Analytic Number Theory

Davoud Cheraghi

May 13, 2016

Contents

1 Introduction **2**

2 Arithmetic Functions **6**

3 Dirichlet Series **18**

4 Analytic Properties of the Riemann Zeta-Function **26**

5 The Proof of the Prime Number Theorem **37**

6 Further Properties of $\zeta(s)$ **54**

7 References **66**

1 Introduction

The fundamental questions in number theory concern the interplay between the additive and multiplicative structures on the integers. An example of a typical theorem from number theory is:

Theorem. *(Lagrange's Theorem) Every $n \in \mathbb{N}$ is a sum of 4 squares*

$$n = \sum_{i=1}^{4} n_i^2,$$

where $n_i \in \mathbb{Z}$.

The proof of the above theorem "works in" $\mathbb{Z}$.

This course is an introduction to analytic number theory. That is, we turn to techniques from analysis, where we apply continuous methods to study discrete phenomena. Often these are statements involving approximations. In analytic number theory we often ask roughly how frequent are integers with a certain property P. For instance, one cannot give an exact formula for the number of primes in an interval $[1, x]$, but we can establish an asymptotic formula, and give some upper bounds for the discrepancy between the exact and asymptotic formulas. Although this methodology turns out to be unexpectedly powerful, we must remain humble. It is easy to pose simple looking open (and probably extremely hard) questions about prime numbers, including:

- (Twin primes problem) Are there infinitely many pairs of consecutive primes which differ by 2?
- (Sophie Germain problem) Are there infinitely many pairs of primes p, q such that $q = 2p + 1$?
- (Goldbach problem) Is every even integer $n > 2$ equal to the sum of two primes?

There are also many number theoretic statements where it is not obvious that analytic methods are appropriate. Example of theorems whose proofs use analysis are the following

1. Every integer is a sum of at most

   (a) 4 squares,

   (b) 9 cubes,
   (c) 19 fourth powers,
   (d) 37 fifth powers, etc.

   This was proved, by the combined efforts of many mathematicians, in 1986. It answers a question of Waring dating from 1770.

2. The sequence of primes contains arbitrarily long arithmetic progressions. eg: 7, 37, 67, 97, 127, 157 is a progression of 6 primes. This was proved in 2004.

3. The ring $\left\{a + b\sqrt{14} : a, b \in \mathbb{Z}\right\} = \mathbb{Z}[\sqrt{14}]$ is a Euclidean domain.

4. Every odd number $n \geq 7$ is a sum of 3 primes. (Proved in 2013). Goldbach's conjecture (still undecided) was that every even number $n \geq 4$ is a sum of 2 primes and every odd number $n \geq 7$ is a sum of 3 primes.

In this course our use of analysis will mainly involve the theory of complex functions, specifically the notions of analytic (holomorphic) and meromorphic functions. One can argue that one is really using properties of real harmonic functions, since the real and imaginary parts of a holomorphic function have that property. There are instances where one gets number-theoretic information by considering harmonic functions in a setting where there is no complex structure.

This course is primarily concerned with arithmetic functions and prime numbers. We make the following definition.

Definition 1.1. $\pi(x) = \#\{p \leq x : p \text{ prime}\}$.

The key question we shall examine is: How fast does $\pi(x)$ grow? The first result on this question was proved by Euclid:

Theorem 1.2. *$\pi(x) \to \infty$ as $x \to \infty$.*

Numerical results suggest that $\pi(x)$ is roughly $x/\log x$. The primes appear to thin out the higher one goes, so that for numbers up to x, about one number out of $\log x$ is prime. This conjecture is due to Gauss and dates from 1849.

Let us define

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \quad .$$

In problem sheet one you will show that

$$\lim_{x\to\infty} \frac{x/\log x}{\mathrm{Li}(x)} = 1.$$

The fundamental result, verifying Gauss' conjecture is:

Theorem 1.3. *(***The Prime Number Theorem** *– Hadamard, de la Valleé Poussin 1896)*

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

or equivalently

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

It is convenient to introduce some notation.

Definition 1.4. If $f, g : [1, \infty) \to \mathbb{R}$ with $g(x) > 0$ for all x, we say that $f(x) \sim g(x)$ if $\frac{f(x)}{g(x)} \to 1$ as $x \to \infty$.

Hence the PNT (Prime Number Theorem) states that $\pi(x) \sim \frac{x}{\log x} \sim \mathrm{Li}(x)$.

Definition 1.5. Let $f, g : [1, \infty) \to \mathbb{R}$ be functions with $g(x) > 0$, for all x. We say that $f(x) = O(g(x))$ if $|f(x)/g(x)|$ is bounded from above, that is, if there exists a constant $c > 0$ such that for all x we have $|f(x)| \le cg(x)$.

In particular, a relation of the form $f(x) = g(x) + O(h(x))$ for real functions f, g, and h defined on $(0, \infty)$ means that $|f(x) - g(x)| = O(h(x)$.

Example. We have $\sin x = O(1)$ and $\sin x = O(x)$. Observe that, with the $O(\cdot)$ notation, equality is no longer symmetric (!) Note also the fact that $f(x) = O(g(x))$ does not imply that $f'(x) = O(g'(x))$.

Tables reveal that the detailed distribution of primes is very erratic. There are a lot of pairs of primes which differ by 2, such as $(11, 13)$, $(17, 19)$, $(29, 31)$, etc. It is a famous open problem however whether there are infinitely many such "prime-twins".

There are arbitrarily large gaps among the primes. Consider the numbers $N!+2, N!+3, \ldots, N!+N$. These are all composite, since if $k \leq N$ then $k \mid N!+k$.

Open problem: Roughly how large is the largest gap between consecutive primes up to N? A plausible conjecture is that the largest gap is $\sim (\log N)^2$.

For all $x \geq 20$ for which $\pi(x)$ has been calculated one finds that

$$\frac{x}{\log x} < \pi(x) < \mathrm{Li}(x).$$

The first inequality has in fact been proved to hold for $x \geq 20$. As to the second inequality, there are good reasons to suppose $\pi(x) < \mathrm{Li}(x)$ for all $x \leq 10^{100}$. However Littlewood showed in 1912 that $\pi(x) - \mathrm{Li}(x)$ changes sign infinitely often, and it is now known that there exists an $x \leq 10^{316}$ such that $\pi(x) > \mathrm{Li}(x)$. This is a remarkable result. In every case that $\pi(x)$ has ever been calculated, comprising billions of data points, one has $\pi(x) < \mathrm{Li}(x)$. However we know that the inequality eventually fails: In mathematics "experimental evidence" is not good enough – only proper proof will do!

2 Arithmetic Functions

We denote the set of positive integers with $\mathbb{N}$.

Definition. An *arithmetic* function is a mapping $f : \mathbb{N} \to \mathbb{C}$.

Definition. A *multiplicative* arithmetic function is one for which $f(mn) = f(m)f(n)$, whenever $(m, n) = 1$.

One might imagine that it would be more natural to define a multiplicative function to be one satisfying $f(mn) = f(m)f(n)$ for all m, n. However, this condition is too restrictive.

Example. We define the *unit function* $u : \mathbb{N} \to \mathbb{C}$ as $u(n) = 1$ for all n. This is a multiplicative arithmetic function. Similarly $u_c(n) = n^c$, where $c \in \mathbb{R}$ is fixed, is multiplicative.

The function $\omega(n) = \#\{p \mid n : p \text{ prime}\}$ is not multiplicative, since, for example $\omega(2) = 1, \omega(3) = 1$ but $\omega(6) = 2 \neq 1 \times 1$.

Other important arithmetic functions are:-

- $d(n) = \#\{k \in \mathbb{N} : k \mid n\}$. This is called the *divisor function*.
- $\sigma(n) = \sum_{k|n} k$,
- $\phi(n) = \#\{k \in \mathbb{N} : k \leq n, (k, n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{k + n\mathbb{Z} : (k, n) = 1\}$. This is called the *Euler function*.

The notations $\omega(n), d(n), \sigma(n)$ and $\phi(n)$ are standard; but $u(n)$ and $u_c(n)$ were invented for these notes!

An obvious fact is that if f, g are multiplicative, then so is $(fg)(n) = f(n)g(n)$.

Definition. The Dirichlet convolution of f and g is defined as

$$(f * g)(n) = \sum_{ab=n; a,b \in \mathbb{N}} f(a)g(b).$$

For example,

$$\begin{aligned}(d * \omega)(6) &= d(1)\omega(6) + d(2)\omega(3) + d(3)\omega(2) + d(6)\omega(1) \\ &= 1 \times 2 + 2 \times 1 + 2 \times 1 + 4 \times 0 = 6.\end{aligned}$$

Note also the following facts

1. $(u * u)(n) = \sum_{ab=n} u(a)u(b) = \sum_{ab=n} 1 = d(n)$. Hence $u * u = d$.

2. $(u * u_1)(n) = \sum_{ab=n} u(a)u_1(b) = \sum_{ab=n} b = \sum_{b|n} b = \sigma(n)$. Hence, $u * u_1 = \sigma$.

Theorem 2.1. *If F and G are multiplicative, then so is $F * G$.*

Corollary 2.2. *The functions $d(n)$ and $\sigma(n)$ are multiplicative.*

Lemma 2.3. *Suppose that $(m, n) = 1$. Then every pair $a, b \in \mathbb{N}$ with $ab = mn$, takes the form $a = cd$ and $b = ef$ with $ce = m$, $df = n$; and this expression is unique.*

Proof

First we prove the existence of c, d, e, f. Take

$$c = (a, m), \quad d = a/c, \quad e = (b, m), \quad f = b/e.$$

It follows that $c, d, e, f \in \mathbb{N}$. So it remains to show that $ce = m$, $df = n$. We will show that $(a, m)(b, m) = m$ $(\star)$. It will follow that $ce = m$, and that $df = ab/ce = mn/ce = n$ as required.

To show $(\star)$, we use repeatedly the fact that $(\alpha, \beta)\gamma = (\alpha\gamma, \beta\gamma)$. This yields

$$\begin{aligned} (a, m)(b, m) &= (a(b, m), m(b, m)) \\ &= ((ab, am), m(b, m)) \\ &= ((mn, am), m(b, m)) \\ &= (m(n, a), m(b, m)) \\ &= m((n, a), (b, m)). \end{aligned}$$

However $(n, a) \mid n$ and $(b, m) \mid m$ and we know that $(m, n) = 1$. Hence $((n, a), (b, m)) = 1$, and so the expression above reduces to m.

It remains to prove uniqueness. Suppose $a = c'd'$ and $b = e'f'$, with $c'e' = m$ and $d'f' = n$. Then, since $(m, n) = 1$, we have $(e', d') = 1$. Hence

$$c = (a, m) = (c'd', c'e') = c'(d', e') = c'.$$

Similarly, $d = d'$ and so $e = e'$ and $f = f'$. $\square$

Proof (Of Theorem 2.1)

Take $(m,n)=1$. We have to show that $(F*G)(m)(F*G)(n)=(F*G)(mn)$.

$$LHS=\left\{\sum_{m=ce}F(c)G(e)\right\}\left\{\sum_{df=n}F(d)G(f)\right\}=\sum_{\substack{c,d,e,f\in\mathbb{N}\\ ce=m,\,df=n}}F(c)F(d)G(e)G(f).$$

However, $c\mid m$ and $d\mid n$ where $(m,n)=1$. Hence $(c,d)=1$. This gives $F(c)F(d)=F(cd)$. Similarly for $(e,f)=1$. Hence

$$LHS=\sum_{ce=m,df=n}F(cd)G(ef)$$

and by Lemma 2.3, each pair a,b for which $ab=mn$, arises just once as $a=cd$ and $b=ef$. Thus

$$LHS=\sum_{ab=mn}F(a)G(b)=(F*G)(mn).$$

□

Theorem 2.4. *If $f(n)$ is multiplicative and $n=p_1^{e_1}\cdots p_k^{e_k}$, where p_i are distinct primes, then $f(n)=\prod_{i=1}^{k}f(p_i^{e_i})$.*

Corollary 2.5. *We have $d(p_1^{e_1}\cdots p_k^{e_k})=(e_1+1)\cdots(e_k+1)$.*

Proof $d(p_i^{e_i})=\#\{1,p_i,\ldots,p_i^{e_i}\}=e_i+1$. □

Corollary 2.6.

$$\sigma(p_1^{e_1}\cdots p_k^{e_k})=\prod_{i=1}^{k}\frac{p_i^{e_i+1}-1}{p_i-1}.$$

Proof $\sigma(p_i^{e_i})=1+p_i+\ldots+p_i^{e_i}=\frac{p_i^{e_i+1}-1}{p_i-1}$. □

Proof (Of Theorem 2.4)

We work by induction on k. For $k=1$ we have $f(p_1^{e_1})=f(p_1^{e_1})$. In general,

$$f(p_1^{e_1}\cdots p_k^{e_k})=f(p_1^{e_1}\cdots p_{k-1}^{e_{k-1}})f(p_k^{e_k})$$

since $(p_1^{e_1}\dots p_{k-1}^{e_{k-1}}, p_k^{e_k}) = 1$. The induction hypothesis then yields

$$\prod_{i=1}^{k-1} f(p_i^{e_i}) f(p_k^{e_k})$$

which produces the required result. $\square$

Corollary 2.7. *If f, g are multiplicative then $f = g$ if and only if $f(p^e) = g(p^e)$ for all prime powers p^e.*

As an example of a typical question we can now answer, we ask how large is $d(n)$? Clearly $d(p) = 2$ for all primes p, but sometimes $d(n)$ is large.

Theorem 2.8. *For all $k \in \mathbb{N}$ one has $d(n) \geq (\log n)^k$ for infinitely many n.*

Proof

Let $p_1, \dots, p_{k+1}$ be the first $k+1$ primes. Set $n = (p_1 \cdots p_{k+1})^m$. We claim that if m is large enough, then $d(n) \geq (\log n)^k$.

We have

$$d(n) = (m+1)^{k+1} > m^{k+1} = \left(\frac{\log n}{\log p_1 \cdots p_{k+1}}\right)^{k+1}$$

and this exceeds $(\log n)^k$ providing that $\log n > (\log p_1 \cdots p_{k+1})^{k+1}$. It therefore suffices to take $m > (\log p_1 \cdots p_{k+1})^k$. $\square$

Theorem 2.9. *For every $\epsilon > 0$ there exists a constant c_ϵ such that $d(n) \leq c_\epsilon n^\epsilon$ for all $n \in \mathbb{N}$.*

Remark. This result can be re-phrased as saying that $d(n) = O(n^\epsilon)$ for all $\epsilon > 0$.

Proof

We have $d(n) \leq n$, so we can take $c_\epsilon = 1$ for all $\epsilon \geq 1$. Thus we may now assume that $\epsilon < 1$. For $n = p_1^{e_1} \cdots p_r^{e_r}$ we have

$$\frac{d(n)}{n^\epsilon} = \prod \frac{1 + e_i}{p_i^{\epsilon e_i}}.$$

Then, for primes p_i with $p_i \geq 2^{1/\epsilon}$ we have

$$\frac{1 + e_i}{p_i^{\epsilon e_i}} \leq \frac{1 + e_i}{2^{e_i}} \leq 1,$$

since $2^m \geq 1+m$ for all $m \in \mathbb{N}$. For the remaining primes, for which $2 \leq p_i < 2^{1/\epsilon}$, we have

$$p_i^{\epsilon e_i} \geq 2^{\epsilon e_i} = e^{\epsilon e_i \log 2} \geq 1 + \epsilon e_i \log 2 > \epsilon \log 2 + \epsilon e_i \log 2 = \epsilon(\log 2)(1+e_i).$$

Hence,

$$\frac{1+e_i}{p_i^{\epsilon e_i}} \leq \begin{cases} 1 & \text{for } p_i \geq 2^{1/\epsilon}, \\ \frac{1}{\epsilon \log 2} & \text{for } p_i < 2^{1/\epsilon}. \end{cases}$$

Hence, with p_i ranging through the various prime factors of n, we have

$$\frac{d(n)}{n^\epsilon} \leq \prod_{p_i < 2^{1/\epsilon}} \left(\frac{1}{\epsilon \log 2}\right).$$

Thus, if p ranges over all primes less than $2^{1/\epsilon}$, whether or not they divide n, we have

$$\frac{d(n)}{n^\epsilon} \leq \prod_{p < 2^{1/\epsilon}} \left(\frac{1}{\epsilon \log 2}\right).$$

Denote the product on the right by c_ϵ, and note that this does not depend on n. Then $\frac{d(n)}{n^\epsilon} \leq c_\epsilon$ for all n, as required. □

We may also ask how large is $d(n)$ on average?

