

Analytic Number Theory

Ben Green

MATHEMATICAL INSTITUTE, OXFORD

E-mail address: `ben.green@maths.ox.ac.uk`

2000 *Mathematics Subject Classification.* Primary

Contents

0.1. Synopsis	1
0.2. Overview	1
0.3. Notation	2
0.4. Quantities	3
Chapter 1. Basic facts about the primes	5
1.1. Euclid's proof	5
1.2. Elementary bounds	5
1.3. The prime number theorem	8
Chapter 2. Arithmetic functions	11
2.1. Möbius inversion.	11
Chapter 3. Introducing the Riemann ζ -function	13
3.1. Dirichlet series	13
3.2. The ζ -function	13
3.3. Looking forward	15
3.4. Meromorphic continuation to $\operatorname{Re} s > 0$.	16
Chapter 4. Some Fourier analysis	17
4.1. Introduction	17
4.2. Fourier analysis of Schwarz functions on \mathbb{R}	18
4.3. Fourier analysis on \mathbb{Z} and \mathbb{R}/\mathbb{Z}	22
4.4. The Poisson summation formula	26
Chapter 5. The analytic continuation and functional equation	27
5.1. The Γ -function	27
5.2. Statement of the functional equation for ζ	30
5.3. Proof of the functional equation	30
Chapter 6. The partial fraction expansion	33
6.1. Statement of the partial fraction expansion	33
6.2. The product formula for ζ	34
6.3. The size of a holomorphic function and its zeros	35

6.4. *Weierstrass product of an integral function of order one: details	38
Chapter 7. Mellin transforms and the explicit formula	43
7.1. Definitions and statement of the formula	43
7.2. Proof of the explicit formula – overview	45
7.3. Estimates for the Mellin transforms.	47
Chapter 8. The prime number theorem	53
Chapter 9. The zero-free region. Error terms.	57
9.1. The classical zero-free region	57
9.2. The prime number theorem with classical error term	59
9.3. The Riemann hypothesis and its significance	61
Chapter 10. *An introduction to sieve theory	63
10.1. Introduction	63
10.2. Selberg’s weights	64
Appendix A. *Some smooth bump functions	69
Bibliography	73

0.1. Synopsis

Introductory material on primes. Arithmetic functions: Möbius function, Euler's ϕ -function, the divisor function, the σ -function. Multiplicativity. Dirichlet series and Euler products. The von Mangoldt function.

The Riemann ζ -function for $\operatorname{Re}(s) > 1$. Euler's proof of the infinitude of primes. ζ and the von Mangoldt function.

Schwarz functions on \mathbf{R} , \mathbf{Z} , \mathbf{R}/\mathbf{Z} and their Fourier transforms. *Inversion formulas and uniqueness*. The Poisson summation formula.

The θ -function and its functional equation. The Γ -function and the meromorphic continuation and functional equation of the ζ -function. Poles and zeros of ζ and statement of the Riemann hypothesis. Basic estimates for ζ .

Product theorems for entire functions. Hadamard's product formula for ζ and the partial fraction expansion.

The Mellin transform of a smooth compactly supported function. The Mellin inversion formula. Decay of the Mellin transform in vertical strips. Statement and proof of the explicit formula.

The classical zero-free region. Proof of the prime number theorem. Implications of the Riemann hypothesis for the distribution of primes.

*Introduction to sieve theory.

0.2. Overview

These notes are from a 16-lecture graduate course given in Oxford in 2016. The main aim of this course is to give a proof of the prime number theorem in what I consider to be the most conceptually natural fashion, via the explicit formula which links the primes to the zeros of zeta. I could have called the course "Music of the Primes" but decided against it.

Liberal use is made of smooth cutoff functions, and so one will not find any mention of "Perron's formula" here. Although this demands a little more sophistication on the part of the reader, the payoff is that different types of error terms are cleanly separated, and one can see very clearly the link between the primes and the zeta zeros. A technical advantage is that one may establish the prime number theorem using only the nonvanishing of ζ on $\operatorname{Re} s = 1$, rather than a zero-free region.

There are surprisingly few accounts along these lines in the literature. The closest I know of is Kowalski's nice book [2]. However, this is a little faster-paced, wider-ranging and lighter on detail than we aim to be here, and some readers may be put off by the fact that it is in French.

Two essential books for the serious student are [1] and [3]. Davenport's book is the traditional connoisseur's choice for a course of this nature. It remains an excellent book. However, there are some notable differences in emphasis with our approach here. The book of Iwaniec and Kowalski contains a vast amount of material and is really for the expert, but it should find space on the shelf of any person wishing to describe themselves in that way.

0.3. Notation

As with any course, a certain amount of notation will be introduced as we go along.

One very important point to be made at the outset is that $\log x$ *always* means the natural logarithm of x . Some people consider the notation $\ln x$, which can be found in some books, tasteless. $\log^C x$ is the same as $(\log x)^C$.

We will very often use the notation $[t]$, which means the greatest integer less than or equal to t .

Throughout the course we will be using *asymptotic notation*. This is vital in handling the many inequalities and rough estimates we will encounter. Here is a summary of the notation we will see. We suggest the reader not worry too much about this now; we will gain plenty of practice with this notation.

- $A \ll B$ means that there is an absolute constant $C > 0$ such that $|A| \leq CB$. In this notation, A and B will typically be variable quantities, depending on some other parameter. For example, $x + 1 \ll x$ for $x \geq 1$, because $|x + 1| \leq 2x$ in this range. It is important to note that the constant C may be different in different instances of the notation.
- $A = O(B)$ means the same thing.
- $A \ll_{k,l,m} B$ means that $|A| \leq CB$, but now C is allowed to depend on some other parameters k, l, m . For example, $kx \ll_k x$, $k + l + m = O_{k,l,m}(1)$.
- $A \ll B$ is the same as $B \gg A$.
- $O(A)$ means some quantity bounded in magnitude by CA for some absolute constant $C > 0$. In particular, $O(1)$ simply means a quantity bounded by an absolute positive constant. For example, $\frac{5x}{1+x} = O(1)$ for $x \geq 0$.

- $A = o(B)$ means that $|A| \leq \varepsilon B$ as some other parameter becomes large enough. The other parameter will usually be clear from context. For example, $\frac{1}{\log x} = o(1)$ (as $x \rightarrow \infty$).
- $A = o_{k,l,m}(B)$ means that $|A| \leq \varepsilon B$ as some other parameter becomes large enough, but how large it needs to be may depend on the other parameters k, l, m . For example, $\frac{k}{\log x} = o_k(1)$.
- $A \sim B$ means that $A = (1 + o(1))B$.

0.4. Quantities

In understanding analytic number theory, it is important to develop a robust intuitive feeling for the rough size of certain quantities. For example, one should be absolutely clear about the fact that, for X large,

$$\log^{10} X \lll e^{\sqrt{\log X}} \lll X^{0.01}.$$

CHAPTER 1

Basic facts about the primes

1.1. Euclid's proof

This course is largely about the *prime numbers* 2, 3, 5, 7, The most basic fact about them is the following, proven by Euclid over 2000 years ago.

THEOREM 1.1. *There are infinitely many primes.*

Proof. Suppose not, and that p_1, \dots, p_N is a complete list of the primes. Consider the number $M = p_1 \cdots p_N + 1$. It must have a prime factor q . However, M is manifestly not divisible by any of p_1, \dots, p_N , and so $q \notin \{p_1, \dots, p_N\}$. This is a contradiction. \square

Of course, it is possible to ask more refined questions. Does the sequence of prime numbers grow extremely rapidly (like the powers of two $1, 2, 2^2, 2^3, \dots$), or slowly like the odd numbers $1, 3, 5, 7, \dots$, or somewhere in between? This is the question that will occupy us in this course.

1.2. Elementary bounds

If $X > 1$ is a real number then we write $\pi(X)$ for the number of primes less than or equal to X . Rather elementary methods suffice to get the correct order of magnitude for $\pi(X)$.

THEOREM 1.2. *There are constants $0 < c_1 < 1 < c_2$ such that, for all sufficiently large X ,*

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

Remarks. In asymptotic notation, we may thus assert that $\frac{X}{\log X} \ll \pi(X) \ll \frac{X}{\log X}$, and the upper bound is saying that $\pi(X) = O(X/\log X)$. The lower bound immediately implies the infinitude of primes (and with a much better bound than Euclid's proof). The upper bound implies, in particular, that the density of the primes up to X , that is to say $\pi(X)/X$, tends to zero as $X \rightarrow \infty$.

Proof. We begin with the lower bound, which is slightly easier. For this, it suffices to show that

$$(1.1) \quad \prod_{p \leq 2n} p \geq C_1^n$$

for some $C_1 > 1$, and for sufficiently large n . Indeed, we then have

$$C_1^n \leq \prod_{p \leq 2n} p \leq (2n)^{\pi(2n)},$$

from which we obtain $\pi(2n) \gg \frac{n}{\log(2n)}$. This implies the lower bound in Theorem 1.2 when X is an even integer; the general case follows very quickly from this.

To prove (1.1), we look at the prime factorisation of $\binom{2n}{n}$, which we write as

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{v_p(n)}.$$

Now we claim the following three facts.

- (i) If $p > \sqrt{2n}$ then $v_p(n) \leq 1$;
- (ii) For all p , $p^{v_p(n)} \leq 2n$.
- (iii) $\binom{2n}{n} \geq \frac{4^n}{2n+1}$.

For items (i) and (ii) we use the formula

$$(1.2) \quad v_p(n) = \sum_{i=1}^{\infty} \left[\frac{2n}{p^i} \right] - 2 \left[\frac{n}{p^i} \right].$$

This is a consequence of the fact that the power of p dividing $m!$ is $\sum_{i=1}^{\infty} \left[\frac{m}{p^i} \right]$, this sum being composed of $\left[\frac{m}{p} \right]$ multiples of p , $\left[\frac{m}{p^2} \right]$ multiples of p^2 , and so on. (We remark that sums such as (1.2) are all finite, since for example $\left[\frac{2n}{p^i} \right] = 0$ when $p^i > 2n$.)

Proof of (i): each term in (1.2) is at most 1, since $[2x] - 2[x] \in \{0, 1\}$ for all real x . For $p > \sqrt{2n}$, only the term with $i = 1$ can be nonzero.

Proof of (ii): all terms in (1.2) are zero or 1, and those with $i > \frac{\log(2n)}{\log p}$, that is to say with $p^i > 2n$, are zero. Therefore $v_p(n) \leq \frac{\log(2n)}{\log p}$, from which (ii) follows immediately.

Proof of (iii): note that $\sum_{j=0}^{2n} \binom{2n}{j} = 4^n$ and, in this sum, the middle term $\binom{2n}{n}$ is the largest one.

Putting these facts together gives

$$\frac{4^n}{2n+1} \leq (2n)^{\pi(\sqrt{2n})} \prod_{p \leq 2n} p \leq (2n)^{\sqrt{2n}} \prod_{p \leq 2n} p.$$

It follows that (1.1) holds for any $C_1 < 4$, provided n is sufficiently large.

We turn now to the upper bound in Theorem 1.2. We claim that now it suffices to show that

$$(1.3) \quad \prod_{X/2 < p \leq X} p \leq C_2^X$$

for some C_2 , provided X is sufficiently large. Indeed, this evidently implies that

$$\left(\frac{X}{2}\right)^{\pi(X) - \pi(X/2)} \leq C_2^X.$$

Taking logs gives

$$\pi(X) \leq \pi\left(\frac{X}{2}\right) + \frac{X \log C_2}{\log(X/2)}.$$

Replacing X by $X/2, X/4, \dots$ we obtain

$$(1.4) \quad \pi(X) \leq \pi\left(\frac{X}{2^m}\right) + 2 \log C_2 \sum_{i=1}^m \frac{X/2^i}{\log(X/2^i)}.$$

Let m be the largest integer for which $2^m \leq \sqrt{X}$. Then certainly $2^m \geq \sqrt{X}/2$, and so

$$\pi\left(\frac{X}{2^m}\right) \leq \frac{X}{2^m} \leq 2\sqrt{X}.$$

For $i \leq m$ we have $\log(X/2^i) \leq \log \sqrt{X} = \frac{1}{2} \log X$. Combining these observations with (1.4) gives

$$\pi(X) \leq 2\sqrt{X} + \frac{2 \log C_2}{\frac{1}{2} \log X} \sum_{i=1}^m \frac{X}{2^i}.$$

This is evidently $O\left(\frac{X}{\log X}\right)$, which is the upper bound in Theorem 1.2.

It remains to establish (1.3). For this, note that if n is an integer and if $p > n$ then p divides $\binom{2n}{n}$ precisely once. Therefore

$$\prod_{n < p \leq 2n} p \leq 4^n.$$

Taking $n = \lfloor X/2 \rfloor$, we have

$$\prod_{X/2 < p \leq 2\lfloor X/2 \rfloor} p \leq 2^X.$$

There is at most one prime in the range $2\lfloor X/2 \rfloor < p \leq X$, and so

$$\prod_{X/2 < p \leq X} p \leq X 2^X.$$

From this, (1.3) follows immediately (with any $C_2 > 2$). \square

Additional remark. Euclid's proof of the infinitude of primes can be modified to give an explicit lower bound on $\pi(X)$, but it is very weak: we leave it as an exercise to show that $\pi(X) \gg \log \log X$ by this method.

1.3. The prime number theorem

The main aim of this course will be to prove the *prime number theorem*, which states that c_1 and c_2 in Theorem 1.2 can be taken arbitrarily close to 1.

THEOREM 1.3 (Prime number theorem). *Suppose that $0 < c_1 < 1 < c_2$. Then, if X is sufficiently large, we have*

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

Equivalently, $\pi(X) = (1 + o(1)) \frac{X}{\log X}$, or $\pi(X) \sim \frac{X}{\log X}$.

It is convenient to reformulate the prime number theorem in various ways. One very simple way of doing so is to observe that it is (tautologically) equivalent to the statement that

$$\sum_{n \leq X} 1_P(n) \sim \frac{X}{\log X},$$

where 1_P is the characteristic function of the primes, that is to say the function which is 1 on the primes and 0 elsewhere.

It turns out that a much more natural function than the characteristic function of the primes is the *von Mangoldt function*. It is defined by

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

One should think of Λ as being roughly a function that assigns weight $\log p$ to the prime p ; the contribution of the genuine prime powers p^k , $k \geq 2$, is negligible.

The reason this is a natural definition will become gradually apparent. For now, however, let us note that the prime number theorem has an equivalent formulation in terms of the von Mangoldt function.

We define

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

PROPOSITION 1.1. *The prime number theorem is equivalent to the statement that $\psi(X) \sim X$, that is to say that the average value of $\Lambda(n)$ over $n \leq X$ is asymptotically 1.*

Proof. Write

$$a(X) := \frac{\pi(X)}{X/\log X}, \quad b(X) := \psi(X)/X.$$

Thus the task is to show that $a(X) \rightarrow 1$ if and only if $b(X) \rightarrow 1$.

We first obtain an upper bound for $b(X)$ in terms of $a(X)$. For a given prime p , the maximum k for which $p^k \leq X$ is $k = \lfloor \log X / \log p \rfloor$. The contribution of this

p to $\psi(X)$,

$$\sum_{k:p^k \leq X} \log p,$$

is therefore at most

$$\log p \lfloor \frac{\log X}{\log p} \rfloor \leq \log X.$$

Only those primes p with $p \leq X$ contribute at all, and so we have the inequality

$$\psi(X) \leq \pi(X) \log X,$$

and thus

$$(1.5) \quad b(X) \leq a(X).$$

Now we obtain a bound in the other direction. To this end, note that

$$(1.6) \quad a(X) - b(X) \leq \frac{1}{X} \sum_{p \leq X} (\log X - \log p),$$

the contribution of the proper prime powers p^k , $k \geq 2$, to $-b(X)$ being negative.

We split the sum over p into two ranges $p \leq X(\log X)^{-2}$ and $X(\log X)^{-2} < p \leq X$ (there is a certain amount of flexibility in these choices). We bound the contribution from the first range trivially:

$$(1.7) \quad \frac{1}{X} \sum_{p \leq X(\log X)^{-2}} (\log X - \log p) < \frac{1}{\log X}.$$

On the second range,

$$(1.8) \quad \log X - \log p \ll \log \log X.$$

Thus

$$\begin{aligned} \frac{1}{X} \sum_{X(\log X)^{-2} < p \leq X} (\log X - \log p) &\ll \frac{\log \log X}{X} \#\{p : X(\log X)^{-2} < p \leq X\} \\ &\leq \frac{2 \log \log X}{\log X} b(X), \end{aligned}$$

since each of the p 's under consideration here contributes at least $\frac{1}{2} \log X$ to $\psi(X)$.

Combining (1.6), (1.7) and (1.8) gives

$$a(X) \leq \left(1 + \frac{2 \log \log X}{\log X}\right) b(X) + O\left(\frac{1}{\log X}\right).$$

This certainly implies that

$$(1.9) \quad a(X) \leq (1 + o(1))b(X) + o(1),$$

which is enough for our purposes.

The fact that if $b(X) \rightarrow 1$ then $a(X) \rightarrow 1$ follows immediately from (1.5), (1.9).

The other direction is just slightly trickier: if $a(X) \rightarrow 1$ then it certainly follows from (1.5) that $b(X) \leq 1 + o(1)$. In particular $b(X) \leq 2$ for X sufficiently large, and so the term $o(1)b(X)$ in (1.9) may be replaced by $o(1)$. We then have $a(X) \leq b(X) + o(1)$, which implies that $b(X) \geq 1 + o(1)$ as well. \square

CHAPTER 2

Arithmetic functions

An *arithmetic function* is simply a function f from \mathbb{N} to \mathbb{C} .

The most important arithmetic function in this course is the von Mangoldt function Λ , introduced in the last section. However, this is far from the only interesting arithmetic function.

2.1. Möbius inversion.

Some of the material of this section is not really necessary for the main development of the course, and in particular for proving the prime number theorem. However, it is certainly part of the general culture of analytic number theory, and helps us place Λ in a more general context.

The *Möbius function* μ is defined by $\mu(n) = (-1)^k$ if $n = p_1 \cdots p_k$ for distinct primes p_1, \dots, p_k , and $\mu(n) = 0$ otherwise.

Dirichlet convolution If $f, g : \mathbb{N} \rightarrow \mathbb{C}$ are two arithmetical functions then we define

$$f \star g(n) := \sum_{d|n} f(d)g(n/d) = \sum_{ab=n} f(a)g(b).$$

PROPOSITION 2.1 (Möbius inversion). *Let $f, g : \mathbb{N} \rightarrow \mathbb{C}$ be two arithmetical functions. Then $g = f \star 1$ if and only if $f = g \star \mu$.*

Proof. Observe that Dirichlet convolution is commutative and associative. Note that $\mu \star 1 = \delta$, where $\delta(n) = 1$ if $n = 1$ and 0 otherwise. This is a routine check: if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then

$$\sum_{d|n} \mu(d) = \sum_{\varepsilon_i \in \{0,1\}} \mu(p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}) = (1-1) \cdots (1-1) = 0.$$

Now if $g = f \star 1$ then

$$g \star \mu = (f \star 1) \star \mu = f \star (1 \star \mu) = f \star \delta = f.$$

Conversely if $f = g \star \mu$ then

$$f \star 1 = (g \star \mu) \star 1 = g \star (\mu \star 1) = g \star \delta = g.$$

This concludes the proof. □

This leads to an important link between the von Mangoldt function and the Möbius function.

