ANALYTIC NUMBER THEORY

Graham Everest

Contents

Figure 1: Level of Difficulty of the Course

Analytic Number Theory

1 Elementary Number Theory and Easy Asymptotics

Recommended text:
Tom APOSTOL, "Introduction to Analytic Number Theory", 5th edition, Springer. ISBN 0-387-90163-9.

Course content:

- Integers, especially prime integers
- connections with complex functions

How did the subject arise? E. g. Gauss and Legendre did extensive calculations, calculated tables of primes. By looking at these tables, Gauss reckoned that the real function

$$\pi(x) := \#\{p \leq x : \ p \text{ is prime}\}$$

grows quite regularly, namely

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

although the individual primes are scattered rather irregularly among the natural numbers. Equation (1) is known as the Great Prime Number Theorem - or just THE Prime Number Theorem. The first proof of it used the developing theory of complex functions.

Definition 1.1
In this course, a *prime* is a positive integer p which admits no divisors except 1 and itself [1]. By definition, 1 is not a prime.

Theorem 1.2 (Fundamental Theorem of Arithmetic - FTA)
Every integer $n > 1$ can be expressed as a finite product of primes, unique up to order.

Example: $6 = 2 \cdot 3 = 3 \cdot 2$.
From the FTA follows the

Corollary 1.3
There must be infinitely many primes.

Proof 1 (Euclid): If there are only finitely many primes, we can list them $p_1, \ldots, p_r$. Define

$$N := p_1 \cdot \ldots \cdot p_r + 1.$$

By FTA, N can be factorized, so it must be divisible by some prime p_k of our list. Since p_k also divides $p_1 \cdot \ldots \cdot p_r$, it must divide 1 - an absurdity. $\square$
Proof 2 (Euler): If there are only finitely many primes $p_1, \ldots p_r$, consider the product

$$X := \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)^{-1}.$$

Note that the product is well defined, since 1 is not a prime and since, by hypothesis, there are only finitely many primes. Now expand each factor into a geometric series:

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots$$

[1] In Ring theory, primes are defined in a different way, i. e. an element x of a commutative ring R, not a unit, is *prime in* R iff for all products in R divisible by x, at least one factor must be divisible by x. For positive integers, this amounts to the same as our definition.

Put this into the equation for X:

$$\begin{aligned} X &= \left(1+\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\dots\right)\cdot\left(1+\frac{1}{3}+\frac{1}{3^2}+\frac{1}{3^3}+\dots\right) \\ &\quad \cdot\left(1+\frac{1}{5}+\frac{1}{5^2}+\frac{1}{5^3}+\dots\right)\cdots\left(1+\frac{1}{p_r}+\frac{1}{p_r^2}+\frac{1}{p_r^3}+\dots\right) \\ &= 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\dots \\ &= \sum_n \frac{1}{n}, \end{aligned}$$

the harmonic series! But this series diverges, and again we have reached an absurdity. □

Why exactly does the harmonic series diverge???

Proof 1 (typical year One proof):

$$\begin{aligned} & 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\dots \\ > \; & 1+\frac{1}{2}+\frac{1}{4}+\frac{1}{4}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\dots \\ = \; & 1+\frac{1}{2}+\frac{2}{4}+\frac{4}{8}+\dots \\ = \; & 1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\dots \end{aligned}$$

which cleary diverges. □

Exercise: Try to prove that $\sum 1/n^2$ diverges using the same technique. Of course, this will not work, since this series converges, but you will see something "mildly" interesting.

Proof 2: Compare $\sum_{n=1}^{N} \frac{1}{n}$ with the integral $\int_1^N \frac{1}{x}\,dx = \log(N)$.

Figure 2: The harmonic series as integral of a step function

The result is:

$$\log(N) \le \sum_{n=1}^{N} \frac{1}{n} \le \log(N)+1. \tag{2}$$

The first inequality in (2) is enough to show the divergence of the harmonic series. But together with the second, we are given information about the speed of the divergence! Proof 2 is a typical example of a proof leading forward. □

1.1 The Log of the Zeta Function

Definition 1.4
Given two functions f : $\mathbb{R} \to \mathbb{C}$ and g : $\mathbb{R} \to \mathbb{R}_+$, we write

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

if there exist constants C and x_0 such that $|\mathrm{f}(x)| \leq C\mathrm{g}(x)$ for all $x \geq x_0$. This is used to isolate the dominant term in a complicated expression. Examples:

- $x^3 + 501x = O(x^3)$
- Any bounded function is $O(1)$, e. g. $\sin(x) = O(1)$
- Can have complex f: $e^{ix} = O(1)$ for real x.

Thus we can write $\sum_1^N \frac{1}{n} = \log(N) + O(1)$. You may also see $\mathrm{f} = o(\mathrm{g})$. This means $\frac{|\mathrm{f}|}{g} \to 0$ as x tends to infinity. The Prime Number Theorem can be written

$$\begin{aligned} \pi(x) &= \frac{x}{\log(x)} + o\left(\frac{x}{\log(x)}\right) \qquad \text{or} \\ \frac{\pi(x)\log(x)}{x} &= 1 + o(1). \end{aligned}$$

Theorem 1.5
The series $\sum_p \frac{1}{p}$ diverges.