Theorem 2.10. *We have*

$$\lim_{N\to\infty} \frac{\sum_{n\leq N} d(n)}{\sum_{n \leq N} \log n} = 1.$$

Equivalently, $\sum_{n\leq N} d(n) \sim \sum_{n\leq N} \log n$. *More precisely,*

$$\begin{aligned} \sum_{n\leq N} d(n) &= N \log N + O(N), \\ \sum_{n\leq N} \log n &= N \log N + O(N). \end{aligned}$$

So $d(n)$ is, on average, of size $\log n$

Lemma 2.11. *If $f : [1, \infty) \to [0, \infty)$ is increasing, then*

$$\int_1^N f(x)dx \le \sum_1^N f(n) \le f(N) + \int_1^N f(x)dx$$

while if f is decreasing, then

$$\int_1^N f(x)dx \le \sum_1^N f(n) \le f(1) + \int_1^N f(x)dx.$$

Proof

If f is increasing

$$\int_{n-1}^n f(x)dx \le f(n) \le \int_n^{n+1} f(x)dx$$

and so

$$\sum_1^N f(n) \ge f(1) + \sum_{n=2}^N \int_{n-1}^n f(x)dx = f(1) + \int_1^N f(x)dx \ge \int_1^N f(x)dx$$

and

$$\sum_1^N f(n) \le f(N) + \sum_{n=1}^{N-1} \int_n^{n+1} f(x)dx = f(N) + \int_1^N f(x)dx.$$

The decreasing case is similar. □

Corollary 2.12. *We have*

$$\log N \le \sum_{n=1}^N \frac{1}{n} \le 1 + \log N,$$

$$N \log N - N \le \sum_{n=1}^N \log n \le N \log N.$$

Proof

Apply Lemma 2.11 with $f(x) = 1/x$ (the decreasing case), and the first statement follows.

For $f(x) = \log x$ (the increasing case), we have

$$\int_1^N f(x)dx = \int_1^N \log x \, dx = N \log N - N + 1$$

so

$$N \log N - N \leq N \log N - N + 1 = \int_1^N f(x)dx \leq \sum_1^N \log n$$

and

$$\sum_1^N \log n \leq \sum_1^N \log N = N \log N.$$

□

We now prove Theorem 2.10

Proof

We have

$$\sum_{n \leq N} d(n) = \sum_{n=ab \leq N} 1 = \sum_{\substack{a,b \\ ab \leq N}} 1 = \sum_{a \leq N} \# \left\{ b : b \leq \frac{N}{a} \right\}.$$

For $\theta \in \mathbb{R}$ set $[\theta] = \max \{k \in \mathbb{Z} : k \leq \theta\}$. Then if $\theta \geq 0$ one sees that $\# \{b \in \mathbb{N} : b \leq \theta\} = [\theta]$.

For example, $[\pi] = 3$ and $\{b \in \mathbb{N} : b \leq \pi\} = \{1, 2, 3\}$. Hence

$$\sum_{n \leq N} d(n) = \sum_{a \leq N} \left[\frac{N}{a} \right].$$

However, for all $\theta \in \mathbb{R}$ we have $[\theta] = \theta + O(1)$, and so $[N/a] = N/a + O(1)$. This produces

$$\sum_{a \leq N} \left[\frac{N}{a} \right] = \sum_{a \leq N} \left(\frac{N}{a} + O(1) \right) = \sum_{a \leq N} \frac{N}{a} + O(N) = N \sum_{a \leq N} \frac{1}{a} + O(N)$$

which in turn is $N\{\log N + O(1)\} + O(N)$, by Corollary 2.12. Finally, this is $N \log N + O(N) + O(N)$, and so

$$\sum_{a \leq N} \left[\frac{N}{a} \right] = N \log N + O(N).$$

□

We now introduce another important arithmetic function.

Definition. (The Möbius Function)

Set $\mu(1) = 1$ and

$$\mu(p_1^{e_1} \cdots p_k^{e_k}) = \begin{cases} (-1)^k & \text{if } e_i = 1 \text{ for all } i, \\ 0 & \text{if } e_i \geq 2 \text{ for some } i, \end{cases}$$

where p_i are distinct primes.

Note that $\mu(n)$ is a multiplicative function. This follows directly from the definition, but may take a moment's thought.

The following result gives the key property for the Möbius function.

Theorem 2.13. *We have*

$$(\mu * u)(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

Proof

Set $f = \mu * u$. Then f is multiplicative, by Theorem 2.1, since μ, u are multiplicative. Now if $e \geq 1$ then

$$f(p^e) = \sum_{ab=p^e} \mu(a)u(b) = \sum_{a|p^e} \mu(a)$$
$$= \mu(1) + \mu(p) + \ldots + \mu(p^e) = 1 + (-1) + 0 + \ldots + 0 = 0.$$

Hence, in general, $f(p_1^{e_1} \cdots p_k^{e_k}) = 0$ if any exponent is greater than or equal to 1. The case where $n = 1$ is trivial. □

Remark. Set

$$I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

This function is trivially multiplicative. The result above tells us that $\mu * u = I$. Note also that

$$(I * f)(n) = \sum_{ab=n} I(a)f(b) = I(1)f(n) = f(n)$$

for all f. Hence, $I * f = f$.

Theorem 2.14. *Let* $M = \{f : \mathbb{N} \to \mathbb{C} : f(1) = 1\}$ *and*

$$M_0 = \{f \in M : f \, \textit{multiplicative}\}.$$

Then $(M, *)$ *is an abelian group with identity* I*, and* M_0 *is a subgroup.*

Proof

It is trivial that $f * g = g * f$, that $I * f = f$, and also that M is closed under the $*$ operation. For associativity we note that

$$\begin{aligned}(f * (g * h))(n) &= \sum_{ab=n} f(a)(g * h)(b) \\ &= \sum_{ab=n} f(a) \sum_{cd=b} g(c)h(d) \\ &= \sum_{\substack{a,c,d \\ acd=n}} f(a)g(c)h(d),\end{aligned}$$

which is clearly independent of the ordering and the bracketing of f, g, h. This proves associativity. In the last step of the above we used the fact that there exists a one-to-one correspondence between

$$\big\{(a, b, c, d) \in \mathbb{N}^4 : ab = n, b = cd\big\} \quad \text{and} \quad \big\{(a, c, d) \in \mathbb{N}^3 : n = acd\big\}$$

via the maps $(a, b, c, d) \mapsto (a, c, d)$ and $(a, c, d) \mapsto (a, cd, c, d)$.

The existence of inverses requires a little more work. Given $f \in M$, define g inductively by setting $g(1) = 1$ and then, if $g(1), \ldots, g(n-1)$ have been defined, putting

$$g(n) := -\sum_{\substack{a,b \\ ab=n,\, b<n}} f(a)g(b).$$

Then

$$(f * g)(n) = \sum_{\substack{ab=n \\ b<n}} f(a)g(b) + f(1)g(n) = \sum_{\substack{ab=n \\ b<n}} f(a)g(b) + g(n) = 0$$

if $n \geq 2$. Trivially, $(f * g)(1) = f(1)g(1) = 1$. It follows that $f * g = I$, which completes the proof that M is a group.

As for M_0, we know that $f, g \in M_0$ means that f, g are multiplicative. Hence $f * g$ is also multiplicative, whence $f * g \in M_0$. It remains to prove that if f is multiplicative, then so is f^{-1}.

We proceed to define a function h on prime powers. Let $h(1) = 1$, and inductively set

$$h(p^e) = -\sum_{0 \leq k < e} h(p^k) f(p^{e-k}).$$

We then define h on the whole of $\mathbb{N}$ by setting $h(p_1^{e_1} \cdots p_r^{e_r}) = h(p_1^{e_1}) \cdots h(p_r^{e_r})$. Thus h is automatically multiplicative. We claim that $f * h = I$. It will follow that f^{-1} is multiplicative, since $f^{-1} = h$.

To prove that $f * h = I$ we note that f and h are multiplicative, whence $f * h$ is too. The function I is multiplicative. It is therefore sufficient to show that $f * h$ agrees with I for every prime power p^e. To do so, we note that

$$(f * h)(p^0) = f(1)h(1) = 1 = I(p^0).$$

Moreover, for $e \geq 1$ we have

$$\begin{aligned}
(f * h)(p^e) &= \sum_{0 \leq k \leq e} h(p^k) f(p^{e-k}) \\
&= \sum_{0 \leq k < e} h(p^k) f(p^{e-k}) + h(p^e) f(1) \\
&= \sum_{0 \leq k < e} h(p^k) f(p^{e-k}) + h(p^e) \\
&= 0 = I(p^e).
\end{aligned}$$

This is sufficient to show that $f * h = I$, which completes the proof. □

Theorem 2.15. *(The Möbius Inversion Formula) Given arithmetic functions f, g, we have that*

$$\sum_{d|n} g(d) = f(n) \;\; \forall n \Leftrightarrow g(n) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right) \;\; \forall n.$$

Proof

We have

$$\sum_{d|n} g(d) = f(n) \Leftrightarrow \sum_{de=n} g(d)u(e) = f(n) \Leftrightarrow g * u = f.$$

Similarly

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

Hence the theorem is equivalent to the claim that $g * u = f \Leftrightarrow g = f * \mu$. But $g * u = f \Rightarrow (g * u) * \mu = f * \mu \Rightarrow g * (u * \mu) = f * \mu \Rightarrow g * I = f * \mu \Rightarrow g = f * \mu$. Similarly, $f * \mu = g \Rightarrow (f * \mu) * u = g * u \Rightarrow f * (\mu * u) = g * u \Rightarrow f = g * u$. □

We now examine the function $\phi(n) = \#\{k : k \leq n, (k,n) = 1\}$.

Theorem 2.16. *We have $\phi * u = u_1$, or equivalently $\sum_{d|n} \phi(d) = n$.*

Proof

Let n be given. We partition $\{1, 2, \ldots, n\}$ into disjoint subsets according to the highest common factor which each element has with n. This produces sets $A_d = \{k \in \mathbb{N} : k \leq n, (k,n) = d\}$. There is one such set for each $d \mid n$.

We claim that $\#A_d = \phi(n/d)$, from which it will follow that

$$n = \sum_{d|n} \#A_d = \sum_{d|n} \phi(n/d) = \sum_{n=de} \phi(e) = \sum_{e|n} \phi(e)$$

as required.

To prove the claim we observe that if $(k,n) = d$ then $d \mid k$. Set $k = dj$ and $n = de$, so that $d = (k,n) = (dj, de) = d(j,e)$. It follows that $(j,e) = 1$. Thus, $\#A_d = \#\{dj : dj \leq de, (j,e) = 1\} = \#\{j : j \leq e, (j,e) = 1\} = \phi(e)$, as required. □

Corollary 2.17. *We have $\phi = \mu * u_1$, so that $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n} \frac{\mu(d)}{d}$.*

Proof

The result follows from Theorem 2.16, by the Möbius inversion formula, Theorem 2.15. Specifically, we have $\phi = \phi * I = \phi * (u * \mu) = (\phi * u) * \mu = u_1 * \mu$. □

Corollary 2.18. *The function ϕ is multiplicative.*

Proof

The functions μ and u_1 are multiplicative, and hence their convolution is also multiplicative. $\square$

Corollary 2.19.

$$\phi(p_1^{e_1} \cdots p_k^{e_k}) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1)$$

and

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

Proof

We have

$$\phi(p^e) = \# \{n : n \leq p^e, (n, p^e) = 1\} = \# \{n : n \leq p^e, p \nmid n\}$$

$$= \# \{n : n \leq p^e\} - \# \{n : n \leq p^e, p \mid n\} = p^e - p^{e-1} = p^e(1 - 1/p).$$

$\square$

3 Dirichlet Series

We recall the Euler's viewpoint on the fact, originally due to Euclid, that there are infinitely many prime numbers. Euclids original proof was quite simple, and entirely algebraic: assume there are only finitely many primes, multiply them together, add 1, then factor the result. Euler realized instead that a basic fact from analysis also leads to the infinitude of primes. This fact is the divergence of the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots.$$

On the other hand, if there were only finitely many primes, then unique factorization of positive integers into prime powers would imply that

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) = \prod_p \left(1 - \frac{1}{p}\right)^{-1}.$$

This would give the equality between a divergent series and a finite quantity. Euler's idea turns out to be quite fruitful: the introduction of analysis into the study of prime numbers allows us to prove distribution statements about primes in a much more flexible fashion than is allowed by algebraic techniques.

A Dirichlet series is a series of the form

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

where $f(n)$ is an arithmetic function, and $s \in \mathbb{C}$.

It is conventional, for historical reasons, to use s as a complex variable in this setting, and to write it as a sum of real and imaginary parts as $s = \sigma + it$. Since s is complex we must be careful to specify what we mean by n^{-s}. We define it as $n^{-s} = e^{-s \log n}$ where the branch of the logarithm function is chosen so that $\log n$ is real.

The series above may converge for all s, as in the example $\sum_{n=1}^{\infty} e^{-n} n^{-s}$, or it may diverge for all s, as shown by the series $\sum_{n=1}^{\infty} e^{n} n^{-s}$. However in many cases there are some values where the series converges and others where it diverges.

Theorem 3.1. *Suppose that there exists an s_1 such that $F(s_1)$ is absolutely convergent, and an s_2 such that $F(s_2)$ is not absolutely convergent. Define*

$$S = \{\mathrm{Re}(s) : F(s) \textit{ is absolutely convergent}\}.$$

We then have that

1. *The set S has an infimum, σ_0 say.*

2. *$F(s)$ is absolutely convergent for all s with $\mathrm{Re}(s) > \sigma_0$.*

3. *If $\eta > 0$ then $F(s)$ is uniformly convergent on $\{s : \mathrm{Re}(s) \geq \sigma_0 + \eta\}$.*

4. *$F(s)$ is holomorphic on $\{s : \mathrm{Re}(s) > \sigma_0\}$ with derivatives*

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

5. *The series for $F^{(k)}(s)$ is absolutely convergent for $\mathrm{Re}(s) > \sigma_0$.*

Remark. The number σ_0 is known as the "abscissa of absolute convergence" for the series $\sum f(n)n^{-s}$, which we will abbreviate as AAC.

Before we embark on proving the above theorem we recall a basic result from complex analysis.

Lemma 3.2. *Let U be an open subset of $\mathbb{C}$ and let $F_1(z), \ldots, F_n(z), \ldots$ be holomorphic on U. Suppose $\sum_n F_n(z)$ is uniformly convergent on U to $F(z)$. Then $F(z)$ is holomorphic on U, with $F^{(k)}(z) = \sum_n F_n^{(k)}(z)$.*

Proof

See the complex analysis course. □

Proof (Of Theorem 3.1)

1) Suppose that $\mathrm{Re}(s) < \mathrm{Re}(s_2)$. Then

$$\sum \left|f(n)n^{-s}\right| \geq \sum \left|f(n)n^{-s_2}\right| = \infty.$$

Thus $\mathrm{Re}(s) \notin S$, whence S is bounded below by $\mathrm{Re}(s_2)$. Moreover S is non-empty, since $\mathrm{Re}(s_1) \in S$. Thus S is non-empty and bounded below, and hence has an infimum.

2) If $\mathrm{Re}(s) > \sigma_0$ then by the definition of an infimum, there exists an s_3 such that $\mathrm{Re}(s_3) \leq \mathrm{Re}(s)$ and $\sum |f(n)n^{-s_3}| < \infty$. It follows that $\sum |f(n)n^{-s}| < \infty$ by the comparison test, since $|f(n)n^{-s}| \leq |f(n)n^{-s_3}|$ for $\mathrm{Re}(s) \geq \mathrm{Re}(s_3)$.

3) Recall the Weierstrass M-test. This states that if one has sequences of functions $f_n(z)$ and of real numbers M_n, such that $|f_n(z)| \leq M_n$ for all z in some region D, then $\sum_1^\infty f_n(z)$ converges uniformly on D providing that $\sum_1^\infty M_n$ converges.

We apply this to the functions $f_n(s) = f(n)n^{-s}$ and the region $\{s : \mathrm{Re}(s) \geq \sigma_0 + \eta\}$. We take $M_n = |f(n)|n^{-\sigma_0-\eta}$, so that we do indeed have the required condition $|f(n)n^{-s}| \leq M_n$. We know from part 2 that $\sum M_n$ converges, since $\sigma_0 + \eta > \sigma_0$. The result of part 3 then follows from the M-test.

4) Suppose that $\mathrm{Re}(s) = \sigma > \sigma_0$. Define $\eta = (\sigma - \sigma_0)/2$ and $U = \{z : \mathrm{Re}(z) > \sigma_0 + \eta\}$. By part 3 of the theorem the sum for $F(z)$ is uniformly convergent on U. Thus, by Lemma 3.2 (below) we deduce that $F(s)$ is holomorphic at s, with

$$\begin{aligned} F^{(k)}(s) &= \sum_{n=1}^{\infty} \left(\frac{d}{ds}\right)^k \left(f(n)n^{-s}\right) \\ &= (-1)^k \sum_{n=1}^{\infty} f(n)(\log n)^k n^{-s}. \end{aligned}$$

5) Let $\sigma_0 < \sigma^* < \mathrm{Re}(s)$. Then $\sum |f(n)n^{-\sigma^*}|$ is absolutely convergent by part 2 of the theorem. Moreover

$$\left|\frac{(\log n)^k n^{-s}}{n^{-\sigma^*}}\right| = (\log n)^k n^{-(\mathrm{Re}(s)-\sigma^*)} \to 0.$$

Hence, by the comparison test, the series for $F^{(k)}(s)$ is absolutely convergent.

