1.16 that

$$\frac{\phi(p^u)}{p^u} = \sum_{m|n^u} \frac{\mu(m)}{m} = 1 + \frac{\mu(p)}{p} = 1 - \frac{1}{p}.$$

The result now follows since ϕ is multiplicative. \clubsuit

We not study the magnitude of $\phi(n)$ as $n \to \infty$. Clearly $\phi(1) = 1$ and $\phi(n) < n$ if n > 1.

Suppose first of all that n has many different prime factors. Then n must have many different divisors, and so $\sigma(n)$ must be large relative to n. But then many of the numbers $1, \ldots, n$ cannot be coprime to n, and so $\phi(n)$ must be small relative to n. On the other hand, suppose that n has very few prime factors. Then n must have very few divisors, and so $\sigma(n)$ must be small relative to n. But then many of the numbers $1, \ldots, n$ are coprime to n, and so $\phi(n)$ must be large relative to n. It therefore appears that if one of the two values $\sigma(n)$ and $\phi(n)$ is large relative to n, then the other must be small relative to n. Indeed, our heuristics are upheld by the following result.

THEOREM 1.19. For every $n \in \mathbb{N}$, we have

$$\frac{1}{2} < \frac{\sigma(n)\phi(n)}{n^2} \le 1.$$

PROOF. The result is obvious if n=1, so suppose that n>1. Let $n=p_1^{u_1}\dots p_r^{u_r}$ be the canonical decomposition of n. Recall Theorems 1.2 and 1.18. We have

$$\sigma(n) = \prod_{j=1}^{r} \frac{p_j^{u_j+1} - 1}{p_j - 1} = n \prod_{j=1}^{r} \frac{1 - p_j^{-u_j - 1}}{1 - p_j^{-1}}$$

and

$$\phi(n) = n \prod_{j=1}^{r} (1 - p_j^{-1}).$$

Hence

$$\frac{\sigma(n)\phi(n)}{n^2} = \prod_{j=1}^r (1 - p_j^{-u_j - 1}).$$

The upper bound follows at once. On the other hand, the lower bound follows on observing that

$$\prod_{j=1}^{r} (1 - p_j^{-u_j - 1}) \ge \prod_{p|n} (1 - p^{-2}) \ge \prod_{m=2}^{n} \left(1 - \frac{1}{m^2} \right) = \frac{n+1}{2n} > \frac{1}{2}.$$

Combining Theorems 1.9 and 1.19, we have the following result.

THEOREM 1.20. We have $\phi(n) \gg n/\log n$ as $n \to \infty$.

We now consider some average version of the Euler function.

THEOREM 1.21. (Mertens) As $X \to \infty$, we have

$$\sum_{n \le X} \phi(n) = \frac{3}{\pi^2} X^2 + O(X \log X).$$

PROOF. As $X \to \infty$, we have, by Theorem 1.16, that

$$\begin{split} \sum_{n \leq X} \phi(n) &= \sum_{n \leq X} \sum_{m \mid n} \mu(m) \frac{n}{m} = \sum_{m \leq X} \mu(m) \sum_{\substack{n \leq X \\ m \mid n}} \frac{n}{m} = \sum_{m \leq X} \mu(m) \sum_{r \leq X / m} r \\ &= \sum_{m \leq X} \mu(m) \frac{1}{2} \left[\frac{X}{m} \right] \left(1 + \left[\frac{X}{m} \right] \right) = \frac{1}{2} \sum_{m \leq X} \mu(m) \left(\frac{X}{m} + O(1) \right)^2 \\ &= \frac{X^2}{2} \sum_{m \leq X} \frac{\mu(m)}{m^2} + O\left(X \sum_{m \leq X} \frac{1}{m} \right) + O\left(\sum_{m \leq X} 1 \right) \\ &= \frac{X^2}{2} \sum_{m = 1}^{\infty} \frac{\mu(m)}{m^2} + O\left(X^2 \sum_{m > X} \frac{1}{m^2} \right) + O(X \log X) \\ &= \frac{X^2}{2} \sum_{m = 1}^{\infty} \frac{\mu(m)}{m^2} + O(X \log X) \end{split}$$

It remains to show that

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{m^2} = \frac{6}{\pi^2}.$$

But

$$\left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right) \left(\sum_{m=1}^{\infty} \frac{\mu(m)}{m^2}\right) = \sum_{k=1}^{\infty} \frac{1}{k^2} \left(\sum_{\substack{n,m\\nm=k}} \mu(m)\right) = \sum_{k=1}^{\infty} \frac{1}{k^2} \left(\sum_{m|k} \mu(m)\right) = 1,$$

in view of Theorem 1.12. ♣

Dirichlet Convolution

We shall denote the class of all arithmetic functions by A, and the class of all multiplicative functions

Given arithmetic functions $f, g \in \mathcal{A}$, we define the function $f * g : \mathbb{N} \to \mathbb{C}$ by writing

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

for every $n \in \mathbb{N}$. This function is called the Dirichlet convolution of f and g.

It is not difficult to show that Dirichlet convolution of arithmetic functions is commutative and associative. In other words, for every $f, g, h \in \mathcal{A}$, we have

$$f * g = g * f$$
 and $(f * g) * h = f * (g * h).$

Furthermore, the arithmetic function $I: \mathbb{N} \to \mathbb{C}$, defined by I(1) = 1 and I(n) = 0 for every $n \in \mathbb{N}$ satisfying n > 1, is an identity element for Dirichlet convolution. It is easy to check that I * f = f * I = ffor every $f \in \mathcal{A}$.

On the other hand, an inverse may not exist under Dirichlet convolution. Consider, for example, the function $f \in \mathcal{A}$ satisfying f(n) = 0 for every $n \in \mathbb{N}$.

THEOREM 1.22. For any $f \in \mathcal{A}$, the following two statements are equivalent:

- (i) We have $f(1) \neq 0$.
- (ii) There exists a unique $g \in A$ such that f * g = g * f = I.

PROOF. Suppose that (ii) holds. Then f(1)g(1) = 1, so that $f(1) \neq 0$. Conversely, suppose that $f(1) \neq 0$. We shall define $g \in \mathcal{A}$ iteratively by writing

$$g(1) = \frac{1}{f(1)} \tag{5}$$

and

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n\\d>1}} f(d)g\left(\frac{n}{d}\right) \tag{6}$$

for every $n \in \mathbb{N}$ satisfying n > 1. It is easy to check that this gives an inverse. Moreover, every inverse must satisfy (5) and (6), and so must be unique.

We now describe Theorem 1.12 and Möbius inversion in terms of Dirichlet convolution. Recall that the function $U \in \mathcal{A}$ is defined by U(n) = 1 for all $n \in \mathbb{N}$.

THEOREM 1.23.

- (i) We have $\mu * U = I$.
- (ii) If $f \in \mathcal{A}$ and g = f * U, then $f = g * \mu$.
- (iii) If $g \in \mathcal{A}$ and $f = g * \mu$, then g = f * U.

PROOF. (i) follows from Theorem 1.12. To prove (ii), note that

$$g * \mu = (f * U) * \mu = f * (U * \mu) = f * I = f.$$

To prove (iii), note that

$$f * U = (g * \mu) * U = g * (\mu * U) = g * I = g.$$

We conclude this chapter by exhibiting some group structure within \mathcal{A} and \mathcal{M} .

THEOREM 1.24. The sets $A' = \{f \in A : f(1) \neq 0\}$ and $M' = \{f \in M : f(1) = 1\}$ form abelian groups under Dirichlet convolution.

REMARK. Note that if $f \in \mathcal{M}$ is not identically zero, then $f(n) \neq 0$ for some $n \in \mathbb{N}$. Since f(n) =f(1)f(n), we must have f(1) = 1.

PROOF OF THEOREM 1.24. For \mathcal{A}' , this is now trivial. We now consider \mathcal{M}' . Clearly $I \in \mathcal{M}'$. If $f, g \in \mathcal{M}'$ and (m, n) = 1, then

$$(f * g)(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{d_1|m} \sum_{d_2|n} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right)$$
$$= \left(\sum_{d_1|m} f(d_1)g\left(\frac{m}{d_1}\right)\right) \left(\sum_{d_2|n} f(d_2)g\left(\frac{n}{d_2}\right)\right) = (f * g)(m)(f * g)(n),$$

so that $f * g \in \mathcal{M}$. Since $(f * g)(1) = f(1)g(1) \neq 0$, we have $f * g \in \mathcal{M}'$. It remains to show that if $f \in \mathcal{M}'$, then f has an inverse in \mathcal{M}' . Clearly f has an inverse in \mathcal{A}' under Dirichlet convolution. Let this inverse be h. We now define $g \in \mathcal{A}$ by writing g(1) = 1,

$$g(p^k) = h(p^k)$$

for every prime p and $k \in \mathbb{N}$, and

$$g(n) = \prod_{p^k || n} g(p^k)$$

for every n > 1. Then $g \in \mathcal{M}'$. Furthermore, for every integer n > 1, we have

$$(f*g)(n) = \prod_{p^k \mid \mid n} (f*g)(p^k) = \prod_{p^k \mid \mid n} (f*h)(p^k) = \prod_{p^k \mid \mid n} I(p^k) = I(n),$$

so that g is an inverse of f.

ELEMENTARY AND ANALYTIC NUMBER THEORY

W W L CHEN

(c) W W L Chen, 1981.

This work is available free, in the hope that it will be useful.

Any part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, with or without permission from the author.

Chapter 2

DISTRIBUTION OF PRIMES I: INTRODUCTION

2.1. Euclid's Theorem Revisited

We have already seen the elegant and simple proof of Euclid's theorem, that there are infinitely many primes. Here we shall begin by proving a slightly stronger result.

THEOREM 2.1. The series

$$\sum_{p} \frac{1}{p}$$

is divergent.

PROOF. For every real number $X \geq 2$, write

$$P_X = \prod_{p \le X} \left(1 - \frac{1}{p} \right)^{-1}.$$

Then

$$\log P_X = -\sum_{p \le X} \log \left(1 - \frac{1}{p} \right) = S_1 + S_2,$$

where

$$S_1 = \sum_{p \le X} \frac{1}{p}$$
 and $S_2 = \sum_{p \le X} \sum_{h=2}^{\infty} \frac{1}{hp^h}$.

[†] This chapter was first used in lectures given by the author at Imperial College, University of London, in 1981.

Since

$$0 \le \sum_{h=2}^{\infty} \frac{1}{hp^h} \le \sum_{h=2}^{\infty} \frac{1}{p^h} = \frac{1}{p(p-1)},$$

we have

$$0 \le S_2 \le \sum_{p} \frac{1}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1,$$

so that $0 \leq S_2 \leq 1$. On the other hand, as $X \to \infty$, we have

$$P_X = \prod_{p \le X} \left(\sum_{h=0}^{\infty} \frac{1}{p^h} \right) \ge \sum_{n \le X} \frac{1}{n} \to \infty.$$

The result follows. ♣

For every real number $X \geq 2$, we write

$$\pi(X) = \sum_{p \le X} 1,$$

so that $\pi(X)$ denotes the number of primes in the interval [2, X]. This function has been studied extensively by number theorists, and attempts to study it in depth have led to major developments in other important branches of mathematics.

As can be expected, many conjectures concerning the distribution of primes were made based purely on numerical evidence, including the celebrated Prime number theorem, proved in 1896 by Hadamard and de la Vallée Poussin, that

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

We shall give an analytic proof of this in Chapter 5. Here we shall be concerned with the weaker result of Tchebycheff, that there exist positive absolute constants c_1 and c_2 such that for every real number $X \geq 2$, we have

$$c_1 \frac{X}{\log X} < \pi(X) < c_2 \frac{X}{\log X}.$$

2.2. The Von Mangoldt Function

The study of the function $\pi(X)$ usually involves, instead of the characteristic function of the primes, a function which counts not only primes, but prime powers as well, and with weights. Accordingly, we introduce the von Mangoldt function $\Lambda: \mathbb{N} \to \mathbb{C}$, defined for every $n \in \mathbb{N}$ by writing

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^r \text{, with } p \text{ prime and } r \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$$

THEOREM 2.2. For every $n \in \mathbb{N}$, we have

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

PROOF. The result is clearly true for n=1, so it remains to consider the case $n \geq 2$. Suppose that $n=p_1^{u_1}\dots p_r^{u_r}$ is the canonical decomposition of n. Then the only non-zero contribution to the sum

on the left hand side comes from those natural numbers m of the form $m=p_j^{v_j}$ with $j=1,\ldots,r$ and $1 \leq v_j \leq u_j$. It follows that

$$\sum_{m|n} \Lambda(m) = \sum_{j=1}^{r} \sum_{v_j=1}^{u_j} \log p_j = \sum_{j=1}^{r} \log p_j^{u_j} = \log n.$$

THEOREM 2.3. As $X \to \infty$, we have

$$\sum_{m \le X} \Lambda(m) \left[\frac{X}{m} \right] = X \log X - X + O(\log X).$$

PROOF. It follows from Theorem 2.2 that

$$\sum_{n \le X} \log n = \sum_{n \le X} \sum_{m \mid n} \Lambda(m) = \sum_{m \le X} \Lambda(m) \sum_{\substack{n \le X \\ m \mid n}} 1 = \sum_{m \le X} \Lambda(m) \left[\frac{X}{m} \right].$$

It therefore suffices to prove that as $X \to \infty$, we have

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

To prove (1), note that $\log X$ is an increasing function of X. In particular, for every $n \in \mathbb{N}$, we have

$$\log n \le \int_n^{n+1} \log u \, \mathrm{d}u,$$

so that

$$\sum_{n \le X} \log n - \log(X+1) \le \int_1^X \log u \, \mathrm{d}u.$$

On the other hand, for every $n \in \mathbb{N}$, we have

$$\log n \ge \int_{n-1}^{n} \log u \, \mathrm{d}u,$$

so that

$$\sum_{n \le X} \log n = \sum_{2 \le n \le X} \log n \ge \int_1^{[X]} \log u \, \mathrm{d}u$$
$$= \int_1^X \log u \, \mathrm{d}u - \int_{[X]}^X \log u \, \mathrm{d}u \ge \int_1^X \log u \, \mathrm{d}u - \log X.$$

The inequality (1) now follows on noting that

$$\int_{1}^{X} \log u \, \mathrm{d}u = X \log X - X + 1.$$

2.3. Tchebycheff's Theorem

The crucial step in the proof of Tchebycheff's theorem concerns obtaining bounds on sums involving the von Mangoldt function. More precisely, we prove the following result.

THEOREM 2.4. There exist positive absolute constants c_3 and c_4 such that

$$\sum_{m \le X} \Lambda(m) \ge \frac{1}{2} X \log 2 \quad (X \ge c_3) \tag{2}$$

and

$$\sum_{\frac{X}{2} < m \le X} \Lambda(m) \le c_4 X \quad (X \ge 0). \tag{3}$$

PROOF. If $m \in \mathbb{N}$ satisfies $X/2 < m \le X$, then clearly [X/2m] = 0. It follows from this and Theorem 2.3 that as $X \to \infty$, we have

$$\begin{split} \sum_{m \leq X} \Lambda(m) \left(\left[\frac{X}{m} \right] - 2 \left[\frac{X}{2m} \right] \right) &= \sum_{m \leq X} \Lambda(m) \left[\frac{X}{m} \right] - 2 \sum_{m \leq \frac{X}{2}} \Lambda(m) \left[\frac{X}{2m} \right] \\ &= \left(X \log X - X + O(\log X) \right) - 2 \left(\frac{X}{2} \log \frac{X}{2} - \frac{X}{2} + O(\log X) \right) \\ &= X \log 2 + O(\log X). \end{split}$$

Hence there exists a positive absolute constant c_5 such that for all sufficiently large X, we have

$$\frac{1}{2}X\log 2 < \sum_{m \le X} \Lambda(m) \left(\left[\frac{X}{m} \right] - 2 \left[\frac{X}{2m} \right] \right) < c_5 X.$$

We now consider the function $[\alpha] - 2[\alpha/2]$. Clearly $[\alpha] - 2[\alpha/2] < \alpha - 2(\alpha/2 - 1) = 2$. Note that the left hand side is an integer, so we must have $[\alpha] - 2[\alpha/2] \le 1$. It follows that for all sufficiently large X, we have

$$\frac{1}{2}X\log 2 < \sum_{m \le X} \Lambda(m).$$

The inequality (2) follows. On the other hand, if $X/2 < m \le X$, then [X/m] = 1 and [X/2m] = 0, so that for all sufficiently large X, we have

$$\sum_{\frac{X}{2} < m \le X} \Lambda(m) \le c_5 X.$$

The inequality (3) follows easily. \clubsuit

We now state and prove Tchebycheff's theorem.