Proof 1 (see Apostol p. 18): By absurdity. Assume that the series converges, i. e.

$$\sum_p \frac{1}{p} < \infty.$$

So there is some N such that $\sum_{p>N} \frac{1}{p} < \frac{1}{2}$. Let $Q := \prod_{p \leq N} p$. The numbers $1 + nQ$, $n \in \mathbb{N}$, are never divisible by primes less than N (because those divide Q). Now consider

$$\sum_{t=1}^{\infty} \left(\sum_{p>N} \frac{1}{p}\right)^t < \sum_t \frac{1}{2^t} = 1.$$

We claim that

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{p>N} \frac{1}{p} \right)^t \tag{3}$$

because every term of the l.h.s. appears on the right at least once (convince yourself of this claim by assuming e. g. $N = 11$ and find some terms in the r.h.s.!) But the series on the l.h.s. of (3) diverges! This follows from the 'limit comparison test':

> If for two real sequences a_n and b_n holds $\frac{a_n}{b_n} \to L \neq 0$, then $\sum_n a_n$ converges iff $\sum_n b_n$ does.

Apply this test with $a_n = \frac{1}{1+nQ}$, $b_n = \frac{1}{n}$ and $L = 1/Q$. This absurdity proves the theorem. □

Proof 2: We will show that

$$\sum_{p \leq N} \frac{1}{p} > \log\log(N) - 1. \tag{4}$$

Remark 1.6
In these notes, we will always define $\mathbb{N} = \{1, 2, 3, \dots\}$ (excluding 0). If 0 is to be included, we will write $\mathbb{N}_0$.

Let

$$\mathcal{N} := \{n \in \mathbb{N} : \text{ all prime factors of } n \text{ are less than } N\}$$

Then

$$\begin{aligned} \sum_{n \in \mathcal{N}} \frac{1}{n} &= \prod_{p \leq N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots \right) \\ &= \prod_{p \leq N} \left(\frac{1}{1 - \frac{1}{p}} \right) \end{aligned} \tag{5}$$

If $n \leq N$, then $n \in \mathcal{N}$, therefore

$$\sum_{n \leq N} \frac{1}{n} \leq \sum_{n \in \mathcal{N}} \frac{1}{n}.$$

But $\log(N)$ is less than the l.h.s., so

$$\log(N) \leq \sum_{n \in \mathcal{N}} \frac{1}{n} = \prod_{p \leq N} \left(1 - \frac{1}{p}\right)^{-1}. \tag{6}$$

Lemma 1.7
For all $v \in [0, 1/2]$ holds

$$\frac{1}{1-v} \leq e^{v+v^2}.$$

Apply this with $v = \frac{1}{p}$ (note primes are at least 2, so the lemma does apply):

$$\prod_{p \leq N} \left(1 - \frac{1}{p}\right)^{-1} \leq \prod_{p \leq N} \exp\left(\frac{1}{p} + \frac{1}{p^2}\right). \tag{7}$$

Now combine this with equation (6) and take logs:

$$\log\log(N) \leq \sum_{p \leq N} \frac{1}{p} + \frac{1}{p^2}. \tag{8}$$

Finally, we observe that

$$\sum_{p} \frac{1}{p^2} < \sum_{n=2}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} - 1 < 1$$

Proof of lemma 1.7: Put $\mathrm{f}(v) := (1-v)\exp(v+v^2)$. We claim $1 \leq \mathrm{f}(v)$ for all $v \in [0, 1/2]$. To prove this, we check $\mathrm{f}(0) = 1$ and

$$\mathrm{f}'(v) = v(1-2v)\exp(v+v^2)$$

which is nonnegative for $v \in [0, 1/2]$. □
This completes Proof 2 of theorem 1.5. □

We will prove later

$$\sum_{p \leq N} \frac{1}{p} = \log\log(N) + A + O\left(\frac{1}{\log(N)}\right), \tag{9}$$

where A is a constant.

> Question: Is it possible to prove (9) with $O(1)$ in place of $A + O(\dots)$ using only methods of Proof 2?

29.1.99

Third proof that $\sum_p \frac{1}{p}$ diverges:
The following identity holds for all $\sigma > 1$:

$$\begin{aligned} \log(\zeta(\sigma)) &= -\sum_p \log\left(1 - \frac{1}{p^\sigma}\right) \qquad (10) \\ &= -\sum_p \sum_{m=1}^{\infty} \frac{-1}{mp^{m\sigma}} = \sum_p \frac{1}{p^\sigma} + \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^{m\sigma}} \end{aligned}$$

We will prove the identity (10) later. Note however, that the series involved converge absolutely.
We claim: The last double sum on the right-hand side is bounded. Proof:

$$\begin{aligned} \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^{m\sigma}} &< \sum_p \sum_{m=2}^{\infty} \frac{1}{p^{m\sigma}} \\ = \sum_p \frac{1}{p^{2\sigma}} \frac{1}{1 - \frac{1}{p^{2\sigma}}} &\leq 2\sum_p \frac{1}{p^{2\sigma}} \leq 2\zeta(2) \end{aligned}$$

because $1 - \frac{1}{p^{2\sigma}} \geq \frac{1}{2}$.
Note in passing:

> Our bound holds for all $\sigma \geq 1$, and the double sum converges for all $\sigma > 1/2$.

So we can summarise:

$$\log(\zeta(\sigma)) = \sum_p \frac{1}{p^\sigma} + O(1).$$

The left-hand side goes to infinity as $\sigma \to 1$, so the sum on the right-hand side must do the same. This completes proof 3 of theorem 1.5. □

Proof of equation (10): Let P be a large prime. Then repeat the argument leading to

$$\left(1 - \frac{1}{2^\sigma}\right)\zeta(\sigma) = 1 + \sum_{2 < n \text{ odd}} \frac{1}{n^\sigma}$$

with all the primes $3, 5, \ldots, P$. This gives

$$\left(1-\frac{1}{2^\sigma}\right)\left(1-\frac{1}{3^\sigma}\right)\left(1-\frac{1}{5^\sigma}\right)\cdot\ldots\cdot\left(1-\frac{1}{P^\sigma}\right)\zeta(\sigma) = 1 + \sum_{p|n\Rightarrow p>P}\frac{1}{n^\sigma}.$$

The last sum ranges only over those n with all prime factors bigger than P. So it is a subsum of a tail end of the series for $\zeta(\sigma)$, hence tends to zero as P goes to infinity. This gives

$$\zeta(\sigma) = \prod_p \left(1-\frac{1}{p^\sigma}\right)^{-1} \tag{11}$$

and taking logs, we obtain (10). □

Equation (11) is known as the 'Euler product representation of ζ'.