Remark. One may also define an "abscissa of conditional convergence" by

$$\sigma_1 = \inf\{\mathrm{Re}(s) : F(s) \text{ is convergent}\}.$$

One always has $\sigma_1 \leq \sigma_0$, but in some cases σ_1 is strictly less than σ_0. However we always have $\sigma_0 - 1 \leq \sigma_1 \leq \sigma_0$. One can show that the series for $F(s)$ is convergent for all s such that $\mathrm{Re}(s) > \sigma_1$ and $F(s)$ is holomorphic for $\mathrm{Re}(s) > \sigma_1$. (See problem sheet 2).

We now relate all this to the Dirichlet convolution.

Theorem 3.3. *Let $f_1(n)$ and $f_2(n)$ be arithmetic functions and define $f_3 = f_1 * f_2$. Assume that the Dirichlet series $F_1(s) = \sum_n f_1(n)n^{-s}$ and $F_2(s) = \sum_n f_2(n)n^{-s}$ have abscissae of absolute convergence equal to σ_1, σ_2 respectively. Then $F_3(s) = \sum_n f_3(n)n^{-s}$ converges absolutely for $\sigma > \max(\sigma_1, \sigma_2)$ and $F_3(s) = F_1(s)F_2(s)$.*

Proof

If $\sigma > \max(\sigma_1, \sigma_2)$ then $\sum f_1(n)n^{-s}$ and $\sum f_2(n)n^{-s}$ are absolutely convergent. We may therefore multiply them together and rearrange the terms at will, and the result will still be absolutely convergent.

It follows that

$$\begin{aligned} F_1(s)F_2(s) &= \sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty} f_1(n_1)f_2(n_2)n_1^{-s}n_2^{-s} \\ &= \sum_{n=1}^{\infty}\left[\sum_{n_1n_2=n} f_1(n_1)f_2(n_2)\right] n^{-s} \\ &= \sum_{n=1}^{\infty}(f_1 * f_2)(n)n^{-s} \\ &= \sum_{n=1}^{\infty} f_3(n)n^{-s}, \end{aligned}$$

as required. □

Theorem 3.4. *Suppose that $f(n)$ is a multiplicative function and suppose that $F(s) = \sum_n f(n)n^{-s}$ has AAC equal to σ_0. Then*

$$F(s) = \prod_{p\ prime}\left\{\sum_{e=0}^{\infty} f(p^e)p^{-es}\right\}$$

for $\sigma > \sigma_0$, in the sense that the sums $F_p(s) = \sum_{e=0}^{\infty} f(p^e)p^{-es}$ have AAC less than or equal to σ_0, and

$$F(s) = \lim_{x\to\infty}\prod_{p\le x} F_p(s)$$

for $\sigma > \sigma_0$.

Proof

The sum $\sum_{e=0}^{\infty} f(p^e)p^{-es}$ contains a subset of the terms in $\sum_1^{\infty} f(n)n^{-s}$ and so has AAC at most σ_0. Let $p_1, \ldots, p_k$ be the primes less than or equal to x. Then

$$\prod_{p\le x} F_p(s) = \prod_{j\le k}\left\{\sum_{e=0}^{\infty} f(p_j^e)p_j^{-es}\right\}.$$

When $\sigma > \sigma_0$ this is a finite product of absolutely convergent series. It is therefore permissible to multiply out the product and rearrange the terms freely. We therefore produce

$$\sum_{n=1}^{\infty} n^{-s} \left\{ \sum_{n=p_1^{e_1}\cdots p_k^{e_k}} f(p_1^{e_1}\cdots, p_k^{e_k}) \right\}.$$

We shall write $\theta_x(n)$ for the number of different ways that n can be written as a product $p_1^{e_1}\cdots p_k^{e_k}$. The unique factorisation property for $\mathbb{N}$ tells us that $\theta_x(n) = 0$ or 1; and $\theta_x(n) = 1$ for $n \le x$. Moreover, because f is multiplicative, we have $f(n) = f(p_1^{e_1}\cdots p_k^{e_k}) = f(p_1^{e_1})\cdots f(p_k^{e_k})$. It follows that

$$\prod_{p\le x} F_p(s) = \sum_{n=1}^{\infty} n^{-s} f(n)\theta_x(n).$$

We may therefore conclude that

$$\begin{aligned}
\left| F(s) - \prod_{p\le x} F_p(s) \right| &= \left| \sum_{n=1}^{\infty} n^{-s} f(n)(1-\theta_x(n)) \right| \\
&\le \sum_{n=1}^{\infty} n^{-\sigma} \left| f(n) \right| (1-\theta_x(n)) \quad (\text{ since } \left| n^{-s} \right| = n^{-\sigma}) \\
&\le \sum_{n>x} n^{-\sigma} \left| f(n) \right|.
\end{aligned}$$

However, since $\sum_1^\infty n^{-\sigma} \left| f(n) \right|$ converges we know that

$$\lim_{x\to\infty} \sum_{n>x} n^{-\sigma} \left| f(n) \right| = 0.$$

It follows that

$$\lim_{x\to\infty} \left| F(s) - \prod_{p\le x} F_p(s) \right| = 0$$

as required. □

Definition. An arithmetic function f_n is said to be *totally multiplicative* if $f(mn) = f(m)f(n)$ for all m and n in $\mathbb{N}$.

Corollary 3.5. *If $f(n)$ is totally multiplicative then, under the conditions of Theorem* 3.4 *we have*

$$F(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{f(p)}{p^s}}$$

for $\sigma > \sigma_0$.

Proof

$$\begin{aligned} F_p(s) &= \sum_{e=0}^{\infty} f(p^e) p^{-es} = \sum_{e=0}^{\infty} f(p)^e p^{-es} \\ &= \frac{1}{1 - f(p)p^{-s}}. \end{aligned}$$

□

Definition. The Riemann Zeta-function is given by the series

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

which has AAC= 1.

According to the above corollary we then have

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}.$$

This important relation is known as the Euler product.

Remark. The Euler product identity for $\zeta(s)$ is the key to the importance of the zeta-function. It is, in effect, an analytic statement of the Fundamental Theorem of Arithmetic. It relates the additive structure of the integers, through the infinite sum, to the multiplicative structure, given by the product. The fact that the primes appear in the product, but not in the sum, allows us to use the zeta-function to extract information about the primes.

In order to motivate the next stage of the argument we will argue informally for a moment. If we could take logarithms we would obtain $\log \zeta(s) = \sum_p - \log(1 - p^{-s})$. Differentiating this gives

$$\begin{aligned}\frac{d}{ds}\log\zeta(s) &= \zeta'(s)/\zeta(s) = -\sum_p \frac{d}{ds}\log(1-p^{-s})\\ &= -\sum_p \frac{p^{-s}\log p}{1-p^{-s}}\\ &= -\sum_p \sum_{e=1}^{\infty} p^{-es}\log p.\end{aligned}$$

Of course, taking the logarithm of $\zeta(s)$ is dangerous, partly because $\zeta(s)$ is complex valued, but mainly because we do not know that $\zeta(s)$ is non-zero.

It is convenient to write the final sum above as a Dirichlet series of the form

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

We therefore make the following definition

Definition. Define the von Mangold function by setting

$$\Lambda(n) = \begin{cases}\log p & \text{if } n = p^e \text{ for some prime } p \text{ and integer } e \geq 1,\\ 0 & \text{otherwise.}\end{cases}$$

Note that Λ is not a multiplicative function.

Lemma 3.6. *We have* $(\Lambda * u)(n) = \log n$ *for all* $n \in \mathbb{N}$.

Proof

$$(\Lambda * u)(n) = \sum_{ab=n}\Lambda(a) = \sum_{a|n}\Lambda(a) = \sum_{p^e|n,\, e\geq 1}\log p.$$

If $n = p_1^{e_1}\cdots p_k^{e_k}$, we get terms for

$$p^e = p_1, p_1^2, \ldots, p_1^{e_1}, p_2, p_2^2, \ldots, p_2^{e_2}, p_3, p_3^2, \ldots.$$

There are e_1 such terms corresponding to powers of p_1, each of which contributes $\log p_1$, and then e_2 terms corresponding to powers of p_2, each contributing $\log p_2$, and so on. It follows that $(\Lambda * u)(n) = e_1\log p_1 + e_2\log p_2 + \ldots = \log n$. $\square$

Theorem 3.7. *Let* $F(s) = \sum_1^\infty \Lambda(n) n^{-s}$. *Then* F *is absolutely convergent for* $\mathrm{Re}(s) = \sigma > 1$ *and* $F(s)\zeta(s) = -\zeta'(s)$.

Proof

We have

$$\sum_1^\infty \left|\Lambda(n) n^{-s}\right| \leq \sum_1^\infty (\log n) n^{-\sigma} = -\zeta'(\sigma)$$

which is absolutely convergent for $\sigma > 1$ by Theorem 3.1 part 5. By Theorem 3.3 and the above lemma we have

$$F(s)\zeta(s) = \sum_{n=1}^\infty (\Lambda * u)(n) n^{-s} = \sum_{n=1}^\infty \log n \, n^{-s} = -\zeta'(s).$$

$\square$

4 Analytic Properties of the Riemann Zeta-Function

Recall that a complex number s is written as $\sigma + it$ with σ and t real numbers. The arithmetic method developed in the previous sections provides us with the following property of the Zeta function.

Theorem 4.1. *If* $\mathrm{Re}(s) > 1$ *then*

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

In particular we deduce that $\zeta(s) \neq 0$ *for* $\sigma > 1$*, whence*

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

Proof

The series $\sum_1^\infty \mu(n)/n^s$ has AAC at most 1, by comparison with $\sum_1^\infty n^{-\sigma}$. Moreover, $u*\mu = I$. Hence, by Theorem 3.3 we have

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

for $\sigma > 1$. $\square$

To extract useful information about the primes it turns out that we need to use the zeta-function for values of s with $\mathrm{Re}(s) < 1$. However, our definition $\zeta(s) = \sum n^{-s}$ is not helpful for $\mathrm{Re}(s) < 1$. Here we give a different formulation of the Zeta function that extends the domain of definition of $\zeta(s)$. It also allows us to derive asymptotic estimates on the size of this important function.

Theorem 4.2. *For* $s \in \mathbb{C}$ *and* $n \in \mathbb{N}$ *define the functions*

$$f_n(s) = \int_n^{n+1} \frac{x - n}{x^{s+1}} dx$$

and let

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

Then, for every $n \in \mathbb{N}$ *we have* *a) each $f_n(s)$ is holomorphic on $\mathbb{C}$;*

b) for any $\eta > 0$, $\sum_{n=1}^{\infty} f_n(s)$ is uniformly convergent on $\{s \in \mathbb{C} : \mathrm{Re}(s) > \eta\}$;

c) the function $\zeta^*(s)$ is meromorphic on the region $\mathrm{Re}(s) > 0$, with the only singularity being a simple pole at $s = 1$, with residue 1;

d) for all s with $\mathrm{Re}(s) > 1$ we have $\zeta^*(s) = \zeta(s)$.

Remark. This theorem defines a function $\zeta^*(s)$ on a region $\sigma > 0$, which is strictly larger than the domain of the original function $\zeta(s)$. Moreover the two functions agree wherever they are both defined. We therefore discard our old definition of $\zeta(s)$ and use instead the new one, for $\zeta^*(s)$. This process, in which we extend the domain of definition for a function, is called "analytic continuation".

Proof

a) We want to show that $f_n(s)$ is holomorphic. For this, we can differentiate under the integral sign

$$f_n'(s) = \int_n^{n+1} (-\log x)\frac{x-n}{x^{s+1}}dx$$

using standard results on integration theory. The conditions for this are readily checked, since $(-\log x)\frac{x-n}{x^{s+1}}$ is continuous in x and s, and $[n+1, n]$ is finite.

b) Next we show that $\sum_1^{\infty} f_n(s)$ converges uniformly for $\mathrm{Re}(s) > \eta$. For this we use the Weierstrass M-test. When $\mathrm{Re}(s) > \eta$ we have

$$|f_n(s)| \leq \int_n^{n+1} \frac{dx}{|x^{s+1}|} = \int_n^{n+1} \frac{dx}{x^{\sigma+1}} \leq \int_n^{n+1} \frac{dx}{n^{\sigma+1}} = \frac{1}{n^{\sigma+1}} \leq \frac{1}{n^{\eta+1}}.$$

We therefore set $M_n = n^{-\eta-1}$, so that $|f_n(s)| \leq M_n$ for all s in the region $\mathrm{Re}(s) > \eta$. Since $\sum_1^{\infty} M_n = \sum n^{-1-\eta} < \infty$ we may now apply the M-test and deduce that $\sum_1^{\infty} f_n(s)$ is uniformly convergent.

c) Let $F(s) = \sum_n f_n(s)$. Since this is a uniformly convergent sum of holomorphic functions (for $\mathrm{Re}(s) > \eta$) we deduce from Lemma 3.2 that $F(s)$ is holomorphic on $\{s : \mathrm{Re}(s) > \eta\}$. However $\eta > 0$ is arbitrary, so $F(s)$ must be holomorphic on $\{s : \mathrm{Re}(s) > 0\}$. It follows that $\zeta^*(s)$ is meromorphic for $s > 0$, with the only singularity a simple pole at $s = 1$.

Recall that the residue of a meromorphic function at some point s_0 is equal to the coefficient of the term $1/(s-s_0)$ in the Laurent series of the function about s_0. In particular, since $sF(s)$ is bounded at $s=1$, its Laurent series has no term of the form $1/(s-1)$. The only contribution comes from $s/(s-1) = 1 + 1/(s-1)$, so the residue is equal to 1.

d) Finally we show that $\zeta^*(s) = \zeta(s)$ for $\mathrm{Re}(s) > 1$. We begin by calculating that

$$\begin{aligned} f_n(s) &= \int_n^{n+1} \frac{x}{x^{s+1}} dx - \int_n^{n+1} \frac{n}{x^{s+1}} dx \\ &= \frac{1}{s-1}\left\{n^{-(s-1)} - (n+1)^{-(s-1)}\right\} - \frac{n}{s}\left\{n^{-s} - (n+1)^{-s}\right\}, \end{aligned}$$

whence

$$\begin{aligned} \sum_{n=1}^{N} f_n(s) = &\ \tfrac{1}{s-1} \textstyle\sum_{n=1}^{N} \left\{n^{-(s-1)} - (n+1)^{-(s-1)}\right\} \\ &-\tfrac{1}{s} \textstyle\sum_{n=1}^{N} \left\{n^{-(s-1)} - n(n+1)^{-s}\right\}. \end{aligned}$$

The first sum cancels as

$$\begin{aligned} \left\{1^{-(s-1)} - 2^{-(s-1)}\right\} + \left\{2^{-(s-1)} - 3^{-(s-1)}\right\} + \cdots + \left\{N^{-(s-1)} - (N+1)^{-(s-1)}\right\} \\ = 1^{-(s-1)} - (N+1)^{-(s-1)}. \end{aligned}$$

Similarly the second sum is

$$\begin{aligned} \left\{1 \cdot 1^{-s} - 1 \cdot 2^{-s}\right\} + \quad \left\{2 \cdot 2^{-s} - 2 \cdot 3^{-s}\right\} + \cdots + \left\{N \cdot N^{-s} - N \cdot (N+1)^{-s}\right\} \\ = 1^{-s} + 2^{-s} + \cdots + N^{-s} - N(N+1)^{-s}. \end{aligned}$$

It follows that

$$\begin{aligned} \sum_{n=1}^{N} f_n(s) &= \frac{1}{s-1}\left\{1 - (N+1)^{-(s-1)}\right\} \\ &\quad -\frac{1}{s}\left\{1^{-s} + 2^{-s} + \cdots + N^{-s} - N(N+1)^{-s}\right\}. \end{aligned}$$

We therefore deduce that

$$\begin{aligned} \frac{s}{s-1} - s\sum_{1}^{N} f_n(s) &= \frac{s}{s-1}(N+1)^{-(s-1)} \\ &\quad + \left\{1^{-s} + 2^{-s} + \cdots + N^{-s}\right\} - N(N+1)^{-s}. \end{aligned}$$

Up to this point, any $s \neq 1$ or 0 would be admissible, but we now assume that $\mathrm{Re}(s) > 1$. Then as $N \to \infty$ we have $\frac{s}{s-1}(N+1)^{-(s-1)} \to 0$. Similarly $1^{-s} + \cdots + N^{-s} \to \sum_1^\infty n^{-s} = \zeta(s)$ and also $-N(N+1)^{-s} \to 0$. It then follows that

$$\zeta^*(s) = \lim_{N\to\infty} \frac{s}{s-1} - s\sum_1^N f_n(s) = \zeta(s),$$

as required. $\square$

By adapting this proof we can get information on the size of $\zeta(s)$ when $\mathrm{Re}(s) > 0$. For our purposes it turns out to be sufficient to look at the range $\mathrm{Re}(s) \geq 1$. Notice in particular that this includes the case $\mathrm{Re}(s) = 1$ where previously we did not even know that $\zeta(s)$ was defined.