THEOREM 2.5. (Tchebycheff) There exist positive absolute constants c_1 and c_2 such that for every real number $X \geq 2$, we have

$$c_1 \frac{X}{\log X} < \pi(X) < c_2 \frac{X}{\log X}.$$

PROOF. To prove the lower bound, note that

$$\begin{split} \sum_{m \leq X} \Lambda(m) &= \sum_{\substack{p,n \\ p^n \leq X}} \log p = \sum_{p \leq X} (\log p) \sum_{1 \leq n \leq \left[\frac{\log X}{\log p}\right]} 1 \\ &= \sum_{p < X} (\log p) \left[\frac{\log X}{\log p}\right] \leq \pi(X) \log X. \end{split}$$

It follows from (2) that

$$\pi(X) \ge \frac{X \log 2}{2 \log X} \quad (X \ge c_3).$$

Since $\pi(2) = 1$, we get the lower bound for a suitable choice of c_1 .

To prove the upper bound, note that in view of (3) and the definition of the von Mangoldt function, the inequality

$$\sum_{\frac{X}{2^j+1}$$

holds for every integer $j \geq 0$ and every real number $X \geq 0$. Suppose that $X \geq 2$. Let the integer $k \geq 0$ be defined such that $2^k < X^{1/2} \le 2^{k+1}$. Then

$$\sum_{X^{1/2}$$

so that

$$\sum_{X^{1/2}$$

whence

$$\pi(X) \le X^{1/2} + \frac{4c_4X}{\log X} < \frac{c_2X}{\log X}$$

for a suitable c_2 .

Some Results of Mertens

We conclude this chapter by obtaining an improvement of Theorem 2.1.

THEOREM 2.6. (Mertens) As $X \to \infty$, we have

$$\sum_{m \le X} \frac{\Lambda(m)}{m} = \log X + O(1),\tag{4}$$

$$\sum_{p \leqslant X} \frac{\log p}{p} = \log X + O(1),\tag{5}$$

and

$$\sum_{p \le X} \frac{1}{p} = \log \log X + O(1). \tag{6}$$

PROOF. Recall Theorem 2.3. As $X \to \infty$, we have

$$\sum_{m \le X} \Lambda(m) \left[\frac{X}{m} \right] = X \log X - X + O(\log X).$$

Clearly [X/m] = X/m + O(1), so that as $X \to \infty$, we have

$$\sum_{m \leq X} \Lambda(m) \left[\frac{X}{m} \right] = X \sum_{m \leq X} \frac{\Lambda(m)}{m} + O\left(\sum_{m \leq X} \Lambda(m) \right).$$

It follows from (3) that

$$\sum_{m \le X} \Lambda(m) \le \sum_{j=0}^{\infty} \sum_{\frac{X}{2^{j+1}} < m \le \frac{X}{2^{j}}} \Lambda(m) \le 2c_4 X,$$

so that as $X \to \infty$, we have

$$X \sum_{m \le X} \frac{\Lambda(m)}{m} = X \log X + O(X).$$

The inequality (4) follows. Next, note that

$$\sum_{m \le X} \frac{\Lambda(m)}{m} = \sum_{\substack{p,k \\ p^k < X}} \frac{\log p}{p^k} = \sum_{p \le X} \frac{\log p}{p} + \sum_{\substack{p \le X}} (\log p) \sum_{\substack{2 \le k \le \frac{\log X}{\log p}}} \frac{1}{p^k}.$$

As $X \to \infty$, we have

$$\sum_{p \le X} (\log p) \sum_{2 \le k \le \frac{\log X}{\log p}} \frac{1}{p^k} \le \sum_{p \le X} (\log p) \sum_{k=2}^{\infty} \frac{1}{p^k} = \sum_{p \le X} \frac{\log p}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(1).$$

The inequality (5) follows. Finally, for every real number $X \geq 2$, let

$$T(X) = \sum_{p \le X} \frac{\log p}{p}.$$

Then it follows from (5) that there exists a positive absolute constant c_6 such that $|T(X) - \log X| < c_6$ whenever $X \geq 2$. On the other hand,

$$\sum_{p \le X} \frac{1}{p} = \sum_{p \le X} \frac{\log p}{p} \left(\frac{1}{\log X} + \int_{p}^{X} \frac{\mathrm{d}y}{y \log^{2} y} \right) = \frac{T(X)}{\log X} + \int_{2}^{X} \frac{T(y) \, \mathrm{d}y}{y \log^{2} y}$$
$$= \frac{T(X) - \log X}{\log X} + \int_{2}^{X} \frac{(T(y) - \log y) \, \mathrm{d}y}{y \log^{2} y} + 1 + \int_{2}^{X} \frac{\mathrm{d}y}{y \log y}.$$

It follows that as $X \to \infty$, we have

$$\left| \sum_{p \le X} \frac{1}{p} - \log \log X \right| < \frac{c_6}{\log X} + \int_2^X \frac{c_6 \, \mathrm{d}y}{y \log^2 y} + 1 - \log \log 2 = O(1).$$

The inequality (6) follows. ♣

ELEMENTARY AND ANALYTIC NUMBER THEORY

W W L CHEN

(c) W W L Chen, 1990.

This work is available free, in the hope that it will be useful.

Any part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, with or without permission from the author.

Chapter 3

DIRICHLET SERIES

3.1. Convergence Properties

A Dirichlet series is a series of the type

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

where $f: \mathbb{N} \to \mathbb{C}$ is an arithmetic function and $s \in \mathbb{C}$. We usually write $s = \sigma + \mathrm{i}t$, where $\sigma, t \in \mathbb{R}$. Our first task is to investigate convergence of Dirichlet series.

THEOREM 3.1. Suppose that the series (1) converges for some $s \in \mathbb{C}$. Then there exist unique real numbers $\sigma_0, \sigma_1, \sigma_2$ satisfying $-\infty \le \sigma_0 \le \sigma_1 \le \sigma_2 < \infty$ and such that the following statements hold:

- (i) The series (1) converges for every $s \in \mathbb{C}$ with $\sigma > \sigma_0$. Furthermore, for every $\epsilon > 0$, the series (1) diverges for some $s \in \mathbb{C}$ with $\sigma_0 \epsilon < \sigma \le \sigma_0$.
- (ii) For every $\eta > 0$, the series (1) converges uniformly on the set $\{s \in \mathbb{C} : \sigma > \sigma_1 + \eta\}$ and does not converge uniformly on the set $\{s \in \mathbb{C} : \sigma > \sigma_1 \eta\}$.
- (iii) The series (1) converges absolutely for every $s \in \mathbb{C}$ with $\sigma > \sigma_2$. Furthermore, for every $\epsilon > 0$, the series (1) does not converge absolutely for some $s \in \mathbb{C}$ with $\sigma_2 \epsilon < \sigma \le \sigma_2$.

EXAMPLE. The Dirichlet series

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

converges absolutely for every $s \in \mathbb{C}$ with $\sigma > 1$ and diverges for every real s < 1. It follows that $\sigma_0 = \sigma_1 = \sigma_2 = 1$ in this case.

[†] This chapter was first used in lectures given by the author at Imperial College, University of London, in 1990.

PROOF OF THEOREM 3.1. Suppose that the series (1) converges for $s = s^* = \sigma^* + it^*$. Then $f(n)n^{-s^*} \to 0$ as $n \to \infty$, so that $|f(n)n^{-s^*}| = O(1)$, and so $|f(n)| = O(n^{\sigma^*})$. It follows that for every $s \in \mathbb{C}$ with $\sigma > \sigma^* + 1$, we have

$$|f(n)n^{-s}| = |f(n)n^{-\sigma}| = O(n^{\sigma^* - \sigma}),$$

so that the series (1) converges by the Comparison test. Now let

$$\sigma_0 = \inf\{u \in \mathbb{R} : \text{the series (1) converges for all } s \in \mathbb{C} \text{ with } \sigma > u\}$$

and

 $\sigma_2 = \inf\{u \in \mathbb{R} : \text{the series (1) converges absolutely for all } s \in \mathbb{C} \text{ with } \sigma > u\}.$

Clearly (i) and (iii) follow, and $\sigma_0 \leq \sigma_2$. To prove (ii), let $\delta > 0$ and $\epsilon > 0$ be chosen. Then there exists $N \in \mathbb{N}$ such that

$$\sum_{n=N+1}^{\infty} |f(n)| n^{-\sigma_2 - \delta} < \epsilon.$$

Hence

$$\sup \left\{ \left| \sum_{n=1}^{N} f(n) n^{-s} - \sum_{n=1}^{\infty} f(n) n^{-s} \right| : \sigma \ge \sigma_2 + \delta \right\} \le \sum_{n=N+1}^{\infty} |f(n)| n^{-\sigma_2 - \delta} < \epsilon.$$

It follows that the series (1) converges uniformly on the set $\{s \in \mathbb{C} : \sigma \geq \sigma_2 + \delta\}$. Now let

$$\sigma_1 = \inf\{u \in \mathbb{R} : \text{the series (1) converges uniformly on } \{z \in \mathbb{C} : \sigma \ge u\}\}.$$

Clearly $\sigma_0 \leq \sigma_1 \leq \sigma_2 + \delta$. Since $\delta > 0$ is arbitrary, we must have $\sigma_0 \leq \sigma_1 \leq \sigma_2$.

A simple consequence of uniform convergence is the following result concerning differentiation term by term.

THEOREM 3.2. For every $s \in \mathbb{C}$ with $\sigma > \sigma_1$, the series (1) may be differentiated term by term. In particular, F'(s) exists and

$$F'(s) = -\sum_{n=1}^{\infty} f(n)(\log n)n^{-s}.$$

Uniqueness Properties

Our next task is to prove the uniqueness theorem of Dirichlet series, a result of great importance in view of the applications we have in mind.

THEOREM 3.3. Suppose that

$$F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$$
 and $G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$,

where $f: \mathbb{N} \to \mathbb{C}$ and $g: \mathbb{N} \to \mathbb{C}$ are arithmetic functions and $s \in \mathbb{C}$. Suppose further that there exists $\sigma_3 \in \mathbb{R}$ such that for every $s \in \mathbb{C}$ satisfying $\sigma \geq \sigma_3$, we have F(s) = G(s). Then f(n) = g(n) for every

It is clearly sufficient to prove the following special case.

THEOREM 3.4. Suppose that

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

where $f: \mathbb{N} \to \mathbb{C}$ is an arithmetic function and $s \in \mathbb{C}$. Suppose further that there exists $\sigma_3 \in \mathbb{R}$ such that for every $s \in \mathbb{C}$ satisfying $\sigma \geq \sigma_3$, we have F(s) = 0. Then f(n) = 0 for every $n \in \mathbb{N}$.

PROOF. Since the series converges for $s = \sigma_3$, we must have $|f(n)| = O(n^{\sigma_3})$ for all $n \in \mathbb{N}$. Now let $\sigma \geq \sigma_3 + 2$. Then

$$\sum_{n=N}^{\infty} f(n)n^{-\sigma} = O\left(\sum_{n=N}^{\infty} n^{\sigma_3 - \sigma}\right). \tag{2}$$

Note next that $y^{\sigma_3-\sigma}$ is a decreasing function of y, so that

$$\sum_{n=N}^{\infty} n^{\sigma_3 - \sigma} = N^{\sigma_3 - \sigma} + \sum_{n=N+1}^{\infty} n^{\sigma_3 - \sigma} \le N^{\sigma_3 - \sigma} + \int_{N}^{\infty} y^{\sigma_3 - \sigma} \, \mathrm{d}y = O(N^{\sigma_3 - \sigma + 1}). \tag{3}$$

Combining (2) and (3), we see that for every $N \in \mathbb{N}$, we have

$$\sum_{n=N}^{\infty} f(n)n^{-\sigma} = O(N^{\sigma_3 - \sigma + 1}). \tag{4}$$

Using (4) with N=2, we obtain, for $\sigma \geq \sigma_3 + 2$,

$$0 = F(\sigma) = f(1) + \sum_{n=2}^{\infty} f(n)n^{-\sigma} = f(1) + O(2^{\sigma_3 - \sigma + 1}) \to f(1)$$

as $\sigma \to +\infty$. Hence f(1)=0. Suppose now that $f(1)=f(2)=\ldots=f(M-1)=0$. Using (4) with N = M + 1, we obtain, for $\sigma \geq \sigma_3 + 2$,

$$0 = F(\sigma) = f(M)M^{-\sigma} + \sum_{n=M+1}^{\infty} f(n)n^{-\sigma} = f(M)M^{-\sigma} + O((M+1)^{\sigma_3 - \sigma + 1}),$$

so that

$$0 = f(M) + O\left((M+1)^{\sigma_3+1} \left(\frac{M}{M+1}\right)^{\sigma}\right) \to f(M)$$

as $\sigma \to +\infty$. Hence f(M)=0. The result now follows from induction.

3.3. **Multiplicative Properties**

Dirichlet series are extremely useful in tackling problems in number theory as well as in other branches of mathematics. The main properties that underpin most of these applications are the multiplicative aspects of these series.

THEOREM 3.5. Suppose that for every j = 1, 2, 3, we have

$$F_j(s) = \sum_{n=1}^{\infty} f_j(n) n^{-s},$$

where $f_j: \mathbb{N} \to \mathbb{C}$ is an arithmetic function and $s \in \mathbb{C}$. Suppose further that for every $n \in \mathbb{N}$, we have

$$f_3(n) = \sum_{\substack{x,y\\xy=n}} f_1(x)f_2(y) = \sum_{x|n} f_1(x)f_2\left(\frac{n}{x}\right) = \sum_{y|n} f_1\left(\frac{n}{y}\right)f_2(y).$$

Then

$$F_1(s)F_2(s) = F_3(s),$$

provided that $\sigma > \max\{\sigma_2^{(1)}, \sigma_2^{(2)}\}$, where, for every j = 1, 2, the series $F_j(s)$ converges absolutely for every $s \in \mathbb{C}$ with $\sigma > \sigma_2^{(j)}$.

PROOF. We have

$$\sum_{n=1}^{N} f_3(n) n^{-s} = \sum_{\substack{1 \le x \le N \\ 1 \le y \le N \\ xy \le N}} f_1(x) x^{-s} f_2(y) y^{-s},$$

so that

$$\sum_{n=1}^{N} f_3(n) n^{-s} - \sum_{x \le \sqrt{N}} f_1(x) x^{-s} \sum_{y \le \sqrt{N}} f_2(y) y^{-s}$$

$$= \sum_{\sqrt{N} < x \le N} f_1(x) x^{-s} \sum_{y \le N/x} f_2(y) y^{-s} + \sum_{x \le \sqrt{N}} f_1(x) x^{-s} \sum_{\sqrt{N} < y \le N/x} f_2(y) y^{-s}.$$

It follows that

$$\left| \sum_{n=1}^{N} f_{3}(n) n^{-s} - \sum_{x \leq \sqrt{N}} f_{1}(x) x^{-s} \sum_{y \leq \sqrt{N}} f_{2}(y) y^{-s} \right|$$

$$< \left(\sum_{x > \sqrt{N}} |f_{1}(x)| x^{-\sigma} \right) \left(\sum_{y=1}^{\infty} |f_{2}(y)| y^{-\sigma} \right)$$

$$+ \left(\sum_{x=1}^{\infty} |f_{1}(x)| x^{-\sigma} \right) \left(\sum_{y > \sqrt{N}} |f_{2}(y)| y^{-\sigma} \right).$$
(5)

Suppose now that $\sigma > \max\{\sigma_2^{(1)}, \sigma_2^{(2)}\}$. Clearly

$$\sum_{x>\sqrt{N}} |f_1(x)| x^{-\sigma} \quad \text{and} \quad \sum_{y>\sqrt{N}} |f_2(y)| y^{-\sigma}$$

converge to 0 as $N \to \infty$. Furthermore, the series

$$\sum_{x=1}^{\infty} |f_1(x)| x^{-\sigma} \quad \text{and} \quad \sum_{y=1}^{\infty} |f_2(y)| y^{-\sigma}$$

are convergent. It follows that the right hand side of (5) converges to 0 as $N \to \infty$. On the other hand,

$$\sum_{x \le \sqrt{N}} f_1(x) x^{-s} \quad \text{and} \quad \sum_{y \le \sqrt{N}} f_2(y) y^{-s}$$

converge to $F_1(s)$ and $F_2(s)$ respectively as $N \to \infty$. The result follows. \clubsuit

REMARK. Theorem 3.5 generalizes to a product of k Dirichlet series $F_1(s), \ldots, F_k(s)$, where the general coefficient is

$$\sum_{\substack{x_1,\ldots,x_k\\x_1\ldots x_k=n}} f_1(x_1)\ldots f_k(x_k).$$

In many applications, the coefficients f(n) of the Dirichlet series will be given by various important arithmetic functions in number theory. We therefore study next some consequences when the function $f: \mathbb{N} \to \mathbb{C}$ is multiplicative.