LEMMA 2.1. *We have $\Lambda = \mu \star \log$, that is to say $\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d)$.*

Proof. This follows from Möbius inversion and the fact, obvious upon considering the prime factorization of n , that

$$\Lambda \star 1(n) = \sum_{d|n} \Lambda(d) = \log n.$$

□

Here are some other commonly occurring arithmetical functions.

- Euler's ϕ -function $\phi(n)$ is defined to be the number of integers $x \leq n$ which are coprime to n , which is the same thing as the order of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, the group of invertible elements in $\mathbb{Z}/n\mathbb{Z}$.
- The divisor function $\tau(n)$ (sometimes written $d(n)$) is defined to be the number of positive integer divisors of n , including 1 and n itself.
- The sum-of-divisors function $\sigma(n)$ is defined to be $\sum_{d|n} d$.

Various properties of these may be found in the exercises.

Introducing the Riemann ζ -function

3.1. Dirichlet series

An important tool for working with arithmetical functions – particularly when they arise from considerations that are somehow multiplicative – is that of *Dirichlet series*.

Let $f : \mathbb{N} \rightarrow \mathbb{C}$ be an arithmetical function. Then the *Dirichlet Series* of f is

$$D_f(s) := \sum_n f(n)n^{-s}.$$

We say that f has *reasonable growth* if $|f(n)| = n^{o(1)}$. Examples of functions with reasonable growth are the constant function 1, the Möbius function and the von Mangoldt function.

In this case the series for $D_f(s)$ converges, and defines a holomorphic function of s , in the domain $\operatorname{Re} s > 1$.

In fact if $\operatorname{Re} s \geq 1 + \delta$ then for $N > N_0(\delta)$ sufficiently large we have

$$\left| \sum_{n=N+1}^{\infty} f(n)n^{-s} \right| \leq \sum_{n=N+1}^{\infty} n^{\delta/2} n^{-1-\delta} \ll N^{-\delta/2}.$$

Thus if we set

$$D_f^{(N)}(s) := \sum_{n=1}^N f(n)n^{-s}$$

then $D_f^{(N)} \rightarrow D_f(s)$ uniformly in $\operatorname{Re} s \geq 1 + \delta$, which implies that D_f is holomorphic on the interior of any such domain.

3.2. The ζ -function

Perhaps the most basic arithmetical function is the constant function $f = 1$. The Dirichlet series of this function is called the *Riemann ζ -function*. Thus

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

As just noted, the series converges and defines a holomorphic function in the domain $\operatorname{Re} s > 1$.

Euler product. Unique factorization into primes convinces us of the identity

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots\right) \left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots\right) \cdots,$$

where there is one product for each prime $p = 2, 3, 5, \dots$. Summing each of the geometric series suggests then that

$$(3.1) \quad \zeta(s) = \prod_p (1 - p^{-s})^{-1}.$$

Let us pause to justify this formally. Let s , $\operatorname{Re} s > 1$, be fixed. Fix an N , and suppose that $m > \log_2 N$. Then the product

$$P(m, N) := \prod_{p \leq N} \left(\sum_{j=0}^m p^{-js} \right)$$

may be expanded, and it equals $1 + 2^{-s} + \cdots + N^{-s}$ plus a number of further, distinct, terms n^{-s} with $n > N$. Thus

$$|P(m, N) - \zeta(s)| \leq \sum_{n=N+1}^{\infty} |n^{-s}| \ll N^{-\delta}$$

uniformly in m . Letting $m \rightarrow \infty$, we thus obtain

$$\left| \prod_{p \leq N} (1 - p^{-s})^{-1} - \zeta(s) \right| \ll N^{-\delta}.$$

Finally, letting $N \rightarrow \infty$, we confirm the equality (3.1).

Equation (3.1) is called the Euler product for ζ and it is valid for $\operatorname{Re} s > 1$.

An amusing consequence of the above is yet another proof (our third) that there are infinitely many primes. Suppose not. Then, letting $s \rightarrow 1^+$ in (3.1) we see that $\lim_{s \rightarrow 1^+} \zeta(s) < \infty$. However this is not the case, since

$$\lim_{s \rightarrow 1^+} \sum_{n=1}^N n^{-s} = \sum_{n=1}^N n^{-1},$$

and the harmonic series diverges.

It turns out that the Dirichlet series of many of the basic arithmetical functions can be expressed in terms of ζ . In the following proposition we detail the most basic such relations; others may be found on the exercise sheet.

PROPOSITION 3.1. *Suppose that $\operatorname{Re} s > 1$. Then*

- (i) *If the Dirichlet series of f is $F(s)$, and that of g is $G(s)$, then the Dirichlet series of the convolution $f \star g$ is FG .*
- (ii) $\sum_n \mu(n)n^{-s} = 1/\zeta(s)$;
- (iii) $\sum_n \Lambda(n)n^{-s} = -\zeta'(s)/\zeta(s)$;

Proof. For (i), note that the Dirichlet Series of $f \star g$ is

$$\sum_n \left(\sum_{ab=n} f(a)g(b) \right) n^{-s} = \sum_{a,b} f(a)g(b)(ab)^{-s}.$$

This proves the result. (ii) is best proved using the Euler product for ζ , which gives

$$\frac{1}{\zeta}(s) = \prod_p (1 - p^{-s}) = \sum_n \mu(n)n^{-s}$$

(the second step follows on expanding out the product). Part (iii) can be proven using (i), (ii), the fact that $\Lambda = \mu \star \log$ and the observation that

$$\zeta'(s) = - \sum_n \log n \cdot n^{-s}.$$

Alternatively, write

$$\log \zeta(s) = - \sum_p \log(1 - p^{-s})$$

and differentiate. □

COROLLARY 3.1. *We have $\zeta(s) \neq 0$ when $\operatorname{Re} s > 1$.*

Proof. This follows immediately from (ii). □

3.3. Looking forward

One of the central results of the course is the fact that ζ , though it is currently defined only for $\operatorname{Re} s > 1$, extends to a meromorphic function on the complex plane, holomorphic except for a simple pole at $s = 1$. The function $(s - 1)\zeta(s)$ is then *entire* (holomorphic on the whole complex plane). It has zeros ρ , and we shall show that they are of two types: the *trivial zeros* $-2, -4, -6, \dots$ and the *nontrivial zeros*, which all lie in the region $0 \leq \operatorname{Re} s \leq 1$. To understand ζ in terms of its zeros, it is natural to ask to what extent $(s - 1)\zeta(s) \sim \prod_{\rho} (s - \rho)$. Though it is not quite possible to make sense of *this* statement, a slight variant of it does hold.

Here, then, is a summary of the main facts about ζ we will establish in this chapter that will be important for the later theory.

THEOREM 3.1. *The Riemann ζ -function extends to a meromorphic function, analytic except for a simple pole at $s = 1$. It has “trivial” zeros at $s = -2, -4, -6, \dots$, all simple, and (possibly) “nontrivial zeros” in the critical strip $0 \leq \operatorname{Re} s \leq 1$. Finally, we have the Weierstrass product expansion*

$$(s - 1)\zeta(s) = e^{As+B} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho},$$

where the product is over all zeros of ζ and A, B are some constants (which can be evaluated explicitly).

Let us remark that at least one of the facts used in the proof of this theorem – the functional equation, Theorem 5.1 – is of great importance in its own right.

3.4. Meromorphic continuation to $\operatorname{Re} s > 0$.

To conclude this introductory discussion of the ζ -function, we give a quick proof that it may be meromorphically continued a little to the left of its current domain of definition.

PROPOSITION 3.2. *The Riemann zeta function $\zeta(s)$ has a meromorphic continuation to the right half-plane $\operatorname{Re}(s) > 0$, analytic except for a simple pole at $s = 1$.*

Proof. For $\operatorname{Re} s > 1$ we have

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

(Here, $\{x\} := x - [x]$.) The integral here defines an analytic function on $\operatorname{Re} s > 0$.

□

The formula for $\zeta(s)$ found here will sometimes be useful in its own right.

Some Fourier analysis

A key role will be played in the rest of the course by Fourier analysis. We take the time to develop the parts of the subject that we need in this chapter.

4.1. Introduction

Most students will have met both the Fourier transform and “Fourier series” at undergraduate level. It turns out that these are just two instances of the same concept, that of a Fourier transform on a locally compact abelian group (LCAG). We will not go into any details of the theory in this generality – in fact there is not even any need to define a LCAG. The reader may, however, benefit from seeing the unified context at least in vague outline.

If G is a LCAG then we associate to G its *dual* \widehat{G} , which consists of all continuous homomorphisms (characters) from G to S^1 , the unit circle $\{z \in \mathbb{C} : |z| = 1\}$. It is easy to see that \widehat{G} is a group under pointwise multiplication. If $f : G \rightarrow \mathbb{C}$ is a “suitably nice” function and $\gamma \in \widehat{G}$ is a character then the Fourier transform $\widehat{f}(\gamma)$ is defined to be

$$\widehat{f}(\gamma) := \int_G f(x) \overline{\gamma(x)} d\mu_G(x) = \langle f, \gamma \rangle,$$

where μ_G is the *Haar measure* on G , a certain uniquely-defined measure with natural properties. We will not need the general theory here, and instead illustrate with examples.

EXAMPLE 4.1 ($G = \mathbb{R}$). It turns out that all characters have the form $x \mapsto e^{i\xi x}$, for $\xi \in \mathbb{R}$. Thus $\widehat{\mathbb{R}} = \mathbb{R}$, that is \mathbb{R} is self-dual. If $f : \mathbb{R} \rightarrow \mathbb{C}$ is integrable then we define

$$\widehat{f}(\xi) := \int_{-\infty}^{\infty} f(x) e^{-i\xi x} dx.$$

(Strictly speaking, this is an abuse of notation: the Fourier transform is really defined “at the character $x \mapsto e^{i\xi x}$, and not at ξ .)

EXAMPLE 4.2 ($G = \mathbb{Z}$). It turns out that all characters have the form $n \mapsto e^{2\pi i\theta n}$, where $\theta \in \mathbb{R}/\mathbb{Z}$. Thus $\widehat{\mathbb{Z}} = \mathbb{R}/\mathbb{Z}$. If $f : \mathbb{Z} \rightarrow \mathbb{C}$ is suitably nice we define

$$\widehat{f}(\theta) := \sum_{n \in \mathbb{Z}} f(n) e^{-2\pi i\theta n}.$$

(This is again an abuse of notation, similar to the previous one.)

EXAMPLE 4.3 ($G = \mathbb{R}/\mathbb{Z}$: “Fourier series”). Here all the characters have the form $\theta \mapsto e^{2\pi i n \theta}$, where $n \in \mathbb{Z}$. Thus $\widehat{\mathbb{R}/\mathbb{Z}} = \mathbb{Z}$. If $f : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$ is suitably nice we define

$$\widehat{f}(n) := \int_0^1 f(\theta) e^{-2\pi i n \theta} d\theta.$$

The last two groups, \mathbb{Z} and \mathbb{R}/\mathbb{Z} , are an example of a *dual pair*.

EXAMPLE 4.4 ($G = \mathbb{Z}/N\mathbb{Z}$: Discrete Fourier transform). Here all characters have the form $x \mapsto e^{2\pi i r x/N}$, where $r \in \mathbb{Z}/N\mathbb{Z}$ (thus $\widehat{G} \cong G$). In this finite setting all functions are “suitably nice” and we define

$$\widehat{f}(r) := \mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) e^{-2\pi i r x/N} = \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) e^{-2\pi i r x/N}.$$

EXAMPLE 4.5 ($G = \mathbb{R}_{\geq 0}^\times$: Mellin transform). In fact, G is isomorphic to \mathbb{R} via the logarithm map $x \mapsto \log x$. The characters are $x \mapsto x^{i\xi}$ for $\xi \in \mathbb{R}$. We have

$$\widehat{f}(\xi) = \int_0^\infty f(x) x^{-i\xi} d^\times x,$$

where $d^\times x = \frac{dx}{x}$.

The Mellin transform will feature prominently later on. We will need to extend its domain of definition from $i\mathbb{R}$ to all of \mathbb{C} , defining

$$\widetilde{f}(s) := \int_0^\infty f(x) x^s d^\times x$$

(we recover the previous definition on taking $s = -i\xi$). Often we will be look at a fixed vertical contour $s = \sigma + i\mathbb{R}$, in which case the Mellin transform really is a Fourier transform, in fact of the function $f(x)x^{-\sigma}$ on $\mathbb{R}_{\geq 0}^\times$.

Much of the theory of Fourier analysis is concerned with what is meant by “suitably nice”, and with such questions as when one can prove an inversion formula and what the decay of Fourier coefficients tells us about the smoothness of a function. This is a fascinating theory. However for much of analytic number theory the deeper parts of this theory can be avoided.

In this course we will work with particularly nice classes of functions called Schwartz functions, where most of the analytic issues can be avoided and Fourier analysis takes on an almost “algebraic” flavour.

4.2. Fourier analysis of Schwarz functions on \mathbb{R}

In this section, and for the rest of the course, we use the symbol ∂ for the differentiation operator. We also use the notation $\|f\|_1 := \int_{-\infty}^\infty |f(x)| dx$.

The Fourier transform of a smooth function decays rapidly. This fundamental fact will be used repeatedly in this course.

LEMMA 4.1 (Fourier decay properties). *Suppose that $g : \mathbb{R} \rightarrow \mathbb{R}$ is a smooth function, all of whose derivatives lie in $L^1(\mathbb{R})$ (that is, are integrable) and decay to infinity. Then for any m we have the decay estimate*

$$|\widehat{g}(\xi)| \leq |\xi|^{-m} \|\partial^m g\|_1.$$

Remark. In particular, if g is regarded as fixed then we have $|\widehat{g}(\xi)| \ll_m |\xi|^{-m}$ for all m .

Proof. Recall the definition of the Fourier transform, that is to say

$$\widehat{g}(\xi) := \int_{-\infty}^{\infty} g(x) e^{-i\xi x} dx.$$

Repeated integration by parts gives

$$\widehat{g}(\xi) = \left(-\frac{1}{i\xi}\right)^m \int_{-\infty}^{\infty} \partial^m g(x) e^{i\xi x} dx.$$

The result then follows immediately from the triangle inequality. \square

We now introduce a proper notion of “sufficiently nice” function which is appropriate to Fourier analysis on \mathbb{R} is that of a *Schwartz function*. This is a smooth function, all of whose derivatives decay rapidly at infinity.

DEFINITION 4.1 (Schwartz space $\mathcal{S}(\mathbb{R})$). Let $f \in C^\infty(\mathbb{R})$, that is to say suppose that f is infinitely differentiable. We say that f belongs to Schwartz space $\mathcal{S}(\mathbb{R})$ if

$$\lim_{|x| \rightarrow \infty} |x|^n \partial^m f(x) = 0$$

for all integers $m, n \geq 0$.

We note in particular that, since $\partial^m f(x) \ll |x|^{-2}$ for large x , every derivative of a Schwartz function f lies in $L^1(\mathbb{R})$ and hence has well-defined Fourier transform.

One of the main reasons for introducing this definition is that the Fourier transform maps Schwartz functions to Schwartz functions.

LEMMA 4.2 (Fourier transforms of Schwartz functions are Schwartz). *Suppose that $f \in \mathcal{S}(\mathbb{R})$. Then $\widehat{f} \in \mathcal{S}(\mathbb{R})$.*

Proof. Note first of all that if $f \in \mathcal{S}(\mathbb{R})$ then, for any fixed $n \in \mathbb{Z}_{\geq 0}$, $x^n f \in \mathcal{S}(\mathbb{R})$ as well. This follows easily by differentiating $x^n f$ repeatedly using the product rule; each term is of the form $x^{n'} \partial^j f$ for some $n' \leq n$ and $j \geq 0$, and every such term decays quicker than any power of x .

Now differentiation under the integral in the definition of Fourier transform furnishes the following relation:

$$\partial^n \widehat{f}(\xi) = (-2\pi i)^n (x^n f)^\wedge(\xi).$$

Since $x^n f$ is a Schwarz function, all of its derivatives lie in $L^1(\mathbb{R})$. It follows from Lemma 4.1 that $\partial^n \widehat{f}(\xi)$ decays quicker than any polynomial, and hence $\widehat{f} \in \mathcal{S}(\mathbb{R})$.

□

Using Fubini's theorem, which is always valid when dealing with Schwartz functions, we can deduce the following important property of the Fourier transform.

LEMMA 4.3. *Suppose that $f, g \in \mathcal{S}(\mathbb{R})$. Then*

$$\int_{\mathbb{R}} f\widehat{g} = \int_{\mathbb{R}} \widehat{f}g.$$

We will need an explicit form for the Fourier transform of Gaussian functions. This is also used, in its own right, in the proof of Lemma 5.1.

LEMMA 4.4 (Fourier transform of Gaussians). *Suppose that $t \in \mathbb{R}^+$, and set $f(x) = e^{-\pi x^2 t}$. Then $\widehat{f}(\xi) = \frac{1}{\sqrt{t}} e^{-\xi^2/4\pi t}$.*

Proof. Observe that

$$(4.1) \quad \widehat{f}(\xi) = e^{-\xi^2/4\pi t} \int_{-\infty}^{\infty} e^{-\pi t(x + \frac{i\xi}{2\pi t})^2} dx = e^{-\xi^2/4\pi t} \int_{\Gamma_1} f(z) dz,$$

where Γ_1 is the line contour running from $\infty + i\xi/2\pi t$ to $-\infty + i\xi/2\pi t$. To evaluate this contour integral, integrate f (which is clearly defined on all of \mathbb{C}) around the box defined by contours $\Gamma_{1,R} = [R + i\xi/2\pi t, -R + i\xi/2\pi t]$, $\Gamma_{2,R} = [-R + i\xi/2\pi t, -R]$, $\Gamma_{3,R} = [-R, R]$ and $\Gamma_{4,R} = [R, R + i\xi/2\pi t]$. Clearly $\int_{\Gamma_{2,R}} f(z) dz$ and $\int_{\Gamma_{4,R}} f(z) dz$ both tend to 0 as $R \rightarrow \infty$, and so by Cauchy's theorem

$$\int_{\Gamma_1} f(z) dz = \lim_{R \rightarrow \infty} \int_{\Gamma_{1,R}} f(z) dz = - \lim_{R \rightarrow \infty} \int_{\Gamma_{3,R}} f(z) dz = \int_{-\infty}^{\infty} e^{-\pi x^2 t} dx.$$

This last integral may be evaluated as $1/\sqrt{t}$ by making a simple substitution and recalling the Gaussian integral

$$\int_{-\infty}^{\infty} e^{-\pi x^2} dx = 1.$$

This concludes the proof of the lemma. □

Let $\epsilon > 0$. Taking $t = \epsilon^2/4\pi^2$ in the preceding lemma we see that if

$$g_\epsilon(x) := \frac{1}{\epsilon} e^{-\pi x^2/\epsilon^2}$$

then $g_\epsilon(u) = \widehat{\phi}_\epsilon(u)$, where

$$\phi_\epsilon(x) := \frac{1}{2\pi} e^{-x^2 \epsilon^2 / 4\pi}.$$

We are now in a position to prove one of the key results concerning Fourier analysis on \mathbb{R} , the *Fourier inversion formula*.