Note that for s with $\mathrm{Re}(s) \geq 2$, $|\zeta(s)| \leq |\zeta(2)| < \infty$. Near the line $\mathrm{Re}(s) = 1$ we have the following estimate.

Theorem 4.3. *If* $1 \leq \mathrm{Re}(s) \leq 2$ *and* $|t| \geq 2$ *then* $\zeta(s) = O(\log|t|)$, *and* $\zeta'(s) = O(\log^2|t|)$.

Remark. Using only the fact that $\zeta(s) = \sum_1^\infty n^{-s}$, we see that

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

This provides a bound for $\zeta(s)$, but as $\sigma \downarrow 1$ the bound tends to infinity, whereas the theorem gives a uniform bound throughout the range $1 \leq \sigma \leq 2$. Of course we have to exclude values of s too close to $s = 1$, since $\zeta(s)$ is unbounded near $s = 1$. By requiring that $|t| \geq 2$ we ensure that $\log|t|$ is bounded away from zero. Thus the terms involving $\log|t|$ in the $O(\ldots)$ notation are always at least a positive constant.

Proof

The argument used for the previous theorem shows that

$$\begin{aligned}\frac{s}{s-1} - s\sum_1^N f_n(s) &= \frac{s}{s-1}(N+1)^{-(s-1)} \\ &\quad + \left\{1^{-s} + 2^{-s} + \ldots + N^{-s}\right\} - N(N+1)^{-s},\end{aligned}$$

whence, setting $M = N + 1$ we have

$$\begin{aligned}
\frac{s}{s-1} - s\sum_{1}^{M-1} f_n(s) &= \frac{s}{s-1}M^{-(s-1)} + \sum_{1}^{M-1} n^{-s} - (M-1)M^{-s}, \\
&= M^{1-s}\{1 + \frac{1}{s-1}\} + \{\sum_{1}^{M} n^{-s} - M^{-s}\} - \{M^{1-s} - M^{-s}\} \\
&= \frac{M^{s-1}}{s-1} + \sum_{n=1}^{M} n^{-s}.
\end{aligned}$$

It then follows that

$$\begin{aligned}
\zeta^*(s) &= \frac{s}{s-1} - s\sum_{n=1}^{\infty} f_n(s) \\
&= \frac{M^{1-s}}{s-1} + \sum_{1}^{M} n^{-s} - s\sum_{M}^{\infty} f_n(s).
\end{aligned}$$

We can use this formula with any positive integer value of M, and we shall choose $M = [|t|]$. This produces

$$|\zeta^*(\sigma + it)| \leq \frac{1}{|s-1|} + \sum_{n \leq [|t|]} n^{-\sigma} + |s| \sum_{n \geq [|t|]} \frac{1}{n^{\sigma+1}},$$

since $|M^{1-s}| \leq 1$ for $\sigma \geq 1$, and $|f_n(s)| \leq n^{-\sigma-1}$.

The second term is $\leq \sum_{1}^{M} n^{-1} = O(\log |t|)$, whereas the third is at most

$$\begin{aligned}
(2 + |t|)\sum_{M}^{\infty} \frac{1}{n^{\sigma+1}} &\leq (2 + |t|)\sum_{M}^{\infty} \frac{1}{n^2} \\
&= O(|t| \int_{|t|}^{\infty} \frac{dx}{x^2}) = O(1).
\end{aligned}$$

Overall this gives us

$$\begin{aligned}
|\zeta^*(\sigma + it)| &= O(1) + O(\log |t|) + O(1) \\
&= O(\log |t|).
\end{aligned}$$

To handle $\zeta'(s)$ we differentiate our previous representation for $\zeta^*(s)$ termwise. This is permissible by Lemma 3.2 since the resulting infinite sum is uniformly convergent. We then find that

$$
\begin{aligned}
|\zeta'(s)| &= \Big|\frac{d}{ds}\frac{M^{1-s}}{s-1}\Big| - \Big|\sum_{1}^{M} n^{-s}\log n\Big| - \Big|\sum_{M}^{\infty} f_n(s)\Big| - |s|\Big|\sum_{M}^{\infty} f_n'(s)\Big| \\
&= O\left(\log M\right) + O\left(\sum_{1}^{M}\frac{\log n}{n}\right) + O\left(\sum_{M}^{\infty}\frac{1}{n^2}\right) + O\left(|t|\sum_{M}^{\infty}\left|f_n'(s)\right|\right).
\end{aligned}
$$

Here

$$
\begin{aligned}
|f_n'(s)| &= \Big|\frac{d}{ds}\left\{\int_{n}^{n+1}\frac{x-n}{x^{s+1}}dx\right\}\Big| \\
&= \Big|-\int_{n}^{n+1}\frac{x-n}{x^{s+1}}\log x dx\Big| \\
&= O\left(\int_{n}^{n+1}\frac{\log x}{x^2}dx\right)
\end{aligned}
$$

since $\frac{1}{|x^{s+1}|} = \frac{1}{x^{\sigma+1}} \leq \frac{1}{x^2}$. It follows that

$$
\begin{aligned}
\sum_{M}^{\infty}\left|f_n'(s)\right| &= O\left(\sum_{M}^{\infty}\int_{n}^{n+1}\frac{\log x}{x^2}dx\right) \\
&= O\left(\int_{M}^{\infty}\frac{\log x}{x^2}dx\right) \\
&= O\left(\frac{\log M}{M}\right) \\
&= O\left(\frac{\log|t|}{|t|}\right).
\end{aligned}
$$

In the second equality of the above equation we have used the integration by parts formula $\int fg' = fg - \int gf'$ with $f(x) = \log(x)$ and $g(x) = 1/x$.

We also have

$$
\begin{aligned}
\sum_{1}^{M}\frac{\log n}{n} &= O\left(\int_{1}^{|t|}\frac{\log x}{x}dx\right) \\
&= O\left(\left[\frac{1}{2}\log^2 x\right]_1^M\right) \\
&= O\left(\log^2 M\right) \\
&= O\left(\log^2|t|\right).
\end{aligned}
$$

In the second equality of the above equation we have used the integration by parts formula $\int fg' = fg - \int gf'$ with $f(x) = \log(x)$ and $g(x) = \log x$.

We can therefore conclude that

$$\begin{aligned} |\zeta'(s)| &= O\left(\log M\right) + O\left(\log^s |t|\right) + O\left(\frac{1}{|t|}\right) + O\left(|t|\frac{\log|t|}{|t|}\right) \\ &= O\left(\log^2 |t|\right). \end{aligned}$$

□

Since we want to use the formula $-\zeta'(s)/\zeta(s) = \sum \Lambda(n)n^{-s}$, we will need to know at which points s the function $\zeta'(s)/\zeta(s)$ is regular. We have therefore to say something about possible zeros of $\zeta(s)$. This is in general a very difficult issue, but we begin with a rather simple result.

Theorem 4.4. *Let $s_0 = 1 + it$. Then s_0 cannot be a multiple zero of $\zeta(s)$.*

Proof

We argue by contradiction. Consider the Taylor series around s_0, which takes the form

$$\zeta(s) = a_0 + a_1(s - s_0) + a_2(s - s_0)^2 + \dots$$

Since $\zeta(s)$ is supposed to have a multiple zero at s_0 we must have $a_0 = a_1 = 0$. Then if $s = s_0 + \delta = 1 + it + \delta$ with $0 < \delta < 1$ we see that $\zeta(s) = O(\delta^2)$ (where the implied constant is allowed to depend on s_0). Thus

$$\frac{\zeta(1 + it + \delta)}{\delta^2}$$

is bounded as δ tends down to 0. However

$$\begin{aligned} \left|\frac{1}{\zeta(s)}\right| &= \left|\sum_1^M \mu(n)n^{-s}\right| \leq \sum_1^\infty n^{-\mathrm{Re}(s)} \\ &= \sum_1^\infty n^{-1-\delta} = \zeta(1+\delta). \end{aligned}$$

We now use the fact that $\zeta(s)$ has a simple pole at $s = 1$, whence $\zeta(1 + \delta) = O(\delta^{-1})$ as δ tends down to 1. It follows that $1/\zeta(s) = O(\delta^{-1})$, whence

$$1 = \zeta(s)\frac{1}{\zeta(s)} = O(\delta^2)O(\delta^{-1}) = O(\delta)$$

for $s = 1 + it + \delta$ with $\delta \downarrow 0$. This gives us a contradiction if δ is small enough. $\square$

The key facts used in this proof were that $\zeta(s)$ has a first order pole at $s = 1$, and that

$$\left|\frac{1}{\zeta(\sigma + it)}\right| = \left|\sum \mu(n) n^{-\sigma - it}\right| \le \zeta(\sigma).$$

This latter inequality can be reformulated by saying that

$$\zeta(\sigma)\,|\zeta(\sigma + it)| \ge 1$$

for all $\sigma > 1$. By giving a slightly more complicated inequality of this type we can get a better result.

Theorem 4.5. *The function $\zeta(s)$ has no zeros on $\mathrm{Re}(s) = 1$. Indeed we have $\frac{1}{\zeta(s)} = O(\log^7 |t|)$ for $1 \le \mathrm{Re}(s) \le 2$ and $|t| \ge 2$.*

Remark. The exponent 7 on $\log |t|$ is fairly unimportant, and other arguments allow one to remove it entirely, so that $\zeta(s)^{-1} = O(\log |t|)$ for $1 \le \mathrm{Re}(s) \le 2$ and $|t| \ge 2$. For our purposes it will be enough to know that *some* positive constant exponent is admissible.

The inequality we shall use for the proof is:-

Lemma 4.6. *If $\sigma > 1$ then for all $t \neq 0$ we have*

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

Proof

We use the Euler product and take logarithms to give

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

for some branch of the logarithms. It will not matter which branch or branches one uses, since we will take real parts later. The power series for $\log(1 - z) = -\sum_{n=1}^{\infty} z^n/n$ shows that

$$\log \zeta(s) = \sum_p \sum_m \frac{1}{m} \frac{1}{p^{ms}}$$

which is absolutely convergent for $\sigma > 1$. Taking real parts we get

$$\log|\zeta(s)| = \mathrm{Re}(\log\zeta(s)) = \sum_p \sum_m \frac{1}{m}\mathrm{Re}(p^{-ms}),$$

whence

$$\begin{aligned}
& \log\left\{\zeta^3(\sigma)\,|\zeta(\sigma+it)|^4\,|\zeta(\sigma+2it)|\right\} \\
= & \sum_p \sum_m \frac{1}{m}\left\{3\,\mathrm{Re}(p^{-m\sigma}) + 4\,\mathrm{Re}(p^{-m(\sigma+it)}) + \mathrm{Re}(p^{-m(\sigma+2it)})\right\} \\
= & \sum_p \sum_m \frac{p^{-m\sigma}}{m}\left\{3 + 4\,\mathrm{Re}(p^{-mit}) + \mathrm{Re}(p^{-2mit})\right\} \\
= & \sum_p \sum_m \frac{p^{-m\sigma}}{m}(3 + 4\cos(\theta) + \cos(2\theta)),
\end{aligned}$$

with $\theta = mt\log p$. However for any real θ we have

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

Thus the above infinite sum is positive, which implies that

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

as required. □

We are now ready to prove Theorem 4.5.

Proof

We shall first show that there are no zeros for $\mathrm{Re}(s) = 1$. Suppose that $\zeta(1+it) = 0$ for some $t \neq 0$. Then, using the Taylor series expansion we have

$$\begin{aligned}
\zeta(\sigma+it) &= \zeta(1+it) + (\sigma-1)\zeta'(1+it) + \frac{(\sigma-1)^2}{2}\zeta''(1+it) + \ldots \\
&= 0 + (\sigma-1)\zeta'(1+it) + \ldots \\
&= O(\sigma-1)
\end{aligned}$$

as $\sigma \downarrow 1$. Here we allow the implied constant to depend on t, but not of course on σ. We also know that $\zeta(\sigma) = 1/(\sigma-1) + O(1) \sim 1/(\sigma-1)$ by using the Laurent series around $s = 1$. Thus

$\zeta(\sigma) = O((\sigma-1)^{-1})$. Finally we note that $\zeta(\sigma+2it) \to \zeta(1+2it)$, so that $\zeta(\sigma+2it) = O(1)$ as $\sigma \to 1$. Here again we allow the implied constant to depend on t. Putting these inequalities together we find that if $\zeta(1+it) = 0$ then

$$\begin{aligned} 1 &\leq \zeta^3(\sigma)\,|\zeta(\sigma+it)|^4\,|\zeta(\sigma+2it)| \\ &= O\left(\left(\frac{1}{\sigma-1}\right)^3 \times (\sigma-1)^4 \times 1\right) \\ &= O(\sigma-1) \to 0. \end{aligned}$$

This gives us a contradiction if $\sigma - 1$ is small enough, so that we cannot have $\zeta(1+it) = 0$. We now give a more careful argument, in which the dependence on the size of $|t|$ is made explicit. As before we have $\zeta(\sigma) = O((\sigma-1)^{-1})$, and by Theorem 4.3 we know that

$$\zeta(\sigma+2it) \quad = \quad O(\log|t|).$$

It follows from Lemma 4.6 that

$$\frac{1}{|\zeta(\sigma+it)|} \leq \zeta(\sigma)^{\frac{3}{4}}\,|\zeta(\sigma+2it)|^{\frac{1}{4}} = O\left((\sigma-1)^{-\frac{3}{4}}(\log|t|)^{\frac{1}{4}}\right).$$

We now choose a parameter $\sigma_0 \in (1,2]$, which we shall specify later. From our estimate above we see that

$$\frac{1}{|\zeta(\sigma+it)|} = O\left(\frac{1}{(\sigma_0-1)^{\frac{3}{4}}}(\log|t|)^{\frac{1}{4}}\right)$$

for $\sigma_0 \leq \sigma \leq 2$. We write this in the form

$$\frac{1}{|\zeta(\sigma+it)|} \leq B(\sigma_0-1)^{-\frac{3}{4}}(\log|t|)^{\frac{1}{4}}$$

with an appropriate real constant B. Thus we have

$$|\zeta(\sigma+it)| \geq B^{-1}(\sigma_0-1)^{\frac{3}{4}}(\log|t|)^{-\frac{1}{4}}, \tag{*}$$

for $\sigma_0 \leq \sigma \leq 2$. This gives us a suitable lower bound when σ is not too close to 1, but unfortunately the lower bound vanishes as $\sigma_0 \downarrow 1$.

To cover the remaining range $1 \le \sigma \le \sigma_0$ we use a further idea. By Theorem 4.3 we have

$$\begin{aligned}\zeta(\sigma_0+it)-\zeta(\sigma+it) &= \int_{\sigma+it}^{\sigma_0+it} \zeta'(s)ds \\ &= O\left((\sigma_0-\sigma)\log^2|t|\right) \\ &= O\left((\sigma_0-1)\log^2|t|\right).\end{aligned}$$

If we write A for the numerical constant implied by the $O(\ldots)$ notation we deduce that

$$|\zeta(\sigma_0+it)-\zeta(\sigma+it)| \le A(\sigma_0-1)\log^2|t|$$

for $1 \le \sigma \le \sigma_0$. If we now use (*) with $\sigma=\sigma_0$ we have

$$\begin{aligned}|\zeta(\sigma+it)| &\ge |\zeta(\sigma_0+it)| - A(\sigma_0-1)\log^2|t| \\ &\ge B^{-1}(\sigma_0-1)^{\frac{3}{4}}(\log|t|)^{-\frac{1}{4}} - A(\sigma_0-1)\log^2|t|.\end{aligned}$$

We are now ready to choose σ_0. We select a value designed to make the first term above twice the second term. Thus we take $\sigma_0-1=(2AB)^{-4}(\log|t|)^{-9}$. Remember that we required σ_0 to lie in the range $1<\sigma_0\le 2$. If necessary one can increase the value of A obtained from Theorem 4.3 to ensure that σ_0-1 is sufficiently small.

With the above choice of σ_0 we now get

$$|\zeta(\sigma+it)| \ge \frac{1}{8A^3B^4}(\log|t|)^{-7} - \frac{1}{16A^3B^4}(\log|t|)^{-7} = \frac{1}{16A^3B^4}(\log|t|)^{-7}.$$

It follows that

$$|\zeta(\sigma+it)| \ge \frac{1}{16A^3B^4}(\log|t|)^{-7}$$

for $1 \le \sigma \le \sigma_0$. Moreover in the remaining range $\sigma_0 \le \sigma \le 2$ we have

$$|\zeta(\sigma+it)| \ge \frac{1}{8A^3B^4}(\log|t|)^{-7}$$

by (*). Thus in either case we have

$$\frac{1}{\zeta(\sigma+it)} = O(\log^7|t|),$$

as required. $\square$

5 The Proof of the Prime Number Theorem

In the proof of the Prime Number Theorem it is natural to use $-\zeta'(s)/\zeta(s) = \sum \Lambda(n)n^{-s}$, for $\mathrm{Re}(s) > 1$. However this forces us to deal with $\Lambda(n)$, which counts not only primes but also prime powers. Moreover, even at primes it counts numbers with "weight" $\log p$, rather than 1. It therefore turns out that it is better to investigate the following function, in place of $\pi(x)$.