THEOREM 3.6. Suppose that the function $f: \mathbb{N} \to \mathbb{C}$ is multiplicative. Then for every $s \in \mathbb{C}$ satisfying $\sigma > \sigma_2$, the series (1) satisfies

$$F(s) = \prod_{p} \left(\sum_{h=0}^{\infty} f(p^h) p^{-hs} \right).$$

PROOF. By the Remark, if p_j is the j-th prime in increasing order, then

$$\prod_{j=1}^{k} \left(\sum_{h=0}^{\infty} f(p_j^h) p_j^{-hs} \right) = \sum_{n=1}^{\infty} \left(\sum_{\substack{h_1, \dots, h_k \\ p_1^{h_1} \dots p_k^{h_k} = n}} f(p_1^{h_1}) \dots f(p_k^{h_k}) \right) n^{-s}.$$

By the uniqueness of factorization, the inner sum on the right hand side contains at most one term. Hence

$$\prod_{j=1}^{k} \left(\sum_{h=0}^{\infty} f(p_j^h) p_j^{-hs} \right) = \sum_{n=1}^{\infty} \theta_k(n) f(n) n^{-s},$$

where

$$\theta_k(n) = \begin{cases} 1 & \text{if all the prime factors of } n \text{ are among } p_1, \dots, p_k, \\ 0 & \text{otherwise.} \end{cases}$$

It follows that as $k \to \infty$, we have

$$\prod_{j=1}^{k} \left(\sum_{h=0}^{\infty} f(p_j^h) p_j^{-hs} \right) - \sum_{n=1}^{\infty} f(n) n^{-s} = \sum_{n=1}^{\infty} (\theta_k(n) - 1) f(n) n^{-s}
= O\left(\sum_{n=k+1}^{\infty} |f(n)| n^{-\sigma} \right) \to 0.$$

An arithmetic function $f: \mathbb{N} \to \mathbb{C}$ is said to be totally multiplicative or strongly multiplicative if f(mn) = f(m)f(n) for every $m, n \in \mathbb{N}$.

THEOREM 3.7. Suppose that the function $f: \mathbb{N} \to \mathbb{C}$ is totally multiplicative. Then for every $s \in \mathbb{C}$ satisfying $\sigma > \sigma_2$, the series (1) satisfies

$$F(s) = \prod_{p} (1 - f(p)p^{-s})^{-1}.$$

PROOF. The absolute convergence of the series

$$\sum_{h=0}^{\infty} f(p^h) p^{-hs} \tag{6}$$

is immediate for $\sigma > \sigma_2$ by comparison with the series

$$\sum_{n=1}^{\infty} |f(n)| n^{-\sigma}.$$

Furthermore, if f is not identically zero, then it is easy to see that f(1) = 1, so that the series (6) is now a convergent geometric series with sum $(1 - f(p)p^{-s})^{-1}$.

EXAMPLE. Consider again the Dirichlet series

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

For every $s \in \mathbb{C}$ satisfying $\sigma > 1$, we have

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1}.$$

This is called the Euler product of the Riemann zeta function $\zeta(s)$.

ELEMENTARY AND ANALYTIC NUMBER THEORY

W W L CHEN

© WWL Chen, 1990.

This work is available free, in the hope that it will be useful.

Any part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, with or without permission from the author.

Chapter 4

DISTRIBUTION OF PRIMES II : ARITHMETIC PROGRESSIONS

4.1. Dirichlet's Theorem

The purpose of this chapter is to prove the following remarkable result of Dirichlet, widely regarded as one of the greatest achievements in mathematics.

THEOREM 4.1. Suppose that $q \in \mathbb{N}$ and $a \in \mathbb{Z}$ satisfy (a,q) = 1. Then there are infinitely many primes $p \equiv a \pmod{q}$.

Note that the requirement (a,q)=1 is crucial. If $n\equiv a\pmod q$, then clearly $(a,q)\mid n$. It follows that if (a,q)>1, then the residue class $n\equiv a\pmod q$ of natural numbers contains at most one prime. In other words, Dirichlet's theorem asserts that any residue class $n\equiv a\pmod q$ of natural numbers must contain infinitely many primes if there is no simple reason to support the contrary.

It is easy to prove Theorem 4.1 by elementary methods for some special values of a and q.

EXAMPLE. There are infinitely many primes $p \equiv -1 \pmod{4}$. Suppose on the contrary that p_1, \ldots, p_r represent all such primes. Then $4p_1 \ldots p_r - 1$ must have a prime factor $p \equiv -1 \pmod{4}$. But p cannot be any of p_1, \ldots, p_r .

EXAMPLE. There are infinitely many primes $p \equiv 1 \pmod 4$. Suppose on the contrary that p_1, \ldots, p_r represent all such primes. Consider the number $4(p_1 \ldots p_r)^2 + 1$. Suppose that a prime p divides $4(p_1 \ldots p_r)^2 + 1$. Then $4(p_1 \ldots p_r)^2 + 1 \equiv 0 \pmod p$. It follows that -1 is a quadratic residue modulo p, so that we must have $p \equiv 1 \pmod 4$. Clearly p cannot be any of p_1, \ldots, p_r .

[†] This chapter was first used in lectures given by the author at Imperial College, University of London, in 1990.

4.2. A Special Case

The idea of Dirichlet is to show that if (a, q) = 1, then the series

$$\sum_{p \equiv a \pmod{q}} \frac{1}{p}$$

is divergent. For technical reasons, it is easier to show that if (a,q)=1, then

$$\sum_{p \equiv a \pmod{q}} \frac{\log p}{p^{\sigma}} \to +\infty \quad \text{as } \sigma \to 1+.$$

Let us illustrate the idea of Dirichlet by studying the case $n \equiv 1 \pmod{4}$.

First of all, we need a function that distinguishes between integers $n \equiv 1 \pmod{4}$ and the others. Suppose that n is odd. Then it is easy to check that

$$\frac{1 + (-1)^{\frac{n-1}{2}}}{2} = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ 0 & \text{if } n \equiv -1 \pmod{4}; \end{cases}$$

so that

$$\sum_{p\equiv 1 \pmod 4} \frac{\log p}{p^\sigma} = \frac{1}{2} \sum_{p \text{ odd}} \frac{\log p}{p^\sigma} \left(1 + (-1)^{\frac{p-1}{2}}\right).$$

Now the series

$$\sum_{p \text{ odd}} \frac{\log p}{p^{\sigma}} \to +\infty \quad \text{as } \sigma \to 1+,$$

so it suffices to show that the series

$$\sum_{p \text{ odd}} \frac{(-1)^{\frac{p-1}{2}} \log p}{p^{\sigma}}$$

converges as $\sigma \to 1+$.

The next idea is to show that if we consider the series

$$\sum_{\substack{n=1\\n \text{ odd}}}^{\infty} \frac{(-1)^{\frac{n-1}{2}}\Lambda(n)}{n^{\sigma}} \tag{1}$$

instead, then the contribution from the terms corresponding to non-prime odd natural numbers n is convergent. It therefore suffices to show that the series (1) converges as $\sigma \to 1+$.

Note now that the function

$$\chi(n) = \begin{cases} (-1)^{\frac{n-1}{2}} & \text{if } n \text{ is odd,} \\ 0 & \text{if } n \text{ is even,} \end{cases}$$

is totally multiplicative; in other words, $\chi(mn) = \chi(m)\chi(n)$ for every $m, n \in \mathbb{N}$. Write

$$L(\sigma) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{\sigma}},\tag{2}$$

and note that for every $n \in \mathbb{N}$, we have

$$\chi(n)\log n = \chi(n)\sum_{m|n}\Lambda(m) = \sum_{m|n}\chi(m)\Lambda(m)\chi\left(\frac{n}{m}\right).$$

It follows from Theorems 3.2 and 3.5 that for $\sigma > 1$, we have

$$L'(\sigma) = -\sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n^{\sigma}} = -\left(\sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^{\sigma}}\right) \left(\sum_{n=1}^{\infty} \frac{\chi(n)}{n^{\sigma}}\right).$$

Hence

$$\sum_{\substack{n=1\\ r=1}}^{\infty} \frac{(-1)^{\frac{n-1}{2}} \Lambda(n)}{n^{\sigma}} = \sum_{n=1}^{\infty} \frac{\chi(n) \Lambda(n)}{n^{\sigma}} = -\frac{L'(\sigma)}{L(\sigma)}.$$

Now as $\sigma \to 1+$, we expect

$$L(\sigma) \to L(1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots > 0$$

and

$$L'(\sigma) \to \frac{\log 3}{3} - \frac{\log 5}{5} + \frac{\log 7}{7} - \dots$$

which converges by the Alternating series test. We therefore expect the series (1) to converge to a finite limit.

Dirichlet Characters 4.3.

Dirichlet's most crucial discovery is that for every $q \in \mathbb{N}$, there is a family of $\phi(q)$ functions $\chi : \mathbb{N} \to \mathbb{C}$, known nowadays as the Dirichlet characters modulo q, which generalize the function χ in the special case and which satisfy

$$\frac{1}{\phi(q)} \sum_{\substack{\chi \bmod q}} \frac{\chi(n)}{\chi(a)} = \begin{cases} 1 & \text{if } n \equiv a \pmod q, \\ 0 & \text{if } n \not\equiv a \pmod q. \end{cases}$$

To understand Dirichlet's ideas, we shall first of all study group characters. This is slightly more general than is necessary, but easier to understand.

Let G be a finite abelian group of order h and with identity element e. A character on G is a non-zero complex-valued function χ on G for which $\chi(uv) = \chi(u)\chi(v)$ for every $u, v \in G$. It is easy to check the following simple results.

Remark. We have

- (i) $\chi(e) = 1$;
- (ii) for every $u \in G$, $\chi(u)$ is an h-th root of unity;
- (iii) the number c of characters is finite; and
- (iv) the characters form an abelian group.

Slightly less trivial is the following.

REMARK. If $u \in G$ and $u \neq e$, then there exists a character χ on G such that $\chi(u) \neq 1$. To see this, note that G can be expressed as a direct product of cyclic groups G_1, \ldots, G_s of orders h_1, \ldots, h_s respectively, where $h = h_1 \dots h_s$. Suppose that for each $j = 1, \dots, s$, the cyclic group G_j is generated by v_j . Then we can write $u=v_1^{y_1}\dots v_s^{y_s}$, where $y_j\pmod{h_j}$ is uniquely determined for every $j=1,\dots,s$. Since $u \neq e$, there exists k = 1, ..., s such that $y_k \not\equiv 0 \pmod{h_k}$. Let $\chi(v_k) = e(1/h_k)$, and let $\chi(v_j) = 1$ for every j = 1, ..., s such that $j \neq k$. Clearly $\chi(u) = e(y_k/h_k) \neq 1$.

We shall denote by χ_0 the principal character on G. In other words, $\chi_0(u) = 1$ for every $u \in G$. Also, \sum_{χ} denotes a summation over all the distinct characters on G.

THEOREM 4.2. Suppose that G is a finite abelian group of order h and with identity element e. Suppose further that χ_0 is the principal character on G.

(i) For every character χ on G, we have

$$\sum_{u \in G} \chi(u) = \begin{cases} h & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

(ii) For every $u \in G$, we have

$$\sum_{\chi} \chi(u) = \begin{cases} c & \text{if } u = e, \\ 0 & \text{if } u \neq e, \end{cases}$$

where c denotes the number of distinct characters on G.

- (iii) We have c = h.
- (iv) For every $u, v \in G$, we have

$$\frac{1}{h} \sum_{\chi} \frac{\chi(u)}{\chi(v)} = \begin{cases} 1 & \text{if } u = v, \\ 0 & \text{if } u \neq v. \end{cases}$$

PROOF. (i) If $\chi = \chi_0$, then the result is obvious. If $\chi \neq \chi_0$, then there exists $v \in G$ such that $\chi(v) \neq 1$, and so

$$\chi(v)\sum_{u\in G}\chi(u)=\sum_{u\in G}\chi(u)\chi(v)=\sum_{u\in G}\chi(uv)=\sum_{u\in G}\chi(u),$$

the last equality following from the fact that uv runs over all the elements of G as u runs over all the elements of G. Hence

$$(1 - \chi(v)) \sum_{u \in G} \chi(u) = 0.$$

The result follows since $\chi(v) \neq 1$.

(ii) If u=e, then the result is obvious. If $u\neq e$, then we have already shown that there exists a character χ_1 such that $\chi_1(u) \neq 1$, so that

$$\chi_1(u) \sum_{\chi} \chi(u) = \sum_{\chi} \chi_1(u) \chi(u) = \sum_{\chi} (\chi_1 \chi)(u) = \sum_{\chi} \chi(u),$$

the last equality following from noting that the characters on G form an abelian group so that $\chi_1 \chi$ runs through all the characters on G as χ runs through all the characters on G. Hence

$$(1 - \chi_1(u)) \sum_{\chi} \chi(u) = 0.$$

The result follows since $\chi_1(u) \neq 1$.

(iii) Note that

$$h = \sum_{X} \sum_{u \in G} \chi(u) = \sum_{u \in G} \sum_{X} \chi(u) = c.$$

(iv) Note that

$$\frac{1}{h} \sum_{v} \frac{\chi(u)}{\chi(v)} = \frac{1}{h} \sum_{v} \chi(u) \chi(v^{-1}) = \frac{1}{h} \sum_{v} \chi(uv^{-1}) = \begin{cases} c/h & \text{if } uv^{-1} = e, \\ 0 & \text{if } uv^{-1} \neq e. \end{cases}$$

The result follows since h = c.

We are now in a position to introduce Dirichlet characters. Let $q \in \mathbb{N}$ be given. Then there are exactly $\phi(q)$ residue classes $n \equiv a \pmod{q}$ satisfying (a,q) = 1. Under multiplication of residue classes, they form an abelian group of order $\phi(q)$. Suppose that these residue classes are represented by $a_1, \ldots, a_{\phi(q)}$ modulo q. Let $G = \{a_1, \ldots, a_{\phi(q)}\}$. We can now define a character χ on the group G

as described earlier, interpreting the group elements as residue classes. Furthermore, we can extend the definition to cover the remaining residue classes. Precisely, for every $n \in \mathbb{N}$, let

$$\chi(n) = \begin{cases} \chi(a_j) & \text{if } n \equiv a_j \pmod{q} \text{ for some } j = 1, \dots, \phi(q), \\ 0 & \text{if } (n, q) > 1. \end{cases}$$
 (3)

A function $\chi: \mathbb{N} \to \mathbb{C}$ of the form (3) is called a Dirichlet character modulo q. Note that χ is totally multiplicative. Also, clearly there are exactly $\phi(q)$ Dirichlet characters modulo q. Furthermore, the principal Dirichlet character χ_0 modulo q is defined by

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n,q) = 1, \\ 0 & \text{if } (n,q) > 1. \end{cases}$$

The following theorem follows immediately from these observations and Theorem 4.2.

THEOREM 4.3. Suppose that $q \in \mathbb{N}$. Suppose further that χ_0 is the principal Dirichlet character

(i) For every Dirichlet character χ modulo q, we have

$$\sum_{n \pmod{q}} \chi(n) = \begin{cases} \phi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

(ii) For every $n \in \mathbb{N}$, we have

$$\sum_{\chi \pmod{q}} \chi(n) = \begin{cases} \phi(q) & \text{if } n \equiv 1 \pmod{q}, \\ 0 & \text{if } n \not\equiv 1 \pmod{q}. \end{cases}$$

(iii) For every $a \in \mathbb{Z}$ satisfying (a,q) = 1 and for every $n \in \mathbb{N}$, we have

$$\frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \frac{\chi(n)}{\chi(a)} = \begin{cases} 1 & \text{if } n \equiv a \pmod{q}, \\ 0 & \text{if } n \not\equiv a \pmod{q}. \end{cases}$$

4.4. Some Dirichlet Series

Our next task is to introduce the functions analogous to the function (2) earlier. Let $s = \sigma + it \in \mathbb{C}$, where $\sigma, t \in \mathbb{R}$. For $\sigma > 1$, let

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s};\tag{4}$$

furthermore, for any Dirichlet character χ modulo q, let

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}.$$
 (5)

The functions (4) and (5) are called the Riemann zeta function and Dirichlet L-functions respectively. Note that the series are Dirichlet series and converge absolutely for $\sigma > 1$ and uniformly for $\sigma > 1 + \delta$ for any $\delta > 0$. Furthermore, the coefficients are totally multiplicative. It follows from Theorem 3.7 that for $\sigma > 1$, the series (4) and (5) have the Euler product representations

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1}$$
 and $L(s, \chi) = \prod_{p} (1 - \chi(p)p^{-s})^{-1}$

respectively. The following are some simple properties of these functions.