PROPOSITION 4.1 (Fourier inversion formula for Schwartz functions). *Suppose that $f \in \mathcal{S}(\mathbb{R})$. Then*

$$f(x) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \widehat{f}(\xi) e^{ix\xi} d\xi.$$

REMARK. The factor 2π is a manifestation of the fact that we have two copies of \mathbb{R} here, namely \mathbb{R} and $\widehat{\mathbb{R}}$. In our definition of the Fourier transform we have implicitly given an isomorphism from \mathbb{R} to $\widehat{\mathbb{R}}$. Under this isomorphism Lebesgue measure on \mathbb{R} gets multiplied by a factor of 2π .

Proof. It suffices to establish this when $x = 0$, since if f is Schwartz then so is the function $(T_x f)(y) = f(x + y)$, and $(T_x f)^\wedge(\xi) = e^{ix\xi} \widehat{f}(\xi)$. This affords some notational simplicity.

Using Lemma 4.3 we obtain

$$\int_{-\infty}^{\infty} f(u) g_\epsilon(u) du = \frac{1}{2\pi} \int_{-\infty}^{\infty} \widehat{f}(\xi) e^{-\xi^2 \epsilon^2 / 4\pi} d\xi.$$

Taking limits as $\epsilon \rightarrow 0$, we see that

$$\frac{1}{2\pi} \int_{-\infty}^{\infty} \widehat{f}(\xi) e^{-\xi^2 \epsilon^2 / 4\pi} d\xi \rightarrow \frac{1}{2\pi} \int_{-\infty}^{\infty} \widehat{f}(\xi) d\xi.$$

It suffices, then, to show that

$$f(0) = \lim_{\epsilon \rightarrow 0} \int_{-\infty}^{\infty} f(u) g_\epsilon(u) du.$$

This is “clear” and not too difficult to justify rigorously either. To do so, let $\delta > 0$. Since $\int g_\epsilon = 1$, we see that it suffices to show that

$$\lim_{\epsilon \rightarrow 0} \int_{-\infty}^{\infty} (f(u) - f(0)) g_\epsilon(u) du = 0.$$

To do this we divide the integral into the two ranges $|u| \leq \delta$ and $|u| \geq \delta$. The integral over the first range is bounded by

$$\sup_{|u| \leq \delta} |f(u) - f(0)|.$$

The integral over the second is at most

$$2\|f\|_\infty \int_{|u| \geq \delta} g_\epsilon(u) du.$$

Note that

$$\int_{x \geq \delta} g_\epsilon(x) dx = \int_{x \geq \delta/\epsilon} e^{-\pi x^2} dx,$$

which clearly tends to 0 as $\delta/\epsilon \rightarrow \infty$. Putting these two facts together we obtain

$$\left| \int_{-\infty}^{\infty} (f(u) - f(0))g_\epsilon(u) du \right| \leq \sup_{|u| \leq \delta} |f(0) - f(u)| + \|f\|_\infty o_{\delta/\epsilon \rightarrow \infty}(1).$$

Since f is continuous at 0, this can be made as small as desired by choosing δ small, and then ϵ even smaller (say $\epsilon = \delta^2$) so that $\delta/\epsilon \rightarrow \infty$. \square

REMARK. It is possible to axiomatize the properties of the system (g_ϵ) that made this work, obtaining the notion of a sequence of “approximations to the identity”. We shall not do so here.

A consequence of this and Lemma 4.3 is Plancherel’s formula.

PROPOSITION 4.2 (Plancherel). *Suppose that $f \in \mathcal{S}(\mathbb{R})$. Then*

$$\int_{-\infty}^{\infty} |f(x)|^2 dx = 2\pi \int_{-\infty}^{\infty} |\widehat{f}(\xi)|^2 d\xi.$$

Proof. Take $g := \widehat{\widehat{f}}$ in Lemma 4.3, which stated that

$$\int_{-\infty}^{\infty} f\widehat{g} = \int_{-\infty}^{\infty} \widehat{f}g.$$

The right hand side is $\int |\widehat{f}|^2$. Meanwhile

$$\widehat{g}(x) = \int \widehat{\widehat{f}(\xi)} e^{-i\xi x} = \frac{1}{2\pi} \overline{f(x)},$$

by the inversion formula. The result follows. \square

4.3. Fourier analysis on \mathbb{Z} and \mathbb{R}/\mathbb{Z}

In the proof of the functional equation for ζ we will make use of some Fourier analysis on the group \mathbb{Z} and its dual \mathbb{R}/\mathbb{Z} . We will only develop this theory for sufficiently smooth “Schwartz” functions, and it parallels the theory over \mathbb{R} – just discussed very closely. This is an illustration of the fact that the natural place for harmonic analysis is on a general LCAG.

DEFINITION 4.2 (Schwarz spaces). We define $\mathcal{S}(\mathbb{R}/\mathbb{Z})$ to be the same as $C^\infty(\mathbb{R}/\mathbb{Z})$, the space of smooth functions on \mathbb{R}/\mathbb{Z} . (There is no “decay at infinity” condition for this group, which is compact.) We define $\mathcal{S}(\mathbb{Z})$ to be the space of functions $f : \mathbb{Z} \rightarrow \mathbb{C}$ with the property that $\lim_{|n| \rightarrow \infty} |n|^k |f(n)| = 0$ for all k . (There is no “smoothness” condition for this group, which is discrete.)

Recall the definition of the Fourier transform on \mathbb{R}/\mathbb{Z} :

$$(4.2) \quad \widehat{f}(n) := \int_0^1 f(\theta) e^{-2\pi i n \theta} d\theta$$

for $n \in \mathbb{Z}$. Recall also the definition of the Fourier transform on \mathbb{Z} :

$$(4.3) \quad \widehat{f}(\theta) = \sum_{n \in \mathbb{Z}} f(n) e^{-2\pi i \theta n}$$

for $\theta \in \mathbb{R}/\mathbb{Z}$. Although we are using the hat symbol in two rather different contexts at once, little(!) confusion should result so long as the reader is careful to note which group function under consideration is defined upon.

Differentiation of (4.2) tells us that if $f \in \mathcal{S}(\mathbb{Z})$ then $\partial^k \widehat{f}(\theta) = (-2\pi i)^k (n^k f)^\wedge(\theta)$. Integration by parts of (4.3) tells us that if $f \in \mathcal{S}(\mathbb{R}/\mathbb{Z})$ then $(2\pi i n)^k \widehat{f}(n) = (\partial^k f)^\wedge(n)$.

These properties once again allow us to establish closure of the Schwartz classes under the Fourier transform.

LEMMA 4.5 (Fourier transform respects Schwartz classes). *If $f \in \mathcal{S}(\mathbb{R}/\mathbb{Z})$ then $\widehat{f} \in \mathcal{S}(\mathbb{Z})$. If $f \in \mathcal{S}(\mathbb{Z})$ then $\widehat{f} \in \mathcal{S}(\mathbb{R}/\mathbb{Z})$.*

Proof. This is actually somewhat easier than the proof of Lemma 4.2 and is left to the reader. □

Once again an application of Fubini's theorem (in this case an interchange of integration and summation) allows one to conclude the following.

LEMMA 4.6. *Suppose that $f \in \mathcal{S}(\mathbb{R}/\mathbb{Z})$ and $g \in \mathcal{S}(\mathbb{Z})$. Then $\sum_n \widehat{f}(n)g(n) = \int_0^1 f(\theta)\widehat{g}(\theta) d\theta$.*

Now it is time to prove the inversion formula. In this setting, with two different groups \mathbb{Z} and \mathbb{R}/\mathbb{Z} , there are two different inversion formulæ. One is almost trivial:

PROPOSITION 4.3 (Fourier inversion formula for $\mathcal{S}(\mathbb{Z})$). *Suppose that $f \in \mathcal{S}(\mathbb{Z})$. Then*

$$f(n) = \int_0^1 \widehat{f}(\theta) e^{2\pi i n \theta} d\theta.$$

Proof. Substitute in the definition of $\widehat{f}(\theta)$ and swap the order of summation and integration. Then use the fact that

$$\int_0^1 e^{2\pi i m \theta} d\theta = 0$$

when $m \in \mathbb{Z} \setminus \{0\}$. □

The other inversion formula is less trivial (it is also the one that we need in establishing the Poisson summation formula). It is proved using a type of “approximation to the identity” rather analogous to the use of gaussians in the proof of Proposition 4.1.

PROPOSITION 4.4 (Fourier inversion formula for $\mathcal{S}(\mathbb{R}/\mathbb{Z})$). *Suppose that $f \in \mathcal{S}(\mathbb{R}/\mathbb{Z})$. Then*

$$f(\alpha) = \sum_{n \in \mathbb{Z}} \widehat{f}(n) e^{2\pi i n \alpha}.$$

Proof. We will use Lemma 4.6 and will deal with the case $\alpha = 0$ for notational simplicity (the general case may, as before, be deduced from this rather easily). Define, for $N \in \mathbb{N}$,

$$g_N(n) := \left(1 - \frac{|n|}{N}\right) 1_{|n| \leq N}.$$

By direct computation one may see that

$$\widehat{g}_N(\theta) = \frac{1}{N} \left| \frac{1 - e^{-2\pi i \theta N}}{1 - e^{-2\pi i \theta}} \right|^2 = \frac{\sin^2(\pi \theta N)}{N \sin^2(\pi \theta)}.$$

(A more conceptual way to establish this is to observe that $g_N = N h_N * h_N^\circ$, where $h_N(n) := N^{-1} 1_{0 \leq n \leq N-1}$, the $*$ denotes convolution and $h_N^\circ(n) = h_N(-n)$. The Fourier transform of g_N is then just the absolute value of the square of \widehat{h}_N . We note that the gaussian g_ϵ is also the convolution of a function with itself, that function being a gaussian of half the width.)

Write

$$K_N(\theta) := \frac{\sin^2(\pi \theta N)}{N \sin^2(\pi \theta)}.$$

This is called the *Fejér kernel*.

From Lemma 4.6 we know that

$$\sum_{n \in \mathbb{Z}} \widehat{f}(n) g_N(n) = \int_{-1/2}^{1/2} f(\theta) K_N(\theta) d\theta.$$

(Later on, it is notationally convenient to take the range of integration over $[-1/2, 1/2]$; since the integrand has period 1, this is permissible.) It is quite easy to see that

$$\lim_{N \rightarrow \infty} \sum_{n \in \mathbb{Z}} \widehat{f}(n) g_N(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(n).$$

It remains, then, to show that

$$(4.4) \quad \lim_{N \rightarrow \infty} \int_{-1/2}^{1/2} f(\theta) K_N(\theta) d\theta = f(0).$$

Since for large N the mass of $K_N(\theta)$ is concentrated near $\theta \approx 0$, so this is “intuitively clear”, in the same way it was in the proof of Proposition 4.1. The details are

remarkably similar as well, and depend on the following properties of the Fejér kernel, which again constitute a notion of “approximation to the identity”:

- (i) $K_N(\theta) \geq 0$
- (ii) $\int_0^1 K_N(\theta) d\theta = 1$
- (iii) $\int_{1/2 \geq |\theta| \geq \delta} K_N(\theta) d\theta \ll \frac{1}{N\delta}$.

To prove (ii), one would do best to recall the definition of $K_N(\theta)$ as $\widehat{g}_N(\theta)$, rather than attempt to integrate the closed form of K_N directly. The proof of (iii) is straightforward using the fact that $|\sin t| \geq 2|t|/\pi$ for $|t| \leq \pi/2$. Indeed we have

$$\int_{1/2 \geq |\theta| \geq \delta} K_N(\theta) d\theta \ll \frac{1}{N} \int_{\delta}^{1/2} \frac{1}{|\theta|^2} d\theta \ll \frac{1}{\delta N}.$$

Returning to the proof of (??), observe that from (ii) we have

$$\int_{-1/2}^{1/2} f(\theta) K_N(\theta) d\theta - f(0) = \int_{-1/2}^{1/2} (f(\theta) - f(0)) K_N(\theta) d\theta.$$

Split the range of integration into two ranges, $|\theta| \leq \delta$ and $\delta < |\theta| \leq \frac{1}{2}$. The integral over the first range is bounded by

$$\sup_{|\theta| \leq \delta} |f(\theta) - f(0)| \int_{-1/2}^{1/2} |K_N(\theta)| d\theta$$

which, by (i) and (ii), is at most

$$(4.5) \quad \sup_{|\theta| \leq \delta} |f(\theta) - f(0)|.$$

The integral over the second range is bounded by

$$2\|f\|_{\infty} \int_{\delta < |\theta| \leq \frac{1}{2}} |K_N(\theta)| d\theta$$

which, by (iii), is at most

$$(4.6) \quad \ll \|f\|_{\infty} \frac{1}{N\delta}.$$

Taking $N = \lceil 1/\delta^2 \rceil$ (say) and letting $\delta \rightarrow 0$, we see that both (4.5) and (4.6) tend to 0. This concludes the proof of Theorem 4.4.

We conclude this section by stating, as a corollary, the only result concerning Fourier series that is actually needed in the course (in the proof of the Poisson summation formula).

COROLLARY 4.1 (Uniqueness for Fourier series). *Suppose that $f_1, f_2 \in C^{\infty}(\mathbb{R}/\mathbb{Z})$ are two functions with $\widehat{f}_1(n) = \widehat{f}_2(n)$ for all $n \in \mathbb{Z}$. Then $f_1 \equiv f_2$ identically.*

Proof. This is absolutely immediate from Proposition 4.4. □

4.4. The Poisson summation formula

An important ingredient in the proof of the functional equation for the ζ -function is a version of the *Poisson summation formula*.

LEMMA 4.7 (Poisson summation). *Suppose that $f \in \mathcal{S}(\mathbb{R})$. Then*

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(2\pi n).$$

Proof. Consider two functions $F, G : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$, defined by

$$F(\theta) := \sum_{n \in \mathbb{Z}} \widehat{f}(2\pi n) e^{2\pi i n \theta}$$

and

$$G(\theta) := \sum_{k \in \mathbb{Z}} f(\theta + k).$$

Due to our conditions on f it is straightforward to check that F and G are C^∞ -functions. We will compute their Fourier coefficients, the aim being to show that these are equal. On the one hand we have, for $m \in \mathbb{Z}$,

$$\begin{aligned} \widehat{F}(m) &:= \int_0^1 \left(\sum_{n \in \mathbb{Z}} \widehat{f}(2\pi n) e^{2\pi i n \theta} \right) e^{-2\pi i m \theta} d\theta \\ &= \sum_{n \in \mathbb{Z}} \widehat{f}(2\pi n) \int_0^1 e^{2\pi i (n-m)\theta} d\theta \\ &= \widehat{f}(2\pi m). \end{aligned}$$

On the other hand, we have

$$\begin{aligned} \widehat{G}(m) &:= \int_0^1 \left(\sum_{k \in \mathbb{Z}} f(\theta + k) \right) e^{-2\pi i m \theta} d\theta \\ &= \int_0^1 \left(\sum_{k \in \mathbb{Z}} f(\theta + k) \right) e^{-2\pi i m (\theta + k)} d\theta \\ &= \sum_{k \in \mathbb{Z}} \int_k^{k+1} f(x) e^{-2\pi i m x} dx, \end{aligned}$$

which is also equal to $\widehat{f}(2\pi m)$. Thus indeed $\widehat{F}(n) = \widehat{G}(n)$, which by Corollary 4.1 implies that $F = G$ identically. In particular $F(0) = G(0)$, which is exactly the Poisson summation formula. \square

The analytic continuation and functional equation

5.1. The Γ -function

Define the Γ -function by

$$(5.1) \quad \Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt.$$

for $\operatorname{Re} z > 0$. Observe that if $\operatorname{Re} z > 0$ then, since $|t^{z-1}| = t^{\operatorname{Re} z - 1}$, the integral converges.

In Proposition 5.1 below, we establish the basic facts about Γ . Before doing this we record a result from complex analysis connected with “Weierstrass products”.

PROPOSITION ?? (Weierstrass product). Suppose that Ω is such that $0 \notin \Omega$ and $\sum_{\rho \in \Omega} |\rho|^{-2} < \infty$ (where the sum over Ω is taken with multiplicity). Then the function

$$E_\Omega(z) := \prod_{\rho \in \Omega} \left(1 - \frac{z}{\rho}\right) e^{z/\rho}$$

is well-defined, entire (i.e. holomorphic on the whole complex plane), and has zeros at Ω with the correct multiplicities and nowhere else.

A proof of this proposition may be found in Appendix ???. Of course, the proposition seems eminently reasonable and if Ω were finite it would be trivial. The factors of $e^{z/\rho}$ ensure that the product converges; note that $(1-w)e^w \approx 1-w^2 \approx e^{-w^2}$ for small w , and so one sees that convergence of the product is intimately tied to convergence of $\sum \rho^{-2}$.

PROPOSITION 5.1. *We have the following basic facts about the Γ -function.*

- (i) $\Gamma(z)$, as defined by (5.1), is holomorphic in $\operatorname{Re} z > 0$.
- (ii) $\Gamma(z)$ extends to a meromorphic function all of \mathbb{C} , satisfying the functional equation $z\Gamma(z) = \Gamma(z+1)$. It has simple poles at $z = 0, -1, -2, \dots$ and no other poles.
- (iii) We have the Weierstrass product

$$\frac{1}{\Gamma(z)} = ze^{\gamma z} \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right) e^{-z/n}$$

for all complex z , where

$$\gamma := \lim_{n \rightarrow \infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n \right).$$

In particular, $\Gamma(z)$ is never 0.

Remark. One can easily establish that γ exists by comparing the sum $\sum_{j=1}^n j^{-1}$ with the integral $\int_1^n dx/x$. We have $\gamma = 0.577215665\dots$. The number γ is rather mysterious, and in fact it is not even known to be irrational.

Proof. (i) We claim that the derivative of Γ is $\int_0^\infty e^{-t} t^{z-1} \log t dt$ (that is, the “obvious” choice based on differentiating under the integral). To prove this we must show that

$$\lim_{h \rightarrow 0} \int_0^\infty e^{-t} t^{z-1} \left(\frac{t^h - 1}{h} - \log t \right) dt = 0.$$

Since the derivative of t^s at $s = 0$ is $\log t$, this follows by interchanging the order of the limit and the integral, provided this can be justified. Suppose that $\operatorname{Re} z = \delta$. By the dominated convergence theorem, it is enough to show that

$$(5.2) \quad e^{-t} t^{z-1} \sup_{|h| \leq \delta/2} \left| \frac{t^h - 1}{h} - \log t \right|$$

is integrable from 0 to ∞ . Now $(t^h - 1)/h$ is an analytic function of h (it has a removable singularity at $h = 0$). By the maximum modulus principle we have

$$\sup_{|h| \leq \delta/2} \left| \frac{t^h - 1}{h} \right| = \sup_{|h| = \delta/2} \left| \frac{t^h - 1}{h} \right| \ll_\delta 1 + t^{\delta/2}.$$

Thus (5.2) is bounded by

$$\ll_\delta e^{-t} t^{\delta-1} (1 + t^{\delta/2} + |\log t|).$$

This function is indeed integrable: as $t \rightarrow \infty$, the e^{-t} more than compensates for the other terms, and as $t \rightarrow 0$ we are only integrating functions that behave like t^{-c} for $c < 1$.