Definition. $\psi(x) := \sum_{n\le x} \Lambda(n)$.

Fortunately it is easy to "translate" between $\pi(x)$ and $\psi(x)$.

Theorem 5.1. *We have* $\frac{\psi(x)}{x} \to 1$ *if and only if* $\frac{\pi(x)}{x/\log x} \to 1$.

Proof
Since $p^e \le x$ if and only if $e \le \log x/\log p$, we have

$$\begin{aligned} \psi(x) &= \sum_{n\le x} \Lambda(n) = \sum_{p^e\le x} \log p = \sum_{p\le x} \log p \sum_e 1 \\ &= \sum_{p\le x} \log p \left[\frac{\log x}{\log p}\right] \le \sum_{p\le x} (\log p)\left(\frac{\log x}{\log p}\right) \\ &= \pi(x)\log x. \end{aligned}$$

On the other hand, if $0 < \theta < 1$, then

$$\begin{aligned} \psi(x) &\ge \sum_{p\le x} \log p \ge \sum_{x^\theta<p\le x} \log p \ge \sum_{x^\theta<p\le x} \log x^\theta \\ &= (\theta\log x)(\pi(x) - \pi(x^\theta)) \ge (\theta\log x)(\pi(x) - x^\theta). \end{aligned}$$

The above inequalities give

$$\theta\frac{\pi(x)}{x/\log x} - \theta x^{\theta-1}\log x \le \frac{\psi(x)}{x} \le \frac{\pi(x)}{x/\log x}.$$

We now observe that $\theta x^{\theta-1}\log x \to 0$ as $x \to \infty$ for every $\theta \in (0, 1)$. Thus, if

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

then

$$\theta \le \liminf_{x\to\infty} \frac{\psi(x)}{x}$$

and

$$\limsup_{x\to\infty} \frac{\psi(x)}{x} \le 1.$$

Since $\theta < 1$ was arbitrary we deduce that $1 \le \liminf \le \limsup \le 1$. It follows that the limit exists and $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1$.

Similarly we have

$$\frac{\psi(x)}{x} \le \frac{\pi(x)}{x/\log x} \le \frac{\psi(x)}{\theta x} + x^{\theta-1}\log x.$$

Thus, if $\psi(x)/x \to 1$ then $1 \le \liminf \frac{\pi(x)}{x/\log x}$ and $\limsup \frac{\pi(x)}{x/\log x} \le \theta^{-1}$ for any $\theta \in (0,1)$. It follows that $1 \le \liminf \le \limsup \le 1$. Thus the limit $\lim \frac{\pi(x)}{x/\log x}$ exists and is equal to 1. $\square$

We have seen that $\psi(x) \sim x$ implies the Prime Number Theorem. We now produce another statement equivalent to the Prime Number Theorem.

Definition. Let

$$\psi_1(x) = \int_0^x \psi(t)dt.$$

Lemma 5.2. *If $\psi(t) \sim t$, then*

$$\psi_1(x) \sim \int_0^x tdt = x^2/2$$

Proof

By the hypothesis, for every $\epsilon > 0$ there is $x_0 > 0$ such that for all $t \ge x_0$ we have

$$(1-\epsilon)t \le \psi(t) \le (1+\epsilon)t.$$

Hence, for all $x > x_0$ we have

$$\psi_1(x) = \int_0^{x_0} \psi(t)\,dt + \int_{x_0}^{x} \psi(t)\,dt \le \int_0^{x_0} \psi(t)\,dt + (1+\epsilon)\frac{x^2}{2}$$

This implies that

$$\limsup_{x\to\infty} \frac{\psi_1(x)}{x^2/2} \le 1+\epsilon.$$

Using the lower bound on ψ we can see that

$$\liminf_{x\to\infty} \frac{\psi_1(x)}{x^2/2} \ge 1-\epsilon.$$

Putting these inequalities together we see that

$$1-\epsilon \le \liminf_{x\to\infty} \frac{\psi_1(x)}{x^2/2} \le \limsup_{x\to\infty} \frac{\psi_1(x)}{x^2/2} \le 1+\epsilon$$

Since $\epsilon > 0$ was arbitrary, we conclude that

$$1 \le \liminf_{x\to\infty} \frac{\psi_1(x)}{x^2/2} \le \limsup_{x\to\infty} \frac{\psi_1(x)}{x^2/2} \le 1.$$

Therefore, $\lim_{x\to\infty} \frac{\psi_1(x)}{x^2/2}$ exists and is equal to 1. □

Theorem 5.3. *If $\psi_1(x) \sim \frac{x^2}{2}$ then $\psi(x) \sim x$.*

Proof

Note that $\psi(t)$ is increasing for $t \ge 0$ (since $\Lambda(n) \ge 0$). Let $0 < \alpha < 1 < \beta$ be constants. Then

$$\psi_1(\beta x) - \psi_1(x) = \int_x^{\beta x} \psi(t)dt \ge \int_x^{\beta x} \psi(x)\, dt = (\beta-1)x\psi(x),$$

whence

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

We know that $\psi_1(\beta x) \sim (\beta x)^2/2$ and $\psi_1(x) \sim x^2/2$, and we would like to subtract the second of these from the first. However a little care is needed when subtracting asymptotic relations. We have

$$\psi_1(\beta x) = (\beta x)^2/2 + o((\beta x)^2) = (\beta x)^2/2 + o(x^2),$$

since β is constant. Similarly we have $\psi_1(x) = x^2/2 + o(x^2)$. Thus

$$\psi_1(\beta x) - \psi_1(x) = \left\{\frac{(\beta x)^2}{2} + o(x^2)\right\} - \left\{\frac{x^2}{2} + o(x^2)\right\} = \frac{1}{2}(\beta^2-1)x^2 + o(x^2).$$

It follows that

$$\frac{\psi_1(\beta x) - \psi_1(x)}{(\beta-1)x^2} \to \frac{1}{2}\frac{\beta^2-1}{\beta-1} = \frac{\beta+1}{2}.$$

Thus, $\limsup_{x\to\infty} \frac{\psi(x)}{x} \le \frac{\beta+1}{2}$ for any constant $\beta > 1$, whence

$$\limsup_{x\to\infty} \frac{\psi(x)}{x} \le 1.$$

Similarly,

$$\psi_1(x) - \psi_1(\alpha x) = \int_{\alpha x}^{x} \psi(t)dt \leq \int_{\alpha x}^{x} \psi(x)dx = (1-\alpha)x\psi(x),$$

and if $\psi_1(t) \sim \frac{t^2}{2}$, we have

$$\frac{\psi(x)}{x} \geq \frac{\psi_1(x) - \psi_1(\alpha x)}{(1-\alpha)x^2}.$$

Here, $\psi_1(x) - \psi_1(\alpha x) \sim (1-\alpha^2)\frac{x^2}{2}$ for any constant $\alpha < 1$. So

$$\frac{\psi_1(x) - \psi_1(\alpha x)}{(1-\alpha)} \to \frac{1-\alpha^2}{2(1-\alpha)} = \frac{1+\alpha}{2}.$$

It follows that $\lim_{x\to\infty} \inf \frac{\psi(x)}{x} \geq \frac{1+\alpha}{2}$ for all $\alpha < 1$, and hence

$$\lim_{x\to\infty} \inf \frac{\psi(x)}{x} \geq 1.$$

We therefore have

$$1 \leq \liminf \frac{\psi(x)}{x} \leq \limsup \frac{\psi(x)}{x} \leq 1.$$

It follows that $\psi(x)/x \to 1$ as required. □

This type of argument, going from information about the average of $\psi(x)$, to information about $\psi(x)$, and also using monotonicity, is what is called a "Tauberian argumen".

Our goal is now to prove that $\psi_1(x) \sim \frac{x^2}{2}$. This will lead to $\psi(x) \sim x$, which then yields $\pi(x) \sim x/\log x$.

We begin by connecting $\psi_1(x)$ with $\zeta'(s)/\zeta(s)$.

Theorem 5.4. *For any $c > 1$ and $x > 0$, we have*

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

the integral being along a straight line path.

Remark. The integrand in the above integral is bounded along the path of integration. Specifically, we have

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leq \sum_{1}^{\infty} \Lambda(n)n^{-c} < \infty$$

since $c > 1$, and also $\left|x^{s+1}\right| = x^{c+1}$.

Lemma 5.5. *If $y > 0$ and $c > 0$, then*

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

Proof

Let $R \ge 4$ and define the curves

$$\gamma_1(R) = \{c + ti, -R \le t \le R\},$$

$$\gamma_2(R) = \{s \in \mathbb{C} : |s| = R, \mathrm{Re}(s) \ge c\},$$

$$\gamma_3(R) = \{s \in \mathbb{C} : |s| = R, \mathrm{Re}(s) \le c\}.$$

The unions $\gamma_1 \cup \gamma_2$ and $\gamma_1 \cup \gamma_3$ are closed curves.

For $y \ge 1$ we have

$$\Big|\int_{\gamma_2} \frac{y^s}{s(s+1)}ds\Big| \le \int_{\gamma_2} \Big|\frac{y^s}{s(s+1)}\Big|ds \le \int_{\gamma_2} \Big|\frac{y^c}{R^2}\Big|ds \le 2\pi R\frac{y^c}{R^2} = 2\pi\frac{y^c}{R}$$

For $y \le 1$ we have

$$\Big|\int_{\gamma_3} \frac{y^s}{s(s+1)}ds\Big| \le \int_{\gamma_3} \Big|\frac{y^s}{s(s+1)}\Big|ds \le \int_{\gamma_3} \Big|\frac{y^c}{R^2/2}\Big|ds \le 2\pi R\frac{y^c}{R^2/2} = 4\pi\frac{y^c}{R}.$$

We see that both of the above integrals tends to 0 as R tends to infinity.

Since the integrand is analytic inside the closed curve $\gamma_1 \cup \gamma_2$, then

$$\oint_{\gamma_1\cup\gamma_2} \frac{y^s}{s(s+1)}ds = 0.$$

Taking limit as $R \to \infty$ we obtain the value of the integral when $y \le 1$.

On the other hand, the integrand has two singularities inside the closed curve $\gamma_1 \cup \gamma_3$. By the residue formula,

$$\oint_{\gamma_1\cup\gamma_3} \frac{y^s}{s(s+1)}ds = \frac{1}{2\pi i}\operatorname{Res}_{s=0} \frac{y^s}{s(s+1)} + \operatorname{Res}_{s=-1} \frac{y^s}{s(s+1)} = 1 - \frac{1}{y}.$$

Then, by taking limit as R tends to ∞, we conclude the value of the integral in the lemma for $y \ge 1$. □

When we replace the function $-\zeta'(s)/\zeta(s)$ with the infinite series $\sum_{n=1}^{\infty} \Lambda(n)n^{-s}$ in the expression in Theorem 5.4, we wish to switch the place of integral and sum. To that end we use the following lemma from analysis.

Lemma 5.6. *Suppose that f_j, for $j \in \mathbb{N}$, is a sequence of complex valued functions defined on the same interval $I \subseteq \mathbb{R}$ such that for each j, $\int_I |f_j|$ is finite, and moreover $\sum_{j=1}^{\infty} \int_I |f_j|$ is also finite. Then, $\sum_{j=1}^{\infty} f_j$ converges at almost every point in I to a function f defined on I such that $\int_I |f|$ is finite, and $\int_I \sum_{j=1}^{\infty} f_j = \sum_{j=1}^{\infty} \int_I f_j$.*

For proof one may refer to standard books on functional analysis, for instance, *real analysis* by Gerald B. Foland.

Proof (of theorem 5.4) For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, by Theorem 4.1, we may write the integral on the right as

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(\sum_{1}^{\infty} \frac{\Lambda(n)}{n^s} \right) \frac{x^{s+1}}{s(s+1)} ds.$$

We want to integrate the series termwise. By the previous lemma, it is enough to show that the infinite sum

$$x \sum_{1}^{\infty} \Lambda(n) \int_{-\infty}^{\infty} \left| \frac{(x/n)^{c+it}}{(c+it)(1+c+it)} \right| dt$$

converges. However this is equal to

$$x^{1+c} \sum_{1}^{\infty} \frac{\Lambda(n)}{n^c} \int_{-\infty}^{\infty} \frac{dt}{|(c+it)(1+c+it)|}.$$

The integral

$$\int_{-\infty}^{\infty} \frac{dt}{|(c+it)(1+c+it)|}$$

is independent of n, and converges to a finite value. Moreover $\sum_{1}^{\infty} \frac{\Lambda(n)}{n^c}$ also converges, since $c > 1$. Thus the sum of integrals converges, which suffices to show that the switch of summation and integration above is permissible.

By the above argument, the integral in the theorem produces

$$\begin{aligned} x \sum_{1}^{\infty} \Lambda(n) \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{(x/n)^s}{s(s+1)} ds &= x \sum_{n:\, \frac{x}{n} \geq 1} \Lambda(n) \left(1 - \left(\frac{x}{n} \right)^{-1} \right) \\ &= \sum_{n \leq x} \Lambda(n)(x-n). \end{aligned}$$

On the other hand,

$$\begin{aligned}\psi_1(x) &= \int_0^x \psi(t)dt = \int_0^x \left(\sum_{n\le t}\Lambda(n)\right) dt \\ &= \sum_{n\le x}\Lambda(n)\int_n^x 1\,dt = \sum_{n\le x}\Lambda(n)(x-n).\end{aligned}$$

This finishes the proof of the theorem. □

Finally we can prove the Prime Number Theorem.

Theorem 5.7. *We have $\psi_1(x) \sim \frac{x^2}{2}$, and hence $\pi(x) \sim \frac{x}{\log x}$.*

Proof
It will be convenient to write

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

For $1 \le \mathrm{Re}(s) \le 2$ and $|t| \ge 2$ we have $\zeta'(s) = O(\log^2|t|)$ by Theorem 4.3, and $\frac{1}{\zeta(s)} = O(\log^7|t|)$ by Theorem 4.5. Thus

$$F(s) = O\left(\frac{\log^9|t|}{|t|^2}\right) = O\left(|t|^{-\frac{3}{2}}\right).$$

We apply Theorem 5.4, with the special choice $c = 1 + \frac{1}{\log x}$. This value is chosen so that

$$\left|x^{s+1}\right| = x^{c+1} = x^2 x^{1/\log x} = x^2\exp\left(\frac{\log x}{\log x}\right) = x^2 e.$$

For $T > 0$, we now have a bound

$$\int_{c+iT}^{c+i\infty} F(s)x^{s+1}ds = O\left(\int_T^\infty |t|^{-\frac{3}{2}}x^2dt\right) = O\left(T^{-\frac{1}{2}}x^2\right).$$

Thus, given any positive ϵ, there exists a value T_ϵ such that

$$\left|\frac{1}{2\pi i}\int_{c+iT_\epsilon}^{c+i\infty} F(s)x^{s+1}ds\right| < \epsilon x^2,$$

and similarly

$$\left|\frac{1}{2\pi i}\int_{c-i\infty}^{c-iT_\epsilon} F(s)x^{s+1}ds\right| < \epsilon x^2.$$

Notice particularly that T_ϵ may depend on ϵ, but is certainly independent of x.

We now show that there is a number $\alpha \in (0,1)$ such that $\zeta(s)$ has no zeros in the rectangle given by $\alpha \le \sigma \le 1$ and $|t| \le T_\epsilon$. To prove this we argue by contradiction. Suppose that none of the numbers $\alpha = 1 - \frac{1}{k}$ are admissible. Then for each k, there exists a value ρ_k such $\zeta(\rho_k) = 0$ and for which $1 - \frac{1}{k} \le \mathrm{Re}(\rho) \le 1$ and $|\mathrm{Im}(\rho_k)| \le T_\epsilon$. and $\zeta(\rho_k) = 0$. We therefore have an infinite sequence ρ_k, all in the compact set

$$0 \le \mathrm{Re}(\rho) \le 1, \quad |\mathrm{Im}(\rho)| \le T_\epsilon.$$

By the Bolzano-Weierstrass Theorem, there is convergent subsequence $\rho_{k_j} \to \rho^*$ say. Clearly $\mathrm{Re}(\rho_{k_j}) \to 1$, whence $\mathrm{Re}(\rho^*) = 1$. Now $\zeta(\rho^*) = \lim_{j\to\infty} \zeta(\rho_{k_j}) = 0$, which is a contradiction since $\zeta(1+it) \ne 0$.

This proves our claim. Notice that α may depend on T_ϵ, but is independent of x.