THEOREM 4.4. Suppose that $\sigma > 1$. Then $\zeta(s) \neq 0$. Furthermore, $L(s, \chi) \neq 0$ for every Dirichlet character χ modulo q.

PROOF. Since $\sigma > 1$, we have

$$|\zeta(s)| = \left| \prod_{p} (1 - p^{-s})^{-1} \right| \ge \prod_{p} (1 + p^{-\sigma})^{-1} = \prod_{p} \frac{1 - p^{-\sigma}}{1 - p^{-2\sigma}} = \frac{\zeta(2\sigma)}{\zeta(\sigma)} > 0$$

and

$$|L(s,\chi)| = \left| \prod_{p} (1 - \chi(p)p^{-s})^{-1} \right| \ge \prod_{p\nmid q} (1 + p^{-\sigma})^{-1} \ge \prod_{p} (1 + p^{-\sigma})^{-1} > 0.$$

THEOREM 4.5. Suppose that χ_0 is the principal Dirichlet character modulo q. Then for $\sigma > 1$, we have

$$L(s, \chi_0) = \zeta(s) \prod_{p|q} (1 - p^{-s}).$$

PROOF. Since $\sigma > 1$, we have

$$L(s,\chi_0) = \prod_p (1 - \chi_0(p)p^{-s})^{-1} = \prod_{p \nmid q} (1 - p^{-s})^{-1}$$

$$= \frac{\prod_p (1 - p^{-s})^{-1}}{\prod_{p \mid q} (1 - p^{-s})^{-1}} = \zeta(s) \prod_{p \mid q} (1 - p^{-s}).$$

THEOREM 4.6. Suppose that $\sigma > 1$. Then

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

Furthermore, for every Dirichlet character χ modulo q, we have

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

PROOF. Since $\sigma > 1$, it follows from Theorem 3.2 that

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

It now follows from Theorem 3.5 and

$$\log n = \sum_{m|n} \Lambda(m)$$

that

$$-\zeta'(s) = \left(\sum_{n=1}^{\infty} \Lambda(n) n^{-s}\right) \left(\sum_{n=1}^{\infty} n^{-s}\right).$$

The first assertion follows. On the other hand, it also follows from Theorem 3.2 that

$$-L'(s,\chi) = \sum_{n=1}^{\infty} \chi(n)(\log n)n^{-s}.$$

It now follows from Theorem 3.5 and

$$\chi(n) \log n = \sum_{m|n} \chi(m) \Lambda(m) \chi\left(\frac{n}{m}\right)$$

that

$$-L'(s,\chi) = \left(\sum_{n=1}^{\infty} \chi(n)\Lambda(n)n^{-s}\right) \left(\sum_{n=1}^{\infty} \chi(n)n^{-s}\right).$$

The second assertion follows. ♣

THEOREM 4.7. If $\sigma > 1$, then for every Dirichlet character χ modulo q, we have

$$\log L(s,\chi) = \sum_{p} \sum_{m=1}^{\infty} m^{-1} \chi(p^{m}) p^{-ms}.$$

Taking logarithms on the Euler product representation, we have

$$\log L(s,\chi) = \log \prod_{p} (1 - \chi(p)p^{-s})^{-1} = \sum_{p} \log(1 - \chi(p)p^{-s})^{-1}, \tag{6}$$

so that

$$-\log L(s,\chi) = \sum_{p} \log(1 - \chi(p)p^{-s}).$$

The justification for (6) is that the series on the right hand side converges uniformly for $\sigma > 1 + \delta$, as can be deduced from the Weierstrass M-test on noting that

$$|\log(1-\chi(p)p^{-s})| \le 2|\chi(p)p^{-s}| \le 2p^{-1-\delta}$$
.

The proof is now completed by expanding $\log(1-\chi(p)p^{-s})$.

Analytic Continuation 4.5.

Our next task is to extend the definition of $\zeta(s)$ and $L(s,\chi)$ to the half plane $\sigma>0$. This is achieved by analytic continuation.

An example of analytic continuation is the following: Consider the geometric series

$$f(s) = \sum_{n=0}^{\infty} s^n.$$

This series converges absolutely in the set $\{s \in \mathbb{C} : |s| < 1\}$ and uniformly in the set $\{s \in \mathbb{C} : |s| < 1 - \delta\}$ for any $\delta > 0$ to the sum 1/(1-s). Now let

$$g(s) = \frac{1}{1-s}$$

in \mathbb{C} . Then g is analytic in the set $\mathbb{C} \setminus \{1\}$, g(s) = f(s) in the set $\{s \in \mathbb{C} : |s| < 1\}$, and g has a pole at s=1. So g can be viewed as an analytic continuation of f to $\mathbb C$ with a pole at s=1.

We shall prove the following results on analytic continuation of $\zeta(s)$ and $L(s,\chi)$.

THEOREM 4.8. The function $\zeta(s)$ admits an analytic continuation to the half plane $\sigma > 0$. Furthermore, $\zeta(s)$ is analytic for $\sigma > 0$ except for a simple pole at s = 1 with residue 1.

THEOREM 4.9. Suppose that $q \in \mathbb{N}$ and χ_0 is the principal Dirichlet character modulo q. Then the function $L(s,\chi_0)$ admits an analytic continuation to the half plane $\sigma>0$. Furthermore, $L(s,\chi_0)$ is analytic for $\sigma > 0$ except for a simple pole at s = 1 with residue $\phi(q)/q$.

THEOREM 4.10. Suppose that $q \in \mathbb{N}$ and χ is a non-principal Dirichlet character modulo q. Then the function $L(s,\chi)$ admits an analytic continuation to the half plane $\sigma>0$. Furthermore, $L(s,\chi)$ is analytic for $\sigma > 0$.

The proofs of these three theorems depend on the following two simple technical results. The first of these is basically a result on partial summation.

THEOREM 4.11. Suppose that a(n) = O(1) for every $n \in \mathbb{N}$. For every x > 0, write

$$S(x) = \sum_{n \le x} a(n).$$

Suppose further that for $\sigma > 1$, we have

$$F(s) = \sum_{n=1}^{\infty} a(n)n^{-s}.$$

Then for every X > 0 and $\sigma > 1$, we have

$$\sum_{n \le X} a(n)n^{-s} = S(X)X^{-s} + s \int_1^X S(x)x^{-s-1} \, \mathrm{d}x. \tag{7}$$

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

$$F(s) = s \int_{1}^{\infty} S(x)x^{-s-1} dx.$$
(8)

PROOF. To prove (7), simply note that

$$\sum_{n \le X} a(n)n^{-s} - S(X)X^{-s} = \sum_{n \le X} a(n)(n^{-s} - X^{-s}) = \sum_{n \le X} a(n) \int_{n}^{X} sx^{-s-1} dx$$
$$= s \int_{1}^{X} \left(\sum_{n \le x} a(n)\right) x^{-s-1} dx = s \int_{1}^{X} S(x)x^{-s-1} dx.$$

Also, (8) follows from (7) on letting $X \to \infty$.

The second technical result, standard in complex function theory, will be stated without proof.

THEOREM 4.12. Suppose that the path Γ is defined by w(t) = u(t) + iv(t), where $u(t), v(t) \in \mathbb{R}$ for every $t \in [0,1]$. Suppose further that u'(t) and v'(t) are continuous on [0,1]. Let D be a domain in \mathbb{C} . For every $s \in D$, let

$$F(s) = \int_{\Gamma} f(s, w) \, \mathrm{d}w,$$

where

- (i) f(s, w) is continuous for every $s \in D$ and every $w \in \Gamma$; and
- (ii) for every $w \in \Gamma$, the function f(s, w) is analytic in D.

Then F(s) is analytic in D.

PROOF OF THEOREM 4.8. Let $F(s) = \zeta(s)$. In the notation of Theorem 4.11, we have a(n) = 1 for every $n \in \mathbb{N}$, so that S(x) = [x] for every x > 0. It follows from (8) that

$$\zeta(s) = s \int_{1}^{\infty} [x] x^{-s-1} dx = s \int_{1}^{\infty} x^{-s} dx - s \int_{1}^{\infty} \{x\} x^{-s-1} dx$$
$$= 1 + \frac{1}{s-1} - s \int_{1}^{\infty} \{x\} x^{-s-1} dx.$$

We shall show that the last term on the right hand side represents an analytic function for $\sigma > 0$. We can write

$$\int_{1}^{\infty} \{x\} x^{-s-1} \, \mathrm{d}x = \sum_{n=1}^{\infty} F_n(s),$$

where for every $n \in \mathbb{N}$,

$$F_n(s) = \int_{r}^{r+1} \{x\} x^{-s-1} dx.$$

It remains to show that (i) for every $n \in \mathbb{N}$, the function $F_n(s)$ is analytic in \mathbb{C} ; and (ii) for every $\delta > 0$, the series $\sum_{n=1}^{\infty} F_n(s)$ converges uniformly for $\sigma > \delta$. To show (i), note that by a change of variable,

$$F_n(s) = \int_0^1 t(n+t)^{-s-1} dt = \int_0^1 t e^{-(s+1)\log(n+t)} dt,$$

and (i) follows from Theorem 4.12. To show (ii), note that for $\sigma > \delta$, we have

$$|F_n(s)| = \left| \int_n^{n+1} \{x\} x^{-s-1} \, \mathrm{d}x \right| \le n^{-\sigma - 1} < n^{-1 - \delta},$$

and (ii) follows from the Weierstrass M-test. \clubsuit

PROOF OF THEOREM 4.9. Suppose that $\sigma > 1$. Recall Theorem 4.5, that

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

Clearly the right hand side is analytic for $\sigma > 0$ except for a simple pole at s = 1. Furthermore, at s=1, the function $\zeta(s)$ has a simple pole with residue 1, while

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

The result follows. ♣

The proof of Theorem 4.10 is left as an exercise.

Proof of Dirichlet's Theorem

We now attempt to prove Theorem 4.1. The following theorem will enable us to consider the analogue of (1).

THEOREM 4.13. Suppose that $\sigma > 1$. Then

$$\sum_{p \equiv a \pmod{q}} \frac{\log p}{p^{\sigma}} = \sum_{n \equiv a \pmod{q}} \frac{\Lambda(n)}{n^{\sigma}} + O(1).$$

PROOF. Note first of all that the sum on the left hand side does not exceed the first term on the right hand side. On the other hand, we have

$$\sum_{n \equiv a \pmod{q}} \frac{\Lambda(n)}{n^{\sigma}} - \sum_{p \equiv a \pmod{q}} \frac{\log p}{p^{\sigma}} \le \sum_{p} \sum_{m=2}^{\infty} \frac{\log p}{p^{m\sigma}}$$
$$\le \sum_{p} \sum_{m=2}^{\infty} \frac{\log p}{p^{m}} = \sum_{p} \frac{\log p}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(1).$$

The result follows. ♣

Combining Theorems 4.13, 4.3 and 4.6, we have

$$\sum_{p \equiv a \pmod{q}} \frac{\log p}{p^{\sigma}} = \sum_{n \equiv a \pmod{q}} \Lambda(n) n^{-\sigma} + O(1)$$

$$= \sum_{n=1}^{\infty} \left(\frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \frac{\chi(n)}{\chi(a)} \right) \Lambda(n) n^{-\sigma} + O(1)$$

$$= \frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \frac{1}{\chi(a)} \sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-\sigma} + O(1)$$

$$= -\frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \frac{1}{\chi(a)} \frac{L'(\sigma, \chi)}{L(\sigma, \chi)} + O(1). \tag{9}$$

Suppose now that

$$\sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \frac{1}{\chi(a)} \frac{L'(\sigma, \chi)}{L(\sigma, \chi)} = O(1) \quad \text{as } \sigma \to 1 + . \tag{10}$$

Then combining (9) and (10), as $\sigma \to 1+$, we have

$$\sum_{p=q \pmod{q}} \frac{\log p}{p^{\sigma}} = -\frac{1}{\phi(q)} \frac{L'(\sigma, \chi_0)}{L(\sigma, \chi_0)} + O(1) = \frac{1}{\phi(q)} \frac{1}{\sigma - 1} + O(1) \to \infty,$$

since the function $L'(s,\chi_0)/L(s,\chi_0)$ has a simple pole at s=1 with residue -1 by Theorem 4.9. To complete the proof of Dirichlet's theorem, it remains to prove (10). Clearly (10) will follow if we can show that for every non-principal Dirichlet character $\chi \pmod{q}$, we have $L(1,\chi) \neq 0$. Here we need to distinguish two cases, represented by the following two theorems.

THEOREM 4.14. Suppose that $q \in \mathbb{N}$ and χ is a non-real Dirichlet character modulo q. Then $L(1,\chi) \neq 0$.

PROOF. For $\sigma > 1$, we have, in view of Theorem 4.7, that

$$\sum_{\chi \pmod{q}} \log L(\sigma, \chi) = \sum_{\chi \pmod{q}} \sum_{p} \sum_{m=1}^{\infty} \chi(p^m) m^{-1} p^{-m\sigma}$$

$$= \sum_{p} \sum_{m=1}^{\infty} \left(\sum_{\chi \pmod{q}} \chi(p^m) \right) m^{-1} p^{-m\sigma}$$

$$= \phi(q) \sum_{p} \sum_{\substack{m=1 \ p^m = 1 \pmod{q}}}^{\infty} m^{-1} p^{-m\sigma} > 0,$$

where the change of order of summation is justified since

$$\sum_{\chi \pmod{q}} \sum_{p} \sum_{m=1}^{\infty} |\chi(p^m)m^{-1}p^{-m\sigma}|$$

is finite. It follows that

$$\left| \prod_{\chi \pmod{q}} L(\sigma, \chi) \right| > 1. \tag{11}$$

Suppose that χ_1 is a non-real Dirichlet character modulo q, and $L(1,\chi_1)=0$. Then $\chi_1\neq\overline{\chi_1}$, and $L(1,\overline{\chi_1}) = L(1,\chi_1) = 0$ also. It follows that these two zeros more than cancel the simple pole of $L(\sigma,\chi_0)$ at $\sigma = 1$, so that the product on the left hand side of (11) has a zero at $\sigma = 1$. This gives a contradiction.

Clearly this approach does not work when χ is real.

THEOREM 4.15. Suppose that $q \in \mathbb{N}$ and χ is a real, non-principal Dirichlet character modulo q. Then $L(1,\chi) \neq 0$.

PROOF. Suppose that the result is false, so that there exists a real Dirichlet character χ modulo q such that $L(1,\chi) = 0$. Then the function

$$F(s) = \zeta(s)L(s,\chi)$$

is analytic for $\sigma > 0$. Note that for $\sigma > 1$, we have

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

where for every $n \in \mathbb{N}$,

$$f(n) = \sum_{m|n} \chi(m).$$

Let the function $g: \mathbb{N} \to \mathbb{R}$ be defined by

$$g(n) = \begin{cases} 1 & \text{if } n \text{ is a perfect square,} \\ 0 & \text{otherwise.} \end{cases}$$

We shall first of all show that for every $n \in \mathbb{N}$, we have

$$f(n) \ge g(n). \tag{12}$$

Since χ is totally multiplicative, it suffices to prove (12) when $n=p^k$, where p is a prime and $k \in \mathbb{N}$. Indeed, since χ assumes only the values ± 1 and 0, we have

$$f(p^k) = 1 + \chi(p) + (\chi(p))^2 + \ldots + (\chi(p))^k = \begin{cases} 1 & \text{if } \chi(p) = 0, \\ k+1 & \text{if } \chi(p) = 1, \\ 1 & \text{if } \chi(p) = -1 \text{ and } k \text{ is even,} \\ 0 & \text{if } \chi(p) = -1 \text{ and } k \text{ is odd,} \end{cases}$$

so that

$$f(p^k) \ge g(p^k) = \begin{cases} 1 & \text{if } k \text{ is even,} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

Suppose now that 0 < r < 3/2. Since F(s) is analytic for $\sigma > 0$, we must have the Taylor expansion

$$F(2-r) = \sum_{\nu=0}^{\infty} \frac{F^{(\nu)}(2)}{\nu!} (-r)^{\nu}.$$

Now by Theorem 3.2, we have

$$F^{(\nu)}(2) = \sum_{n=1}^{\infty} f(n)(-\log n)^{\nu} n^{-2}.$$

It follows that for every $\nu \in \mathbb{N} \cup \{0\}$, we have, in view of (12),

$$\frac{F^{(\nu)}(2)}{\nu!}(-r)^{\nu} = \frac{r^{\nu}}{\nu!} \sum_{n=1}^{\infty} f(n)(\log n)^{\nu} n^{-2} \ge \frac{r^{\nu}}{\nu!} \sum_{n=1}^{\infty} g(n)(\log n)^{\nu} n^{-2}$$

$$= \frac{r^{\nu}}{\nu!} \sum_{k=1}^{\infty} (\log k^{2})^{\nu} (k^{2})^{-2} = \frac{(2r)^{\nu}}{\nu!} \sum_{k=1}^{\infty} (\log k)^{\nu} k^{-4}$$

$$= \frac{(-2r)^{\nu}}{\nu!} \sum_{k=1}^{\infty} (-\log k)^{\nu} k^{-4} = \frac{(-2r)^{\nu}}{\nu!} \zeta^{(\nu)}(4)$$

by Theorem 3.2. It follows that for 0 < r < 3/2, we have

$$F(2-r) \ge \sum_{\nu=0}^{\infty} \frac{(-2r)^{\nu}}{\nu!} \zeta^{(\nu)}(4) = \zeta(4-2r).$$

Now as $r \to 3/2-$, we must therefore have $F(2-r) \to +\infty$. This contradicts our assertion that F(s) is analytic for $\sigma > 0$ and hence continuous at s = 1/2.