(ii) Suppose first that $\operatorname{Re} z > 0$. Integrating by parts we have, provided $\operatorname{Re} z > 0$,

$$\begin{aligned} \Gamma(z+1) &= [-t^z e^{-t}]_0^\infty + z \int_0^\infty e^{-t} t^{z-1} dt \\ &= z\Gamma(z). \end{aligned}$$

This relation may be used to extend Γ meromorphically to the entire complex plane. One begins by extending it to the domain $\operatorname{Re} z > -1$ via the formula $\Gamma(z) := \Gamma(z+1)/z$. One can then iterate, extending in turn to the domains $\operatorname{Re} z > -n$, $n = 2, 3, \dots$. Note that in the process of extending to $\operatorname{Re} z > -1$ we introduce a pole at $z = 0$. This propagates along so that we get simple poles at all negative

integers $n = -1, -2, \dots$ as well. $\Gamma(z)$ is meromorphic, and the poles just described are the only ones.

(iii) Define the function $\tilde{\Gamma}$ by

$$(5.3) \quad \frac{1}{\tilde{\Gamma}(z)} := ze^{\gamma z} \prod_{n=1}^{\infty} (1 + z/n)e^{-z/n}.$$

By Proposition ??, $\frac{1}{\tilde{\Gamma}}$ is entire and has zeros only at $0, -1, -2, \dots$. Therefore $\tilde{\Gamma}$ is meromorphic on \mathbb{C} (with poles at $0, -1, -2, \dots$).

Our aim, of course, is to show that $\Gamma(z) = \tilde{\Gamma}(z)$ for all $z \in \mathbb{C}$. By the identity principle and the fact that both Γ and $\tilde{\Gamma}$ are meromorphic, it suffices to establish this when $\operatorname{Re} z > 0$.

Consider, for positive integer m , the function

$$f_m(t) := (1 - t/m)^m \mathbf{1}_{[0, m]}(t).$$

Note that $f_m(t) \leq e^{-t}$ for all m (since $1 - x \leq e^{-x}$ when $x \geq 0$) and that $\lim_{m \rightarrow \infty} f_m(t) = e^{-t}$ for every t . By the dominated convergence theorem it follows that if $\operatorname{Re} z > 0$ then

$$(5.4) \quad \lim_{m \rightarrow \infty} \int_0^{\infty} f_m(t) t^{z-1} dt = \int_0^{\infty} e^{-t} t^{z-1} dt = \Gamma(z).$$

On the other hand one may verify, by repeated integration by parts, the formula

$$(5.5) \quad \int_0^{\infty} f_m(t) t^{z-1} dt = \frac{m^z m!}{z(z+1)\dots(z+m)}$$

(first make the substitution $t = mu$ to write the integral as

$$m^z \int_0^1 (1-u)^m u^{z-1} du.)$$

Thus, from (5.3) and some rearrangement we have

$$\int_0^{\infty} f_m(t) t^{z-1} dt = \tilde{\Gamma}(z) e^{(\gamma - 1 - \frac{1}{2} - \dots - \frac{1}{m} + \log m)z} \prod_{n=m+1}^{\infty} (1 + z/n) e^{-z/n}.$$

Since the infinite product converges for every z , it follows from this and the definition of γ that

$$\lim_{m \rightarrow \infty} \int_0^{\infty} f_m(t) t^{z-1} dt = \tilde{\Gamma}(z).$$

Comparing this with (5.4) tells us that indeed $\Gamma(z) = \tilde{\Gamma}(z)$ for $\operatorname{Re} z > 0$. \square

We note that, as an easy deduction from (ii), we have $\Gamma(k+1) = k!$ for all positive integers k .

5.2. Statement of the functional equation for ζ

Define the *completed ζ -function* by

$$\Xi(s) = \gamma(s)\zeta(s),$$

where the *gamma factor* $\gamma(s)$ is defined to equal $\pi^{-s/2}\Gamma(s/2)$. Our objective in this section is to prove the following theorem, the functional equation for ζ .

THEOREM 5.1. *The completed ζ -function Ξ is meromorphic in \mathbb{C} , and its only poles are simple ones at $s = 0$ and 1 . It satisfies the functional equation*

$$\Xi(s) = \Xi(1 - s).$$

As a corollary we obtain the first part of Theorem 3.1, the main result of this chapter about the ζ -function.

COROLLARY 5.1. *The ζ -function has a meromorphic continuation to all of \mathbb{C} . It has a simple pole at $s = 1$ and no other poles. It has zeros at $s = -2, -4, -6, \dots$ and no other zeros outside of the critical strip $0 \leq \operatorname{Re} s \leq 1$.*

Proof. The meromorphic continuation is obvious, since $\zeta(s) = \pi^{s/2}(\Gamma(s/2))^{-1}\Xi(s)$ and the three functions here are all meromorphic. The statements about zeros and poles are a consequence of the following information, which we have assembled at various earlier points of the course:

- $\Xi(s) = \Xi(1 - s)$ and the only poles of Ξ are simple ones at $s = 0$ and $s = 1$;
- Γ has no zeros and simple poles at $0, -1, -2, \dots$;
- ζ has no zeros with $\operatorname{Re} s > 1$.

□

The set of all zeros of ζ will be denoted by Z . We further divide this set into the set of *trivial zeros* Z_{triv} , by which we mean $-2, -4, -6, \dots$, and *nontrivial zeros* Z_{nontriv} , by which we mean all the other zeros. By the above corollary every zero in Z_{nontriv} lies in the critical strip $0 \leq \operatorname{Re} s \leq 1$.

Note that, with our knowledge at this point, Z_{nontriv} could be empty. In fact it is infinite and one can obtain quite good control on the number of nontrivial zeros with imaginary part at most T . We will return to this later.

5.3. Proof of the functional equation

We turn now to the proof of Theorem 5.1. A key tool here will be the θ -function.

We will apply Lemma 4.7 to derive a functional equation for the θ -function. Let us now define that function. For z in the upper half-plane $\mathcal{H} := \{z : \Im z > 0\}$ set

$$\theta(z) := \sum_{n \in \mathbb{Z}} e^{i\pi n^2 z}.$$

It is quite easy to see that θ is analytic in \mathcal{H} .

LEMMA 5.1. *Suppose that $t \in \mathbb{R}^+$. Then $\theta(it) = \frac{1}{\sqrt{t}}\theta(i/t)$.*

Remark which may be of interest to some: Then this functional equation for θ may be analytically extended to all of \mathcal{H} to give something like $\theta(-1/z) = \sqrt{z}\theta(z)$. We have been deliberately vague about the branch of square root to be taken here. In conjunction with the easily verified relation $\theta(z+2) = \theta(z)$, this means that the function $\theta(2z)$ is a *modular form* of weight $1/2$ for the group $\Gamma_0(4)$ of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$ and $4|c$.

Proof. Suppose that $t \in \mathbb{R}^+$, and set $f(x) = e^{-\pi x^2 t}$. We calculated (by direct calculation) the Fourier transform $\hat{f}(\lambda)$ in Lemma 4.4; indeed

$$\hat{f}(\xi) = \frac{1}{\sqrt{t}} e^{-\xi^2/4\pi t}.$$

Lemma 5.1 is simply a matter of applying the Poisson summation formula in this case. \square

The next lemma relates the ζ -function to the θ -function. It turns out that the ζ -function is, roughly speaking, the *Mellin transform* of θ (we will see Mellin transforms again later).

LEMMA 5.2. *Suppose that $\operatorname{Re} s > 1$. Then*

$$\Xi(s) = \int_0^\infty \left(\frac{\theta(ix) - 1}{2} \right) x^{s/2} \frac{dx}{x}.$$

Proof. Observe that

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

Now simply sum over $n \in \mathbb{N}$. \square

Proof of Theorem 5.1. Suppose that $\operatorname{Re} s > 1$. We split the integral in Lemma 5.2 into the ranges $[0, 1]$ and $[1, \infty)$, and then apply Lemma 5.1 to the first of these.

We have

$$\begin{aligned}
\int_0^1 \left(\frac{\theta(ix) - 1}{2} \right) x^{s/2} \frac{dx}{x} &= \frac{1}{2} \int_0^1 \theta(ix) x^{s/2} \frac{dx}{x} - \frac{1}{s} \\
&= \frac{1}{2} \int_0^1 \theta\left(\frac{i}{x}\right) x^{(s-1)/2} \frac{dx}{x} - \frac{1}{s} \\
&= \frac{1}{2} \int_1^\infty \theta(iu) u^{(1-s)/2} \frac{du}{u} - \frac{1}{s} \\
&= \int_1^\infty \left(\frac{\theta(iu) - 1}{2} \right) u^{(1-s)/2} \frac{du}{u} - \frac{1}{s} - \frac{1}{1-s}.
\end{aligned}$$

Thus

$$\int_0^\infty \left(\frac{\theta(ix) - 1}{2} \right) x^{s/2} \frac{dx}{x} = \int_1^\infty \left(\frac{\theta(ix) - 1}{2} \right) (x^{s/2} + x^{(1-s)/2}) \frac{dx}{x} - \frac{1}{s} - \frac{1}{1-s},$$

which implies that

$$\Xi(s) = \int_1^\infty \left(\frac{\theta(ix) - 1}{2} \right) (x^{s/2} + x^{(1-s)/2}) \frac{dx}{x} - \frac{1}{s} - \frac{1}{1-s}.$$

A priori this formula is valid only for $\operatorname{Re} s > 1$. Note, however, that the right-hand side defines a function which is meromorphic in the whole complex plane, with simple poles at $s = 0$ and 1 , and which manifestly satisfies the claimed relation $\Xi(s) = \Xi(1-s)$. \square

The partial fraction expansion

6.1. Statement of the partial fraction expansion

In prime number theory, the ζ -function itself is less important than the logarithmic derivative ζ'/ζ . This is, of course, because ζ'/ζ is the Dirichlet series of the von Mangoldt function Λ , that is to say $\zeta'(s)/\zeta(s) = \sum_n \Lambda(n)n^{-s}$.

The heart of the link between primes and zeros of ζ is the *partial fraction expansion* of ζ'/ζ .

PROPOSITION 6.1. *There is a constant C such that*

$$\frac{\zeta'(s)}{\zeta(s)} = C - \frac{1}{s-1} + \sum_{\rho \in Z} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right).$$

Here sum is over all zeros $Z = Z_{\text{triv}} \cup Z_{\text{nontriv}}$ of ζ : the trivial zeros $Z_{\text{triv}} := \{-2, -4, -6, \dots\}$ and the nontrivial zeros Z_{nontriv} in the critical strip $0 \leq \text{Re } s \leq 1$.

The constant C can be computed explicitly, but this is not important for most applications; in fact $e^C = \pi\sqrt{2}/e$.

Proposition 6.1 is a consequence of the following *product expansion* and repeated use of the fact that

$$\frac{(fg)'}{fg} = \frac{f'}{f} + \frac{g'}{g}.$$

In fact, we need some version of this for *infinite products*; the justification of this is an exercise on sheet 4.

THEOREM 6.1 (Hadamard Product for ζ). *There are constants A and B (which can be evaluated explicitly) such that*

$$(s-1)\zeta(s) = e^{As+B} \prod_{\rho \in Z} \left(1 - \frac{s}{\rho}\right) e^{s/\rho},$$

where again Z denotes both trivial and nontrivial zeros of ζ . The partial products $\prod_{|\rho| \leq N} \left(1 - \frac{s}{\rho}\right) e^{s/\rho}$ are finite (that is, there are only finitely many ρ with $|\rho| \leq N$) and converge uniformly on any compact set of s . In fact, we have $\sum_{\rho \in Z} |\rho|^{-1-\varepsilon} < \infty$ for any $\varepsilon > 0$.

Theorem 6.1 is quite reminiscent of the well-known fact that if $f : \mathbb{C} \rightarrow \mathbb{C}$ is a polynomial then $f(z) = C \prod_{\rho} (z-\rho)$, where the product is over the (finite) collection

of zeros of f . Of course, $(s-1)\zeta(s)$ is not a polynomial. However, Theorem 6.1 may still be obtained as a consequence of a quite general theorem about entire functions, rather than any particular specific properties of ζ . We state such a theorem now.

DEFINITION 6.1. Suppose that $f : \mathbb{C} \rightarrow \mathbb{C}$ is an entire function satisfying a growth condition $|f(z)| \ll_{\varepsilon} e^{C_{\varepsilon}|z|^{1+\varepsilon}}$ for all $\varepsilon > 0$. Then we say that f is an integral function of order 1.

PROPOSITION 6.2. *Suppose that f is an integral function of order 1. Suppose that f has a zero of order r at 0, and write Ω for the set of other zeros of f . Then $\sum_{\rho \in \Omega} |\rho|^{-1-\varepsilon} < \infty$ and there are constants A and B such that*

$$f(z) = z^r e^{Az+B} \prod_{\rho} \left(1 - \frac{z}{\rho}\right) e^{z/\rho}.$$

Proposition 6.2 is, as we said, a result of complex analysis and has no arithmetic content. The proof is given in Sections 6.3 and 6.4. Some of the details in Section 6.4 are a little technical and this section is not examinable.

6.2. The product formula for ζ

In this section we will deduce Theorem 6.1, the Hadamard product for ζ , from Proposition 6.2, the product expansion for integral functions of order one.

Rather than prove that $(s-1)\zeta(s)$ is an integral function of order one, it is convenient to first include some Γ - and other factors.

LEMMA 6.1. *The function $f(s) = s(1-s)\pi^{-s/2}\Gamma(s/2)\zeta(s) = s(1-s)\Xi(s)$ is an integral function of order one.*

Proof. We have already noted that Ξ is meromorphic except for simple poles at $s = 0, 1$, so f is entire. Therefore we need only establish a growth condition of the form

$$|f(s)| \ll e^{C_{\varepsilon}|s|^{1+\varepsilon}}$$

for all $\varepsilon > 0$. In fact we will establish the stronger bound

$$|f(s)| \ll \exp(O(|s| \log |s|)).$$

Moreover, from the functional equation we have $f(s) = f(1-s)$, and so it is enough to prove this when $\operatorname{Re} s \geq \frac{1}{2}$. When $\operatorname{Re} s \geq \frac{1}{2}$ we have the integral representation

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

that we found in Proposition 3.2. This in fact implies that $|(s-1)\zeta(s)| = O(|s|^2)$ in this domain. For the Γ -factor we also have the integral representation

$$\Gamma(s/2) = \int_0^{\infty} e^{-t} t^{s/2-1} dt,$$

so

$$|\Gamma(s/2)| \leq \Gamma(\frac{1}{2} \operatorname{Re} s) \leq [\frac{1}{2} \operatorname{Re} s + 1]! = \exp(O(|s| \log |s|))$$

This final bound follows from the fact that $X! \ll \exp(O(X \log X))$, which in turn follows from the estimate $\sum_{n \leq X} \log n \sim X \log X$. This may be established by comparison with the integral $\int_1^X \log t dt$. See Exercises 1, Q8 for a more precise result.

It follows from Proposition 6.2 that

$$(6.1) \quad f(s) = e^{As+B} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho},$$

where the product is over the zeros ρ of f . In making this claim we have observed that $f(0) \neq 0$; the simple zero of s cancels the simple pole of $\Gamma(s/2)$, and $\zeta(0) \neq 0$ (the calculation of its exact value being an exercise on sheet 3). The zeros ρ satisfy

$$\sum_{\rho} |\rho|^{-1-\epsilon} < \infty$$

for any $\epsilon > 0$. Note that these zeros ρ are precisely the nontrivial zeros of $\zeta(s)$, namely those in the critical strip $0 \leq \operatorname{Re} s \leq 1$, because the factor of $\Gamma(\frac{1}{2}s)$ cancels out the trivial zeros of ζ at $-2, -4, -6, \dots$

Of course,

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

We may now recover the claimed product formula for $(s-1)\zeta(s)$ from (6.1) and the Weierstrass product for $1/\Gamma$, that is to say Proposition 5.1 (iii). \square

6.3. The size of a holomorphic function and its zeros

To prove Proposition 6.2 we need various facts about the relation between the size of a holomorphic function and the number of its zeros. We collect the facts we need in this section.

Write B_R for the domain $|z| < R$.

THEOREM 6.2 (Jensen's formula). *Let $R, \epsilon > 0$. Suppose that f is holomorphic on $B_{R+\epsilon}$, and that $f(z) \neq 0$ for $R \leq |z| < R + \epsilon$ and for $z = 0$. Then*

$$(6.2) \quad \frac{1}{2\pi} \int_0^{2\pi} \log |f(Re^{i\theta})| d\theta = \log |f(0)| + \sum_{\rho} \log \frac{R}{|\rho|},$$

where the sum is over zeros ρ of f in B_R , counted with multiplicity.

Proof. Observe that if the identity is true for functions f_1 and f_2 then it is also true for $f_1 f_2$. Write

$$g_{\rho}(z) = \frac{R(z - \rho)}{R^2 - \bar{\rho}z}$$

and define a meromorphic function F by

$$f(z) = CF(z) \prod_{\rho} g_{\rho}(z),$$

where C is chosen so that $F(0) = 1$. If ϵ is chosen so small that the poles $z = R^2/\bar{\rho}$ lie outside of $B_{R+\epsilon}$ then F has no zeros in $B_{R+\epsilon}$. Jensen's formula being manifestly true for constant functions, it suffices to check it for F and for the functions g_{ρ} . Now we may define a single-valued, holomorphic logarithm of F in $B_{R+\epsilon}$ by the formula

$$\log F(z) := \int_{[0 \rightarrow z]} \frac{F'(w)}{F(w)} dw.$$

Since $F(0) = 1$ the function $z^{-1} \log F(z)$ is also holomorphic in $B_{R+\epsilon}$. Hence by Cauchy's theorem we have

$$\int_{\partial B_R} \frac{\log F(z)}{z} dz = 0.$$

Parametrising the circle ∂B_R by $z = Re^{i\theta}$, $0 \leq \theta < 2\pi$ we get

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

Taking real parts gives

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

This is one side of (6.2); the other side is clearly zero. Thus we have verified the formula for F .

Turning our attention to the functions g_{ρ} , note that if $|z| = R$ then

$$|g_{\rho}(z)| = \left| \frac{\bar{z}(z - \rho)}{R^2 - \bar{\rho}z} \right| = 1.$$

Thus the left-hand side of (6.2) equals 0. As for the right-hand side, note that $|g_{\rho}(0)| = |\rho|/R$. Thus the right-hand side is zero as well. \square

The next result applies Jensen's formula to get a fairly tight relation between the size of a holomorphic function and the number of its zeros.