1.2 Euler's Summation Formula

This is a tool do derive sharp asymptotic formulae.

Theorem 1.8
Given a real interval $[a, b]$ with $a < b$, suppose f is a function on (a, b) with continuous derivative. Then

$$\sum_{a<n\le b} \mathrm{f}(n) = \int_a^b \mathrm{f}(t)\,dt + \int_a^b \{t\}\mathrm{f}'(t)\,dt - \mathrm{f}(b)\{b\} + \mathrm{f}(a)\{a\}. \tag{12}$$

Here, $\{t\}$ denotes the *fractional part* of t, defined for any real t by

$$\{t\} = t - [t]$$

and $[t]$ is the greatest integer not bigger than t. Example:

$$\{-2.1\} = -2.1 - (-3) = 0.9.$$

Note that the formula applies to real as well as complex-valued functions.

Proof in the case $a, b \in \mathbb{N}$: Suppose $a < n-1 < n \le b$, then

$$\int_{n-1}^{n} [t]\mathrm{f}'(t)\,dt = (n-1)[\mathrm{f}(n) - \mathrm{f}(n-1)] = n\mathrm{f}(n) - (n-1)\mathrm{f}(n-1) - \mathrm{f}(n).$$

Sum this from $a+1$ to b:

$$\begin{aligned}\int_a^b [t]\mathrm{f}'(t)\,dt &= \sum_{n=a+1}^{b}(n-1)[\mathrm{f}(n)-\mathrm{f}(n-1)]\\ &= b\mathrm{f}(b)-a\mathrm{f}(a)-\sum_{n=a+1}^{b}\mathrm{f}(n).\end{aligned}$$

Rearrange this:

$$\sum_{n=a+1}^{b}\mathrm{f}(n)=b\mathrm{f}(b)-a\mathrm{f}(a)-\int_a^b [t]\mathrm{f}'(t)\,dt \tag{13}$$

On the other hand, play with $\int_a^b \mathrm{f}$:

$$\int_a^n \mathrm{f}(t)\,dt=[t\mathrm{f}(t)]_a^b-\int_a^b t\mathrm{f}'(t)\,dt \tag{14}$$

Now equations (13) and (14) together give the requested

$$\sum_{n=a+1}^{b}\mathrm{f}(n)=\int_a^b \mathrm{f}(t)\,dt+\int_a^b \{t\}\mathrm{f}'(t)\,dt.$$

□

We apply the ESF to the harmonic series $\sum_2^N \frac{1}{k}$. Here, $a=1$, $b=N$ and $\mathrm{f}(t)=1/t$. Note that $a=0$ would not work! ESF gives

$$\sum_2^N \frac{1}{n}=\int_1^N \frac{1}{t}\,dt-\int_1^N \frac{\{t\}}{t^2}\,dt=\log(N)-\int_1^N \frac{\{t\}}{t^2}\,dt. \tag{15}$$

Now obviously

$$\int_1^N \frac{\{t\}}{t^2}\,dt=\int_1^\infty \frac{\{t\}}{t^2}\,dt-\int_N^\infty \frac{\{t\}}{t^2}\,dt$$

and the last term is less than $\int_N^\infty \frac{1}{t^2}\,dt=\frac{1}{N}$. So we have proved (add One on both sides of (15))

Proposition 1.9

$$\begin{aligned} \sum_{n=1}^{N} \frac{1}{n} &= \log(N) + \gamma + O\left(\frac{1}{N}\right), \qquad \text{where} \\ \gamma &:= 1 + \int_1^{\infty} \frac{\{t\}}{t^2}\, dt \end{aligned}$$

is known as the EULER-MASCHERONI-constant (some call it just EULER's constant).

See the MTH Website for the 'constants' page', or see

http://www.mathsoft.com/asolve/constant/euler/euler.html

Definition 1.10
For $1 \leq n \in \mathbb{N}$, let

$$\mathrm{d}(n) := \text{number of divisors of } n.$$

E. g. $\mathrm{d}(n) = 2$ iff n is a prime.

Information about d reflects something - crudely - about the distribution of the primes themselves.

Proposition 1.11

$$\sum_{n=1}^{N} \mathrm{d}(n) = N \log(N) + (2\gamma - 1)N + O(\sqrt{N}). \tag{16}$$

Proof: ESF in the usual form with integer boundaries just gives a remainder $O(N)$. For the sharper result, we have to apply ESF in the more general form as stated in theorem 1.8. But first, look how the general form applies to the harmonic series: 1.2.99

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

The last summand is $O(\frac{1}{x})$, so goes into the remainder term. The general form does not give us more information, and this is the case in most examples. But now we come to an example, where we really need it. We will use that

$$\#\{(m,q):\ mq\le x\} = 2\#\{(m,q):\ mq\le x,\ m<q\} + O(\sqrt{x}). \qquad (17)$$

If $mq\le x$ and $m<q$, then $m<\sqrt{x}$. The number of q in this set for fixed m is $[x/m]-m$ (draw it!).