ELEMENTARY AND ANALYTIC NUMBER THEORY

W W L CHEN

© WWL Chen, 1990.

This work is available free, in the hope that it will be useful.

Any part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, with or without permission from the author.

Chapter 5

DISTRIBUTION OF PRIMES

III: THE PRIME NUMBER THEOREM

5.1. Some Preliminary Remarks

In this chapter, we give an analytic proof of the famous Prime number theorem, a result first obtained in 1896 independently by Hadamard and de la Vallée Poussin.

THEOREM 5.1. As $X \to \infty$, we have

$$\pi(X) \sim \frac{X}{\log X}.$$

As in our earlier study of the distribution of primes, we use the von Mangoldt function Λ . For every X>0, let

$$\psi(X) = \sum_{n \le X} \Lambda(n).$$

THEOREM 5.2. As $X \to \infty$, we have

$$\psi(X) \sim X$$
 if and only if $\pi(X) \sim \frac{X}{\log X}$.

[†] This chapter was first used in lectures given by the author at Imperial College, University of London, in 1990.

PROOF. Recall the proof of Theorem 2.5 due to Tchebycheff. We have

$$\psi(X) = \sum_{n \le X} \Lambda(n) = \sum_{\substack{p,k \\ p^k \le X}} \log p = \sum_{\substack{p \le X}} (\log p) \sum_{1 \le k \le \frac{\log X}{\log p}} 1$$
$$= \sum_{\substack{p \le X}} (\log p) \left[\frac{\log X}{\log p} \right] \le \pi(X) \log X. \tag{1}$$

On the other hand, for any $\alpha \in (0,1)$, we have

$$\psi(X) \ge \sum_{p \le X} \log p \ge \sum_{X^{\alpha}
$$= \alpha(\pi(X) - \pi(X^{\alpha})) \log X. \tag{2}$$$$

Combining (1) and (2), we have

$$\alpha \frac{\pi(X)}{X/\log X} - \alpha \frac{\pi(X^{\alpha})}{X/\log X} \le \frac{\psi(X)}{X} \le \frac{\pi(X)}{X/\log X}.$$
 (3)

Since $\alpha < 1$, it follows from Tchebycheff's theorem that as $X \to \infty$, we have

$$\frac{\pi(X^{\alpha})}{X/\log X} \to 0.$$

Suppose that as $X \to \infty$, we have $\pi(X) \sim X/\log X$. Then as $X \to \infty$, we have

$$\alpha \frac{\pi(X)}{X/\log X} - \alpha \frac{\pi(X^{\alpha})}{X/\log X} \to \alpha.$$

It follows that for any $\epsilon > 0$, the inequality

$$\alpha - \epsilon \le \frac{\psi(X)}{X} \le 1 + \epsilon$$

holds for all large X. Since $\alpha < 1$ is arbitrary, we must have

$$\frac{\psi(X)}{X} \to 1$$

as $X \to \infty$.

Note next that the inequalities (3) can be rewritten as

$$\frac{\psi(X)}{X} \le \frac{\pi(X)}{X/\log X} \le \frac{1}{\alpha} \frac{\psi(X)}{X} + \frac{\pi(X^{\alpha})}{X/\log X}.$$

Suppose that as $X \to \infty$, we have $\psi(X) \sim X$. Then a similar argument gives

$$\frac{\pi(X)}{X/\log X} \to 1$$

as $X \to \infty$.

A Smoothing Argument

To prove the Prime number theorem, it suffices to show that as $X \to \infty$, we have $\psi(X) \sim X$. However, a direct discussion of $\psi(X)$ introduces various tricky convergence problems. We therefore consider a smooth average of the function ψ . For X > 0, let

$$\psi_1(X) = \int_0^X \psi(x) \, \mathrm{d}x. \tag{4}$$

THEOREM 5.3. Suppose that as $X \to \infty$, we have $\psi_1(X) \sim \frac{1}{2}X^2$. Then as $X \to \infty$, we have $\psi(X) \sim X$.

PROOF. Suppose that $0 < \alpha < 1 < \beta$. Since $\Lambda(n) \ge 0$ for every $n \in \mathbb{N}$, the function ψ is an increasing function. Hence for every X > 0, we have

$$\psi(X) \le \frac{1}{\beta X - X} \int_X^{\beta X} \psi(x) \, \mathrm{d}x = \frac{\psi_1(\beta X) - \psi_1(X)}{(\beta - 1)X},$$

so that

$$\frac{\psi(X)}{X} \le \frac{\psi_1(\beta X) - \psi_1(X)}{(\beta - 1)X^2}.$$
 (5)

On the other hand, for every X > 0, we have

$$\psi(X) \ge \frac{1}{X - \alpha X} \int_{\alpha X}^{X} \psi(x) \, \mathrm{d}x = \frac{\psi_1(X) - \psi_1(\alpha X)}{(1 - \alpha)X},$$

so that

$$\frac{\psi(X)}{X} \ge \frac{\psi_1(X) - \psi_1(\alpha X)}{(1 - \alpha)X^2}.$$
(6)

As $X \to \infty$, we have

$$\frac{\psi_1(\beta X) - \psi_1(X)}{(\beta - 1)X^2} \sim \frac{1}{\beta - 1} \left(\frac{1}{2}\beta^2 - \frac{1}{2}\right) = \frac{1}{2}(\beta + 1) \tag{7}$$

and

$$\frac{\psi_1(X) - \psi_1(\alpha X)}{(1 - \alpha)X^2} \sim \frac{1}{1 - \alpha} \left(\frac{1}{2} - \frac{1}{2}\alpha^2\right) = \frac{1}{2}(\alpha + 1). \tag{8}$$

Since α and β are arbitrary, we conclude, on combining (5)–(8), that as $X \to \infty$, we have $\psi(X)/X \sim 1$.

The rest of this chapter is concerned with establishing the following crucial result.

THEOREM 5.4. As $X \to \infty$, we have

$$\psi_1(X) \sim \frac{1}{2}X^2.$$

A Contour Integral

The following theorem provides a link between $\psi_1(X)$ and the Riemann zeta function $\zeta(s)$.

THEOREM 5.5. Suppose that X > 0 and c > 1. Then

$$\psi_1(X) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{X^{s+1}}{s(s+1)} \frac{\zeta'(s)}{\zeta(s)} ds,$$

where the path of integration is the straight line $\sigma = c$.

A crucial step in the proof of Theorem 5.5 is provided by the following result concerning a particular contour integral.

THEOREM 5.6. Suppose that X > 0 and c > 1. Then

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{X^s}{s(s+1)} ds = \begin{cases} 0 & (X \le 1), \\ 1 - \frac{1}{X} & (X \ge 1). \end{cases}$$

PROOF. Note first of all that the integral is absolutely convergent, as

$$\left| \frac{X^s}{s(s+1)} \right| \le \frac{X^c}{|t|^2}$$

whenever $\sigma = c$. Let T > 1, and write

$$I_T = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{X^s}{s(s+1)} ds.$$

Suppose first of all that $X \geq 1$. Let $A^{-}(c,T)$ denote the circular arc centred at s=0 and passing from c - iT to c + iT on the left of the line $\sigma = c$. Furthermore, let

$$J_T^- = \frac{1}{2\pi i} \int_{A^-(c,T)} \frac{X^s}{s(s+1)} ds.$$

Note that on $A^-(c,T)$, we have $|X^s|=X^\sigma\leq X^c$ since $X\geq 1$; also we have |s|=R and $|s+1|\geq R-1$, where $R=(c^2+T^2)^{1/2}$ is the radius of $A^-(c,T)$. It follows that

$$|J_T^-| \le \frac{1}{2\pi} \frac{X^c}{R(R-1)} 2\pi R \le \frac{X^c}{T-1} \to 0 \text{ as } T \to \infty.$$

By Cauchy's residue theorem, we have

$$I_T = J_T^- + \text{res}\left(\frac{X^s}{s(s+1)}, 0\right) + \text{res}\left(\frac{X^s}{s(s+1)}, -1\right) = J_T^- + 1 - \frac{1}{X}.$$

The result for $X \geq 1$ follows on letting $T \to \infty$.

Suppose now that $X \leq 1$. Let $A^+(c,T)$ denote the circular arc centred at s=0 and passing from c-iT to c+iT on the right of the line $\sigma=c$. Furthermore, let

$$J_T^+ = \frac{1}{2\pi i} \int_{A^+(c,T)} \frac{X^s}{s(s+1)} ds.$$

Note that on $A^+(c,T)$, we have $|X^s|=X^\sigma\leq X^c$ since $X\leq 1$; also we have |s|=R and $|s+1|\geq R$, where $R = (c^2 + T^2)^{1/2}$ is the radius of $A^+(c,T)$. It follows that

$$|J_T^+| \le \frac{1}{2\pi} \frac{X^c}{R^2} 2\pi R \le \frac{X^c}{T} \to 0 \text{ as } T \to \infty.$$

By Cauchy's residue theorem, we have

$$I_T = J_T^+$$
.

The result for $X \leq 1$ follows on letting $T \to \infty$.

PROOF OF THEOREM 5.5. Note that for $X \ge 1$, we have

$$\psi_1(X) = \int_0^X \psi(x) \, \mathrm{d}x = \int_1^X \psi(x) \, \mathrm{d}x = \int_1^X \left(\sum_{n \le x} \Lambda(n) \right) \mathrm{d}x = \sum_{n \le X} (X - n) \Lambda(n),$$

the last equality following from interchanging the order of integration and summation. Note also that the above conclusion holds trivially if 0 < X < 1. It therefore follows from Theorem 5.6 that for every X > 0, we have

$$\frac{\psi_1(X)}{X} = \sum_{n \le X} \left(1 - \frac{n}{X} \right) \Lambda(n) = \sum_{n \le X} \left(1 - \frac{1}{X/n} \right) \Lambda(n)$$
$$= \sum_{n \le X} \frac{\Lambda(n)}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{(X/n)^s}{s(s+1)} ds,$$

where c > 1. Since c > 1, the order of summation and integration can be interchanged, as

$$\sum_{n=1}^{\infty} \int_{c-i\infty}^{c+i\infty} \left| \frac{\Lambda(n)(X/n)^s}{s(s+1)} \right| |\mathrm{d}s| \le X^c \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^c} \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{c^2 + t^2}$$

is finite. It follows that

$$\frac{\psi_1(X)}{X} = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{X^s}{s(s+1)} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} ds = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{X^s}{s(s+1)} \frac{\zeta'(s)}{\zeta(s)} ds$$

as required.

The Riemann Zeta Function

Recall first of all Theorem 4.11. In the case of the Riemann zeta function, equation (7) of Chapter 4 becomes

$$\sum_{n \le X} n^{-s} = s \int_{1}^{X} [x] x^{-s-1} dx + [X] X^{-s}$$

$$= s \int_{1}^{X} x^{-s} dx - s \int_{1}^{X} \{x\} x^{-s-1} dx + X^{-s+1} - \{X\} X^{-s}$$

$$= \frac{s}{s-1} - \frac{s}{(s-1)X^{s-1}} - s \int_{1}^{X} \frac{\{x\}}{x^{s+1}} dx + \frac{1}{X^{s-1}} - \frac{\{X\}}{X^{s}}.$$
(9)

Letting $X \to \infty$, we deduce that

$$\zeta(s) = \frac{s}{s-1} - s \int_{1}^{\infty} \frac{\{x\}}{x^{s+1}} dx$$
 (10)

if $\sigma > 1$. Recall also that (10) gives an analytic continuation of $\zeta(s)$ to $\sigma > 0$, with s simple pole at s=1. We shall use these formulae to deduce important information about the order of magnitude of $|\zeta(s)|$ in the neighbourhood of the line $\sigma=1$ and to the left of it. Note that $\zeta(\sigma+it)$ and $\zeta(\sigma-it)$ are complex conjugates, so it suffices to study $\zeta(s)$ on the upper half plane.

THEOREM 5.7. For every $\sigma \geq 1$ and $t \geq 2$, we have

- (i) $|\zeta(s)| = O(\log t)$; and (ii) $|\zeta'(s)| = O(\log^2 t)$.

Suppose further that $0 < \delta < 1$. Then for every $\sigma \ge \delta$ and $t \ge 1$, we have (iii) $|\zeta(s)| = O_{\delta}(t^{1-\delta}).$

PROOF. For $\sigma > 0$, $t \ge 1$ and $X \ge 1$, we have, by (9) and (10), that

$$\zeta(s) - \sum_{n \le X} \frac{1}{n^s} = \frac{s}{(s-1)X^{s-1}} - \frac{1}{X^{s-1}} + \frac{\{X\}}{X^s} - s \int_X^\infty \frac{\{x\}}{x^{s+1}} dx$$
$$= \frac{1}{(s-1)X^{s-1}} + \frac{\{X\}}{X^s} - s \int_Y^\infty \frac{\{x\}}{x^{s+1}} dx. \tag{11}$$

It follows that

$$|\zeta(s)| \leq \sum_{n \leq X} \frac{1}{n^{\sigma}} + \frac{1}{tX^{\sigma - 1}} + \frac{1}{X^{\sigma}} + |s| \int_{X}^{\infty} \frac{\mathrm{d}x}{x^{\sigma + 1}}$$

$$\leq \sum_{n \leq X} \frac{1}{n^{\sigma}} + \frac{1}{tX^{\sigma - 1}} + \frac{1}{X^{\sigma}} + \left(1 + \frac{t}{\sigma}\right) \frac{1}{X^{\sigma}}.$$
(12)

If $\sigma \geq 1$, $t \geq 1$ and $X \geq 1$, then

$$|\zeta(s)| \le \sum_{n \le X} \frac{1}{n} + \frac{1}{t} + \frac{1}{X} + \frac{1+t}{X} \le (\log X + 1) + 3 + \frac{t}{X}.$$

Choosing X = t, we obtain

$$|\zeta(s)| \le (\log t + 1) + 4 = O(\log t),$$

proving (i). On the other hand, if $\sigma \geq \delta$, $t \geq 1$ and $X \geq 1$, then it follows from (12) that

$$\begin{aligned} |\zeta(s)| &\leq \sum_{n \leq X} \frac{1}{n^{\delta}} + \frac{1}{tX^{\delta - 1}} + \left(2 + \frac{t}{\delta}\right) \frac{1}{X^{\delta}} \\ &\leq \int_{0}^{[X]} \frac{\mathrm{d}x}{x^{\delta}} + \frac{X^{1 - \delta}}{t} + \frac{3t}{\delta X^{\delta}} \leq \frac{X^{1 - \delta}}{1 - \delta} + X^{1 - \delta} + \frac{3t}{\delta X^{\delta}}. \end{aligned}$$