We now move the line of integration from its original straight line path, from $c - i\infty$ to $c + i\infty$, to a union of 5 line segments $L_1, \dots, L_5$, given by

$$\begin{aligned}
L_1 : &\quad c - i\infty \to c - iT_\epsilon, \\
L_2 : &\quad c - iT_\epsilon \to \alpha - iT_\epsilon, \\
L_3 : &\quad \alpha - iT_\epsilon \to \alpha + iT_\epsilon, \\
L_4 : &\quad \alpha + iT_\epsilon \to c + iT_\epsilon, \\
L_5 : &\quad c + iT_\epsilon \to c + i\infty.
\end{aligned}$$

Our choice of α ensures that $\zeta(s)$ has no zeros between the original contour and the new one, so that the only pole of $F(s)x^{s+1}$ is at the point $s = 1$, where $\zeta(s)$ has its pole. (Note that $\zeta(s)$ has no zeros to the right of $\sigma = 1$, by Theorem 4.1.) It follows that

$$\begin{aligned}
\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(s)x^{s+1}ds &= \frac{1}{2\pi i}\left(\int_{L1} + \dots + \int_{L_5}\right) F(s)x^{s+1}ds \\
&\quad + \mathrm{Res}\left(F(s)x^{s+1};\ s = 1\right).
\end{aligned}$$

Since $F(s)$ has a simple pole at $s = 1$ with residue $1/2$, we see that the residue term above is $x^2/2$.

We have already shown that

$$\left|\frac{1}{2\pi i}\int_{L_1}\right|, \left|\frac{1}{2\pi i}\int_{L_5}\right| \le \epsilon x^2$$

for every x, by our choice of T_ϵ. We proceed to consider the integrals along L_2, L_3 and L_4. Since $c = 1 + (\log x)^{-1}$ depends on x it is convenient to define extended line segments

$$\begin{aligned} L_2' : &\quad 2 - iT_\epsilon \to \alpha - iT_\epsilon, \\ L_4' : &\quad \alpha + iT_\epsilon \to 2 + iT_\epsilon, \end{aligned}$$

which do not depend on x. We then set

$$M_\epsilon = \sup_{s \in L_2', L_3, L_4'} |F(s)| \,.$$

Since $F(s)$ is continuous on these line segments (there being no poles), we get a finite number M_ϵ which depends on ϵ, but not on x. We now see that

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{L_2} F(s) x^{s+1} ds \right| &\leq \frac{M_\epsilon}{2\pi} \int_{\alpha_\epsilon}^{c} x^{\sigma+1} d\sigma \\ &= \frac{M_\epsilon}{2\pi} \left[\frac{x^{\sigma+1}}{\log x} \right]_{\alpha_\epsilon}^{c} \\ &\leq \frac{M_\epsilon}{2\pi} \frac{x^{c+1}}{\log x} \\ &= \frac{M_\epsilon}{2\pi} \frac{e x^2}{\log x} \\ &\leq \epsilon x^2 \end{aligned}$$

if x is chosen so large that $\log x \geq (\epsilon 2\pi)^{-1} M_\epsilon e$. We write this latter condition as $x \geq x_\epsilon$, where $x_\epsilon = \exp\{(\epsilon 2\pi)^{-1} M_\epsilon e\}$.

Exactly the same bound ϵx^2 holds for the integral along L_4. Finally

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{L_3} F(s) x^{s+1} ds \right| &\leq \frac{M_\epsilon}{2\pi} \int_{-T_\epsilon}^{T_\epsilon} x^{\alpha+1} dt \\ &= \frac{M_\epsilon}{2\pi} 2 T_\epsilon x^{\alpha+1} \\ &\leq \epsilon x^2 \end{aligned}$$

if x is so large that $x^{1-\alpha} \geq (\epsilon\pi)^{-1} M_\epsilon T_\epsilon$. we may write this final condition in the form $x \geq x_\epsilon'$, where $x_\epsilon' = \{(\epsilon\pi)^{-1} M_\epsilon T_\epsilon\}^{1/(1-\alpha)}$.

We have therefore shown that

$$\psi_1(x) = \frac{1}{2} x^2 + \frac{1}{2\pi i} \left(\int_{L_1} + \ldots + \int_{L_5} \right) F(s) x^{s+1} ds$$

with

$$\left| \frac{1}{2\pi i} \int_{L_j} F(s) x^{s+1} ds \right| \le \epsilon x^2, \quad (j = 1, \ldots, 5)$$

if $x \ge \max(x_\epsilon\,,\, x'_\epsilon)$. Since $\epsilon > 0$ was arbitrary we conclude that $\psi_1(x) \sim \frac{1}{2}x^2$, as required. $\square$

Before moving on, it might be useful to think further about what was involved in the proof of the Prime Number Theorem. The main points are the following.

1. We reduce the problem to proving that $\psi(x) \sim x$, and then to $\psi_1(x) \sim x^2/2$. This is done via a Tauberian argument.

2. One has the formula

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

   which holds for any $c > 1$.

3. As far as x is concerned, the size of the integrand depends on $|x^{s+1}| = x^{\mathrm{Re}(s)+1}$. In order to make this as small as possible we choose c close to 1. The choice $c = 1 + 1/\log x$ gives $|x^{s+1}| = ex^2$.

4. We plan to show that if $\epsilon > 0$ is given, then $|\psi_1(x) - x^2/2| < 5\epsilon x^2$ for large enough x. The parts of the integral in which $|\mathrm{Im}(s)| \ge T_\epsilon$ will be satisfactory, if we choose T_ϵ appropriately. Here we use bounds for $\zeta'(s)$ and $\zeta(s)^{-1}$, and the latter comes from our Theorem 4.5, and is related to the fact that $\zeta(s) \ne 0$ for $\mathrm{Re}(s) = 1$.

5. The remaining integral runs from $c - iT_\epsilon$ to $c + iT_\epsilon$, where T_ϵ depends on ϵ but not x. The central idea is to reduce the size of the factor x^{s+1} in the integrand by moving the path of integration to $\mathrm{Re}(s) = \alpha < 1$. In doing so we pick up a residue at $s = 1$, which provides us with the main term $x^2/2$ in our asymptotic formula for $\psi_1(x)$. However in order to move the line of integration in this way we need to know there are no other singularities of $\zeta'(s)/\zeta(s)$. This entails producing a rectangle containing no zeros of $\zeta(s)$.

6. Since there are no zeros with real part equal to 1, a compactness argument shows that there is an α strictly less than 1, that we can use.

Thus the fundamental point is that we can move the line of integration just a little to the left of $\mathrm{Re}(s) = 1$.

We illustrate all this with another application of these ideas.

Theorem 5.8. *The series* $\sum_1^\infty \frac{\mu(n)}{n}$ *is conditionally convergent, with sum equal to* 0.

Remark. It may be instructive to examine a fallacious proof of the above:- We know that $\sum_1^\infty \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$. Substitute $s = 1$, and use the fact that $\frac{1}{\zeta(s)} = 0$ at $s = 1$.

This does not work since we have only proved that $\sum_1^\infty \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$ for $\mathrm{Re}(s) > 1$.

The fallacious argument is analogous to using the sum

$$\frac{1}{1+x} = \sum_0^\infty (-1)^n x^n$$

and taking $x = 1$ to deduce that $\sum (-1)^n = 1/2$!

We begin the proof of Theorem 5.8 with the following analogue of Lemma 5.5.

Lemma 5.9. *If* $y > 0$ *and* $c > 0$ *then*

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{y^s}{s^2} ds = \begin{cases} \log y & y \geq 1, \\ 0 & y \leq 1. \end{cases}$$

Proof

Define the curves

$$\gamma_1 = \{s \in \mathbb{C} : \mathrm{Re}(s) = c, -R \leq \mathrm{Im}(s) \leq R\},$$
$$\gamma_2 = \{s \in \mathbb{C} : |s| = R, \mathrm{Re}(s) \geq c\},$$
$$\gamma_3 = \{s \in \mathbb{C} : |s| = R, \mathrm{Re}(s) \leq c\}.$$

For $y \geq 1$ we have

$$\Big| \int_{\gamma_3} \frac{y^s}{s^2}\, ds \Big| \leq \int_{\gamma_3} \Big| \frac{y^s}{s^2} \Big|\, |ds| \leq \int_{\gamma_3} \frac{y^c}{R^2}\, |ds| \leq 2\pi R \frac{y^c}{R^2}.$$

Similarly, for $y \leq 1$ we have

$$\Big| \int_{\gamma_2} \frac{y^s}{s^2}\, ds \Big| \leq \int_{\gamma_2} \Big| \frac{y^s}{s^2} \Big|\, |ds| \leq \int_{\gamma_2} \frac{y^c}{R^2}\, |ds| \leq 2\pi R \frac{y^c}{R^2}.$$

Hence, the integrals on γ_2 and γ_3 tend to 0 as R tends to ∞. Since, the function y^s/s^2 has no singularity inside the closed curve $\gamma_1 \cup \gamma_2$, the integral over this closed curve is equal to 0 for all R. This implies the value of the integral for $y \leq 1$.

On the other hand the function $f(s) = y^s$ is defined on the complex plane and has no singularity inside the closed curve $\gamma_1 \cup \gamma_3$. Then by the Cauchy Integral formula for the first derivative, we have

$$\frac{1}{2\pi i} \oint_{\gamma_1 \cup \gamma_2} \frac{y^s}{(s-0)^2} ds = f'(s)\Big|_{s=0} = \log y \cdot y^s\Big|_{s=0} = \log y.$$

This implies the value of the integral for $y \geq 1$, by taking limits as R tends to ∞. $\square$

Theorem 5.10. *For any $c > 0$ and $x > 0$ we have*

$$\sum_{n \leq x} \frac{\mu(n)}{n} \log\left(\frac{x}{n}\right) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{1}{\zeta(s+1)} \frac{x^s}{s^2} ds.$$

Proof

Recall that by Theorem 4.1, for $\mathrm{Re}(s) > 1$ we have $1/\zeta(s) = \sum_{n=1}^{\infty} \mu(n) n^{-s}$. Then,

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{1}{\zeta(s+1)} \frac{x^s}{s^2} ds = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \sum_{n=1}^{\infty} \mu(n) n^{-s-1} \frac{x^s}{s^2} ds$$

At this point we would like to switch the place of integral and infinite sum. By virtue of Lemma 5.6, we need to show that the infinite series

$$\sum_{n=1}^{\infty} \Big| \int_{c-i\infty}^{c+i\infty} \mu(n) n^{-s-1} \frac{x^s}{s^2} ds \Big| \leq \sum_{n=1}^{\infty} \frac{x^c}{n^{c+1}} \int_{c-i\infty}^{c+i\infty} \frac{1}{|s^2|} |ds|$$

is convergent. However, each of the integrals $\int_{c-i\infty}^{c+i\infty} \frac{1}{|s^2|} |ds|$ is finite and is independent of n. So the series is convergent since $\mathrm{Re}(c) > 0$.

Now, using the previous lemma,

$$\begin{aligned} \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \sum_{n=1}^{\infty} \mu(n) n^{-s-1} \frac{x^s}{s^2} ds &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{(x/n)^s}{s^2} ds \\ &= \sum_{n \leq x} \frac{\mu(n)}{n} \log(\frac{x}{n}) \end{aligned}$$

$\square$

Theorem 5.11. *The sum*

$$\sum_{n\le x}\frac{\mu(n)}{n}\log\left(\frac{x}{n}\right)$$

tends to 1 as $x\to\infty$.

Proof (of Theorem 5.11) Apply Theorem 5.10 with $c = 1/\log x$. Note that $|x^s| = x^c = e$ and that

$$\frac{1}{\zeta(s+1)} = O(\log^7|t|) \quad (0\le \mathrm{Re}(s)\le 1,\;\; |t|\ge 2)$$

by Theorem 4.5. It follows that

$$\left|\frac{1}{2\pi i}\int_{c+iT}^{c+i\infty}\frac{1}{\zeta(s+1)}\frac{x^s}{s^2}ds\right| = O\left(\int_T^\infty \frac{\log^7 t}{t^2}\right)$$

$$= O\left(\int_T^\infty \frac{t^{\frac{1}{2}}}{t^2}dt\right) = O\left(T^{-\frac{1}{2}}\right),$$

whence the integral is at most ϵ in modulus, if $T = T_\epsilon$ is large enough.

We next find α_ϵ as before, so that $\zeta(s)$ has no zeros in the rectangle

$$\alpha_\epsilon\le\sigma\le 1, \quad |t|\le T_\epsilon.$$

Define line segments

$$\begin{aligned}
L_1: &\quad c-i\infty\to c-iT_\epsilon,\\
L_2: &\quad c-iT_\epsilon\to \alpha-1-iT_\epsilon,\\
L_3: &\quad \alpha-1-iT_\epsilon\to\alpha-1+iT_\epsilon,\\
L_4: &\quad \alpha-1+iT_\epsilon\to c+iT_\epsilon,\\
L_5: &\quad c+iT_\epsilon\to c+i\infty,
\end{aligned}$$

and

$$\begin{aligned}
L_2': &\quad 1-iT_\epsilon\to\alpha-1-iT_\epsilon,\\
L_4': &\quad \alpha-1+iT_\epsilon\to 1+iT_\epsilon.
\end{aligned}$$

If we now set $F(s) := \frac{1}{s^2\zeta(s+1)}$ we see that $F(s)$ is continuous on L_2', L_3, L_4', so that we can set

$$M_\epsilon = \sup_{s \in L_2', L_3, L_4'} |F(s)|$$

which will depend on ϵ but not x.

We may now replace

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} F(s) x^s ds$$

by

$$\frac{1}{2\pi i} \left(\int_{L_1} + \ldots + \int_{L_5} \right) F(s) x^s ds + \mathrm{Res}(F(s)x^s; s = 0)$$

since $F(s)x^s = \frac{1}{\zeta(s+1)} \frac{x^s}{s^2}$, has a pole at $s = 0$, and no other poles between the contours, (because $\zeta(s+1)$ has no zeros there). We easily calculate that $\mathrm{Res}(F(s)x^s; s = 0) = 1$, using the fact that $\zeta(s)$ has a first order pole at 1 with residue 1.

For the line segment L_2 we have

$$\left| \int_{L_2} F(s) x^s ds \right| \leq M_\epsilon \int_{\alpha - 1}^{c} x^\sigma d\sigma \leq M_\epsilon \frac{x^c}{\log x} = M_\epsilon \frac{e}{\log x}.$$

It follows that this is at most ϵ if $x \geq x(\epsilon)$. We may treat the integral along L_4 similarly.

Finally

$$\left| \frac{1}{2\pi i} \int_{L_3} F(s) x^s ds \right| \leq \frac{M_\epsilon}{2\pi} \int_{-T_\epsilon}^{T_\epsilon} x^{\alpha_\epsilon - 1} dt = \frac{2T_\epsilon M_\epsilon}{2\pi} x^{\alpha_\epsilon - 1}.$$

Since $\alpha_\epsilon - 1 < 0$ the above will be at most ϵ if $x \geq x'(\epsilon)$.

We therefore conclude that

$$\sum_{n \leq x} \frac{\mu(n)}{n} \log \frac{x}{n} = 1 + \frac{1}{2\pi i} \left(\int_{L_1} + \ldots + \int_{L_5} \right) F(s) x^s ds$$

with

$$\left| \frac{1}{2\pi i} \int_{L_j} F(s) x^s ds \right| \leq \epsilon$$

for x large enough. This suffices for the proof. $\square$

Proof (of Theorem 5.8) We shall use a Tauberian argument.

Define $S(y) = \sum_{n \le y} \mu(n)/n$.Then

$$\begin{aligned} \int_0^x S(y) \frac{dy}{y} &= \int_0^x \left(\sum_{n \le y} \frac{\mu(n)}{n} \right) \frac{dy}{y} \\ &= \sum_{n \le x} \frac{\mu(n)}{n} \int_n^x \frac{dy}{y} \\ &= \sum_{n \le x} \frac{\mu(n)}{n} \log\left(\frac{x}{n}\right). \end{aligned}$$

Hence

$$\lim_{x \to \infty} \int_0^x S(y) \frac{dy}{y} = 1.$$

In particular, for any fixed $\delta > 0$ we have

$$\int_x^{x(1+\delta)} S(y) \frac{dy}{y} \to 0 \text{ as } x \to \infty.$$

Suppose then that

$$\left| \int_x^{x(1+\delta)} S(y) \frac{dy}{y} \right| < \epsilon$$

for all $x \ge x(\epsilon)$.

Now the function $S(y)$ varies rather slowly for large values of y. More precisely, for $y \ge x$,

$$\begin{aligned} |S(y) - S(x)| &\le \sum_{x < n \le y} \frac{1}{n} \\ &= \left\{ \log y + \gamma + O\left(\frac{1}{y}\right) \right\} - \left\{ \log x + \gamma + O\left(\frac{1}{x}\right) \right\} \\ &= \log\left(\frac{y}{x}\right) + O\left(\frac{1}{x}\right), \end{aligned}$$

where

$$\gamma = 1 - \int_1^\infty \frac{t - [t]}{t^2}\, dt.$$

See Problem 3 in Problem sheet 2 for more details on the above inequality. When $x \le y \le (1+\delta)x$ we deduce that

$$|S(y) - S(x)| \le \log(1+\delta) + O\left(\frac{1}{x}\right) \le 2\log(1+\delta)$$

if $x \ge x(\delta)$; that is, if x is sufficiently large in terms of δ.