$$\begin{aligned}\sum_{n\le x}\mathrm{d}(n) &= \sum_{m\le x}\sum_{q\le\frac{x}{m}} 1\\ &= 2\sum_{\substack{m,q:\ \\ \ }}{}_{\substack{mq\le x\\ m<q}} 1 + O(\sqrt{x})\\ &= 2\sum_{m<\sqrt{x}}\left(\left[\frac{x}{m}\right]-m\right) + O(\sqrt{x})\\ &= 2x\sum_{m<\sqrt{x}}\frac{1}{m} - \sum_{m<\sqrt{x}} m + O(\sqrt{x}).\end{aligned}$$

Now we can attack each sum with ESF and obtain

$$\begin{aligned}\sum_{n\le x}\mathrm{d}(n) &= 2x(\log(\sqrt{x})+\gamma+O(x^{-1/2})) - 2\left(\frac{x}{2}+O(\sqrt{x})\right)+O(\sqrt{x})\\ &= x\log(x) + (2\gamma-1)x + O(\sqrt{x})\end{aligned}$$

as stated. □

Let us do another nice example: STIRLING's formula says

$$\log(N!) = N\log(N) - N + O(\log(N)). \qquad (18)$$

Proof: $\log(N!) = \sum_{n=2}^{N} \log(n)$. Put $\mathrm{f}(t) = \log(t)$, so by ESF

$$\log(N!) = \int_1^N \log(t)\, dt + \int_1^N \frac{\{t\}}{t}\, dt = N\log(N) - N + O(\log(N)).$$

□

1.3 Multiplicative arithmetical functions

Definition 1.12
An arithmetical function is any function $\mathrm{f}: \mathbb{N} \to \mathbb{C}$, e. g. $\mathrm{f}(n) = 1/n^\sigma$ or

$$\phi(n) = \#\{1 \le a \le n : (a, n) = 1\}, \tag{19}$$

called the *Euler phi-function*. An arithmetical function such that $\mathrm{f}(1) \neq 0$ and

$$\mathrm{f}(mn) = \mathrm{f}(m)\mathrm{f}(n)$$

whenever m and n are coprime is called *multiplicative* (note that this implies $\mathrm{f}(1) = 1$). If f has this property not only for coprime m, n, but for all $m, n \in \mathbb{N}$, f is called *completely multiplicative*.

Lemma 1.13
The Euler phi-function ϕ as defined in (19) is multiplicative.

Corollary 1.14
If n is factorized into powers of distinct primes, $n = \prod_p p^{e_p}$, then

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

Exercise: Show that ϕ is not completely multiplicative but $1/n^\sigma$ is.
The proof of lemma 1.13 depends on the following result.

Lemma 1.15 (Chinese Remainder Theorem - CRT)
Suppose $m, n \in \mathbb{N}$ are coprime, then the simultaneous congruences

$$\begin{aligned} x &= a \pmod m \\ x &= b \pmod n \end{aligned}$$

have a solution $x \in \mathbb{N}$ for any $a, b \in \mathbb{Z}$, and the solution is unique modulo mn.

The Chinese Remainder Theorem was discovered by Chinese mathematicians in the 4th century A.C.
Proof of CRT: We claim that there exist m', n' such that $mm' = 1 \pmod{n}$ $(*)$ and $nn' = 1 \pmod{m}$. Put $x := bmm' + ann'$, this satisfies both the required congruences.
If, on the other hand, x and y satisfy both congruences, $x - y$ is divisible by m and by n. Since m and n are coprime, $x - y$ must be divisible by mn.
Proof of claim $(*)$: First, we reformulate the claim:

$$\begin{aligned} a \text{ is coprime to } n &\Leftrightarrow a \text{ has multiplicative inverse modulo } n \\ &\Leftrightarrow \exists b: \ ab = 1 \pmod{n}. \end{aligned} \tag{20}$$

The implication from right to left is clear, only from left to right we have to work a bit. b is found using the Euclidean algorithm. We do an example that should make the method clear: E. g. to solve $11 \cdot b = 1 \pmod{17}$ we do

$$\begin{aligned} 17 &= 11 \cdot 1 + 6 \\ 11 &= 6 \cdot 1 + 5 \\ 6 &= 5 \cdot 1 + 1. \end{aligned}$$

The last non-zero remainder is the gcd, which is One by hypothesis. From this, work your way backwards, always expressing the remainder by the previous two terms:

$$1 = 6 - 5 = 6 - (11 - 6) = 2 \cdot 6 - 11 = 2(17 - 11) - 11 = 2 \cdot 17 - 3 \cdot 11.$$

□

Example for CRT: Solve $x = 2 \pmod{17}$ and $x = 8 \pmod{11}$. We find $m' = 2$ and $n' = 14$ congruent to -3 as in the proof of CRT. Then

$$x = 8 \cdot (17 \cdot 2) + 2 \cdot (11 \cdot 14) = 580$$

satisfies the two congruences (the smallest solution is the remainder of 580 divided by $(11 \cdot 17)$, namely 19).