Again choosing X = t, we obtain

$$|\zeta(s)| \le t^{1-\delta} \left(\frac{1}{1-\delta} + 1 + \frac{3}{\delta} \right), \tag{13}$$

proving (iii). To deduce (ii), we may differentiate (11) with respect to s and proceed in a similar way. Alternatively, suppose that $s_0 = \sigma_0 + it_0$ satisfies $\sigma_0 \ge 1$ and $t_0 \ge 2$. Let C be the circle with centre s_0 and radius $\rho < 1/2$. Then

$$|\zeta'(s_0)| = \left| \frac{1}{2\pi i} \int_C \frac{\zeta(s)}{(s - s_0)^2} \, \mathrm{d}s \right| \le \frac{M}{\rho},$$

where $M = \sup_{s \in C} |\zeta(s)|$. Now for every $s \in C$, we clearly have $\sigma \geq \sigma_0 - \rho \geq 1 - \rho$ and $2t_0 > t \geq 1 - \rho$ $t_0 - \rho > 1$. It follows from (13) that for every $s \in C$, we must have $(\delta = 1 - \rho)$

$$|\zeta(s)| \le (2t_0)^{\rho} \left(\frac{1}{\rho} + 1 + \frac{3}{1-\rho}\right) \le \frac{10t_0^{\rho}}{\rho},$$

since $\rho < 1/2 < 1 - \rho < 1$. It follows that

$$|\zeta'(s_0)| \le \frac{10t_0^{\rho}}{\rho^2}.$$

We now take $\rho = (\log t_0 + 2)^{-1}$. Then $t_0^{\rho} = e^{\rho \log t_0} < e$, and so

$$|\zeta'(s_0)| < 10e(\log t_0 + 2)^2.$$

(ii) now follows. ♣

THEOREM 5.8. The function $\zeta(s)$ has no zeros on the line $\sigma = 1$. Furthermore, there is a positive constant A such that as $t \to \infty$, we have, for $\sigma \ge 1$, that

$$\frac{1}{\zeta(s)} = O\left((\log t)^A\right).$$

PROOF. For every $\theta \in \mathbb{R}$, we clearly have

$$3 + 4\cos\theta + \cos 2\theta = 2(1 + \cos\theta)^2 > 0. \tag{14}$$

On the other hand, it is easy to check that for $\sigma > 1$, we have

$$\log \zeta(s) = \sum_{p} \sum_{m=1}^{\infty} \frac{1}{mp^{ms}},$$

so that

$$\log|\zeta(\sigma + it)| = \Re\left(\sum_{n=2}^{\infty} c_n n^{-\sigma - it}\right) = \sum_{n=2}^{\infty} c_n n^{-\sigma} \cos(t \log n), \tag{15}$$

where

$$c_n = \begin{cases} 1/m & (n = p^m, \text{ where } p \text{ is prime and } m \in \mathbb{N}), \\ 0 & (\text{otherwise}). \end{cases}$$
 (16)

Combining (14)–(16), we have

$$\log|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| = \sum_{n=2}^{\infty} c_n n^{-\sigma} (3 + 4\cos(t\log n) + \cos(2t\log n)) \ge 0.$$

It follows that for $\sigma > 1$, we have

$$|(\sigma - 1)\zeta(\sigma)|^3 \left| \frac{\zeta(\sigma + it)}{\sigma - 1} \right|^4 |\zeta(\sigma + 2it)| \ge \frac{1}{\sigma - 1}.$$
 (17)

Suppose that the point s = 1 + it is a zero of $\zeta(s)$. Then since $\zeta(s)$ is analytic at the points s = 1 + itand s = 1 + 2it and has a simple pole with residue 1 at s = 1, the left hand side of (17) must converge to a finite limit as $\sigma \to 1+$, contradicting the fact that the right hand side diverges to infinity as $\sigma \to 1+$. Hence s = 1 + it cannot be a zero of $\zeta(s)$. To prove the second assertion, we may assume without loss of generality that $1 \le \sigma \le 2$, since for $\sigma \ge 2$, we have

$$\left| \frac{1}{\zeta(s)} \right| = \left| \prod_{p} (1 - p^{-s}) \right| \le \prod_{p} (1 + p^{-\sigma}) < \zeta(\sigma) \le \zeta(2).$$

Suppose now that $1 < \sigma \le 2$ and $t \ge 2$. Then by (17), we have

$$(\sigma - 1)^3 \le |(\sigma - 1)\zeta(\sigma)|^3 |\zeta(\sigma + it)|^4 |\zeta(\sigma + 2it)| \le A_1 |\zeta(\sigma + it)|^4 \log(2t)$$

by Theorem 5.7(i), where A_1 is a positive absolute constant. Since $\log(2t) \leq 2 \log t$, it follows that

$$|\zeta(\sigma + it)| \ge \frac{(\sigma - 1)^{3/4}}{A_2(\log t)^{1/4}},$$
(18)

where A_2 is a positive absolute constant. Note that (18) holds also when $\sigma = 1$. Suppose now that $1 < \eta < 2$. If $1 \le \sigma \le \eta$ and $t \ge 2$, then it follows from Theorem 5.7(ii) that

$$|\zeta(\sigma + it) - \zeta(\eta + it)| = \left| \int_{\sigma}^{\eta} \zeta'(x + it) dx \right| \le A_3(\eta - 1) \log^2 t,$$

where A_3 is a positive absolute constant. Combining this with (18), we have

$$|\zeta(\sigma + it)| \ge |\zeta(\eta + it)| - A_3(\eta - 1)\log^2 t \ge \frac{(\eta - 1)^{3/4}}{A_2(\log t)^{1/4}} - A_3(\eta - 1)\log^2 t. \tag{19}$$

On the other hand, if $\eta \le \sigma \le 2$ and $t \ge 2$, then in view of (18), the inequality (19) must also hold. It follows that inequality (19) holds if $1 \le \sigma \le 2$, $t \ge 2$ and $1 < \eta < 2$. We now choose η so that

$$\frac{(\eta - 1)^{3/4}}{A_2(\log t)^{1/4}} = 2A_3(\eta - 1)\log^2 t;$$

in other words,

$$\eta = 1 + (2A_2A_3)^{-4}(\log t)^{-9},$$

where $t > t_0$ so that $\eta < 2$. Then

$$|\zeta(\sigma + it)| \ge A_3(\eta - 1)\log^2 t = A_4(\log t)^{-7}$$

for $1 < \sigma < 2$ and $t > t_0$.

5.5. Completion of the Proof

We are now ready to complete the proof of Theorem 5.4. By Theorem 5.5, we have

$$\frac{\psi_1(X)}{X^2} = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} G(s) X^{s-1} ds,$$
 (20)

where c > 1 and X > 0, and where

$$G(s) = -\frac{1}{s(s+1)} \frac{\zeta'(s)}{\zeta(s)} = -\frac{1}{s(s+1)} \zeta'(s) \frac{1}{\zeta(s)}.$$

By Theorems 4.8, 5.7 and 5.8, we know that G(s) is analytic for $\sigma \geq 1$, except at s = 1, and that for some positive absolute constant A, we have

$$G(s) = O\left(|t|^{-2}(\log|t|)^2(\log|t|)^A\right) < |t|^{-3/2}$$
(21)

for all $|t| > t_0$. Let $\epsilon > 0$ be given. We now consider a contour made up of the straight line segments

$$\begin{cases} L_1 = [1 - \mathrm{i}U, 1 - \mathrm{i}T], \\ L_2 = [1 - \mathrm{i}T, \alpha - \mathrm{i}T], \\ L_3 = [\alpha - \mathrm{i}T, \alpha + \mathrm{i}T], \\ L_4 = [\alpha + \mathrm{i}T, 1 + \mathrm{i}T], \\ L_5 = [1 + \mathrm{i}T, 1 + \mathrm{i}U], \end{cases}$$

where $T = T(\epsilon) > \max\{t_0, 2\}$, $\alpha = \alpha(T) = \alpha(\epsilon) \in (0, 1)$ and U are chosen to satisfy the following conditions:

(i) We have

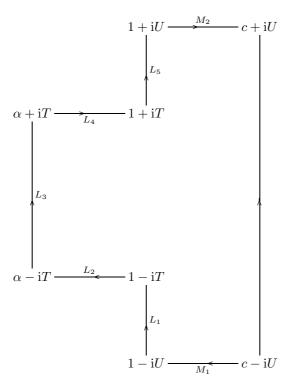
$$\int_{T}^{\infty} |G(1+it)| dt < \epsilon.$$

- (ii) The rectangle $[\alpha, 1] \times [-T, T]$ contains no zeros of $\zeta(s)$. Note that this is possible since $\zeta(s)$ has no zeros on the line $\sigma = 1$ and, as an analytic function, has at most a finite number of zeros in the region $[1/2, 1) \times [-T, T]$.
 - (iii) We have U > T.

Furthermore, define the straight line segments

$$\begin{cases} M_1 = [c - iU, 1 - iU], \\ M_2 = [1 + iU, c + iU]. \end{cases}$$

The above contours are indicated in the diagram below:



By Cauchy's residue theorem, we have

$$\frac{1}{2\pi i} \int_{c-iU}^{c+iU} G(s) X^{s-1} ds = \frac{1}{2\pi i} \sum_{j=1}^{2} \int_{M_j} G(s) X^{s-1} ds
+ \frac{1}{2\pi i} \sum_{j=1}^{5} \int_{L_j} G(s) X^{s-1} ds + \operatorname{res}(G(s) X^{s-1}, 1), \tag{22}$$

where, for every X > 1, we have

$$res(G(s)X^{s-1}, 1) = \frac{1}{2}. (23)$$

Now

$$\left| \int_{L_1} G(s) X^{s-1} \, \mathrm{d}s \right| = \left| \int_{L_5} G(s) X^{s-1} \, \mathrm{d}s \right| \le \int_T^\infty |G(1+\mathrm{i}t)| \, \mathrm{d}t < \epsilon.$$
 (24)

On the other hand.

$$\left| \int_{L_2} G(s) X^{s-1} \, \mathrm{d}s \right| = \left| \int_{L_4} G(s) X^{s-1} \, \mathrm{d}s \right| \le M \int_{\alpha}^1 X^{\sigma-1} \, \mathrm{d}\sigma \le \frac{M}{\log X}$$
 (25)

and

$$\left| \int_{L_3} G(s) X^{s-1} \, \mathrm{d}s \right| \le 2T M X^{\alpha - 1},\tag{26}$$

where

$$M = M(\alpha, T) = M(\epsilon) = \sup_{L_2 \cup L_3 \cup L_4} |G(s)|.$$
 (27)

Furthermore, by (21), we have, for j = 1, 2,

$$\left| \int_{M_j} G(s) X^{s-1} \, \mathrm{d}s \right| \le \int_1^c |U|^{-3/2} X^{\sigma - 1} \, \mathrm{d}\sigma \le \frac{X^{c-1}}{\log X} |U|^{-3/2}. \tag{28}$$

Combining (22)–(28), we have

$$\left| \frac{1}{2\pi \mathrm{i}} \int_{c-\mathrm{i}U}^{c+\mathrm{i}U} G(s) X^{s-1} \, \mathrm{d}s - \frac{1}{2} \right| \leq \frac{\epsilon}{\pi} + \frac{M}{\pi \log X} + \frac{TM}{\pi X^{1-\alpha}} + \frac{X^{c-1} |U|^{-3/2}}{\pi \log X}.$$

On letting $U \to \infty$, we have

$$\left|\frac{\psi_1(X)}{X^2} - \frac{1}{2}\right| \le \frac{\epsilon}{\pi} + \frac{M}{\pi \log X} + \frac{TM}{\pi X^{1-\alpha}}.$$

It clearly follows that as $X \to \infty$, we have

$$\frac{\psi_1(X)}{X^2} \to \frac{1}{2}.$$

ELEMENTARY AND ANALYTIC NUMBER THEORY

W W L CHEN

(c) W W L Chen, 1990.

This work is available free, in the hope that it will be useful.

Any part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, with or without permission from the author.

Chapter 6

THE RIEMANN ZETA FUNCTION

6.1. Riemann's Memoir

In Riemann's only paper on number theory, published in 1860, he proved the following result.

THEOREM 6.1. The function $\zeta(s)$ can be continued analytically over the whole plane, and satisfies the functional equation

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

where Γ denotes the gamma function. In particular, $\zeta(s)$ is analytic everywhere, except for a simple pole at s=1 with residue 1.

Note that the functional equation (1) enables properties of $\zeta(s)$ for $\sigma < 0$ to be inferred from properties of $\zeta(s)$ for $\sigma > 1$. In particular, the only zeros of $\zeta(s)$ for $\sigma < 0$ are at the poles of $\Gamma(s/2)$; in other words, at the points $s = -2, -4, -6, \ldots$ These are called the trivial zeros of $\zeta(s)$.

The part of the plane with $0 \le \sigma \le 1$ is called the critical strip.

Riemann's paper is particularly remarkable in the conjectures it contains. While most of the conjectures have been proved, the famous Riemann hypothesis has so far resisted all attempts to prove or disprove it.

THEOREM 6.2. (Hadamard 1893) The function $\zeta(s)$ has infinitely many zeros in the critical strip.

It is easy to see that the zeros of $\zeta(s)$ in the critical strip are placed symmetrically with respect to the line t=0 as well as with respect to the line $\sigma=1/2$, the latter observation being a consequence of the functional equation (1).

[†] This chapter was first used in lectures given by the author at Imperial College, University of London, in 1990.

THEOREM 6.3. (von Mangoldt 1905) Let N(T) denote the number of zeros $\rho = \beta + i\gamma$ of the function $\zeta(s)$ in the critical strip with $0 < \gamma \le T$. Then

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

THEOREM 6.4. (Hadamard 1893) The entire function

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) \tag{3}$$

has the product representation

$$\xi(s) = e^{A+Bs} \prod_{\rho} \left(1 - \frac{s}{\rho} \right) e^{s/\rho}, \tag{4}$$

where A and B are constants and where ρ runs over all the zeros of $\zeta(s)$ in the critical strip.

We comment here that the product representation (4) plays an important role in the first proof of the Prime number theorem.

The most remarkable of Riemann's conjectures is an explicit formula for the difference $\pi(X) - \text{li}(X)$, containing a term which is a sum over the zeros of $\zeta(s)$ in the critical strip. This shows that the zeros of $\zeta(s)$ plays a crucial role in the study of the distribution of primes. Here we state a result closely related to this formula.

THEOREM 6.5. (von Mangoldt 1895) Let

$$\psi(X) = \sum_{n \le X} \Lambda(n)$$
 and $\psi_0(X) = \frac{\psi(X-0) + \psi(X+0)}{2}$.

Then

$$\psi_0(X) - X = -\sum_{\rho} \frac{X^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2} \log\left(1 - \frac{1}{X^2}\right),$$

where the terms in the sum arising from complex conjugates are taken together.

However, there remains one of Riemann's conjectures which is still unsolved today. The open question below is arguably the most famous unsolved problem in the whole of mathematics.

CONJECTURE. (Riemann Hypothesis) The zeros of the function $\zeta(s)$ in the critical strip all lie on the line $\sigma = 1/2$.

Riemann's Proof of Theorem 6.1 **6.2**.

Suppose that $\sigma > 0$. Writing $t = n^2 \pi x$, we have

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty t^{s/2-1} \mathrm{e}^{-t} \, \mathrm{d}t = (n^2 \pi)^{s/2} \int_0^\infty x^{s/2-1} \mathrm{e}^{-n^2 \pi x} \, \mathrm{d}x,$$

so that

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

It follows that for $\sigma > 1$, we have

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \sum_{n=1}^{\infty} \int_{0}^{\infty} x^{s/2-1} e^{-n^2\pi x} dx = \int_{0}^{\infty} x^{s/2-1} \left(\sum_{n=1}^{\infty} e^{-n^2\pi x}\right) dx,$$

where the change of order of summation and integration is justified by the convergence of

$$\sum_{n=1}^{\infty} \int_0^{\infty} x^{\sigma/2 - 1} e^{-n^2 \pi x} dx.$$

Now write

$$\omega(x) = \sum_{n=1}^{\infty} e^{-n^2 \pi x}.$$

Then for $\sigma > 1$, we have

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_{1}^{\infty} x^{s/2-1}\omega(x) \,dx + \int_{0}^{1} y^{s/2-1}\omega(y) \,dy$$
$$= \int_{1}^{\infty} x^{s/2-1}\omega(x) \,dx + \int_{1}^{\infty} x^{-s/2-1}\omega(x^{-1}) \,dx. \tag{5}$$

We shall show that the function

$$\theta(x) = \sum_{n=-\infty}^{\infty} e^{-n^2 \pi x} = 1 + 2\omega(x)$$

satisfies the functional equation

$$\theta(x^{-1}) = x^{1/2}\theta(x) \tag{6}$$

for every x > 0. It then follows that

$$2\omega(x^{-1}) = \theta(x^{-1}) - 1 = x^{1/2}\theta(x) - 1 = -1 + x^{1/2} + 2x^{1/2}\omega(x),$$

so that for $\sigma > 1$, we have

$$\int_{1}^{\infty} x^{-s/2-1} \omega(x^{-1}) \, \mathrm{d}x = \int_{1}^{\infty} x^{-s/2-1} \left(-\frac{1}{2} + \frac{1}{2} x^{1/2} + x^{1/2} \omega(x) \right) \, \mathrm{d}x$$
$$= \frac{1}{s(s-1)} + \int_{1}^{\infty} x^{-s/2-1/2} \omega(x) \, \mathrm{d}x. \tag{7}$$

It follows on combining (5) and (7) that for $\sigma > 1$, we have

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s(s-1)} + \int_{1}^{\infty} \left(x^{s/2-1} + x^{-s/2-1/2}\right)\omega(x) \,\mathrm{d}x. \tag{8}$$

Note now that the integral on the right hand side of (8) converges absolutely for any s, and uniformly in any bounded part of the plane, since $\omega(x) = O(e^{-\pi x})$ as $x \to +\infty$. Hence the integral represents an entire function of s, and the formula gives the analytic continuation of $\zeta(s)$ over the whole plane. Note also that the right hand side of (8) remains unchanged when s is replaced by 1-s, so that the functional equation (1) follows immediately. Finally, note that the function

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

is analytic everywhere. Since $s\Gamma(s/2)$ has no zeros, the only possible pole of $\zeta(s)$ is at s=1, and we have already shown earlier that $\zeta(s)$ has a simple pole at s=1 with residue 1.