COROLLARY 6.1. *Let f be an entire function with $f(0) = 1$. Then for any R the number of zeros ρ of f with $|\rho| < R$ is at most $2 \sup_{|z| \leq 3R} \log |f(z)|$.*

Proof. Pick a radius $R_0 \in [2R, 3R]$ such that $f(z) \neq 0$ whenever $|z| = R_0$. This is possible since otherwise f would have infinitely many zeros in the compact set $|z| \leq 3R$, contrary to the identity principle. Jensen's formula immediately gives

$$\sum_{\rho} \log \frac{R_0}{|\rho|} = \frac{1}{2\pi} \int_0^{2\pi} \log |f(R_0 e^{2\pi i \theta})| d\theta \leq \sup_{|z|=R_0} \log |f(z)| \leq \sup_{|z| \leq 3R} \log |f(z)|,$$

where the sum is over all zeros ρ inside B_{R_0} . Each term $\log \frac{R_0}{|\rho|}$ is positive, and the terms corresponding to zeros ρ with $|\rho| < R$ contribute at least $\log 2 > \frac{1}{2}$. \square

A corollary of this and some of our earlier estimates is a bound for the number of zeros of ζ .

PROPOSITION 6.3. *The number of nontrivial zeros of ρ of the Riemann ζ -function with imaginary part at most T is $O(T \log T)$*

Proof. Consider the function $f(s) = s(1-s)\pi^{-s/2}\Gamma(s/2)\zeta(s)$, which vanish at all nontrivial zeros of ζ . We showed earlier in the chapter that f is entire and satisfies the growth condition $|f(s)| \ll e^{O(|s| \log |s|)}$. It follows from Corollary 6.1 that the number of nontrivial zeros of ζ with $|\rho| \leq T+1$ is $O(T \log T)$. If ρ is nontrivial and $|\Im \rho| \leq T$ then $|\rho| \leq T+1$, and so the result follows. \square

The next result does not use Jensen's formula. It tells us the structure of entire functions of moderate growth with *no* zeros.

LEMMA 6.2. *Suppose that g is an entire function with no zeros which satisfies the bound $|g(z)| = \exp(O(|z|^{3/2}))$ whenever $|z| = R_j$, $j = 1, 2, \dots$, where $R_j \rightarrow \infty$ as $j \rightarrow \infty$. Then $g(z) = e^{Az+B}$ for some constants A, B .*

Proof. Multiplying through by a constant, we may assume that $g(0) = 1$. Since g is nonvanishing, it has a holomorphic branch of logarithm $h(z) := \log g(z)$ with $h(0) = 0$, exactly as in the proof of Jensen's formula. We *cannot* immediately conclude that $|h(z)| \ll |z|^{3/2} = R_j^{3/2}$ for $|z| = R_j$, but it does at least follow that $\operatorname{Re} h(z) = \log |g(z)| \leq R_j^{3/2}$, and hence

$$|\operatorname{Re} h(z)| \leq CR_j^{3/2} - \operatorname{Re} h(z)$$

(consider the cases $\operatorname{Re} h(z) \geq 0$ and $\operatorname{Re} h(z) \leq 0$ separately). It follows that

$$(6.3) \quad \frac{1}{2\pi} \int_0^{2\pi} |\operatorname{Re} h(R_j e^{i\theta})| d\theta \leq CR_j^{3/2} - \frac{1}{2\pi} \int_0^{2\pi} \operatorname{Re} h(R_j e^{i\theta}) d\theta = CR_j^{3/2},$$

using the fact that $\frac{h(z)}{z}$ is holomorphic, as in the proof of Jensen's formula.

Now if the Taylor expansion of $h(z)$ is $\sum_{n=0}^{\infty} c_n z^n$ then we have

$$2 \operatorname{Re}(h(R_j e^{i\theta})) = \sum_{n \geq 0} c_n R_j^n e^{in\theta} + \sum_{n \geq 0} \bar{c}_n R_j^n e^{-in\theta}.$$

By orthogonality it follows that

$$c_m = R_j^{-m} \frac{1}{\pi} \int_0^{2\pi} \operatorname{Re}(h(R_j e^{i\theta})) e^{-im\theta} d\theta,$$

and so by the triangle inequality

$$|c_m| \leq R_j^{-m} \frac{1}{\pi} \int_0^{2\pi} |\operatorname{Re} h(R_j e^{i\theta})| d\theta.$$

By (6.3) it follows that

$$|c_m| \ll R_j^{3/2-m}.$$

Letting $j \rightarrow \infty$, this implies that $c_2 = c_3 = \dots = 0$, and so $h(z) = c_0 + c_1 z$ is linear. This concludes the proof. \square

Remark. This is quite hard to get right; the argument I gave in lectures was slightly incorrect.

6.4. *Weierstrass product of an integral function of order one: details

The aim of this section, which is not for examination, is to give a detailed proof of Proposition 6.2.

We begin with a statement about products in general. This statement was also used when we discussed the Weierstrass product for $\frac{1}{z}$ in the last chapter.

PROPOSITION 6.4. *Suppose that $\Omega \subset \mathbb{C}$ is such that $0 \notin \Omega$ and $\sum_{\rho \in \Omega} |\rho|^{-2} < \infty$ (where the sum over Ω is taken with multiplicity). Then the function*

$$E_\Omega(z) := \prod_{\rho \in \Omega} \left(1 - \frac{z}{\rho}\right) e^{z/\rho}$$

is well-defined, entire (i.e. holomorphic on the whole complex plane), and has zeros at Ω with the correct multiplicities and nowhere else.

Proof. Consider the truncated products

$$E_\Omega^N(z) := \prod_{\rho \in \Omega: |\rho| \leq N} \left(1 - \frac{z}{\rho}\right) e^{z/\rho}.$$

Here, and in what follows, the product over Ω is taken with multiplicity. The condition $\sum_{\rho \in \Omega} |\rho|^{-2} < \infty$ certainly guarantees that $\{\rho \in \Omega : |\rho| \leq N\}$ is finite for every N , and so $E_\Omega^N(z)$ is well-defined and holomorphic. We claim that $E_\Omega^N(z)$ converges uniformly on compact subsets of \mathbb{C} , which of course implies that $E_\Omega(z)$ is well-defined and entire.

Fix a positive real number K . From now on, implied constants in the $O(\cdot)$ notation may depend on both K and on Ω .

First we claim that for $|z| \leq K$ we have a bound $|E_\Omega^N(z)| = O(1)$, uniformly over all N . To prove the claim, we use the inequality $|(1-w)e^w| \leq 1 + O(|w|^2) \leq e^{O(|w|^2)}$ for $|w| \leq 1$ to conclude that

$$\left| \prod_{K \leq |\rho| \leq N} \left(1 - \frac{z}{\rho}\right) e^{z/\rho} \right| \leq \exp\left(O(K^2 \sum_{|\rho| \geq K} |\rho|^{-2})\right) = O(1).$$

Since, by compactness, we have

$$\left| \prod_{|\rho| < K} \left(1 - \frac{z}{\rho}\right) e^{z/\rho} \right| = O(1)$$

the claim follows.

By similar means we have

$$\left| \prod_{N \leq |\rho| \leq N'} \left(1 - \frac{z}{\rho}\right) e^{z/\rho} \right| \leq \exp \left(O(K^2 \sum_{|\rho| \geq N} |\rho|^{-2}) \right) = o(1)$$

as $N \rightarrow \infty$.

From these facts we have

$$|E_{\Omega}^N(z) - E_{\Omega}^{N'}(z)| = |E_{\Omega}^N(z)| \prod_{N \leq |\rho| \leq N'} \left(1 - \frac{z}{\rho}\right) e^{z/\rho} = o(1)$$

uniformly for $|z| \leq K$. Thus $E_{\Omega}^N(z)$ does indeed converge uniformly for $|z| \leq K$, and hence $E_{\Omega}(z)$ is well-defined and entire.

It remains to show that $E_{\Omega}(z)$ vanishes precisely at the points of Ω , with the correct multiplicity. It is obvious that $E_{\Omega}(z)$ *does* vanish when $z = \rho \in \Omega$, since in this case $E_{\Omega}^N(z) = 0$ for N sufficiently large. However, this does not establish the multiplicity. For this we use the splitting

$$E_{\Omega}(z) = \prod_{\rho \in \Omega: |\rho| \leq K} \left(1 - \frac{z}{\rho}\right) e^{z/\rho} \cdot \prod_{\rho \in \Omega: |\rho| > K} \left(1 - \frac{z}{\rho}\right) e^{z/\rho}.$$

Suppose that $|z| < K$. Then the first term has zeros precisely at the points $z \in \Omega$, with the correct multiplicity.

Meanwhile, using the inequality $|1 + w|e^{-w} \geq e^{-O(|w|^2)}$ for $|w| \leq 1$, we see that the second term is

$$\left| \prod_{\rho \in \Omega: |\rho| \geq K} \left(1 - \frac{z}{\rho}\right) e^{z/\rho} \right| \geq \exp \left(-O(|z|^2 \sum_{|\rho| \geq K} |\rho|^{-2}) \right) > 0,$$

and so this term is not zero. This concludes the proof. \square

We turn now to the proof of Proposition 6.2. The basic structure of the argument is quite straightforward. From the growth condition on f and Corollary 6.1 it follows very easily that

$$(6.4) \quad \#\{\rho : R \leq |\rho| \leq 2R\} \ll_{\varepsilon} R^{1+\varepsilon},$$

for every $\varepsilon > 0$. In particular (taking any $\varepsilon < 1$) we see that $\sum_{\rho \neq 0} |\rho|^{-2} < \infty$. Therefore we may apply Proposition 6.4 with Ω being the set of zeros of f other than 0, obtaining an entire function $E_{\Omega}(z)$ which vanishes (with the correct multiplicity)

precisely at Ω . If f has a zero of order r at $z = 0$, then we define

$$g(z) := \frac{f(z)}{z^r E_\Omega(z)}.$$

By construction, g is an entire function of z with no zeros. To complete the proof of Proposition 6.2, we need only show that $g(z) = e^{Az+B}$. Moreover we already have a tool for doing precisely this, namely Lemma 6.2. Applying this lemma, we see that all we need do is establish an upper bound

$$|g(z)| \leq e^{CR_j^{3/2}}$$

for $|z| = R_j$, for some sequence of radii $R_j \rightarrow \infty$.

Since we already have a bound on f (by assumption) and z^{-r} decays quickly, it is enough to establish the *lower* bound

$$(6.5) \quad |E_\Omega(z)| \geq e^{-C'R_j^{3/2}}$$

for $|z| = R_j$. This is slightly delicate, and must involve a careful choice of the R_j , since $E_\Omega(z)$ vanishes at the points of Ω . In the light of this, it obviously makes sense to choose the radii R_j to lie away from any of the zeros ρ .

We will show that for every j we can choose an $R_j \in [2^j, 2^{j+1}]$ such that (6.5) is satisfied. Write S_j for the number of zeros with $2^j \leq |\rho| \leq 2^{j+1}$. Then, by (6.4) with $\varepsilon = 1$, $S_j \ll 2^{2j}$. It follows easily that R_j may be chosen in such a way that

$$(6.6) \quad |z - \rho| \gg 2^{-j}$$

whenever $|z| = R_j$, for all zeros ρ . Suppose from now on that $|z| = R_j$.

To get a lower bound on $E_\Omega(z)$, we divide the product into dyadic subproducts

$$E_\Omega^{(j')}(z) := \prod_{\rho \in S_{j'}} (1 - z/\rho) e^{z/\rho},$$

$j' = 0, 1, 2, \dots$. The contribution from $|\rho| \leq 1$ is clearly bounded below, independently of R , by some constant (which may depend on f).

Now if $j' < j - 10$ (say) then, for any zero ρ occurring in the product $E_\Omega^{(j')}(z)$, we have $|1 - z/\rho| \geq 1$. Furthermore $|e^{z/\rho}| \geq e^{-2^{j-j'}}$, and so

$$|E_\Omega^{(j')}(z)| \geq (e^{-2^{j-j'}})^{S_{2^{j'}}} \geq e^{-C2^{2j}2^{j'/10}}$$

(say), the last bound here being a consequence of (6.4) with $\varepsilon := 1/10$.

If $j - 10 < j' < j + 10$ then we employ the bound $|1 - z/\rho| \geq c2^{-2j}$, a consequence of (6.6). For any such j' we have $|e^{z/\rho}| \gg 1$, and so

$$|E_\Omega^{(j')}(z)| \gg (c2^{-2j})^{S_{2^{j'}}} \gg e^{-C2^{3j/2}},$$

this last bound following from (6.4) with any value of $\varepsilon < \frac{1}{2}$.

Finally, suppose that $j' \geq j + 10$. By a crude Taylor series expansion one has $|(1-w)e^w| > e^{-10|w|^2}$ for $|w| < 1/10$. Thus, for these values of j ,

$$|E_{\Omega}^{(j')}(z)| > (e^{-10 \cdot 2^{2j-2j'}})_{S_{2j'}} \geq e^{-C2^{2j}2^{-j'/2}},$$

applying (6.4) with $\varepsilon = \frac{1}{2}$.

It is a simple matter to check that the product of all these estimates for $E_{\Omega}^{(j')}(z)$, over all j' , is bounded below by $e^{-C2^{3j/2}}$, for some absolute constant C . This concludes the proof.

Mellin transforms and the explicit formula

In this section we will take steps towards clarifying the relationship between primes and the zeros of the Riemann ζ -function, by proving the so-called *explicit formula*.

7.1. Definitions and statement of the formula

Recall that the von Mangoldt function Λ and it is defined by

$$\Lambda(n) := \begin{cases} \log p & \text{if } n = p^m \text{ is a prime power} \\ 0 & \text{otherwise.} \end{cases}$$

The fact that $\Lambda(n) \neq 0$ for prime powers p^m as well as for the primes themselves is almost never more than a slight annoyance, since the prime powers are so sparse.

The prime number theorem asserts the $\psi(X) \sim X$, where

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

Another way of writing this is

$$\psi(X) = \sum_n \Lambda(n) W\left(\frac{n}{X}\right),$$

where $W : \mathbb{R} \rightarrow \mathbb{R}$ is $1_{[0,1]}$, the function defined to equal 1 on $[0, 1]$, and zero elsewhere. The explicit formula is a formula for sums like this in terms of the zeros of ζ . However, we will only prove the formula when W is *smooth*, that is to say infinitely differentiable, and also compactly supported (that is, zero outside some closed interval). This means that in order to apply it to the prime number theorem we must approximate $1_{[0,1]}$ by smooth, compactly supported functions. This is not especially difficult, but also not entirely straightforward – indeed, even the *existence* of a smooth compactly supported function other than 0 is not immediately obvious. (The smoothness assumption can be relaxed to some condition involving only finitely many derivatives of W , if desired, and the compact support condition can also be relaxed to condition involving sufficiently rapid decay of W and sufficiently many of its derivatives. We will include an exercise about this.)

The explicit formula involves the Mellin transform. This was discussed briefly in Chapter 4. We reintroduce it now: it is convenient to denote it with a tilde

rather than a hat, as we will require the Fourier transform on \mathbb{R} in our arguments. Moreover, the Mellin transform as defined earlier had, as its domain, the imaginary axis $\{it : t \in \mathbb{C}\}$. Now we will extend the domain of definition to the whole complex plane, which takes us a little outside the scope of the discussion in Chapter 4.

DEFINITION 7.1 (Mellin Transform). Suppose that $W : \mathbb{R} \rightarrow \mathbb{R}$ has compact support contained in $(0, \infty)$. For any complex number s we define the Mellin transform \tilde{W} by

$$\tilde{W}(s) := \int_0^\infty W(x)x^s \frac{dx}{x}.$$

The assumption that W has compact support bounded away from 0 means that W is well-defined and entire, the derivative of W being obtained by differentiating under the integral.

THEOREM 7.1 (Explicit formula). *Let W be a smooth, compactly supported function, supported on $[c, \infty)$ for some $c > 0$. Suppose that $X > \frac{1}{c}$. Then*

$$\sum_n \Lambda(n)W\left(\frac{n}{X}\right) = X \left(\int W \right) - \sum_{\rho \in Z} X^\rho \tilde{W}(\rho).$$

The sum here is over the set $Z = Z_{\text{triv}} \cup Z_{\text{nontriv}}$ of all zeros of ζ .

Remarks. Since $\tilde{W}(1) = \int W$, one could if desired write the right-hand side as

$$- \sum_{w \in \mathbb{C}} \text{ord}_\zeta(w) X^w \tilde{W}(w),$$

where $\text{ord}_\zeta(w)$ is the order of ζ at w , that is to say r if w is a zero of order r , and $-r$ if w is a pole of order r .

Things get more complicated if one wishes to remove the condition that the support of W be separated from zero, and we do not plan to discuss this any further in the course. One may wonder how it is possible to use Theorem 7.1 with this restriction to prove the prime number theorem, which concerns $W = 1_{[0,1]}$; one answer is that we may approximate $W = 1_{[1/2,1]}$ by smooth functions and then employ a telescoping sum argument, much as in the proof of Theorem 1.2.

The assumption that W be compactly supported is very convenient for the proof, for instance because in this case it is clear that $\tilde{W}(s)$ is holomorphic. However, Theorem 7.1 does hold under weaker conditions such as Schwarz-like decay. Such statements may be deduced from the compactly supported case; see Example Sheet 4.

Before turning to the proof of the explicit formula, let us make some remarks about its form. The term $X(\int W)$ is the “main term”; one would expect the sum on the left to equal roughly this, at least if one assumes the prime number theorem, since Λ has average value 1 and $\sum_n W(\frac{n}{X}) \approx X(\int W)$. The remaining terms

$\sum_{\rho \in Z} \tilde{W}(\rho)$ are, therefore, to be thought of as “error terms”. It turns out that the contribution from $\rho \in Z_{\text{triv}}$ is negligible, leaving the sum $\sum_{\rho \in Z_{\text{nontriv}}} X^{\text{Re } \rho} \tilde{W}(\rho)$. Let us imagine, for the moment (and we will prove various rigorous assertions about this in the next section) that $\tilde{W}(\rho)$ is on the order of 1. The contribution of this term rather depends on what we know about the location of the nontrivial zeros Z_{nontriv} ; at the moment, all we know is that they lie in $0 \leq \text{Re } \rho \leq 1$. For all we know, it could be that some zero ρ lies on the line $\text{Re } s = 1$, in which case one would expect the term $X^{\text{Re } \rho} \tilde{W}(\rho)$ to have the same order of magnitude, $O(X)$, as the main term. Thus, once one has the explicit formula, further progress on the prime number theorem depends on pinning down further information about the nontrivial zeros.