Proof of lemma 1.13: Define a map

$$\Phi: \ \mathbb{Z}/_{(mn)} \to \mathbb{Z}/_{m} \times \mathbb{Z}/_{n} \tag{21}$$

simply by $x \mapsto (x \bmod m, x \bmod n)$. By CRT, Φ is a bijection (in fact, Φ is an isomorphism of rings). Now define

$$U\left(\mathbb{Z}/_m\right) := \{1 \leq a \leq m : \ (a,m) = 1\}$$

and likewise for n and mn. Since x is coprime to mn iff it is coprime both to m and n, we can restrict Φ to the U-level:

$$\Phi : \ U\left(\mathbb{Z}/_{(mn)}\right) \to U\left(\mathbb{Z}/_m\right) \times U\left(\mathbb{Z}/_n\right) \tag{22}$$

Here Φ is still a bijection (in fact, the sets $U(\dots)$ are the units of $\mathbb{Z}/(mn)$ resp. $\mathbb{Z}/m$ resp. $\mathbb{Z}/n$ by (20), and Φ is an isomorphism of groups). By definition, the cardinality of $U(\mathbb{Z}/m)$ is just $\phi(m)$ and likewise for n and mn, which completes the proof of lemma 1.13. □

Remark 1.16
CRT works in greater generality: If $m_1, \dots m_r$ are pairwise coprime then for any $a_1, \dots a_r$ the simultaneous congruences $x = a_i \pmod{m_i}$ have a solution $x \in \mathbb{Z}$, and it is unique modulo $m_1 \cdot \ldots \cdot m_r$. 2.2.99

Theorem 1.17
For any $n \in \mathbb{N}$ holds

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

Proof: Check the equality for $n = p^r$ (a prime power). The left hand side is

$$1 + \sum_{i=0}^{r-1} (p-1)p^{i-1} = 1 + (p^r - 1) = n$$

as a sum of a geometric progression. Next, observe that both sides of the equation in theorem 1.17 are multiplicative arithmetic functions. For the left-hand side, this follows from

$$\sum_{d|mn} \phi(d) = \sum_{d_1|m} \sum_{d_2|n} \phi(d_1 d_2) = \sum_{d_1|m} \phi(d_1) \sum_{d_2|n} \phi(d_2)$$

for any pair of coprime integers (m, n) (note that d divides mn iff there exist divisors d_1 of m and d_2 of n such that $d = d_1 d_2$). So it was enough to check the prime power case. □

Definition 1.18
The Möbius function μ is defined by

$$\begin{array}{lcll} \mu(1) & = & 1 & \\ \mu(n) & = & (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \\ \mu(n) & = & 0 & \text{otherwise.} \end{array}$$

This course is built around the strange phenomenon, that in order to study integers, especially primes, one needs to study functions. We will prove after Easter (see Apostol, p. 91):

$$\text{PNT} \iff \sum_{n \le x} \mu(n) = o(x), \qquad \text{i. e.}$$
$$\frac{1}{x} \sum_{n \le x} \mu(n) \to 0. \tag{23}$$

Also, the Riemann hypothesis is equivalent to a result about partial sums of μ.

Theorem 1.19
The Möbius function μ is multiplicative. Furthermore

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

Proof: First, we have to show $\mu(mn) = \mu(m)\mu(n)$ for coprime integers (m, n). Factorize m and n as product of prime powers. The primes involved must all be distinct. If anywhere in the factorisation is an exponent of at least Two, we obviously get an equation $0 = 0$. If m and n are products of k resp. l distinct primes, then mn is a product of $k + l$ primes, and they are all distinct, since m and n are coprime. So we get $\mu(m) = (-1)^k$, $\mu(n) = (-1)^l$ and

$$\mu(mn) = (-1)^{k+l} = \mu(m)\mu(n).$$

For the next claim, it is sufficient to check the prime power case, since again both sides of the equation of theorem 1.19 are multiplicative (the same argument as in the proof of theorem 1.17). If $n = p^r$ with $r \ge 1$, the left-hand side is $\mu(1) + \mu(p) = 1 - 1 = 0$, and this is all we have to do! $\square$

Theorem 1.20

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} \tag{24}$$

Proof: We know from corollary 1.14 $\phi(n) = n\prod_{p_i|n}\left(1-\frac{1}{p_i}\right)$, so

$$\frac{\phi(n)}{n} = 1 - \sum_{p_i|n}\frac{1}{p_i} + \sum_{i\neq j}\frac{1}{p_i p_j} - \ldots = \sum_{d|n}\frac{\mu(d)}{d}.$$

□

1.4 Dirichlet Convolution

5.2.99

Theorem 1.20 is a special instance of a general technique:

Definition 1.21
For arithmetical functions f, g let

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

This is a new arithmetical function, called the *convolution of* f *and* g.

Theorem 1.22
Convolution is commutative and associative. In symbols: For all arithmetical functions f,g,h holds
i) $\mathrm{f} * \mathrm{g} = \mathrm{g} * \mathrm{f}$ and
ii) $(\mathrm{f} * \mathrm{g}) * \mathrm{h} = \mathrm{f} * (\mathrm{g} * \mathrm{h})$.

Proof of i): The sum in

$$\sum_{d|n} \mathrm{f}(d)\mathrm{g}\left(\frac{n}{d}\right)$$

runs over all pairs $d, e \in \mathbb{N}$ with $de = n$, so it is equal to

$$\sum_{de=n} \mathrm{f}(d)\mathrm{g}(e),$$

and the latter expression is clearly symmetric (f and g can be interchanged).
Proof of ii): Do for example $n = p$ by hand! the proof in general goes much in the same way as the proof of i): Both sides of ii) are equal to

$$\sum_{cde=n} \mathrm{f}(c)\mathrm{g}(d)\mathrm{h}(e).$$

□

Lemma 1.23
Define the arithmetical function I by $\mathrm{I}(1) = 1$ and $\mathrm{I}(n) = 0$ for all $n > 1$. Then for all arithmetical functions f,

$$\mathrm{f} * \mathrm{I} = \mathrm{I} * \mathrm{f} = \mathrm{f}.$$

Proof: By definition,

$$\mathrm{f} * \mathrm{I}(n) = \sum_{d|n} \mathrm{f}(d)\mathrm{I}\left(\frac{n}{d}\right) = \mathrm{f}(n)\mathrm{I}(1) = \mathrm{f}(n)$$

(all the other summands are zero by the definition of I). □

Theorem 1.24
If f is an arithmetical function with $\mathrm{f}(1) \neq 0$, there exists exactly one arithmetical function g such that $\mathrm{f} * \mathrm{g} = \mathrm{I}$. This function is denoted by f^{-1}.