It remains to establish (6) for every x > 0. In other words, we need to prove that for every x > 0, we have

$$\sum_{n=-\infty}^{\infty} e^{-n^2 \pi/x} = x^{1/2} \sum_{n=-\infty}^{\infty} e^{-n^2 \pi x}.$$

The starting point is the Poisson summation formula, that under certain conditions on a function f(t), we have

$$\sum_{A \le n \le B}' f(n) = \sum_{\nu = -\infty}^{\infty} \int_{A}^{B} f(t) e^{2\pi i \nu t} dt,$$

$$\tag{9}$$

where \sum' denotes that the terms in the sum corresponding to n=A and n=B are $\frac{1}{2}f(A)$ and $\frac{1}{2}f(B)$ respectively. Using (9) with A=-N, B=N and $f(t)=\mathrm{e}^{-t^2\pi/x}$, we have

$$\sum_{n=-N}^{N'} e^{-n^2 \pi/x} = \sum_{\nu=-\infty}^{\infty} \int_{-N}^{N} e^{-t^2 \pi/x} e^{2\pi i \nu t} dt.$$

Letting $N \to \infty$, we obtain

$$\sum_{n=-\infty}^{\infty} e^{-n^2 \pi/x} = \sum_{\nu=-\infty}^{\infty} \int_{-\infty}^{\infty} e^{-t^2 \pi/x} e^{2\pi i \nu t} dt.$$
 (10)

This is justified by noting that

$$\left(\int_{-\infty}^{-N} + \int_{N}^{\infty}\right) e^{-t^2 \pi/x} e^{2\pi i \nu t} dt = 2 \int_{N}^{\infty} e^{-t^2 \pi/x} \cos(2\pi \nu t) dt,$$

and that

$$\left| \sum_{\nu \neq 0} \int_{N}^{\infty} e^{-t^2 \pi/x} \cos(2\pi \nu t) dt \right| \to 0$$

as $N \to \infty$. Writing t = xu and using (10), we have

$$\sum_{n=-\infty}^{\infty} e^{-n^2 \pi/x} = x \sum_{\nu=-\infty}^{\infty} \int_{-\infty}^{\infty} e^{-u^2 \pi x} e^{2\pi i \nu x u} du$$

$$= x \sum_{\nu=-\infty}^{\infty} \int_{-\infty}^{\infty} e^{-(u-i\nu)^2 \pi x - \nu^2 \pi x} du$$

$$= x \sum_{\nu=-\infty}^{\infty} e^{-\nu^2 \pi x} \int_{-\infty}^{\infty} e^{-(u-i\nu)^2 \pi x} du.$$
(11)

Note now that the function $e^{-z^2\pi x}$ is an entire function of the complex variable z. It follows from Cauchy's residue theorem that

$$\int_{-\infty}^{\infty} e^{-(u-i\nu)^2 \pi x} du = \int_{-\infty}^{\infty} e^{-u^2 \pi x} du = Ax^{-1/2},$$
(12)

where

$$A \int_{-\infty}^{\infty} e^{-y^2 \pi} dy = 1.$$
 (13)

Combining (11)–(13), we conclude that

$$\sum_{n=-\infty}^{\infty} e^{-n^2 \pi/x} = x^{1/2} \sum_{\nu=-\infty}^{\infty} e^{-\nu^2 \pi x}.$$

This gives (6), and the proof of Theorem 6.1 is now complete.

6.3. **Entire Functions**

In this section, we shall prove some technical results on entire functions for use later in the proof of Theorems 6.2 and 6.4.

An entire function f(s) is said to be of order 1 if

$$f(s) = O_{\alpha} \left(e^{|s|^{\alpha}} \right) \quad \text{as } |s| \to \infty$$
 (14)

holds for every $\alpha > 1$ and fails for every $\alpha < 1$.

Suppose that the entire function h(s) has no zeros on the plane. Then the function $g(s) = \log h(s)$ can be defined as a single valued function and is also entire. Suppose that

$$h(s) = O_{\alpha} \left(e^{|s|^{\alpha}} \right) \quad \text{as } |s| \to \infty$$
 (15)

holds for every $\alpha > 1$. Then

$$\Re g(Re^{i\theta}) = \log |h(Re^{i\theta})| = O_{\alpha}(R^{\alpha})$$
 as $R \to \infty$

holds for every $\alpha > 1$. Without loss of generality, we may suppose that g(0) = 0. Then we can write

$$g(Re^{i\theta}) = \sum_{k=1}^{\infty} (a_k + ib_k) R^k e^{ik\theta} \quad (a_k, b_k \in \mathbb{R}),$$

so that

$$\Re g(Re^{i\theta}) = \sum_{k=1}^{\infty} a_k R^k \cos k\theta - \sum_{k=1}^{\infty} b_k R^k \sin k\theta.$$

Note now that for every $k, n \in \mathbb{N}$, we have

$$\int_0^{2\pi} \cos k\theta \cos n\theta \, d\theta = \begin{cases} \pi & \text{if } k = n \\ 0 & \text{if } k \neq n \end{cases}$$

and

$$\int_0^{2\pi} \sin k\theta \cos n\theta \, \mathrm{d}\theta = 0.$$

It follows that

$$\int_{0}^{2\pi} \left(\Re g(Re^{i\theta}) \right) \cos n\theta \, d\theta = \pi a_n R^n,$$

so that

$$\pi |a_n| R^n \le \int_0^{2\pi} |\Re g(Re^{i\theta})| d\theta = O_\alpha(R^\alpha)$$
 as $R \to \infty$

holds for every $\alpha > 1$. On letting $R \to \infty$, we see that $a_n = 0$ for every n > 1. A similar argument using the function $\sin n\theta$ instead of the function $\cos n\theta$ gives $b_n = 0$ for every n > 1. We have therefore proved the following result.

THEOREM 6.6. Suppose that the entire function h(s) has no zeros on the plane, and that (15) holds for every $\alpha > 1$. Then $h(s) = e^{A+Bs}$, where A and B are constants.

REMARK. In the preceding argument, note that it is enough to assume that the estimates for h(s) hold for a sequence of values R with limit infinity.

Our next task is to study the distribution of the zeros of an entire function. The first step in this direction is summarized by the result below.

THEOREM 6.7. (Jensen's Formula) Suppose that f(s) is an entire function satisfying $f(0) \neq 0$. Suppose further that s_1, \ldots, s_n are the zeros of f(s) in |s| < R, counted with multiplicities, and that there are no zeros of f(s) on |s| = R. Then

$$\frac{1}{2\pi} \int_0^{2\pi} \log|f(Re^{i\theta})| \, d\theta - \log|f(0)| = \log \frac{R^n}{|s_1 \dots s_n|}.$$
 (16)

PROOF. We may clearly write

$$f(s) = (s - s_1) \dots (s - s_n)k(s),$$

where k(s) is analytic and has no zeros in $|s| \leq R$, so that $\log k(s)$ is analytic in $|s| \leq R$. It follows from Gauss's mean value theorem that

$$\frac{1}{2\pi} \int_0^{2\pi} \log k(Re^{i\theta}) d\theta = \log k(0).$$

Taking real parts, we obtain

$$\frac{1}{2\pi} \int_0^{2\pi} \log|k(Re^{i\theta})| d\theta = \log|k(0)| = \log|f(0)| - \log|s_1 \dots s_n|.$$
 (17)

Unfortunately, for every $j = 1, \ldots, n$, we cannot apply a similar argument to $\log |s - s_j|$, since the function $s - s_j$ has a zero at s_j . Note, however, that the function

$$\frac{R^2 - \overline{s_j}s}{R}$$

has no zeros in $|s| \leq R$ and satisfies

$$\left| \frac{R^2 - \overline{s_j} s}{R} \right| = |s - s_j|$$

on the circle |s| = R, so that

$$\frac{1}{2\pi} \int_0^{2\pi} \log|Re^{i\theta} - s_j| d\theta = \frac{1}{2\pi} \int_0^{2\pi} \log\left|\frac{R^2 - \overline{s_j}Re^{i\theta}}{R}\right| d\theta.$$
 (18)

Clearly the function

$$\log \frac{R^2 - \overline{s_j}s}{R}$$

is analytic in $|s| \leq R$. Applying Gauss's mean value theorem over the circle |s| = R on this function and taking real parts, we conclude that the right hand side of (18) is equal to $\log R$. Finally, note that

$$\log |f(Re^{i\theta})| = \sum_{j=1}^{n} \log |Re^{i\theta} - s_j| + \log |k(Re^{i\theta})|,$$

so that

$$\frac{1}{2\pi} \int_0^{2\pi} \log|f(Re^{i\theta})| d\theta = n \log R + \log|f(0)| - \log|s_1 \dots s_n|,$$

and the result follows. .

REMARKS. (i) It is important to point out that Jensen's formula was in fact only discovered after Hadamard's work in connection with Theorems 6.2 and 6.4.

(ii) Gauss's mean value theorem states that the value of an analytic function at the centre of a circle is equal to the arithmetic mean of its values on the circle. In particular, if the function F(s) is analytic for $|s| < R_0$, then for every $R < R_0$, we have

$$F(0) = \frac{1}{2\pi} \int_0^{2\pi} F(Re^{i\theta}) d\theta.$$

A simple consequence of Jensen's formula is the following result on the zeros of entire functions.

THEOREM 6.8. Suppose that f(s) is an entire function satisfying $f(0) \neq 0$, and that (14) holds for every $\alpha > 1$. Suppose further that s_1, s_2, s_3, \ldots are the zeros of f(s), counted with multiplicities and where $|s_1| \leq |s_2| \leq |s_3| \leq \ldots$. Then for every $\alpha > 1$, the series

$$\sum_{n=1}^{\infty} |s_n|^{-\alpha}$$

is convergent.

PROOF. Note that the right hand side of (16) is equal to

$$\int_0^R r^{-1} n(r) \, \mathrm{d}r,$$

where, for every non-negative $r \leq R$, n(r) denotes the number of zeros of f(s) in $|s| \leq r$. To see this, note that

$$\int_0^R r^{-1} n(r) dr = \sum_{j=1}^{n-1} \int_{|s_j|}^{|s_{j+1}|} r^{-1} j dr + \int_{|s_n|}^R r^{-1} n dr$$

$$= \sum_{j=1}^{n-1} j (\log |s_{j+1}| - \log |s_j|) + n(\log R - \log |s_n|)$$

$$= n \log R - \log |s_1| - \dots - \log |s_n|.$$

For every $\alpha > 1$, write $\alpha^* = (\alpha + 1)/2$, so that $1 < \alpha^* < \alpha$. Then

$$\log |f(Re^{i\theta})| = O_{\alpha}(R^{\alpha^*})$$
 as $R \to \infty$,

so that by Jensen's formula, we have

$$\int_0^R r^{-1} n(r) dr = O_{\alpha}(R^{\alpha^*}) - \log|f(0)| = O_{\alpha}(R^{\alpha^*}) \quad \text{as } R \to \infty.$$

On the other hand, note that

$$\int_{R}^{2R} r^{-1} n(r) \, \mathrm{d}r \ge n(R) \int_{R}^{2R} r^{-1} \, \mathrm{d}r = n(R) \log 2.$$

It follows that

$$n(R) = O_{\alpha}(R^{\alpha^*})$$
 as $R \to \infty$.

Now

$$\sum_{n=1}^{\infty} |s_n|^{-\alpha} = \int_0^{\infty} r^{-\alpha} \, \mathrm{d}n(r) = \alpha \int_0^{\infty} r^{-\alpha - 1} n(r) \, \mathrm{d}r < \infty$$

as required. .

Suppose now that f(s) is an entire function satisfying $f(0) \neq 0$, and that (14) holds for every $\alpha > 1$. Suppose further that s_1, s_2, s_3, \ldots are the zeros of f(s), counted with multiplicities and where $|s_1| \le |s_2| \le |s_3| \le \dots$ Then for every $\epsilon > 0$, the series

$$\sum_{n=1}^{\infty} |s_n|^{-1-\epsilon}$$

converges, so that the series

$$\sum_{n=1}^{\infty} |s_n|^{-2}$$

converges, and so the product

$$P(s) = \prod_{n=1}^{\infty} \left(1 - \frac{s}{s_n} \right) e^{s/s_n}$$
(19)

converges absolutely for every $s \in \mathbb{C}$, and uniformly in any bounded domain not containing any zeros of f(s). It follows that P(s) is an entire function, with zeros at s_1, s_2, s_3, \ldots Now write

$$f(s) = P(s)h(s), (20)$$

where h(s) is an entire function without zeros. If (15) holds for every $\alpha > 1$, then $h(s) = e^{A+Bs}$, where A and B are constants, and so

$$f(s) = e^{A+Bs} \prod_{n=1}^{\infty} \left(1 - \frac{s}{s_n} \right) e^{s/s_n}.$$
 (21)

THEOREM 6.9. Under the hypotheses of Theorem 6.8, the inequality (15) holds for every $\alpha > 1$, where the function h(s) is defined by (19) and (20). In particular, the function f(s) can be expressed in the form (21), where A and B are constants.

PROOF. To show that the inequality (15) holds for every $\alpha > 1$, it clearly suffices, in view of (14) and (20), to establish a suitable lower bound for |P(s)|. Since the series

$$\sum_{n=1}^{\infty} |s_n|^{-2}$$

is convergent, the set

$$S = \bigcup_{n=1}^{\infty} (|s_n| - |s_n|^{-2}, |s_n| + |s_n|^{-2})$$

has finite total length. It follows that there exist arbitrarily large positive values R such that $R \notin \mathcal{S}$, so that

$$|R - |s_n|| \ge |s_n|^{-2}$$
 for every $n \in \mathbb{N}$. (22)

For any such R, write, for j = 1, 2, 3,

$$P_j(s) = \prod_{(23.j)} \left(1 - \frac{s}{s_n} \right) e^{s/s_n},$$

where the products are taken over all $n \in \mathbb{N}$ satisfying

$$|s_n| < \frac{R}{2},\tag{23.1}$$

$$\frac{R}{2} \le |s_n| < 2R,\tag{23.2}$$

$$|s_n| \ge 2R,\tag{23.3}$$

respectively. Clearly

$$P(s) = P_1(s)P_2(s)P_3(s). (24)$$

Let $\epsilon > 0$ be chosen and fixed. Suppose first of all that (23.1) holds. Then on |s| = R, we have

$$\left| \left(1 - \frac{s}{s_n} \right) e^{s/s_n} \right| \ge \left(\left| \frac{s}{s_n} \right| - 1 \right) e^{-|s|/|s_n|} > e^{-R/|s_n|},$$

and so it follows from

$$\sum_{(23.1)} |s_n|^{-1} < \left(\frac{R}{2}\right)^{\epsilon} \sum_{n=1}^{\infty} |s_n|^{-1-\epsilon}$$

that

$$|P_1(s)| \gg_{\epsilon} e^{-R^{1+2\epsilon}}$$
 as $R \to \infty$. (25)

Suppose next that (23.2) holds. Then on |s| = R, we have

$$\left| \left(1 - \frac{s}{s_n} \right) e^{s/s_n} \right| \ge \left| \frac{s_n - s}{s_n} \right| e^{-|s|/|s_n|} > \frac{||s_n| - R|}{2R} e^{-2} \gg R^{-3},$$

in view of (22). Note that there are at most $O_{\epsilon}(R^{1+\epsilon})$ values of n for which (23.2) holds. Hence on |s|=R, we have

$$|P_2(s)| \gg_{\epsilon} (R^{-3})^{R^{1+\epsilon}} \gg_{\epsilon} e^{-R^{1+2\epsilon}} \quad \text{as } R \to \infty.$$
 (26)

Suppose finally that (23.3) holds. Then on |s| = R, we have

$$\left| \left(1 - \frac{s}{s_n} \right) e^{s/s_n} \right| > e^{-c(R/|s_n|)^2} \tag{27}$$

for some positive constant c (see the Remark below), and so it follows from

$$\sum_{(23.3)} |s_n|^{-2} \le (2R)^{-1+\epsilon} \sum_{n=1}^{\infty} |s_n|^{-1-\epsilon}$$

that

$$|P_3(s)| \gg_{\epsilon} e^{-R^{1+2\epsilon}}$$
 as $R \to \infty$. (28)

It now follows from (24)–(26) and (28) that on |s| = R, we have

$$|P(s)| \gg_{\epsilon} e^{-R^{1+3\epsilon}}$$
 as $R \to \infty$. (29)

The result now follows on combining (20) and (29), and noting that the inequality (14) holds for $\alpha = 1 + \epsilon$.