7.2. Proof of the explicit formula – overview

In this section we outline the proof of the explicit formula, leaving some technical details to the next section. We begin by noting that we may assume that W is supported on $[1, \infty)$; if the support of W is $[c, \infty)$ then consider the function $W'(x) := W(cx)$, which is now supported on $[1, \infty)$. Assuming the explicit formula for W' , and replacing X by cX , we have

$$\sum_n \Lambda(n) W\left(\frac{n}{X}\right) = \sum_n \Lambda(n) W'\left(\frac{cn}{X}\right) = cX \left(\int W' \right) - \sum_{\rho \in Z} (cX)^\rho \tilde{W}'(\rho).$$

Now observe that $\int W' = \frac{1}{c} \int W$ and $\tilde{W}(\rho) = c^{-\rho} \tilde{W}'(\rho)$.

A key ingredient is the inversion formula for the Mellin transform, which is basically equivalent to the Fourier inversion formula.

PROPOSITION 7.1. *Let $W : \mathbb{R} \rightarrow \mathbb{R}$ be a smooth function with compact support contained in $(0, \infty)$. Then for any $\sigma \in \mathbb{R}$ we have the Mellin inversion formula*

$$W(x) = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \tilde{W}(s) x^{-s} ds.$$

Proof. From the definition of the Mellin transform and a simple substitution we have, for any $s = \sigma + it$,

$$\begin{aligned} \tilde{W}(s) &= \int_0^\infty W(x) x^s \frac{dx}{x} \\ &= \int_{-\infty}^\infty W(e^u) e^{us} du \\ &= \int_{-\infty}^\infty W(e^u) e^{u\sigma} e^{itu} du \\ &= \hat{g}(-t), \end{aligned}$$

where $g(u) = W(e^u)e^{\sigma u}$. Now g is clearly a Schwartz function (indeed it is smooth and compactly supported) and so by the Fourier inversion formula (followed by the substitution $t \mapsto -t$) we have

$$g(u) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \widehat{g}(-t)e^{-itu} dt,$$

that is to say

$$W(e^u)e^{\sigma u} = \frac{1}{2\pi} \int_{-\infty}^{\infty} \widetilde{W}(\sigma + it)e^{-itu} dt.$$

Multiplying both sides by $e^{-\sigma u}$ gives the result. \square

Now we can outline the proof of the explicit formula as stated in Theorem 7.1. The proof begins with the Dirichlet series

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

valid for $\operatorname{Re} s > 1$. We established this earlier in the course.

By the Mellin inversion formula, Proposition 7.1 and this Dirichlet series expansion we have

$$\begin{aligned} \sum_n \Lambda(n)W\left(\frac{n}{X}\right) &= \sum_n \Lambda(n) \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \widetilde{W}(s)(n/X)^{-s} ds \\ &= \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \left(\sum_n \Lambda(n)n^{-s} \right) X^s \widetilde{W}(s) ds \\ (7.1) \qquad &= \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} -\frac{\zeta'(s)}{\zeta(s)} X^s \widetilde{W}(s) ds, \end{aligned}$$

the interchange in the order of integration and summation being justified if $\sigma > 1$. Take $\sigma = 2$ for definiteness.

We now reach the heart of the argument. The aim is to move the contour of integration far to the left, picking up residues due to the poles of ζ'/ζ at $s = 1$, at the non-trivial zeros $\rho \in Z_{\text{nontriv}}$ in the critical strip, and at the trivial zeros $Z_{\text{triv}} = \{-2, -4, -6, \dots\}$. To this end we note that

$$\operatorname{Res}_{s=1} \frac{\zeta'}{\zeta} = -1,$$

$$\operatorname{Res}_{s=-2k} \frac{\zeta'}{\zeta} = 1,$$

and $\operatorname{Res}_{s=\rho} \frac{\zeta'}{\zeta}$ is equal to the multiplicity of the zero ρ .

To perform this contour integration rigorously we employ a rectangular contour $C_{k,T} = C_T^{(1)} \cup C_{k,T}^{(2)} \cup C_{k,T}^{(3)} \cup C_{k,T}^{(4)}$, where $C_T^{(1)} = [2 - iT, 2 + iT]$, $C_{k,T}^{(2)} = [2 + iT, -2k - 1 + iT]$, $C_{k,T}^{(3)} = [-2k - 1 + iT, -2k - 1 - iT]$ and $C_{k,T}^{(4)} = [-2k - 1 - iT, 2 + iT]$, and then choose suitable values of k, T tending to infinity. Here k is an integer;

with this choice, $C_{k,T}^{(3)}$ avoids the poles of ζ'/ζ at the trivial zeros Z_{triv} . The choice of T is rather more delicate and in particular we need to make sure that neither $C_{k,T}^{(2)}$ nor $C_{k,T}^{(4)}$ pass close to any of the poles of ζ'/ζ at the nontrivial zeros Z_{nontriv} . Later on, we will choose a sequence T_1, T_2, \dots of “good” values of T such that, in particular, neither $C_{k,T}^{(2)}$ nor $C_{k,T}^{(4)}$ contain any zeros of ζ .

For $j = 1, 2, 3, 4$ define

$$(7.2) \quad I_{k,T}^{(j)} := -\frac{1}{2\pi i} \int_{C_{k,T}^{(j)}} \frac{\zeta'(s)}{\zeta(s)} X^s \tilde{W}(s) ds.$$

To calculate $\sum_{j=1}^4 I_{k,T}^{(j)}$ we apply the residue theorem and the preceding remarks, obtaining

$$(7.3) \quad \sum_{j=1}^4 I_{k,T}^{(j)} = X\tilde{W}(1) - \sum_{\substack{\rho \in Z_{\text{nontriv}} \\ |\rho| < T}} X^\rho \tilde{W}(\rho) - \sum_{j=1}^k X^{-2j} \tilde{W}(-2j).$$

Note that

$$\tilde{W}(1) = \int W.$$

Therefore as $k \rightarrow \infty$ and as $T \rightarrow \infty$ along any subsequence, the right-hand side of (7.3) tends towards the right hand side of the explicit formula. To conclude the proof of the explicit formula it therefore suffices to show that

$$(7.4) \quad \lim_{k \rightarrow \infty} \lim_{T_j \rightarrow \infty} I_{k,T_j}^{(1)} = \sum_n \Lambda(n) W\left(\frac{n}{X}\right)$$

as well as

$$(7.5) \quad \lim_{k \rightarrow \infty} \lim_{T_j \rightarrow \infty} I_{k,T_j}^{(2)}, I_{k,T_j}^{(4)} = 0$$

and

$$(7.6) \quad \lim_{k \rightarrow \infty} \lim_{T_j \rightarrow \infty} I_{k,T_j}^{(3)} = 0.$$

We will prove these statements (as well as define the sequence T_j) in the next section.

7.3. Estimates for the Mellin transforms.

In this section we establish some basic facts about the Mellin transform of a compactly supported function W , supported on $[1, \infty)$. Assume that the support of W is contained in $[1, C]$. (the quantity C will later disappear.)

Next we note some rather trivial bounds on $\tilde{W}(\sigma + it)$. We have

$$|\tilde{W}(\sigma + it)| \leq \|W\|_\infty \int_1^C |x^{\sigma+it-1}| dx = \|W\|_\infty \int_1^C x^{\sigma-1} dx.$$

In particular

$$(7.7) \quad |\tilde{W}(\sigma + it)| \ll_W 1$$

uniformly for $-\infty < \sigma \leq 10$ and for all t .

Remark. One could of course state a bound for large positive σ as well, but we will never use this portion of the complex plane. The fact that \tilde{W} becomes very small as σ moves far to the left is useful for showing that the contribution of the trivial zeros $Z_{\text{triv}} = \{-2, -4, -6, \dots\}$ is negligible in the explicit formula.

Next we return to the issue of bounding $\tilde{W}(\sigma + it)$, proving estimates a little more sophisticated than (7.7) and (??) establishing decay properties in the vertical direction, mirroring the Fourier decay estimate given in Lemma 4.1. It is in establishing these estimates that the smoothness of W plays a critical role.

LEMMA 7.1 (Mellin decay properties). *Suppose that $W : \mathbb{R} \rightarrow \mathbb{R}$ is smooth and has compact support contained in $[1, \infty)$. Let m be a positive integer, and suppose that $\sigma \in \mathbb{R}$. Then, uniformly for $|t| \geq 1$, we have*

$$(7.8) \quad |\tilde{W}(\sigma + it)| \ll_{W,m,\sigma} |t|^{-m}.$$

More precisely, if W is supported in $[1, C]$ then the implied constant here is bounded by

$$(7.9) \quad O_m(C(1 + |\sigma|))^m C^{|\sigma|} \sum_{j=1}^m \|\partial^j W\|_1$$

$$(7.10) \quad = O_{m,W}(1 + |\sigma|)^m C^{|\sigma|}.$$

Remark. For the proof of the explicit formula, only the dependence on σ is important. It is important to keep careful track of this as we shall be pulling contours far to the left and in doing so will take $\sigma \rightarrow -\infty$. The detailed dependence on the derivatives of W is of importance when it comes to discussing the error term in the prime number theorem.

Proof. Evidently it suffices to establish the most precise statement, (7.9), the other two statements (7.8) and (7.10) being more easily stated but weaker variants of it. As in the proof of Proposition 7.1, we have

$$(7.11) \quad \tilde{W}(\sigma + it) = \hat{g}_\sigma(-t),$$

where

$$g_\sigma(u) := W(e^u) e^{\sigma u}.$$

It is easy to see by induction that

$$\partial^m g_\sigma(u) = \sum_{j=0}^m P_j(\sigma) e^{u(j+\sigma)} \partial^j W(e^u),$$

where the P_j are polynomials, all of degree at most m , and therefore satisfying an estimate $|P_j(\sigma)| \ll_m (1 + |\sigma|)^m$. It follows that we have the estimate

$$\begin{aligned} \|\partial^m g_\sigma\|_1 &\ll (1 + |\sigma|)^m \sum_{j=0}^m \int_0^\infty |e^{u(j+\sigma)} \partial^j W(e^u)| du \\ &= (1 + |\sigma|)^m \sum_{j=0}^m \int |\partial^j W(x) x^{j+\sigma}| \frac{dx}{x}, \end{aligned}$$

Since W is supported in $[1, C]$, it follows that

$$\begin{aligned} \|\partial^m g_\sigma\|_1 &\ll_m (1 + |\sigma|)^m \sum_{j=0}^m \|\partial^j W\|_1 \sup_{x \in [1, C]} \sup_{j \in \{0, \dots, m\}} x^{j+\sigma-1} \\ &= O_m(C(1 + |\sigma|))^m C^{|\sigma|} \sum_{j=1}^m \|\partial^j W\|_1. \end{aligned}$$

The lemma now follows from (7.11) using Lemma 4.1. \square

Now it is time to start thinking about how to choose the ordinates T_j in such a way that the poles of $\zeta'(s)/\zeta(s)$ do not interfere with the horizontal contours $C_{k, T_j}^{(2)}, C_{k, T_j}^{(4)}$. Very crude estimates suffice, ultimately because we are dealing with smooth functions W which enjoy very advantageous Mellin decay properties.

LEMMA 7.2. *There is a sequence of T tending to infinity such that $\text{dist}(s, Z) \geq 1/T$ uniformly for all s with $\Im s = T$.*

Proof. If $T \geq 1$ then certainly $\text{dist}(s, Z_{\text{triv}}) \geq 1$ and so it suffices to handle the nontrivial zeros. Let U be large, and suppose that for all T with $U \leq T \leq 2U$ there is some $s = \sigma + iT$ with $\text{dist}(s, Z_{\text{triv}}) \leq \frac{1}{U}$. Let $\{T_1, \dots, T_m\} \subset [U, 2U]$ be a set with $|T_i - T_j| > \frac{2}{U}$ for all $i \neq j$. If U is large then there is such a set with $m \geq \frac{U^2}{4}$. For each i there is some σ_i and some zero ρ_i so that $|\sigma_i + iT_i - \rho_i| \leq \frac{1}{U}$. If $i \neq j$,

$$|\Im \rho_i - \Im \rho_j| \geq |T_i - T_j| - \frac{2}{U} > 0,$$

and so $\rho_i \neq \rho_j$. All the zeros ρ_i satisfy $|\rho_i| \leq 3U$, and so we obtain that the number of zeros of ζ with $|\rho| \leq 3U$ is $\gg U^2$. This obviously contradicts Proposition 6.3, by some margin. \square

We call a value of T for which the conclusion of Lemma 7.2 holds *good*. If T is good then certainly there are no elements of Z_{nontriv} , and hence no poles of ζ'/ζ , on the horizontal lines $\Im s = \pm T$, and hence in particular no such poles on the

contours $C_{k,T}^{(2)}, C_{k,T}^{(4)}$. We actually need rather more than this, namely a reasonable upper bound for ζ'/ζ on these contours. That said, a fairly crude bound will do, and we provide such a bound in the next proposition.

PROPOSITION 7.2. *Suppose that $|s| \geq 2$. Then*

$$\frac{\zeta'(s)}{\zeta(s)} \ll |s|^3 \operatorname{dist}(s, Z)^{-1},$$

where Z is the set of all zeros of ζ .

Remark. This is a crude bound, and stronger ones could be obtained. For our purposes, however, a bound of the form $|s|^C \operatorname{dist}(s, Z)^{-C'}$ would be sufficient.

Proof. We use the partial fraction expansion

$$\frac{\zeta'(s)}{\zeta(s)} = B' - \frac{1}{s-1} + \sum_{\rho \in Z} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right).$$

The first two terms are clearly $O(1)$ in the domain $|s| \geq 2$. To bound the sum over the zeros, we will split into the sums over $Z_{\text{triv}} = \{-2, -4, -6, \dots\}$ and over the nontrivial zeros Z_{nontriv} . To bound the latter, we will unsurprisingly need some information about the nontrivial zeros. All we need is the estimate

$$(7.12) \quad \sum_{\rho \in Z} |\rho|^{-2} < \infty.$$

Suppose first that $|\rho| \geq 2|s|$. Then $|s/\rho| \leq \frac{1}{2}$, and hence $|\frac{s}{\rho} - 1| \geq \frac{1}{2}$ and hence $|s - \rho| \geq \frac{1}{2}|\rho|$. Hence

$$(7.13) \quad \sum_{|\rho| \geq 2|s|} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right) \leq |s| \sum_{\rho \in Z(s)} \frac{1}{|s-\rho||\rho|} \leq 2|s| \sum_{\rho \in Z(s)} \frac{1}{|\rho|^2} \ll |s|,$$

the last step of course following from (7.12). To estimate the contribution from the remaining zeros, those with $|\rho| < 2|s|$, we proceed extremely crudely. By (7.12) it follows immediately that the number of such zeros is $O(|s|^2)$. The contribution from a given one is

$$\frac{|s|}{|s-\rho||\rho|} \ll |s| \operatorname{dist}(s, Z)^{-1},$$

where here we used the fact that $\frac{1}{|\rho|} \ll 1$, which follows simply from the fact that 0 is not a zero of ζ . Therefore

$$\sum_{|\rho| < 2|s|} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right) \ll |s|^3 \operatorname{dist}(s, Z)^{-1},$$

and the proposition follows. \square

Now we complete the proof of the explicit formula by verifying (7.4), (7.5) and (7.6).

Proof of (7.4). If $s \in C_T^{(1)}$ then $\operatorname{Re} s = 2$, and so $\operatorname{dist}(s, Z) \geq 1$. It follows from Proposition 7.2 that $\zeta'(2+it)/\zeta(2+it) \ll |t|^3$. However, in this case a better bound is available via an easier route: we have

$$(7.14) \quad \left| \frac{\zeta'(2+it)}{\zeta(2+it)} \right| = \left| \sum_n \Lambda(n)n^{-2-it} \right| \leq \sum_n \Lambda(n)n^{-2} = O(1),$$

uniformly in t . Recall that

$$I_{k,T}^{(1)} = -\frac{1}{2\pi i} \int_{2-iT}^{2+iT} X^s \tilde{W}(s) \frac{\zeta'(s)}{\zeta(s)} ds.$$

(Note that this integral does not, in fact, depend on k .) Recall from (7.8) that we have the decay estimate $|\tilde{W}(2+it)| \ll |t|^{-2}$. Putting this and (7.14) together gives

$$\int_{2+iT}^{2+i\infty} X^s \tilde{W}(s) \frac{\zeta'(s)}{\zeta(s)} ds \ll X^2 \int_T^\infty |t|^{-2} dt \ll \frac{X^2}{T}.$$

Therefore

$$\begin{aligned} I_{k,T}^{(1)} &= -\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} X^s \tilde{W}(s) \frac{\zeta'(s)}{\zeta(s)} ds + O\left(\frac{X^2}{T}\right) \\ &= \sum_n \Lambda(n)W\left(\frac{n}{X}\right) + O\left(\frac{X^2}{T}\right), \end{aligned}$$

by (7.1). The statement (7.4) now follows immediately.

Proof of (7.5). If $s \in C_{k,T}^{(2)} \cup C_{k,T}^{(4)}$ then, since T is good, $\operatorname{dist}(s, Z) \gg \frac{1}{T}$. It follows from Proposition 7.2 that, uniformly for $s \in C_{k,T}^{(2)} \cup C_{k,T}^{(4)}$, we have

$$\frac{\zeta'(s)}{\zeta(s)} \ll |s|^3 T \ll k^3 T^4.$$

It follows that

$$I_{k,T}^{(2)}, I_{k,T}^{(4)} \ll k^3 T^4 \int_{-2k-1}^2 X^\sigma |\tilde{W}(\sigma + iT)| d\sigma.$$

By Lemma 7.1 (specifically, (7.10)) with $m = 5$ we have

$$\begin{aligned} |\tilde{W}(\sigma + iT)| &\ll_W (1 + |\sigma|)^5 T^{-5} \sup_{x \in [1, C]} \sup_{j \in \{0, 1, \dots, 5\}} x^{j+\sigma-1} \\ &\ll_W (1 + |\sigma|)^5 T^{-5} \end{aligned}$$

uniformly for $-\infty < \sigma \leq 2$ (the C dependence has been absorbed into the W dependence.) Therefore we obtain

$$I_{k,T}^{(2)}, I_{k,T}^{(4)} \ll_W k^3 T^{-1} \int_{-2k-1}^2 (1 + |\sigma|)^5 X^\sigma d\sigma \ll_{W,X} k^3 T^{-1},$$

where here we used the fact that $X > 1$. Thus

$$I_{k,T}^{(2)}, I_{k,T}^{(4)} \ll_{W,X} k^3 T^{-1}.$$

Statement (7.5) follows (note that it is important that we take the limit as $T \rightarrow \infty$ first, and only then the limit as $k \rightarrow \infty$).

Proof of (7.6). If $s \in C_{k,T}^{(3)}$ then $\text{dist}(s, Z) \geq 1$ and so Proposition 7.2 furnishes the bound $\frac{\zeta'(s)}{\zeta(s)} \ll |s|^3$. If $s = -2k - 1 + it$ then (crudely) this is $\ll k^3 \max(1, |t|)^3$.