Proof: The equation $(\mathrm{f} * \mathrm{g})(1) = \mathrm{f}(1)\mathrm{g}(1)$ determines $\mathrm{g}(1)$. Then define g recursively: Assuming that $\mathrm{g}(1), \ldots, \mathrm{g}(n-1)$ has been defined (and that there is only one choice), the equation

$$\mathrm{f} * \mathrm{g}(n) = \mathrm{f}(1)\mathrm{g}(n) + \sum_{1<d|n} \mathrm{f}(d)\mathrm{g}\left(\frac{n}{d}\right)$$

permits to calculate $\mathrm{g}(n)$ and determines it uniquely. □

Example: Let $\mathrm{u}(n) = 1$ for all n. Then we have, by theorem 1.19

$$\mathrm{u}^{-1} = \mu. \tag{25}$$

Theorem 1.25 (Möbius Inversion Formula)
Given arithmetical functions f and g, the following are equivalent:

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

Proof of $\Rightarrow$: Let $\mathrm{u}(n) = 1$ for all n as in the example. Then convolve both sides of $\mathrm{f} = \mathrm{g} * \mathrm{u}$ with μ and use (25)

$$\mathrm{f} * \mu = \mathrm{g} * \mathrm{u} * \mu = \mathrm{g} * \mathrm{I} = \mathrm{g}.$$

This proves the implication from left to right. For the converse, convolve with u. □

Corollary 1.26
Theorems 1.17 and 1.20 are equivalent, e. g. from theorem 1.17 we obtain a proof of theorem 1.20 by convolving with the Möbius function.

Corollary 1.27 (Application)
Suppose we have absolutely convergent series of the form

$$\mathrm{F}(\sigma) = \sum_{\mathbb{N}} \frac{\mathrm{f}(n)}{n^\sigma}, \qquad \mathrm{G}(\sigma) = \sum_{\mathbb{N}} \frac{\mathrm{g}(n)}{n^\sigma}.$$

Then

$$\mathrm{F}(\sigma) \cdot \mathrm{G}(\sigma) = \sum_{\mathbb{N}} \frac{(\mathrm{f} * \mathrm{g}(n))}{n^\sigma}.$$

Example: If $\mathrm{f} * \mathrm{g} = \mathrm{I}$, we get $\mathrm{F}(\sigma)\mathrm{G}(\sigma) = 1$. So

$$\frac{1}{\zeta(\sigma)} = \sum_{\mathbb{N}} \frac{\mu(n)}{n^\sigma}.$$

Series as those for F, G and $F \cdot G$ are called Dirichlet series. We are now going to study the Riemann zeta function in the context of Dirichlet series.

8.2.99

Add to Q14: For all s such that $\Re(s) > 2$,

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

2 The Riemann Zeta Function

The traditional notation for the variable is

$$s = \sigma + it \qquad \text{with } \sigma, t \in \mathbb{R}.$$

Claim: For all s such that $\Re(s) > 1$, the series $\sum_{\mathbb{N}} \frac{1}{n^s}$ converges absolutely.
Proof of claim: Calculate the modulus of each term:

$$n^{-s} = n^{-\sigma - it} = n^{-\sigma} e^{-it\log(n)}$$

has modulus $n^{-\sigma}$, and we know already that $\sum_{\mathbb{N}} \frac{1}{n^\sigma}$ is a convergent series.

2.1 Euler Products

We recall equation (11):

$$\zeta(\sigma) = \prod_p \left(1 - \frac{1}{p^\sigma}\right)^{-1}.$$

We will show that this holds for all complex s with $\Re(s) > 1$. Since it is not more difficult, we prove a more general theorem:

Theorem 2.1
If f is a multiplicative arithmetical function, and $\sum_{\mathbb{N}} \mathrm{f}(n)$ converges absolutely, then

$$\sum_{\mathbb{N}} \mathrm{f}(n) = \prod_p (\mathrm{f}(1) + \mathrm{f}(p) + \mathrm{f}(p^2) + \dots) \tag{26}$$

and if moreover, f is completely multiplicative, then

$$\sum_{\mathbb{N}} \mathrm{f}(n) = \prod_p \frac{1}{1 - \mathrm{f}(p)}.$$

Proof of theorem 2.1: Let

$$P(x) := \prod_{p \le x} (\mathrm{f}(1) + \mathrm{f}(p) + \mathrm{f}(p^2) + \dots).$$

Here, each factor is absolutely convergent, and we have a finite number of factors, so

$$P(x) = \sum_{n \in A} \mathrm{f}(n)$$

where

$$A := \{n \in \mathbb{N} : \text{ all prime factors of } n \text{ are less than } x\}.$$

Now estimate the difference

$$\left| \sum_{\mathbb{N}} \mathrm{f}(n) - \sum_{A} \mathrm{f}(n) \right| \leq \sum_{\mathbb{N}-A} |\mathrm{f}(n)| \leq \sum_{n>x} |\mathrm{f}(n)|.$$

The last sum tends to zero as x tends to infinity, because it is the tail end of a convergent series.
The identity for completely multiplicative functions follows from the general Euler product expansion, because in this case each factor of the infinite product is a convergent geometric series. □

Remark 2.2
An infinite product is defined to be convergent, if the corresponding partial products form a convergent sequence, *which does NOT converge to zero.* The non-zero condition is imposed, because we want to take logs of infinite products. Note that it is automatically satisfied in the setting of theorem 2.1 for all completely multiplicative functions f (e. g. $\mathrm{f}(n) = n^{-s}$): The limit of a convergent geometric series cannot be zero.