Remark. Note that the inequality (27) is of the form

$$|(1-z)e^z| > e^{-c|z|^2},$$
 (30)

where $|z| \leq 1/2$. Write z = x + iy, where $x, y \in \mathbb{R}$. Then (30) will follow if we show that

$$(1-x)^2 e^{2x} > e^{-2cx^2}$$

whenever $|x| \leq 1/2$. This last inequality can easily be established by using the theory of real valued functions of a real variable.

Finally, we make the following simple observation.

THEOREM 6.10. Under the hypotheses of Theorem 6.8, suppose further that the series

$$\sum_{n=1}^{\infty} |s_n|^{-1}$$

is convergent. Then there exists a positive constant c such that

$$f(s) = O(e^{c|s|})$$
 as $|s| \to \infty$

holds.

PROOF. This follows from (21) and the inequality $|(1-z)e^z| \le e^{2|z|}$ which holds for every $z \in \mathbb{C}$.

6.4. Proof of Theorems 6.2 and 6.4

Recall that $\xi(s)$, defined by (3), is an entire function, and that $\xi(0) \neq 0$. Note also that the zeros of $\xi(s)$ are precisely the zeros of $\zeta(s)$ in the critical strip. In order to establish Theorem 6.4, we shall use Theorem 6.9. We therefore first need to show that

$$\xi(s) = O_{\alpha} \left(e^{|s|^{\alpha}} \right) \quad \text{as } |s| \to \infty$$

holds for every $\alpha > 1$.

We shall in fact prove the following stronger result.

THEOREM 6.11. There exists a positive constant c such that

$$|\xi(s)| < e^{c|s|\log|s|}$$
 as $|s| \to \infty$. (31)

Furthermore, the inequality

$$|\xi(s)| < e^{c|s|}$$
 as $|s| \to \infty$ (32)

does not hold for any positive constant c.

PROOF. Since $\xi(s) = \xi(1-s)$ for every $s \in \mathbb{C}$, it suffices to prove the inequality (31) for $\sigma \geq 1/2$. First of all, there exists a positive constant c_1 such that

$$\left| \frac{1}{2} s(s-1) \pi^{-s/2} \right| < e^{c_1|s|}.$$

Next, Stirling's formula

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

as $|s| \to \infty$ is valid in the angle $-\pi/2 < \arg s < \pi/2$, and so there exists a positive constant c_2 such that

$$\left|\Gamma\left(\frac{s}{2}\right)\right| < e^{c_2|s|\log|s|}.$$

Finally, note that the formula

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

is valid for $\sigma > 0$, and the integral is bounded for $\sigma \ge 1/2$, so that there exists a positive constant c_3 such that

$$|\zeta(s)| < c_3|s|.$$

This proves (31). On the other hand, note that as $s \to +\infty$ through real values, we have

$$\log \Gamma\left(\frac{s}{2}\right) \sim \frac{s}{2}\log\frac{s}{2} \qquad \text{and} \qquad \zeta(s) \to 1,$$

so that (32) does not hold. \clubsuit

To complete the proof of Theorems 6.2 and 6.4, note that by Theorem 6.10, the series

$$\sum_{\rho} |\rho|^{-1}$$

is divergent, where ρ denotes the zeros of $\xi(s)$ and so the zeros of $\zeta(s)$ in the critical strip. Theorem 6.2 follows immediately. Theorem 6.4 now follows from Theorems 6.9 and 6.11.

An Important Formula

It follows from (4) that

$$\log \xi(s) = A + Bs + \sum_{\rho} \left(\frac{s}{\rho} + \log \left(1 - \frac{s}{\rho} \right) \right).$$

Differentiating with respect to s, we obtain

$$\frac{\xi'(s)}{\xi(s)} = B + \sum_{\rho} \left(\frac{1}{\rho} + \frac{1}{s - \rho} \right). \tag{33}$$

On the other hand, it follows from (3) that

$$\log \xi(s) = \log(s-1) - \frac{s}{2} \log \pi + \log \left(\frac{s}{2} \Gamma\left(\frac{s}{2}\right)\right) + \log \zeta(s)$$
$$= \log(s-1) - \frac{s}{2} \log \pi + \log \Gamma\left(\frac{s}{2} + 1\right) + \log \zeta(s).$$

Differentiating with respect to s, we obtain

$$\frac{\xi'(s)}{\xi(s)} = \frac{1}{s-1} - \frac{1}{2}\log\pi + \frac{1}{2}\frac{\Gamma'(\frac{s}{2}+1)}{\Gamma(\frac{s}{2}+1)} + \frac{\zeta'(s)}{\zeta(s)}.$$
 (34)

Combining (33) and (34), we obtain the following result.

THEOREM 6.12. We have

$$\frac{\zeta'(s)}{\zeta(s)} = B - \frac{1}{s-1} + \frac{1}{2}\log\pi - \frac{1}{2}\frac{\Gamma'(\frac{s}{2}+1)}{\Gamma(\frac{s}{2}+1)} + \sum_{\rho} \left(\frac{1}{\rho} + \frac{1}{s-\rho}\right),\tag{35}$$

where B is a constant and where ρ denotes the zeros of $\zeta(s)$ in the critical strip.

The formula (35) exhibits the pole of $\zeta(s)$ at s=1 and the zeros ρ in the critical strip. The trivial zeros are exhibited by the term

$$-\frac{1}{2}\frac{\Gamma'(\frac{s}{2}+1)}{\Gamma(\frac{s}{2}+1)}.$$

To see this last point, we start from the Weierstrass formula

$$\frac{1}{s\Gamma(s)} = e^{\gamma s} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-s/n},$$

where γ is Euler's constant. This gives

$$\frac{1}{\Gamma(\frac{s}{2}+1)} = e^{\gamma s/2} \prod_{n=1}^{\infty} \left(1 + \frac{s}{2n}\right) e^{-s/2n}.$$

Taking logarithms, we obtain

$$-\log\Gamma\left(\frac{s}{2}+1\right) = \frac{1}{2}\gamma s + \sum_{n=1}^{\infty} \left(\log\left(1+\frac{s}{2n}\right) - \frac{s}{2n}\right).$$

Differentiating with respect to s, we obtain

$$-\frac{1}{2}\frac{\Gamma'(\frac{s}{2}+1)}{\Gamma(\frac{s}{2}+1)} = \frac{1}{2}\gamma + \sum_{n=1}^{\infty} \left(\frac{1}{s+2n} - \frac{1}{2n}\right).$$

6.6. Counting Zeros in the Critical Strip

The starting point of our discussion is based on the Argument principle. Suppose that the function F(s) is analytic, apart from a finite number of poles, in the closure of a domain D bounded by a simple closed positively oriented Jordan curve C. Suppose further that F(s) has no zeros or poles on C. Then

$$\frac{1}{2\pi i} \int_C \frac{F'(s)}{F(s)} ds = \frac{1}{2\pi} \Delta_C \arg F(s)$$

represents the total number of zeros of F(s) in D minus the total number of poles of F(s) in D, counted with multiplicities. Here $\Delta_C \arg F(s)$ denotes the change of argument of the function F(s) along C.

It is convenient to use the function $\xi(s)$, since it is entire and its zeros are precisely the zeros of $\zeta(s)$ in the critical strip. To calculate N(T), it is convenient to take the domain $(-1,2) \times (0,T)$, so that C is the rectangular path passing through the vertices

$$2, \quad 2 + iT, \quad -1 + iT, \quad -1$$

in the anticlockwise direction. If no zeros of $\zeta(s)$ has imaginary part T, then

$$N(T) = \frac{1}{2\pi i} \int_C \frac{\xi'(s)}{\xi(s)} ds = \frac{1}{2\pi} \Delta_C \arg \xi(s).$$

Let us now divide C into the following parts. First, let L_1 denote the line segment from -1 to 2. Next, let L_2 denote the line segment from 2 to 2+iT, followed by the line segment from 2+iT to $\frac{1}{2}+iT$. Finally, let L_3 denote the line segment from $\frac{1}{2}+iT$ to -1+iT, followed by the line segment from -1+iT to -1.

Since $\xi(s)$ is real on L_1 , clearly $\Delta_{L_1} \arg \xi(s) = 0$. On the other hand,

$$\xi(\sigma + it) = \xi(1 - \sigma - it) = \overline{\xi(1 - \sigma + it)},$$

so that $\Delta_{L_2} \arg \xi(s) = \Delta_{L_3} \arg \xi(s)$. If we write $L = L_2$, so that L denotes the line segment from 2 to 2 + iT, followed by the line segment from 2 + iT to $\frac{1}{2} + iT$, then

$$\pi N(T) = \Delta_L \arg \xi(s). \tag{36}$$

Recall that

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

It follows that

$$\Delta_L \arg \xi(s) = \Delta_L \arg(s-1) + \Delta_L \arg \pi^{-s/2} + \Delta_L \arg \Gamma\left(\frac{s}{2} + 1\right) + \Delta_L \arg \zeta(s). \tag{37}$$

Clearly

$$\Delta_L \arg(s-1) = \arg\left(-\frac{1}{2} + iT\right) = \frac{1}{2}\pi + O(T^{-1})$$
(38)

and

$$\Delta_L \arg \pi^{-s/2} = \Delta_L \left(-\frac{1}{2} t \log \pi \right) = -\frac{1}{2} T \log \pi. \tag{39}$$

On the other hand,

$$\Delta_L \arg \Gamma\left(\frac{s}{2} + 1\right) = \Im \log \Gamma\left(\frac{5}{4} + \frac{1}{2}iT\right).$$

By Stirling's formula,

$$\log \Gamma\left(\frac{5}{4} + \frac{1}{2}iT\right) = \left(\frac{3}{4} + \frac{1}{2}iT\right)\log\left(\frac{5}{4} + \frac{1}{2}iT\right) - \frac{5}{4} - \frac{1}{2}iT + \frac{1}{2}\log\pi + O(T^{-1}),$$

so that

$$\Delta_L \arg \Gamma\left(\frac{s}{2} + 1\right) = \frac{T}{2} \log \frac{T}{2} + \frac{3}{8}\pi - \frac{T}{2} + O(T^{-1}). \tag{40}$$

Combining (36)–(40), we have

$$\begin{split} N(T) &= \frac{1}{2} - \frac{T}{2\pi} \log \pi + \frac{T}{2\pi} \log \frac{T}{2} + \frac{3}{8} - \frac{T}{2\pi} + S(T) + O(T^{-1}) \\ &= \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + \frac{7}{8} + S(T) + O(T^{-1}), \end{split}$$

where

$$\pi S(T) = \Delta_L \arg \zeta(s).$$

To prove Theorem 6.3, it suffices to prove the following result.

THEOREM 6.13. We have $S(T) = O(\log T)$ as $T \to \infty$.

PROOF. Note first of all that $\arg \zeta(2) = 0$. On the other hand,

$$\arg \zeta(s) = \tan^{-1} \left(\frac{\Im \zeta(s)}{\Re \zeta(s)} \right)$$

and $\Re \zeta(s) \neq 0$ on the line $\sigma = 2$. It follows that

$$|\arg\zeta(2+\mathrm{i}T)|<\frac{\pi}{2}.$$

Suppose now that $\Re \zeta(s)$ vanishes q times on the line segment from 2+iT to $\frac{1}{2}+iT$. Then this line segment can be divided into q+1 parts, where in each subinterval, $\Re \zeta(s)$ may vanish only at one or both of the endpoints and has constant sign strictly in between, so that the variation of $\arg \zeta(s)$ in each such subinterval does not exceed π . It follows that for $s=\sigma+iT$, we have

$$|\arg \zeta(s)| \le (q+1)\pi + \frac{1}{2}\pi \quad \left(\frac{1}{2} \le \sigma \le 2\right). \tag{41}$$

To prove our result, it remains to find a suitable bound for q. For $s = \sigma + iT$, we have

$$\Re \zeta(s) = \frac{1}{2} (\zeta(\sigma + iT) + \zeta(\sigma - iT)).$$

Let T be fixed, and consider the function

$$f_T(s) = \frac{1}{2}(\zeta(s + iT) + \zeta(s - iT))$$

(note that we no longer insist that $s = \sigma + iT$). Then q is the number of zeros of $f_T(s)$ on the line segment from 1/2 to 2, and so is bounded above by the number of zeros of $f_T(s)$ in the disc $|s-2| \le 3/2$. In other words,

$$q \le n\left(\frac{3}{2}\right),\tag{42}$$

where, for every $r \ge 0$, n(r) denotes the number of zeros of $f_T(s)$ in the disc $|s-2| \le r$. By Jensen's formula and noting that we may assume that $\zeta(\frac{1}{2} + iT) \ne 0$, we have

$$\int_{0}^{7/4} \frac{n(r)}{r} dr = \frac{1}{2\pi} \int_{0}^{2\pi} \log \left| f_T \left(2 + \frac{7}{4} e^{i\theta} \right) \right| d\theta - \log |f_T(2)|. \tag{43}$$

On the other hand.

$$\int_0^{7/4} \frac{n(r)}{r} dr \ge \int_{3/2}^{7/4} \frac{n(r)}{r} dr \ge n \left(\frac{3}{2}\right) \int_{3/2}^{7/4} \frac{1}{r} dr = n \left(\frac{3}{2}\right) \log \frac{7}{6}. \tag{44}$$

Observe that

$$|f_T(2)| = \left| \frac{1}{2} (\zeta(2 + iT) + \zeta(2 - iT)) \right| = |\Re \zeta(2 + iT)|$$
$$= \left| \Re \left(\sum_{n=1}^{\infty} \frac{1}{n^{2+iT}} \right) \right| \ge 1 - \sum_{n=2}^{\infty} \frac{1}{n^2} = 2 - \frac{\pi^2}{6} > 0,$$

so that

$$-\log|f_T(2)| = O(1). \tag{45}$$

Finally, recall that $|\zeta(s)| \ll T^{3/4}$ for every $\sigma \geq 1/4$. It follows that for every $\theta \in [0, 2\pi]$, we have

$$\left| f_T \left(2 + \frac{7}{4} e^{i\theta} \right) \right| \le \frac{1}{2} \left(\left| \zeta \left(2 + \frac{7}{4} e^{i\theta} + iT \right) \right| + \left| \zeta \left(2 + \frac{7}{4} e^{i\theta} - iT \right) \right| \right) \ll T^{3/4},$$

so that

$$\log \left| f_T \left(2 + \frac{7}{4} e^{i\theta} \right) \right| \ll \log T. \tag{46}$$

Combining (43)–(46), we conclude that

$$n\left(\frac{3}{2}\right) \ll \log T. \tag{47}$$

The result now follows on combining (41), (42) and (47).

6.7. Sketch of the Proof of Theorem 6.5

It can be shown that for c > 1, we have

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

It follows that

$$\psi_0(X) = \sum_{n \le X}' \Lambda(n) = \sum_{n=1}^{\infty} \Lambda(n) \left(\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{(X/n)^s}{s} ds \right)$$
$$= \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \right) \frac{X^s}{s} ds = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\zeta'(s)}{\zeta(s)} \frac{X^s}{s} ds,$$

where \sum' denotes that the term in the sum corresponding to n=X is $\frac{1}{2}\Lambda(X)$.

The idea is now to move the line of integration away to infinity on the left, so that we can express $\psi_0(X)$ as a sum of the residues at the poles of the function

$$-\frac{\zeta'(s)}{\zeta(s)}\frac{X^s}{s}$$
.

Here, the pole at s=1 gives rise to a residue X, while the pole at s=0 gives rise to a residue $-\zeta'(0)/\zeta(0)$. On the other hand, each zero ρ of $\zeta(s)$ in the critical strip gives rise to a residue $-X^{\rho}/\rho$, while each trivial zero -2n of $\zeta(s)$ gives rise to a residue $X^{-2n}/2n$. Finally, note that

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

The first step in this process is to consider the integral

$$-\frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{\zeta'(s)}{\zeta(s)} \frac{X^s}{s} ds,$$

and regard the path of integration as one side of a rectangle with vertices at $c \pm iT$ and $-U \pm iT$, where U>0 is large. Here T has to be chosen carefully so that the horizontal sides of the rectangle should avoid the zeros of $\zeta(s)$ in the critical strip. Also U has to be chosen carefully so that the left vertical side of the rectangle should avoid the trivial zeros of $\zeta(s)$. On taking $U \to \infty$, this will result in a finite version of Theorem 6.5, of the form

$$\psi_0(X) = X - \sum_{|\gamma| < T} \frac{X^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2} \log \left(1 - \frac{1}{X^2} \right) + R(X, T),$$

where the error term R(X,T) can be estimated.