From Lemma 7.1 with $m = 5$ we have

$$|\tilde{W}(-2k - 1 + it)| \ll_W k^5 \max(1, |t|)^{-5}.$$

Thus

$$\frac{\zeta'(s)}{\zeta(s)} X^s \tilde{W}(s) \ll_W k^8 \max(1, |t|)^{-2} X^{-2k-1},$$

which implies that

$$I_{k,T}^{(3)} = \int_{-2k-1-iT}^{-2k-1+iT} \frac{\zeta'(s)}{\zeta(s)} X^s \tilde{W}(s) ds \ll_{k,W} (cX)^{-2k-1},$$

uniformly in T . From this and the fact that $X > \frac{1}{c}$ we immediately conclude (7.6), that is to say that indeed

$$\lim_{k \rightarrow \infty} \lim_{T \rightarrow \infty} I_{k,T}^{(3)} = 0$$

Note that for the estimation of $I^{(3)}$ there was no need to restrict to T good.

The prime number theorem

In the last section we established the explicit formula, which provides a relationship between the distribution of prime numbers and the nontrivial zeros ρ of the ζ -function. To make use of this result, and in particular to prove the prime number theorem, it is important to have some information about the location of those zeros.

The prime number theorem turns out to be more-or-less equivalent to the following statement.

PROPOSITION 8.1. *There are no zeros of ζ on the line $\operatorname{Re} s = 1$.*

Proof. Consider the Euler product identity

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

valid for $\operatorname{Re} s > 1$. Set $s = \sigma + it$; we will let $\sigma \rightarrow 1$. Taking logs, we have

$$(8.1) \quad \log \zeta(s) = - \sum_p \log(1 - p^{-s}) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}} = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{m\sigma}} e^{-imt \log p}.$$

Now we invoke the inequality

$$(8.2) \quad 3 + 4 \cos \theta + \cos 2\theta = 2(1 + \cos \theta)^2 \geq 0.$$

Applying this with $\theta = mt \log p$ and comparing with (8.1), we get

$$3 \log \zeta(\sigma) + 4 \operatorname{Re} \log \zeta(\sigma + it) + \operatorname{Re} \log \zeta(\sigma + 2it) \geq 0,$$

and thus

$$\zeta(\sigma)^3 |\zeta(\sigma + it)|^4 |\zeta(\sigma + 2it)| \geq 1.$$

Now suppose that $\zeta(1 + it) = 0$, and let $\sigma \rightarrow 1$ in the inequality just proved. We have $\zeta(\sigma) \sim (\sigma - 1)^{-1}$, but $|\zeta(\sigma + it)|^4 \ll (\sigma - 1)^4$. Since $\zeta(\sigma + 2it)$ remains bounded as $\sigma \rightarrow 1$, we have

$$\zeta(\sigma)^3 |\zeta(\sigma + it)|^4 |\zeta(\sigma + 2it)| \rightarrow 0,$$

a contradiction. □

We will actually prove the following statement, from which the prime number theorem is a relatively easy deduction.

PROPOSITION 8.2. *Suppose that $W : \mathbb{R} \rightarrow \mathbb{R}$ is a compactly supported smooth function, supported on $(0, \infty)$. Then*

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_n \Lambda(n) W\left(\frac{n}{X}\right) = \int W.$$

Proof. We apply the explicit formula Recall the explicit formula

$$\frac{1}{X} \sum_n \Lambda(n) W\left(\frac{n}{X}\right) = \int W - \sum_{\rho \in Z} X^{\rho-1} \tilde{W}(\rho).$$

Evidently it suffices to show that

$$\lim_{X \rightarrow \infty} \sum_{\rho} X^{\rho-1} \tilde{W}(\rho) = 0.$$

We handle the contribution from the trivial zeros and the nontrivial ones separately.

By Lemma ?? we have $\tilde{W}(\rho) \ll_W 1$ uniformly for $\rho \in Z_{\text{triv}}$, and so

$$\sum_{\rho \in Z_{\text{triv}}} X^{\rho-1} \tilde{W}(\rho) \ll_W \sum_{j=1}^{\infty} X^{-2j-1}.$$

This certainly tends to 0 as $X \rightarrow \infty$.

Turning now to the contribution from the nontrivial zeros, we use (7.8) with $m = 2$. This tells us that $\tilde{W}(\rho) \ll |\rho|^{-2}$ uniformly for $\rho \in Z_{\text{nontriv}}$. Noting also that $|X^{\rho-1}| \leq 1$ (since $\text{Re } \rho \leq 1$) we have

$$\sum_{\rho \in Z_{\text{nontriv}}: |\rho| \geq K} X^{\rho-1} \tilde{W}(\rho) \rightarrow 0$$

as $K \rightarrow \infty$, uniformly in X .

For the small zeros we have

$$\sum_{\rho \in Z_{\text{nontriv}}: |\rho| < K} X^{\rho-1} \tilde{W}(\rho) \ll_{K,W} X^{\beta(K)-1},$$

where $\beta(K) = \sup_{\rho \in Z_{\text{nontriv}}: |\rho| \leq K} \text{Re } \rho$. By Proposition 8.1, we have $\beta(K) < 1$. For fixed K , this contribution tends to zero as $X \rightarrow \infty$. Letting $K, X \rightarrow \infty$ appropriately gives the result. \square

Proposition 8.2 is a kind of “smoothed” prime number theorem. Now we show how the prime number theorem itself follows from it. First note that, for any $\varepsilon > 0$, we may find functions $W_{\varepsilon}^+, W_{\varepsilon}^- \in C^{\infty}(\mathbb{R})$, supported on $[\frac{1}{4}, 2]$ such that $W_{\varepsilon}^- \leq 1_{[1/2, 1]} \leq W_{\varepsilon}^+$ pointwise and $\int W_{\varepsilon}^+ - \int W_{\varepsilon}^- < \varepsilon$ (draw a picture). It follows from Proposition 8.2, and letting $\varepsilon \rightarrow 0$, that

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{X/2 < n \leq X} \Lambda(n) = \frac{1}{2}.$$

Thus, if X is large enough in terms of ε ,

$$\sum_{X/2 \leq n < X} \Lambda(n) \leq \frac{1}{2}X(1 + \varepsilon).$$

Replacing X by $X/2, X/4, \dots, X/2^{m-1}$ and summing yields

$$\sum_{2^{-m}X \leq n \leq X} \Lambda(n) \leq (1 - 2^{-m})X(1 + \varepsilon),$$

provided that X is sufficiently large in terms of m, ε . By the elementary bounds established in Chapter 2, we have

$$\sum_{2^{-m}X} \Lambda(n) \ll 2^{-m}X,$$

where the implied constant is absolute. It follows that if X is sufficiently large in terms of m, ε then

$$\sum_{n \leq X} \Lambda(n) \leq O(2^{-m}X) + (1 - 2^{-m})(1 + \varepsilon)X.$$

Taking m sufficiently large, in terms of ε , the right hand side can be made $\leq (1 + 2\varepsilon)X$. Since ε was arbitrary, it follows that $\limsup_{X \rightarrow \infty} \frac{1}{X} \sum_{n \leq X} \Lambda(n) \leq 1$.

Similarly,

$$\liminf_{X \rightarrow \infty} \frac{1}{X} \sum_{n \leq X} \Lambda(n) = 1.$$

A corresponding inequality in the other direction can be established in an identical fashion. By Proposition 1.1, this implies the prime number theorem.

The zero-free region. Error terms.

9.1. The classical zero-free region

In the last section we showed that ζ has no zeros on the line $\operatorname{Re} s = 1$, and we saw that this implies the prime number theorem.

In this section we obtain, using a related argument, a region to the left of $\operatorname{Re} s = 1$ in which there are no zeros of ζ . This may be used to prove a stronger version of the prime number theorem, with a good error term: we provide details of this in the next section.

The following is known as the “classical zero-free region”.

THEOREM 9.1. *There is an absolute constant $c > 0$ such that any zero $\rho = \beta + i\gamma$ with $|\gamma| \geq 2$ satisfies*

$$\beta < 1 - \frac{c}{\log |\gamma|}.$$

Remark. Since there are no zeros on the line $\operatorname{Re} s = 1$, one can if desired state a zero-free region of the form

$$\beta < 1 - \frac{c'}{\log(|\gamma| + 2)}$$

for all γ . *Proof.* We may assume that $|\gamma| \geq 10$, since for small γ the result is a consequence of the fact that there are no zeros on the line $\operatorname{Re} s = 1$ (established in the last chapter) and a compactness argument.

Of course, for $\operatorname{Re} s > 1$ we have

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

Taking real parts gives, provided $\sigma > 1$,

$$- \operatorname{Re} \frac{\zeta'(\sigma + it)}{\zeta(\sigma + it)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-\sigma} \cos(t \log n).$$

Using the inequality

$$3 + 4 \cos \theta + \cos 2\theta = 2(1 + \cos \theta)^2 \geq 0$$

(exactly as in the last section) it follows that

$$(9.1) \quad -3 \operatorname{Re} \frac{\zeta'(\sigma)}{\zeta(\sigma)} - 4 \operatorname{Re} \frac{\zeta'(\sigma + it)}{\zeta(\sigma + it)} - \operatorname{Re} \frac{\zeta'(\sigma + 2it)}{\zeta(\sigma + 2it)} \geq 0$$

for any $\sigma > 1$ and for any $t \in \mathbb{R}$.

Now we assemble some further inequalities. Since $\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1}$ is holomorphic, and hence continuous, it is bounded on the compact interval $[1, 2]$. That is, if $1 < \sigma \leq 2$ then

$$(9.2) \quad -3 \operatorname{Re} \frac{\zeta'(\sigma)}{\zeta(\sigma)} \leq \frac{3}{\sigma-1} + C_1,$$

for some absolute constant C_1 . To get bounds for the other two terms in (9.1), we use the partial fraction expansion

$$\frac{\zeta'(\sigma + it)}{\zeta(\sigma + it)} = B - \frac{1}{\sigma + it - 1} + \sum_{\rho \in Z} \left(\frac{1}{\sigma + it - \rho} + \frac{1}{\rho} \right).$$

The first two terms are bounded by $O(1)$. To bound the sum over ρ , we treat the trivial zeros separately. If $1 \leq \sigma \leq 2$ and $|t| \geq 2$, the contribution from the trivial zeros is

$$\sum_k \sum_{\rho = -2k-1} \frac{\sigma + it}{\rho(\sigma + it - \rho)} \ll \sum_{k \geq 1} \frac{|t|}{k\sqrt{k^2 + t^2}}.$$

To estimate this sum, we split it into $k \leq |t|$ and $k \geq |t|$. On the first range the summand is $\ll \frac{1}{k}$, so we get a contribution of $O(\log |t|)$. On the second range the summand is $\ll \frac{|t|}{k^2}$, and so we get a contribution of $O(1)$. It follows that

$$-4 \operatorname{Re} \frac{\zeta'(\sigma + it)}{\zeta(\sigma + it)} = O(\log |t|) - 4 \operatorname{Re} \sum_{\rho \in Z_{\text{nontriv}}} \left(\frac{1}{\sigma + it - \rho} + \frac{1}{\rho} \right).$$

Of course, we also have

$$-\operatorname{Re} \frac{\zeta'(\sigma + 2it)}{\zeta(\sigma + 2it)} = O(\log |t|) - \operatorname{Re} \sum_{\rho \in Z_{\text{nontriv}}} \left(\frac{1}{\sigma + 2it - \rho} + \frac{1}{\rho} \right).$$

Combining all this information, we obtain

$$(9.3) \quad 4 \operatorname{Re} \sum_{\rho \in Z_{\text{nontriv}}} \left(\frac{1}{\sigma + it - \rho} + \frac{1}{\rho} \right) + \operatorname{Re} \sum_{\rho \in Z_{\text{nontriv}}} \left(\frac{1}{\sigma + 2it - \rho} + \frac{1}{\rho} \right) \leq C_2 \log |t| + \frac{3}{\sigma-1}$$

for some C_2 .

Since $\operatorname{Re} \frac{1}{a+ib} = \frac{a}{a^2+b^2}$ and $\sigma > 1 > \operatorname{Re} \rho > 0$ for every $\rho \in Z_{\text{nontriv}}$, every term on the left here is non-negative. Ignoring all terms except the contribution of the zero $\rho = \beta + i\gamma$ to the leftmost sum, and setting $t = \gamma$, we obtain

$$\frac{4}{\sigma - \beta} \leq C_2 \log |\gamma| + \frac{3}{\sigma - 1}.$$

Setting $\sigma = 1 + 1/2C_2 \log |\gamma|$ and rearranging then gives

$$\beta \leq 1 - \frac{1}{14C_2 \log |\gamma|}.$$

This has been proved whenever $|\gamma| \geq 2$, and this completes the proof. \square

We remark that the classical zero-free region is not the largest one known. In fact, the stronger inequality

$$\beta < 1 - \frac{c}{\log^{2/3+\varepsilon} |\gamma|}$$

is known to hold for any $\varepsilon > 0$, a result of Vinogradov and Korobov. The methods necessary to prove this lie considerably deeper.

9.2. The prime number theorem with classical error term

In this section we examine the implications of the classical zero-free region for the prime number theorem.

The main result is the following.

THEOREM 9.2. *We have $\psi(X) = X + O(Xe^{-c\sqrt{\log X}})$.*

Here, $\psi(X) = \sum_{n \leq X} \Lambda(n)$, as usual. The letter c denotes a positive absolute constant, but it may vary from line to line.

The main point of the proof is to combine the classical zero-free region with a study of how well “rough” functions such as $1_{[1,2]}$ are approximated by smooth ones.

LEMMA 9.1. *Let $\varepsilon > 0$. Then there is $W_\varepsilon \in C^\infty(\mathbb{R})$ such that $W_\varepsilon(x) = 1$ for $1 \leq x \leq 2$, $W_\varepsilon(x) = 0$ for $x \leq 1 - \varepsilon$ and $x \geq 2 + \varepsilon$, $0 \leq W_\varepsilon(x) \leq 1$ everywhere, and satisfying $\|\partial W\|_1 \ll 1$, $\|\partial^2 W\|_1 \ll \varepsilon^{-1}$.*

Proof. This is very similar to Example Sheet 3, Q8. \square

By the explicit formula we have

$$\sum_n \Lambda(n) W\left(\frac{n}{X}\right) = X \int W + \sum_\rho X^\rho \tilde{W}_\varepsilon(\rho).$$

The left-hand side is obviously at least $\psi(2X) - \psi(X)$ (where, as usual, $\psi(X) = \sum_{n \leq X} \Lambda(n)$), and therefore we have

$$\psi(2X) - \psi(X) \leq X + O(\varepsilon X) + \sum_\rho X^\rho \tilde{W}_\varepsilon(\rho).$$

To bound the sum over ρ , we use the estimates on Mellin transforms obtained in Section ???. The contribution from the trivial zeros is entirely negligible, and for

the nontrivial zeros we have

$$\begin{aligned}\tilde{W}_\varepsilon(\rho) &\ll \left(\sum_{j=0}^1 \|\partial^j W\|_1\right) |\rho|^{-1} \ll |\rho|^{-1}. \\ \tilde{W}_\varepsilon(\rho) &\ll \left(\sum_{j=0}^2 \|\partial^j W\|_1\right) |\rho|^{-2} \ll \frac{1}{\varepsilon} |\rho|^{-2}.\end{aligned}$$

Thus

$$\psi(2X) - \psi(X) \leq X + O(\varepsilon X) + O(1) \sum_{\rho \in Z_{\text{nontriv}}} X^\rho \min\left(\frac{1}{|\rho|}, \frac{1}{\varepsilon |\rho|^2}\right).$$

To estimate the sum over ρ , we split into exponential ranges, defining Z_j to be the set of zeros $\rho \in Z_{\text{nontriv}}$ with $e^j \leq |\rho| < e^{j+1}$. The number of zeros in such a range is $\ll j e^j$ by Corollary ???. If $\rho = \beta + i\gamma$ is such a zero then, by the classical zero-free region, $\beta \leq 1 - c/j$, and hence $X^\rho \leq X^{1-c/j}$. In the range $j \leq \log(1/\varepsilon)$ we therefore have

$$\sum_{\rho \in Z_j} X^\rho \frac{1}{|\rho|} \ll j X^{1-c/j},$$

and therefore

$$\sum_{j \leq \log(1/\varepsilon)} \sum_{\rho \in Z_j} X^\rho \frac{1}{|\rho|} \ll \log^2\left(\frac{1}{\varepsilon}\right) X^{1-c/\log(1/\varepsilon)}.$$

In the range $j \geq \log(1/\varepsilon)$ we have

$$\sum_{\rho \in Z_j} X^\rho \frac{1}{\varepsilon |\rho|^2} \ll j X^{1-c/j} \frac{1}{\varepsilon e^j},$$

and so

$$\sum_{j \geq \log(1/\varepsilon)} \sum_{\rho \in Z_j} X^\rho \frac{1}{\varepsilon |\rho|^2} \ll \log(1/\varepsilon) X^{1-c/\log(1/\varepsilon)}.$$

Putting all this together yields

$$\psi(2X) - \psi(X) \leq X + O(\varepsilon X) + O(\log^2(1/\varepsilon) X^{1-c/\log(1/\varepsilon)}).$$

Now we must choose a good value of ε . With the choice $\varepsilon = e^{-\sqrt{\log X}}$ we obtain

$$\psi(2X) - \psi(X) \leq X + O(X e^{-c\sqrt{\log X}}).$$

By the usual telescoping sum argument, using the above with $X/2, X/4, \dots$, we see that

$$\psi(X) \leq X + O(X e^{-c\sqrt{\log X}}).$$

By entirely analogous arguments, only using a minorant to the interval $1_{[1,2]}$ rather than the majorants W_ε , we may obtain the corresponding lower bound

$$\psi(X) \geq X - O(X e^{-c\sqrt{\log X}}).$$

This completes the proof of the prime number theorem with classical error term.

9.3. The Riemann hypothesis and its significance

The Riemann hypothesis is the assertion that all the nontrivial zeros Z_{nontriv} lie on the line $\text{Re } s = 1/2$.

If the Riemann hypothesis holds then we can, of course, improve the estimate $X^\rho \leq X^{1-c/j}$ in the above argument to $X^\rho \leq X^{1/2}$. By essentially the same arguments as before (splitting the zeros into ranges Z_j) we obtain

$$\psi(2X) - \psi(X) \leq X + O(\varepsilon X) + O(\log^2(1/\varepsilon)X^{1/2}).$$

Choosing $\varepsilon = X^{-2/3}$ (say) yields

$$\psi(2X) - \psi(X) \leq X + O(X^{1/2} \log^2 X).$$

Telescoping the sum in the usual manner gives

$$\psi(X) \leq X + O(X^{1/2} \log^2 X).$$

Once again, a corresponding lower bound may be obtained using an analogous argument.

An introduction to sieve theory*10.1. Introduction**

In this chapter we introduce a different kind of method in the study of prime numbers, the sieve. Sieve theory is an enormous topic, but we will only consider one very particular problem: that of bounding from above the quantity $\pi(X+Y) - \pi(X)$, the number of primes between X and $X + Y$.

We note to begin with that, at least if X is much larger than Y , the prime number theorem is totally useless. Moreover, we certainly do not expect any kind of asymptotic formula for this quantity, since there could be no primes at all in such an interval.