Definition 2.3
Just a quick reminder: If S is an open subset of $\mathbb{C}$, a function $\mathrm{f} : \ S \to \mathbb{C}$ is called *complex differentiable* or *holomorphic on* S if the limit

$$\lim_{h \to 0} \frac{\mathrm{f}(z+h) - \mathrm{f}(z)}{h}$$

exists and is finite for all $z \in S$. If for all $z \in S$, f equals its own Taylor series in a small neighbourhood of z,

$$\mathrm{f}(z+h) = \sum_{n=0}^{\infty} \frac{\mathrm{f}^{(n)}(z)}{n!} h^n,$$

f is called *analytic on* S. We know from complex analysis that all functions holomorphic on S are analytic on S and vice versa (whereas for real functions, 'analytic' is a stronger condition than 'differentiable infinitely often').

Our next goal is that $\zeta(s)$ is analytic in the half-plane $\Re(s) > 1$.
Non-proof: Each n^{-s} is analytic, so the sum is analytic with derivative $\sum_{\mathbb{N}} \frac{-\log(n)}{n^s}$. Unfortunately, you can't guarantee that an infinite sum of analytic functions is analytic.
Warning example: Put for all $n \geq 0$

$$\mathrm{f}_n(x) = \frac{x^2}{(1+x^2)^n}.$$

We can sum the f_n, because we can sum a geometric progression.

$$\sum_{n=0}^{N} \mathrm{f}_n(x) = \frac{x^2}{1 - \frac{1}{1+x^2}} - \frac{x^2}{\left(1 - \frac{1}{1+x^2}\right)\left(1+x^2\right)^{N+1}}$$

Now *if* $x \neq 0$ we can let N tend to infinity, the second term vanishes, and the whole sum converges to $\mathrm{f}(x) = 1 + x^2$. But for $x = 0$, all $\mathrm{f}_n(0) = 0$, so the limit $\mathrm{f}(0) = \lim_n \mathrm{f}_n(x) = 0$, too. So the limit function f is not even continuous, although all the f_n are analytic in a neighbourhood of 0! If you look at the complex analogue, you get the same phenomenon in the region $\{s : \ |\arg(s)| < \pi/4\}$. One useful way to make sure that nothing goes wrong is the concept of *uniform convergence*.

2.2 Uniform Convergence

Definition 2.4
Given a non-empty subset S of $\mathbb{C}$, a function F and a sequence (F_N) of functions on S, we say that $\mathrm{F}_N(s)$ *converges to* $\mathrm{F}(s)$ if for all $\varepsilon > 0$ there exists $N_0 = N_0(\varepsilon, s)$ such that for all $N > N_0$,

$$|\mathrm{F}(s) - \mathrm{F}_N(s)| < \varepsilon.$$

We say that the sequence F_N *converges to* F *uniformly on* S, if for all $\varepsilon > 0$ there exists $N_0 = N_0(\varepsilon)$ such that for all $N > N_0$ *and for all* $s \in S$

$$|\mathrm{F}(s) - \mathrm{F}_N(s)| < \varepsilon.$$

Warning: the N_0 in the definition of uniform convergence must not depend on s.
Lots of nice properties of limits of uniformly convergent sequences of functions are inherited. The first example for this is

Proposition 2.5
Suppose that the sequence of functions (F_N) converges to F uniformly on S. If all F_N are continuous on S, then F is continuous on S.

Proof: Let $s_0 \in S$. Given $\varepsilon > 0$, choose N such that for all $s \in S$,

$$|\mathrm{F}(s) - \mathrm{F}_N(s)| < \frac{\varepsilon}{3}. \tag{27}$$

This is possible since the F_N are converging uniformly on S. Next, choose $\delta > 0$ such that for all $s \in S$ with $|s - s_0| < \delta$,

$$|\mathrm{F}_N(s) - \mathrm{F}_N(s_0)| < \frac{\varepsilon}{3}. \tag{28}$$

Now we have set the stage: For all $s \in S$ with $|s - s_0| < \delta$, we have

$$\begin{aligned} |\mathrm{F}(s) - \mathrm{F}(s_0)| &= |\mathrm{F}(s) - \mathrm{F}_N(s) + \mathrm{F}_N(s) - \mathrm{F}_N(s_0) + \mathrm{F}_N(s_0) - \mathrm{F}(s_0)| \\ &\leq |\mathrm{F}(s) - \mathrm{F}_N(s)| + |\mathrm{F}_N(s) - \mathrm{F}_N(s_0)| + |\mathrm{F}_N(s_0) - \mathrm{F}(s_0)| \\ &< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon. \end{aligned}$$

Here, we have used (27) twice, in order to estimate the first and third term, and (28) for the second term. This proves that F is continuous in an arbitrary $s_0 \in S$. □

Proposition 2.6

For every $\delta > 0$, the partial sums of the Riemann zeta function converge uniformly on $S_{1+\delta} := \{s \in \mathbb{C} : \ \Re(s) > 1 + \delta\}$. That is, 9.2.99

$$\sum_{n=1}^{N} \frac{1}{n^s} \to \zeta(s)$$

uniformly on $S_{1+\delta}$. Hence, by proposition 2.5 the Riemann zeta function is continuous on

$$\bigcup_{\delta>0} S_{1+\delta} = \{s \in \mathbb{C} : \ \Re(s) > 1\} = S_1.$$

Note that the convergence is not uniform on the whole of S_1.