It follows that

$$\begin{aligned}\left|\int_x^{x(1+\delta)} S(x)\frac{dy}{y}\right| &\leq \left|\int_x^{x(1+\delta)} S(y)\frac{dy}{y}\right| + \left|\int_x^{x(1+\delta)} (S(y)-S(x))\frac{dy}{y}\right| \\ &< \epsilon + \int_x^{x(1+\delta)} 2\log(1+\delta)\frac{dy}{y} \\ &< \epsilon + 2\log^2(1+\delta)\end{aligned}$$

if $x \geq \max\{x(\epsilon), x(\delta)\}$.

We now choose $\delta = e^{\sqrt{\epsilon}} - 1 > 0$, so that $\log(1+\delta) = \sqrt{\epsilon}$. We then have

$$\left|S(x)\int_x^{x(1+\delta)} \frac{dy}{y}\right| < \epsilon + 2\epsilon.$$

This yields $|S(x)\log(1+\delta)| < 3\epsilon$ or equivalently $|S(x)\sqrt{\epsilon}| < 3\epsilon$. Thus finally we have $|S(x)| < 3\sqrt{\epsilon}$ for sufficiently large x. It follows that $S(x) \to 0$ as claimed. $\square$

A brief history of the Prime Number Theorem:

The first published statement close to PNT came in 1798 by Legendre. He asserted that $\pi(x)$ is of the form $x/(A\log x + B)$ for constants A and B. This was based on numerical works. He later refined the formula to

$$\pi(x) = \frac{x}{\log x + A(x)},$$

where $A(x)$ is approximately equal to 1.08366. Presumably he meant that

$$\lim_{x\to\infty} \psi(x) = 1.08366.$$

He also asserted that there are infinitely many primes of the form $l + kn$, fro $n = 0, 1, 2, 3, \ldots,$ provided the necessary condition $(l, k) = 1$ holds. Dirichlet gave the first proof of this statement in 1837. His method, a refinement of the proof of the infinitude of primes by Euler, introduces key ideas into number theory, in particular that of analytic methods (real analysis).

There are unpublished works by Gauss around 1792-3 which show that he studied the problem of the distribution of primes as a hobby. He made tables of the primes and their distribution up to primes less than equal to $3,000,000$. There are very few errors in his table!

His numerical observation anticipated the error in the Legendre's formula, and remarked that $\mathrm{Li}(x)$ is a good approximation for $\pi(x)$.

A major progress towards PNT is due to Tchelycheff in 1851. He introduced the real functions

$$\psi(x) = \sum_{p \le x} \log p, \theta(x) = \sum_{p^m \le x} \log p,$$

and proved that PNT is equivalent to the statements $\psi(x) \sim x$ and $\theta(x) \sim x$. Indeed, he proved that if the limits exist they must be equal to 1. Furthermore, he proved that

$$.92129 \le \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} \le 1 \le \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} \le 1.10555.$$

His method were elementary with combiantorial nature. They were not powerful enough to prove the full statement.

The next major step towards PNT came from B. Riemann in 1860. He introduced the function now known as the Riemann-Zeta function, and the Euler product formula. He understood the relations between the zeros of the zeta function, and the growth of $\pi(x)$. He made a number of remarkable conjectures that will lead to refinements of PNT. In particular he came up with the precise relation

$$\psi(x) = x - \sum_{\rho, \zeta(\rho)=0} \frac{x^\rho}{\rho} - \log(2\pi).$$

Here $\zeta(s)$ is a meromorphic function defined on the complex plane with only a single pole at $s = 1$.

Although Riemann could not prove the statements on the zero's of ζ (some of these are still open), his method could still be used to derive PNT. The first proof using this method is due to Hadamard and Poussin in 1896. In 1949, Erdos and Selberg gave the first elementary proof of PNT; it relies on the earlier works such as the one of Tchebycheff.

The proof presented in this lecture notes is close to the one given by J. Newman in 1980. It uses Ikehara's Tauberian argument, and the Cauchy integral formula.

6 Further Properties of $\zeta(s)$

Following the discussion in the previous section, an important question now is what zeros might $\zeta(s)$ have in the critical strip $0 \leq \sigma \leq 1$? This has important repercussions for the behavior of $\pi(x)$. Suppose for example that we knew that $\zeta(s) \neq 0$ for $\sigma \geq \frac{2}{3}$ say. When we proved the Prime Number Theorem we had

$$\psi_1(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) x^{s+1} \frac{ds}{s(s+1)}.$$

If there are no zeros with $\sigma \geq 2/3$ then the only pole of $\zeta'(s)/\zeta(s)$ with $\mathrm{Re}(s) \geq 3/4$ is at $s = 1$. We could then hope to move the line of integration to $\mathrm{Re}(s) = 3/4$ to get

$$\psi_1(x) = \frac{x^2}{2} + \frac{1}{2\pi i} \int_{\frac{3}{4}-i\infty}^{\frac{3}{4}+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) x^{s+1} \frac{ds}{s(s+1)},$$

the term $\frac{x^2}{2}$ coming from the residue at $s = 1$ as before. Now $\left|x^{s+1}\right| = x^{7/4}$ and we might expect that

$$\int_{\frac{3}{4}-i\infty}^{\frac{3}{4}+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) x^{s+1} \frac{ds}{s(s+1)} = O(x^{7/4}).$$

This would lead to an asymptotic formula

$$\psi_1(x) = \frac{x^2}{2} + O(x^{7/4})$$

with a good explicit error term, and hence to a correspondingly good asymptotic formula for $\pi(x)$.

This is necessarily somewhat vague, but the key point is that the behavior of the zeros of $\zeta(s)$ is reflected in the accuracy of the asymptotic formula for $\pi(x)$. So we need to investigate $\zeta(s)$ further.

Definition. Define the Gamma function

$$\Gamma(s) := \int_0^\infty e^{-x} x^{s-1} dx$$

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

This is absolutely and uniformly convergent in any set $\alpha \geq \mathrm{Re}(s) \geq \beta$ with $\alpha > \beta > 0$. It follows as usual that $\Gamma(s)$ is holomorphic for $\mathrm{Re}(s) > 0$.

Theorem 6.1. *For* $\mathrm{Re}(s) > 0$ *we have that* $s\Gamma(s) = \Gamma(s+1)$*. Moreover,* $\Gamma(1) = 1$*, whence* $\Gamma(n) = (n-1)!$ *for* $n \in \mathbb{N}$*.*

Remark. Since $\Gamma(1) = 1$ it is natural to define $0! = 1$.

Proof

Integrate by parts, to give

$$\int_0^X e^{-x} x^{(s+1)-1} dx = \left[-e^{-x} x^s\right]_0^X + s \int_0^X e^{-x} x^{s-1} dx.$$

However $e^{-x} x^s|_{x=0} = 0$ for $\mathrm{Re}(s) > 0$, so that the right hand side is

$$-e^{-X} X^s + s \int_0^X e^{-x} x^{s-1} dx.$$

Taking $X \to \infty$ we deduce that $\Gamma(s+1) = s\Gamma(s)$. $\square$

Corollary 6.2. *The function* $\Gamma(s)$ *has an analytic continuation as a meromorphic function on* $\mathbb{C}$*, the only singularities being at* $s = -k \in \mathbb{Z}_{\leq 0}$*. These singularities are simple poles with residue* $(-1)^k/k!$ *at* k*.*

Proof

For all $n \in \mathbb{N}$, if $\mathrm{Re}(s) > 0$ then

$$\Gamma(s+n) = \{s + (n-1)\} \{s + (n-2)\} \ldots \{s+1\} s\Gamma(s)$$

and so

$$\Gamma(s) = \{s + n - 1\}^{-1} \{s + n - 2\}^{-1} \ldots s^{-1} \int_0^\infty e^{-x} x^{s+n-1} dx$$

However, the right hand side defines a meromorphic function for $\mathrm{Re}(s) > -n$, which is regular apart from possible simple order poles at

$$0, -1, -2, \ldots, -(n-1).$$

If $\Gamma_n(s)$ is the extension we produce, then $\Gamma_n(s) = \Gamma_m(s) = \Gamma(s)$ when $\mathrm{Re}(s) > 0$. Hence, by the identity theorem, $\Gamma_n(s) = \Gamma_m(s)$ whenever $\mathrm{Re}(s) > -\min(m, n)$. It follows that this series of extensions $\Gamma_n(s)$ give us a well-defined meromorphic function on the whole of $\mathbb{C}$.

We now consider at $lim_{s\to -k}(s+k)\Gamma(s)$. Applying the previous formula with $n=k+1$, we have

$$(s+k)\Gamma(s)=\frac{1}{(s+k-1)\dots(s+1)s}\int_0^\infty e^{-x}x^{s+k}dx$$

As $s\to -k$, the right hand ride approaches

$$\frac{1}{(-k+k-1)\dots(-k+1)(-k)}\int_0^\infty e^{-x}dx=\frac{1}{(-1)^k k!}\times 1,$$

as required. □

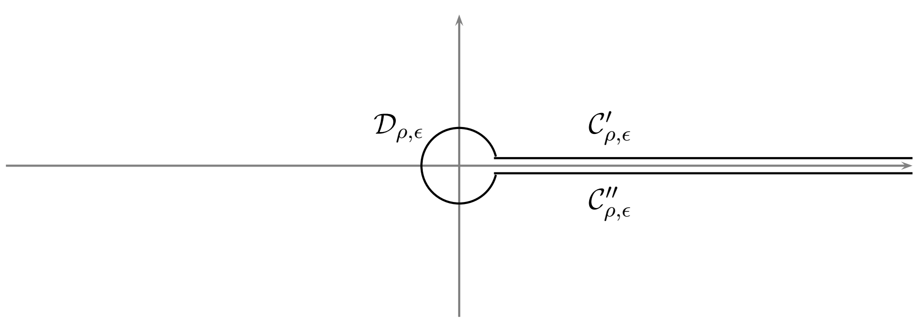
We are now ready to give a new expression for $\zeta(s)$.

From now on we fix the continuous branch of $\log z$ defined on $\mathbb{C}\setminus[0,\infty)$ as $\log|z|+i\arg z$, with $0<\arg z<2\pi$. This allows us to define a continuous branch of $z^{s-1}=\exp\{(s-1)\log z\}$ defined on $\mathbb{C}\setminus[0,\infty)$.

For $\rho\in(0,2\pi)$, and $\epsilon<\rho$ let $\mathcal{C}'_{\rho,\epsilon}$ be a line segment above the real axis at height ϵ up to the circle of radius ρ. Similarly, let $\mathcal{C}''_{\rho,\epsilon}$ be the complex conjugate of $\mathcal{C}'_{\rho,\epsilon}$. Let $\mathcal{D}_{\rho,\epsilon}$ be part of the circle of radius ρ connecting the curve $\mathcal{C}'_{\rho,\epsilon}$ to $\mathcal{C}''_{\rho,\epsilon}$. Define the closed curve

$$\mathcal{C}_{\rho,\epsilon}=\mathcal{D}_{\rho,\epsilon}\cup\mathcal{C}'_{\rho,\epsilon}\cup\mathcal{C}''_{\rho,\epsilon},$$

equipped with a direction inducing positive orientation on the arc of the circle.



Theorem 6.3. *For every* $\mathrm{Re}(s)>1$ *we have*

$$I(s):=\int_{C_\rho}\frac{z^{s-1}}{e^z-1}dz=\left(e^{2\pi is}-1\right)\Gamma(s)\zeta(s).$$

Proof

The integrand is meromorphic on $\mathbb{C} \setminus [0, \infty)$, with poles at $2\pi i n$, for every nonzero integer n. If we vary ρ within the range $0 < \rho < 2\pi$ (with $\epsilon < \rho$) the integral does not change, by Cauchy's theorem. On $\mathcal{D}_{\rho,\epsilon}$ we have $|z| = \rho$ and

$$|e^z - 1| = \left| z + \frac{z^2}{2} + \frac{z^3}{6} + \dots \right| = |z| \left| 1 + \frac{z}{2} + \dots \right| \geq \frac{|z|}{2} = \frac{\rho}{2},$$

if ρ is small enough. Moreover

$$\begin{aligned} \left| z^{s-1} \right| &= |\exp\{(s-1)\log z\}| = \exp\{\mathrm{Re}((s-1)\log z)\} \\ &= \exp\{(\sigma - 1)\log|z| - t \arg z\} \leq \exp\{(\sigma-1)\log\rho + 2\pi|t|\} \\ &= \rho^{\sigma-1} e^{2\pi|t|}. \end{aligned}$$

Hence

$$\left| \int_{\mathcal{D}_{\rho,\epsilon}} \frac{z^{s-1}}{e^z - 1} dz \right| \leq 2\pi\rho \, \frac{\rho^{\sigma-1} e^{2\pi|t|}}{\frac{1}{2}\rho} = 4\pi\rho^{\sigma-1} e^{2\pi|t|} \to 0$$

as $\rho \to 0$, since $\sigma > 1$. Thus, as ρ and ϵ tend to zero,

$$\begin{aligned} I(s) &= \int_{\mathcal{C}'_{\rho,\epsilon}} \frac{z^{s-1}}{e^z - 1} dz + \int_{\mathcal{C}''_{\rho,\epsilon}} \frac{z^{s-1}}{e^z - 1} dz \\ &= -\int_0^\infty \frac{x^{s-1}}{e^x - 1} dx + e^{2\pi i(s-1)} \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx, \end{aligned}$$

since on $\mathcal{C}''_{\rho,\epsilon}$, as $\epsilon \to 0$, we have

$$\begin{aligned} z^{s-1} &= e^{(s-1)(\log|z| + i \arg z)} \\ &= e^{(s-1)(\log x + 2\pi i)} \\ &= x^{s-1} e^{2\pi i(s-1)} = e^{2\pi i s}. \end{aligned}$$

Hence

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

Finally,

$$\frac{1}{Y - 1} = Y^{-1} + Y^{-2} + \dots$$

for $Y > 1$ so that

$$\begin{aligned}
\int_0^\infty \frac{x^{s-1}}{e^x - 1} dx &= \int_0^\infty x^{s-1} \left\{ e^{-x} + e^{-2x} + \ldots \right\} dx \\
&= \sum_{n=1}^\infty \int_0^\infty x^{s-1} e^{-nx} dx
\end{aligned}$$

providing that we can interchange summation and integration. This is permissible if

$$\sum_{n=1}^\infty \int_0^\infty \left| x^{s-1} e^{-nx} \right| dx$$

converges. However

$$\int_0^\infty \left| x^{s-1} e^{-nx} \right| dx = \int_0^\infty x^{\sigma-1} e^{-nx} dx = n^{-\sigma} \int_0^\infty y^{\sigma-1} e^{-y} dy = n^{-\sigma}\Gamma(\sigma),$$

and $\sum n^{-\sigma} < \infty$, since $\sigma > 1$. We are therefore able to deduce that

$$\begin{aligned}
\int_0^\infty \frac{x^{s-1}}{e^x - 1} dx &= \int_0^\infty x^{s-1} \left\{ e^{-x} + e^{-2x} + \ldots \right\} dx \\
&= \sum_{n=1}^\infty \int_0^\infty x^{s-1} e^{-nx} dx \\
&= \sum_{n=1}^\infty n^{-s} \int_0^\infty y^{s-1} e^{-y} dy \\
&= \zeta(s)\Gamma(s).
\end{aligned}$$

The theorem now follows. $\square$

Previously we showed how to extend our original definition of $\zeta(s)$ from the region $\sigma > 1$ to the larger region $\sigma > 0$. We can now go much further, by providing a meaningful definition over the whole complex plane.

Corollary 6.4. *The function $\left(e^{2\pi i s} - 1\right)\zeta(s)\Gamma(s)$ has an analytic continuation as an entire function on $\mathbb{C}$. Thus $\zeta(s)$ has a continuation as a meromorphic function on $\mathbb{C}$, the only possible poles being the points where $\left(e^{2\pi i s} - 1\right)\Gamma(s) = 0$.*

Proof

First we show that the integral $I(s)$ represents a well-defined function of s (with finite complex values). Recall that the value of the integral is independent of the choice of $\rho \in (0, 2\pi)$, so we may as well work with some value of $\rho \geq 1$. Indeed, we show that the integral converges uniformly in any disc $|s| \leq R$.