It is instructive to consider the efficacy of the most naive sieve method, the sieve of Erathosthenes (a.k.a. inclusion-exclusion). Writing $f(d) := \#\{n : X < n \leq X + Y, d|n\}$, an upper bound for $\pi(X + Y) - \pi(X)$ is

$$f(1) - f(2) - f(3) - \cdots + f(6) + f(10) + \cdots = \sum_{I \subset [k]} (-1)^{|I|} f\left(\prod_{i \in I} p_i\right),$$

where p_1, \dots, p_k are the first k primes.

We have

$$f(d) = \frac{Y}{d} + O(1),$$

and in general it is not possible to say anything useful about the $O(1)$ term. Therefore these error terms of $O(1)$ add up to something that cannot be bounded by better than $O(2^k)$, and we have

$$\begin{aligned} \pi(X + Y) - \pi(X) &\leq Y \sum_{I \subset [k]} (-1)^{|I|} \prod_{i \in I} \frac{1}{p_i} + O(2^k) \\ &= Y \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) + O(2^k). \end{aligned}$$

Clearly we cannot take k larger than a multiple of $\log Y$ and hope to get a useful result. However, $\prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$ is of size roughly $1/\log k$, and so the best bound this method can give is

$$\pi(X + Y) - \pi(X) \ll \frac{Y}{\log \log Y}.$$

The main aim of this section is to prove the following result, giving the best possible order of magnitude.

THEOREM 10.1. $\pi(X+Y) - \pi(X)$, the number of primes between X and $X+Y$ is at most $(2 + o(1))\frac{Y}{\log Y}$ (with the $o(1)$ being as $Y \rightarrow \infty$).

Remark. It is in fact known that the number of primes in this range is at most $2\pi(Y)$. The argument we give here can be used, with a little more care, to prove a result almost as good as this, namely that $\pi(X+Y) - \pi(X) \ll (2 + o(1))Y/\log Y$. It is a major unsolved problem to improve the constant 2, though it is conjecture that it can be replaced by 1. However, Hensley and Richards have shown that one should not expect that $\pi(X+Y) - \pi(X) \leq \pi(Y)$, in the sense that they have proved that this inequality fails if one assumes some widely-believed conjectures about configurations of primes.

10.2. Selberg's weights

To get an upper bound on $\pi(X+Y) - \pi(X)$ we use an idea of Selberg which, in retrospect, is very simple. Let $(\lambda_d)_{d \geq 1}$ be an sequence of real numbers with $\lambda_1 = 1$, let $R < Y$ be a threshold to be specified later (we will choose it to be Y^c for c slightly less than $\frac{1}{2}$), and consider the weight function

$$\mu(n) := \left(\sum_{d|n; d \leq R} \lambda_d \right)^2.$$

Evidently $\mu(n) \geq 0$ for all n . Moreover, if n is a prime $> R$, then the sum $\sum_{d|n; d \leq R} \lambda_d$ collapses to simply $\lambda_1 = 1$, and therefore $\mu(n) = 1$. In other words, $\mu(n)$ is a majorant for the characteristic function of the primes, and hence

$$(10.1) \quad \pi(X+Y) - \pi(X) \leq \sum_{X < n \leq X+Y} \nu(n).$$

What has been gained? It turns out that the sum on the right is relatively tractable. Expanding out the square, we have

$$\sum_{X \leq n \leq X+Y} \nu(n) = \sum_{X \leq n < X+Y} \left(\sum_{d|n; d \leq R} \lambda_d \right)^2 = \sum_{d_1, d_2 \leq R} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{X \leq n \leq X+Y \\ d_1, d_2 | n}} 1.$$

The inner sum, that is to say the number of $n \in (X, X+Y]$ divisible by d_1 and d_2 , is $\frac{Y}{[d_1, d_2]} + O(1)$ (where here $[a, b]$ means the l.c.m. of a and b) and so

$$(10.2) \quad \begin{aligned} \pi(X+Y) - \pi(Y) &= \sum_{X \leq n \leq X+Y} \nu(n) \\ &= Y \sum_{d_1, d_2 \leq R} \frac{\lambda_{d_1} \lambda_{d_2}}{[d_1, d_2]} + O(1) \sum_{d_1, d_2 \leq R} |\lambda_{d_1}| |\lambda_{d_2}|. \end{aligned}$$

At this point the λ_d are still completely arbitrary, subject only to $\lambda_1 = 1$. The strategy henceforth is to choose them to minimise the quadratic form

$$Q(\vec{\lambda}) := \sum_{d_1, d_2 \leq R} \frac{\lambda_{d_1} \lambda_{d_2}}{[d_1, d_2]} = \sum_{d_1, d_2 \leq R} \frac{\lambda_{d_1} \lambda_{d_2}}{d_1 d_2},$$

which forms the main term above, and hope that the error term looks after itself. Under what conditions can the error term be “expected to look after itself?” If we assume that the λ_d are “reasonably bounded” in the sense that

$$(10.3) \quad \lambda_d \ll_{\varepsilon} d^{\varepsilon}$$

for any $\varepsilon > 0$, then the error term here is $\ll_{\varepsilon} R^{2+\varepsilon}$. If we choose $R = Y^c$ for some $c < 1/2$ then this will, if we take ε sufficiently small, be much smaller than $Y/\log Y$, the main term in our result.

To carry out this strategy, we need to diagonalise the form Q . To do this, we note that

$$(d_1, d_2) = \sum_{\delta | (d_1, d_2)} \phi(\delta),$$

where ϕ is Euler’s ϕ -function. We showed this earlier in the course. Substituting in to the definition of Q yields

$$(10.4) \quad Q(\vec{\lambda}) = \sum_{\delta \leq R} \phi(\delta) \left(\sum_{\substack{\delta | d \\ d \leq R}} \frac{\lambda_d}{d} \right)^2 = \sum_{\delta \leq R} \phi(\delta) u_{\delta}^2,$$

where

$$u_{\delta} := \sum_{\substack{\delta | d \\ d \leq R}} \frac{\lambda_d}{d}.$$

We claim that the change of variables is invertible, or in other words that we can express λ_d in terms of the u_{δ} . This is a slight twist of the Möbius inversion formula; indeed we claim that

$$(10.5) \quad \frac{\lambda_d}{d} = \sum_{\substack{d | \delta \\ \delta \leq R}} \mu\left(\frac{\delta}{d}\right) u_{\delta}.$$

This is easily verified: the right-hand side is

$$\sum_{d' \leq R} \frac{\lambda_{d'}}{d'} \left(\sum_{d | \delta | d'} \mu\left(\frac{\delta}{d}\right) \right),$$

and the inner sum vanishes except when $d' = d$.

Note in particular that the constraint $\lambda_1 = 1$ becomes

$$(10.6) \quad 1 = \sum_{\delta \leq R} \mu(\delta) u_{\delta}.$$

Minimising $Q(\vec{\lambda})$, as given in (10.4), subject to (10.6), is a standard task. Indeed by Cauchy-Schwarz we have

$$1 = \sum_{\delta \leq R} \mu(\delta) u_\delta \leq \left(\sum_{\delta \leq R} \phi(\delta) u_\delta^2 \right)^{1/2} \left(\sum_{\delta \leq R} \frac{\mu^2(\delta)}{\phi(\delta)} \right)^{1/2},$$

and moreover equality can occur by taking $u_\delta \propto \frac{\mu(\delta)}{\phi(\delta)}$. Thus the minimum value of $Q(\vec{\lambda})$ subject to (10.6) is $1/D$, where

$$D := \sum_{\delta \leq R} \frac{\mu^2(\delta)}{\phi(\delta)} = \sum_{\delta \leq R: \delta \text{ squarefree}} \frac{1}{\phi(\delta)},$$

this being attained when

$$u_\delta = \frac{\mu(\delta)}{D\phi(\delta)}.$$

To complete the proof, it is enough to show that

$$(10.7) \quad D \geq \log R - O(1),$$

as well as the fact that, with this choice of the u_δ , the λ_d as specified in (10.5) satisfy (10.3), that is to say $|\lambda_d| \ll_\varepsilon d^\varepsilon$. We handle these tasks in turn.

Proof of (10.7). By definition we have

$$D = \sum_{d \leq R: d \text{ squarefree}} \frac{1}{\phi(d)}.$$

If d is squarefree then $\phi(d) = \prod_{p|d} (1 - \frac{1}{p})$ and therefore this can be written as

$$\sum_{d \leq R: d \text{ squarefree}} \frac{1}{d} \prod_{p|d} \left(1 + \frac{1}{p} + \frac{1}{p^2} \cdots\right).$$

Now every $m \leq R$ can be written as a product $dp_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where d is squarefree and $p_i | d$ (simply take $d = p_1 \cdots p_k$, where the p_i are the primes dividing m). Therefore

$$D \geq \sum_{m \leq R} \frac{1}{m} = \log R + O(1),$$

which is what we wanted to prove.

Proof of (10.3). By the choice of u_δ and (10.5) we have

$$\lambda_d = \frac{d}{D} \sum_{d|\delta, \delta \leq R} \frac{\mu(\delta/d)\mu(\delta)}{\phi(\delta)}.$$

Note that the sum is supported where δ is squarefree. Thus, writing $\delta' := \delta/d$, we have $\phi(\delta) = \phi(\delta')\phi(d)$. The sum is therefore bounded above by

$$\frac{d}{D\phi(d)} \sum_{\delta' \leq R, \delta' \text{ squarefree}} \frac{1}{\phi(\delta')} = \frac{d}{\phi(d)}.$$

(Note that if $\mu(\delta) \neq 0$ then δ', d are coprime and hence $\phi(\delta) = \phi(d)\phi(\delta')$, and certainly δ' must be squarefree.) Thus we only need prove that

$$(10.8) \quad \phi(d) \gg_{\varepsilon} d^{1-\varepsilon}$$

when d is squarefree. This is clear if we factor d as a product of primes: if $p > p_0(\varepsilon)$ is a sufficiently large prime then $\phi(p) = p - 1 \geq p^{1-\varepsilon}$, whilst the contribution from the smaller primes is just a constant.

APPENDIX A

*Some smooth bump functions

In this appendix we discuss some smooth functions – for example, smooth approximations to the interval $[-1, 1]$. Traditionally a “trick” is used to construct these involving the function

$$f(t) := \begin{cases} e^{1/(1-t^2)} & |t| < 1; \\ 0 & |t| > 1, \end{cases}$$

which can be shown (a standard undergraduate exercise) to lie in $C^\infty(\mathbb{R})$.

I dislike this because it is a “trick”. Furthermore, though we know from Lemma ?? that the Fourier transform \hat{f} satisfies the estimate $|\hat{f}(\xi)| \leq C_m |\xi|^{-m}$ for $|\xi| \geq 1$, it is surprisingly difficult to get any effective bound for C_m .

In this appendix we present a more natural construction. This is no doubt “classical”, but we learned of it in connection with (the easy direction of) something called the Denjoy-Carleman theorem.

The idea is to construct a function f as an infinite convolution of normalised characteristic functions of intervals. If $\delta > 0$, write

$$\nu_\delta(x) := \frac{1}{2\delta} 1_{|x| \leq \delta}.$$

Thus $\|\nu_\delta\|_1 = 1$.

It is extremely easy to compute the Fourier transform of ν_δ : we have

$$\hat{\nu}_\delta(\xi) = \frac{1}{2\delta} \int_{-\delta}^{\delta} e^{-ix\xi} dx = \frac{\sin \delta\xi}{\delta\xi}.$$

In particular we have the trivial bound

$$(A.1) \quad |\hat{\nu}_\delta(\xi)| \leq \frac{2}{\delta|\xi|}.$$

Recall that the convolution of two functions f and g , $f * g$, is defined by

$$(f * g)(x) := \int f(x-y)g(y)dy.$$

Suppose that $f : \mathbb{R} \rightarrow [0, 1]$ is a function with $f(x) = 1$ for $|x| \leq 1 - \eta$ and $f(x) = 0$ for $|x| \geq 1 + \eta$. Then it is easy to see that $f * \nu_\delta$ takes values in $[0, 1]$, has $f(x) = 1$ for $|x| \leq 1 - \eta - \delta$, and $f(x) = 0$ for $|x| \geq 1 + \eta + \delta$. This observation leads quickly to the following lemma.

LEMMA A.1. *Let $\varepsilon > 0$, and let $n \in \mathbb{N}$. Then there is a function $f = f_{n,\varepsilon} : \mathbb{R} \rightarrow [0, 1]$ such that $f(x) = 1$ for $|x| \leq 1 - \varepsilon$, $f(x) = 0$ for $|x| \geq 1 + \varepsilon$, and $|\hat{f}(\xi)| \leq C(n, \varepsilon)|\xi|^{-n-1}$. We may take $C(n, \varepsilon) = 2^{2n+1}(n!)^2\varepsilon^{-n}$.*

Proof. Define

$$f := \nu_1 * \nu_{\delta_1} * \cdots * \nu_{\delta_n},$$

where $\delta_j := \varepsilon/2j^2$. (There is considerable flexibility here; the important feature of the sequence $1/j^2$ is that it is summable but *slowly*.) Since $\sum j^{-2} < 2$, this has the support properties claimed.

We have $\hat{f} = \hat{\nu}_1 \hat{\nu}_{\delta_1} \cdots \hat{\nu}_{\delta_n}$, and so from the trivial bound (A.1) we obtain

$$|\hat{f}(\xi)| \leq \frac{2^{n+1}}{\delta_1 \cdots \delta_n} |\xi|^{-n-1}.$$

The result follows. \square

A slightly more refined analysis allows one to show that, for fixed $\varepsilon > 0$, the sequence $f_{n,\varepsilon}$ converges as $n \rightarrow \infty$. This gives a version of Lemma A.1 in which f depends only on ε , and not on n .

LEMMA A.2. *Let $\varepsilon > 0$ be fixed. Let $(\delta_j)_{j=1}^\infty$ be a sequence of positive real numbers with $\sum_j \delta_j \leq \varepsilon$. Set $f_n = f_{n,\varepsilon} := \nu_1 * \nu_{\delta_1} * \cdots * \nu_{\delta_n}$. Then f_n converges uniformly to a function $f : \mathbb{R} \rightarrow [0, 1]$ with $f(x) = 1$ for $|x| \leq 1 - \varepsilon$ and $f(x) = 0$ for $|x| \geq 1 + \varepsilon$. The Fourier transform $\hat{f}(\xi)$ satisfies*

$$|\hat{f}(\xi)| \leq \inf_n \frac{2^{n+1}}{\delta_1 \cdots \delta_n} |\xi|^{-n-1}.$$

Proof. Since ε is fixed throughout the argument, we write f_n instead of $f_{n,\varepsilon}$. First note that $f_1 = \nu_1 * \nu_{\delta_1}$ satisfies the Lipschitz property

$$|f_1(x) - f_1(x')| \leq \frac{2}{\delta_1} |x - x'|.$$

Indeed

$$\begin{aligned} |f_1(x) - f_1(x')| &= \int \nu_1(y) (\nu_{\delta_1}(x - y) - \nu_{\delta_1}(x' - y)) dy \\ &\leq \frac{1}{2} \int |\nu_{\delta_1}(x - y) - \nu_{\delta_1}(x' - y)| dy, \end{aligned}$$

which can easily be computed to be at most the claimed bound. Next note that any such Lipschitz bound is preserved under convolution with an arbitrary non-negative

function ν with integral 1; indeed if $|f(x) - f(x')| \leq C|x - x'|$ for all x, x' then

$$\begin{aligned} |f * \nu(x) - f * \nu(x')| &= \left| \int \nu(y)(f(x-y) - f(x'-y))dy \right| \\ &\leq \int \nu(y)|f(x-y) - f(x'-y)|dy \\ &\leq C|x - x'|. \end{aligned}$$

It follows that each of the functions f_n satisfies the same Lipschitz bound as f_1 .

Now suppose that f satisfies the Lipschitz bound $|f(x) - f(x')| \leq C|x - x'|$, and that ϕ is a non-negative function with integral 1, supported on $[-\delta, \delta]$. Then

$$\begin{aligned} \|f - f * \phi\|_\infty &= \sup_x \left| \int (f(x) - f(x-y))\phi(y)dy \right| \\ &\leq \sup_{|y| \leq \delta} |f(x) - f(x-y)| \int \phi(y)dy \leq C\delta. \end{aligned}$$

It follows from these observations that

$$\|f_m - f_n\|_\infty \leq \frac{2}{\delta_1} \sum_{j=m+1}^n \delta_j.$$

In particular, (f_n) is Cauchy in the uniform norm and hence f_n tends to some continuous function f .

To obtain the stated bound on the Fourier transform, first note that $\hat{f}(\xi) = \lim_{n \rightarrow \infty} \hat{f}_n(\xi)$. This follows immediately from the fact that $f_n \rightarrow f$ uniformly, and the support of f_n is contained in $[-2, 2]$ for all n . Note also that if $\|\nu\|_1 = 1$ then

$$|(f_n * \nu)^\wedge(\xi)| = |\hat{f}_n(\xi)| |\hat{\nu}(\xi)| \leq |\hat{f}_n(\xi)|.$$

This means that $|\hat{f}_n(\xi)|$ is a non-increasing function of n . The claimed bound now follows using (A.1). \square

COROLLARY A.1. *Let $\varepsilon > 0$. Then for any $\kappa > 0$ there is a continuous function $f = f_{\varepsilon, \kappa} : \mathbb{R} \rightarrow [0, 1]$ such that $f(x) = 1$ for $|x| \leq 1 - \varepsilon$, $f(x) = 0$ for $|x| \geq 1 + \varepsilon$ and*

$$|\hat{f}(\xi)| \leq e^{-C_{\varepsilon, \kappa} |\xi|^{1-\kappa}}.$$

Remark. Taking $\kappa = 1/2$ is certainly sufficient for any application I know of, and usually the bound $|\hat{f}(\xi)| \ll_A |\xi|^{-A}$, with no explicit dependence of the implied constant on A , is enough.

Proof. Apply the preceding lemma with $\delta_j := c/j^{1+\kappa/2}$ for an appropriately small $c = c(\varepsilon, \kappa)$. For every n we have the bound

$$|\hat{f}(\xi)| \leq C^n (n!)^{1+\kappa/2} |\xi|^{-n}.$$

Choosing $n \sim |\xi|^{1-\kappa/2}$ gives the claimed bound. \square

We have said nothing about the smoothness (or otherwise) of the functions f_n and f . One could examine this using the definition in terms of convolution. However, now that we have bounds on Fourier transforms, we may as well use the following lemma.

LEMMA A.3. *Suppose that f is continuous, that $f \in L^1(\mathbb{R})$ and that $|\hat{f}(\xi)| \ll |\xi|^{-n}$. Then f is n times differentiable.*

Bibliography

- [1] H. Davenport, *Multiplicative number theory*, Graduate Texts in Mathematics, **74**. Springer-Verlag, New York, 2000. xiv+177 pp.
- [2] E. Kowalski, *Un cours de théorie analytique des nombres*, Cours Spécialisés **13**, Société Mathématique de France, Paris, 2004.
- [3] E. Kowalski and H. Iwaniec, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, **53**. American Mathematical Society, Providence, RI, 2004.