Fix $s \in \mathbb{C}$ with $|s| \leq R$. Since for $z \in \mathcal{C}_{\rho,\epsilon}$, $|z| \geq 1$, we have

$$\left|\frac{z^{s-1}}{e^z - 1}\right| \leq \frac{|z|^{\sigma-1} e^{2\pi|t|}}{|e^z - 1|} \leq \frac{|z|^{R-1} e^{2\pi R}}{|e^z - 1|}.$$

Moreover the function $|z|^{R-1} e^{2\pi R} |e^z - 1|^{-1}$ has a finite integral along the paths

$$\int_{\mathcal{D}_{\rho,\epsilon}} \frac{|z|^{R-1} e^{2\pi R}}{|e^z - 1|} |dz|$$

and

$$\int_{\mathcal{C}'_{\rho,\epsilon} \text{ or } \mathcal{C}''_{\rho,\epsilon}} \frac{|z|^{R-1} e^{2\pi R}}{|e^z - 1|} |dz| \leq O\Big(\int_0^\infty \frac{x^{R-1} e^{2\pi R}}{e^x - 1} dx\Big)$$

are finite.

In general if $G(z, s)$ is an entire function of s that has uniformly bounded integrals $\int_\gamma G(z, s)\, dz$ on some curve $\gamma \subset \mathbb{C}$, the function $H(s) = \int_\gamma G(z, s)\, dz$ is an entire function of s. Here, since $z^{s-1}/(e^z - 1)$ is an entire function of s, we conclude that $I(s)$ is entire. $\square$

One can check that the function $\frac{z}{e^z-1} + \frac{z}{2}$ is an even function of z. Define the Bernoulli Numbers B_m by

$$\frac{z}{e^z - 1} + \frac{1}{2} z = 1 + B_1 \frac{z^2}{2!} - B_2 \frac{z^4}{4!} + B_3 \frac{z^6}{6!} - \dots.$$

We can also check that B_m are all rational numbers and that

$$B_1 = \frac{1}{6}, B_2 = \frac{1}{30}, B_3 = \frac{1}{42}, \dots.$$

In fact the numbers B_m are all positive. The Bernoulli numbers appear in subjects of combinatorics, probability, and number theory.

Corollary 6.5. *We have,*

a) $\zeta(0) = -\frac{1}{2}$*;*

b) $\zeta(-2m) = 0$ *for all* $m \in \mathbb{N}$*;*

c) $\zeta(1-2m) = \frac{(-1)^m B_m}{2m}$, *for all* $m \in \mathbb{N}$.

Remark. The above result shows in particular that $\zeta(-k) \in \mathbb{Q}$ for all $k \in \mathbb{Z}_{\geq 0}$.

Proof

Take $k \in \mathbb{Z}_{\geq 0}$. By Corollary 6.2 $\Gamma(s)$ has a singularity of order 1 at $-k$, with residue $(-1)^k/k!$. Also $e^{2\pi i s} - 1$ has a simple zero at $-k$, with $\frac{e^{2\pi i s}-1}{s+k} \to 2\pi i$ as $s \to -k$. Hence as $s \to -k$ we have

$$\Gamma(s)\left(e^{2\pi i s} - 1\right) \to \frac{2\pi i (-1)^k}{k!}.$$

Now $I(s) = \Gamma(s)(e^{2\pi i s} - 1)\zeta(s)$ and $I(s)$ is continuous at $s = -k$, so that

$$\zeta(-k) = \frac{k!}{2\pi i (-1)^k} I(-k).$$

However

$$I(-k) = \int_{C_\rho} \frac{z^{-k-1}}{e^z - 1} dz$$

with $\mathcal{C}_\rho$ as before. Since k is integer, the function z^{-k-1} extends from $\mathbb{C} - [0, \infty)$ to $\mathbb{C} - \{0\}$ as a continuous function and

$$\int_{\substack{+\infty \\ \arg z = 0}}^{+\rho} \frac{z^{-k-1}}{e^z - 1} dz = - \int_{\substack{+\rho \\ \arg z = 2\pi}}^{+\infty} \frac{z^{-k-1}}{e^z - 1} dz.$$

It follows that

$$\begin{aligned} I(-k) &= \oint_{|z|=\rho} \frac{z^{-k-1}}{e^z - 1} dz \\ &= \oint_{|z|=\rho} z^{-k-2} \left(\frac{z}{e^z - 1}\right) dz \\ &= \oint_{|z|=\rho} z^{-k-2} \left(1 - \frac{1}{2}z + \frac{B_1}{2!}z^2 - \frac{B_2}{4!}z^4 + \ldots\right) dz \\ &= 2\pi i c, \end{aligned}$$

where c is the coefficient of z^{-1} in

$$z^{-k-2} \left(1 - \frac{1}{2}z + \frac{B_1}{2!}z^2 - \frac{B_2}{4!}z^4 + \ldots\right).$$

It follows that

$$c = \begin{cases} -\frac{1}{2}, & k = 0, \\ 0, & k = 2m > 0, \\ \frac{(-1)^{m-1}}{(2m!)} B_m, & k = 2m-1 > 0. \end{cases}$$

Hence $\zeta(-k) = \frac{(-1)^k k!}{2\pi i} I(-k)$, which is $-\frac{1}{2}$, or 0 or $\frac{(-1)^m}{2m} B_m$ in the three cases. □

We next give an alternative evaluation of $I(s)$, which leads to a new connection with the zeta-function.

Proposition 6.6. *If $\sigma < 0$ then $I(s) = e^{i\pi s/2}(e^{i\pi s} - 1)(2\pi)^s \zeta(1-s)$.*

Proof

Fix $\epsilon < 1$. We define a new contour C_n, for $n \in \mathbb{N}$, starting at $+\infty + \epsilon i$, running to $(2n+1)\pi + \epsilon i$ (above the real axis), along the line segments

$$(2n+1)\pi + \epsilon i \to (2n+1)\pi(1+i) \to (2n+1)\pi(-1+i)$$

$$\to (2n+1)\pi(-1-i) \to (2n+1)\pi(1-i) \to (2n+1)\pi - \epsilon i,$$

and back to $+\infty - \epsilon i$ just below the real axis. It will be convenient to write S_n for the part of the contour running around the square from $(2n+1)\pi + \epsilon i$ to $(2n+1)\pi - \epsilon i$.

We now replace the contour C_ρ by C_n. The integrand $\frac{z^{s-1}}{e^z - 1}$ has poles at $2\pi i k$ for $k \in \mathbb{Z} - \{0\}$. Hence, by Cauchy's residue theorem, we have

$$\begin{aligned} I(s) &= \int_{C_\rho} \frac{z^{s-1}}{e^z - 1} dz \\ &= \int_{C_n} \frac{z^{s-1}}{e^z - 1} dz - \sum_{1 \le |k| \le n} 2\pi i \operatorname{Res}\left(\frac{z^{s-1}}{e^z - 1}; z = 2\pi i k\right). \end{aligned}$$

However, if $k > 0$,

$$\operatorname{Res}\left(\frac{z^{s-1}}{e^z - 1}; z = 2\pi i k\right) = \lim_{z \to 2\pi i k} \frac{z^{s-1}(z - 2\pi i k)}{e^z - 1} = \frac{e^{(s-1)(\log 2\pi k + i\frac{\pi}{2})}}{1},$$

and similarly, for $k > 0$,

$$\operatorname{Res}\left(\frac{z^{s-1}}{e^z - 1}; z = -2\pi i k\right) = e^{(s-1)(\log 2\pi k + 3i\frac{\pi}{2})}.$$

It follows that

$$\begin{aligned}
I(s) &= \int_{C_n} \frac{z^{s-1}}{e^z-1} - 2\pi i \sum_{k=1}^{n} (2\pi k)^{s-1} \left(e^{(s-1)i\pi/2} + e^{(s-1)3i\pi/2} \right) \\
&= \int_{C_n} \frac{z^{s-1}}{e^z-1} - 2\pi i \left(e^{i\pi s/2}(-i) + e^{3i\pi s/2} i \right) \sum_{1}^{n} (2\pi k)^{s-1} \\
&= \int_{C_n} \frac{z^{s-1}}{e^z-1} + (2\pi)^s \left(e^{i\pi s} - 1 \right) e^{i\pi s/2} \sum_{1}^{n} k^{s-1}.
\end{aligned}$$

We now allow n to tend to infinity. On the contour C_n the function $\frac{1}{e^z-1}$ is bounded from above independently of n or z, since $e^z - 1$ is bounded away from zero. Moreover

$$|z^{s-1}| = e^{\mathrm{Re}((s-1)\log z)} = e^{(\sigma-1)\log|z| - t\arg z} \leq e^{(\sigma-1)\log|z| + 2\pi|t|},$$

whence $|z^{s-1}| \leq e^{2\pi|t|}|z|^{\sigma-1}$. So on S_n, which was the square part of the contour, we have $|z^{s-1}| = O(n^{\sigma-1})$, whence

$$\int_{S_n} \frac{z^{s-1}}{e^z-1} dz = O(nn^{\sigma-1}) = O(n^\sigma).$$

This tends to zero as n goes to infinity, since $\sigma < 0$. Moreover, whether we take $\arg(z) = 0$ or 2π, we will have

$$\begin{aligned}
\int_{(2n+1)\pi}^{\infty} \frac{z^{s-1}}{e^z-1} dz &= O\left(\int_{(2n+1)\pi}^{\infty} |z|^{\sigma-1} dz \right) \\
&= O\left(\int_{(2n+1)\pi}^{\infty} x^{\sigma-1} dx \right) \\
&= O\left(\left[\frac{x^\sigma}{\sigma} \right]_{(2n+1)\pi}^{\infty} \right) \\
&= O\left(((2n+1)\pi)^\sigma \right),
\end{aligned}$$

and this also tends to 0 when $\sigma < 0$.

We therefore conclude that

$$\int_{C_n} \frac{z^{s-1}}{e^z-1} dz \to 0 \quad \text{as} \quad n \to \infty$$

so that

$$I(s) = (2\pi)^s e^{i\pi s/2} \left(e^{i\pi s} - 1 \right) \sum_{1}^{\infty} k^{s-1}.$$

This completes the proof, since $\sum_1^\infty k^{s-1} = \zeta(1-s)$ for $\mathrm{Re}(s) < 0$. $\square$

Corollary 6.7. (The Functional Equation for $\zeta(s)$). *We have*

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

for all $s \in \mathbb{C} - \{0\}$. Moreover $\zeta(s)$ is meromorphic on $\mathbb{C}$, with the only singularity being a simple pole at $s = 1$.

Proof

If $\sigma < 0$ then

$$\zeta(1-s) = (2\pi)^{-s}e^{-i\pi s/2}\frac{1}{e^{i\pi s}-1}I(s)$$

when $\frac{1}{2}s \notin \mathbb{Z}$. According to Theorem 6.3 and Corollary 6.4 we have $I(s) = \left(e^{2\pi i s}-1\right)\Gamma(s)\zeta(s)$ on the complex plane, so that

$$\begin{aligned}\zeta(1-s) &= (2\pi)^{-s}e^{-i\pi s/2}\frac{1}{e^{i\pi s}-1}\left(e^{2\pi i s}-1\right)\Gamma(s)\zeta(s)\\ &= (2\pi)^{-s}(e^{\pi i s/2}+e^{-\pi i s/2})\Gamma(s)\zeta(s)\\ &= 2^{1-s}\pi^{-s}\cos(\frac{\pi s}{2})\Gamma(s)\zeta(s),\end{aligned}$$

using the definition $\cos(z) = (e^{iz}+e^{-iz})/2$ on the complex plane.

Now define $f(s) = \zeta(1-s) - 2^{1-s}\pi^{-s}\cos\frac{\pi s}{2}\Gamma(s)\zeta(s)$. This is meromorphic and it vanishes on $D(-1,1)$, for example. Here $D(-1,1)$ denotes the open disk of radius $+1$ about -1 within $\mathbb{C}$. Hence, by the Identity Theorem we have $f(s) = 0$ for all $s \in \mathbb{C}$.

Finally, from Theorem 4.2 we know that $\zeta(s)$ is meromorphic for $\sigma > 0$, with the only singularity being a simple pole at $s = 1$. Thus when $\sigma > 0$ the function $\zeta(s)\cos\frac{\pi s}{2}$ is holomorphic, since $\cos\frac{\pi s}{2}$ has a zero at $s = 1$. It follows that $2^{1-s}\cos\frac{\pi s}{2}\Gamma(s)\zeta(s)$ is holomorphic for $\sigma > 0$. We deduce that $\zeta(1-s)$ is holomorphic for $s > 0$. This means that $\zeta(s)$ is holomorphic in the region $\sigma < 1$. Since $\zeta(s)$ is also regular for $\sigma > 0$, apart from the pole at $s = 1$, we deduce that $\zeta(s)$ is regular everywhere, apart from the point $s = 1$. $\square$

Corollary 6.8. *If $\zeta(s) = 0$ then either $s = -2, -4, -6, \ldots,$ or s lies in the "critical strip" $0 < \mathrm{Re}(s) < 1$.*

Proof

If $\sigma \geq 1$, then $\zeta(s) \neq 0$, by Theorem 4.1 (for $\sigma > 1$) and Theorem 4.5 (for $\sigma = 1$).

If $\zeta(s) = 0$ with $\sigma \leq 0$, then Corollary 6.7 tells us that either $\zeta(1-s)$ vanishes, or $2^{1-s}\pi^{-s}\cos\frac{\pi s}{2}\Gamma(s)$ has a pole. However $\zeta(1-s) \neq 0$ since $\mathrm{Re}(1-s) \geq 1$. Moreover the only possible poles of $2^{1-s}\pi^{-s}\cos\frac{\pi s}{2}\Gamma(s)$ are those of $\Gamma(s)$, which lie at $s = 0, -1, -2, \ldots$. When $s = -n$ with n odd, the pole of $\Gamma(s)$ is cancelled by a zero of $\cos\frac{\pi s}{2}$, so that the only possibility left is that $s = -n$ with $n > 0$ even. According to Corollary 6.5 these points are indeed zeros of $\zeta(s)$. $\square$

Going back to the starting argument on the zeros of $\zeta(s)$ at the beginning of the section, of course all this effort would be pointless if $\zeta(s)$ had no zeros in the critical strip, but in fact there are infinitely many such zeros, and they are a fundamental obstruction to our understanding of the primes.

We can say a little more about the zeros of $\zeta(s)$. In particular,

Corollary 6.7 tells us that if s is in the critical strip then $\zeta(s) = 0$ if and only if $\zeta(1-s) = 0$. However something further is true.

Theorem 6.9. *We have $\zeta(\overline{s}) = \overline{\zeta(s)}$ for all $s \in \mathbb{C} - \{1\}$.*

Lemma. *If $f(s)$ is meromorphic on $\mathbb{C}$, then so is $f^*(s) := \overline{f(\overline{s})}$.*

Proof

Easy exercise, using the fact that

$$\lim_{h\to 0}\frac{f^*(s+h) - f^*(s)}{h} = \overline{f'(\overline{s})}.$$

$\square$

We can now prove Theorem 6.9.

Proof

Set $F(s) = \zeta(s) - \overline{\zeta(\overline{s})}$, which will be meromorphic on $\mathbb{C}$ by the above lemma. When s is real we have $s = \sigma$, and $F(\sigma) = \zeta(\sigma) - \zeta(\sigma) = 0$. Thus $F(s)$ vanishes on the real axis, and hence by the Identity Theorem $F(s) = 0$ for all s. $\square$

Corollary 6.10. *If $\zeta(\rho) = 0$ with ρ in the critical strip, then each of $\rho, 1-\rho, \overline{\rho}$ and $1-\overline{\rho}$ is a zero of $\zeta(s)$.*

Proof

This follows from Theorem 6.9 and Corollary 6.7. $\square$

We conclude with various remarks:- Corollary 6.10 suggests that the zeros occur in groups of 4, unless ρ is real or $\mathrm{Re}(\rho) = 1/2$. In fact one can show that$\zeta(s) \neq 0$ for real $s \in (0,1)$. Indeed it appears that all zeros in the critical strip have $\mathrm{Re}(s) = 1/2$ (so that the zeros are only in pairs, s and $1-s$ $(= \overline{s})$).

It is known that $\zeta(s)$ has infinitely many zeros in the critical strip. Up to height $\mathrm{Im}(s) = T$ there are around $\frac{T}{2\pi}\log T$ such zeros.

The first zero is about $\frac{1}{2} \pm (14.13\ldots)i$ and the next ones are roughly

$$\frac{1}{2} \pm (21.02\ldots)i, \frac{1}{2} \pm (25.01\ldots)i,$$

$$\frac{1}{2} \pm (30.42\ldots)i, \frac{1}{2} \pm (32.93\ldots)i, \frac{1}{2} \pm (37.58\ldots)i.$$

They are irregularly spaced.

Calculations show that $\mathrm{Re}(s) = \frac{1}{2}$ for all zeros in the critical strip with $0 < \mathrm{Im}(s) < 10^{12}$, in which range there are over 10^{13} zeros.

All this evidence points to the following statement, whose proof would have far-reaching consequences for our knowledge of prime numbers.

The Riemann Hypothesis *If $\zeta(s) = 0$ and $0 < \mathrm{Re}(s) < 1$ then $\mathrm{Re}(s) = 1/2$.*

7 References

- T. M. Apostol, Introduction to Analytic Number Theory
- H. Davenport, Multiplicative Number Theory
- G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers
- I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers
- L. V. Ahlfors, complex analysis
- G. B. Foland, Real analysis; modern techniques and their applications