Proof of proposition 2.6:

$$\left|\zeta(s) - \sum_{n=1}^{N} \frac{1}{n^s}\right| \ = \ \left|\sum_{n=N+1}^{\infty} \frac{1}{n^s}\right| \leq \sum_{n=N+1}^{\infty} \frac{1}{n^\sigma}$$

Now we need to show that this is less than ε in a way independent of σ. Use ESF!

$$\sum_{n=N+1}^{\infty} \frac{1}{n^\sigma} = \int_N^\infty \frac{1}{t^\sigma}\, dt + \int_N^\infty \{t\} \frac{1}{t^\sigma}'\, dt. \tag{29}$$

The first term in the right-hand side of equation (29) is

$$\begin{aligned} \left[\frac{t^{1-\sigma}}{1-\sigma}\right]_N^\infty \ &= \ \frac{-N^{1-\sigma}}{1-\sigma} \leq \frac{N^{1-\sigma}}{\delta} \\ &\leq \ \frac{1}{\delta N^\delta} < \varepsilon \end{aligned} \tag{30}$$

for all N large enough, i. e. $N > N_0(\delta, \varepsilon)$. Note that the inequality (30) depends only on δ, not on σ. The second term can be estimated by

$$\int_N^\infty \left(\frac{1}{t^\sigma}\right)' \, dt = \frac{1}{N^\sigma} \leq \frac{1}{N^{1+\delta}} < \varepsilon,$$

as soon as $N > N_0(\delta, \varepsilon)$ with the same N_0 as above (in fact, the second term is smaller than the first term). Hence for all N greater than $N_0(\delta, \varepsilon/2)$, the the series in equation (29) is less than ε. This completes the proof of proposition 2.6. □

2.3 The Zeta Function is Analytic

Theorem 2.7
Suppose $S \subseteq \mathbb{C}$ is open, and we have a function $\mathrm{F}: S \to \mathbb{C}$ and a sequence of functions $\mathrm{F}_N: S \to \mathbb{C}$ converging to F uniformly on S. If all the F_N are analytic, then F is analytic.

Example: $\mathrm{F}_N(s) = \sum_1^N \frac{1}{n^s}$ is analytic and converges uniformly to $\zeta(s)$ on every $S_{1+\delta},\ \delta > 0$ as in proposition 2.6, so by theorem 2.7, the Riemann zeta function is analytic in S_1.
Proof of theorem 2.7: Given a fixed point $a \in S$, we have to prove that F is analytic in a neighbourhood of a. We want to use complex analysis, in particular Cauchy's formula: Let γ be a closed simple curve, which is a finite join of smooth curves, such that $a \in \mathrm{Int}(\gamma)$ and the closure $\overline{\mathrm{Int}}(\gamma) \subseteq S$. Then Cauchy's formula says that for any function f which is analytic in S, and for any $b \in \mathrm{Int}(\gamma)$

$$\mathrm{f}(b) = \frac{1}{2\pi i} \int_\gamma \frac{\mathrm{f}(z)}{z-b}\, dz. \tag{31}$$

Since S is open, it contains a small disc around a. So we can choose γ as a sufficiently small circle around a contained in S, but our argument will work for any γ with the above properties. We will need to use the following

Lemma 2.8
Suppose a sequence of continuous functions $\mathrm{G}_N: \gamma \to \mathbb{C}$ converges to a function $\mathrm{G}: \gamma \to \mathbb{C}$ uniformly on γ. Then G is continuous and we have

$$\lim_{N\to\infty} \int_\gamma \mathrm{G}_N(s)\, ds = \int_\gamma \mathrm{G}(s)\, ds.$$

Proof of lemma 2.8: The continuity of G follows from proposition 2.5, so in particular G is integrable. Now

$$\begin{aligned} \left| \int_\gamma \mathrm{G}(s)\, ds - \int_\gamma \mathrm{G}_N(s)\, ds \right| &= \left| \int_\gamma \mathrm{G}(s) - \mathrm{G}_N(s)\, ds \right| \\ &\le \int_\gamma |\mathrm{G}(s) - \mathrm{G}_N(s)|\, ds \\ &\le \mathrm{length}(\gamma) \max_{s\in\gamma} |\mathrm{G}(s) - \mathrm{G}_N(s)|. \end{aligned}$$

The last quantity tends to zero by the definition of uniform convergence. This completes the proof of the lemma. □

Now the magic wand is waved! By hypothesis, the functions F_N are analytic in S. So for all $b \in \mathrm{Int}(\gamma) \subseteq S$ by Cauchy's formula (31)

$$\mathrm{F}_N(b) = \frac{1}{2\pi i} \int_\gamma \frac{\mathrm{F}_N(s)}{s-b}\, ds$$

Put $\mathrm{G}_N(s) := \frac{\mathrm{F}_N(s)}{s-b}$. Then we claim that G_N converge to $\mathrm{G}(s) := \frac{\mathrm{F}(s)}{s-b}$ uniformly on γ:

$$\begin{aligned} |\mathrm{G}(s) - \mathrm{G_N}(s)| &= \left| \frac{\mathrm{F}(s) - \mathrm{F}_N(s)}{s-b} \right| \\ &\leq C \max_{s\in\gamma} |\mathrm{F}(s) - \mathrm{F}_N(s)| \end{aligned}$$

where $C := \max_{s\in\gamma} \frac{1}{|s-b|}$. This proves that for all $b \in \mathrm{Int}(\gamma)$

$$\mathrm{F}(b) = \lim_N \mathrm{F}_N(b) = \lim_N \frac{1}{2\pi i} \int_\gamma \mathrm{G}_N(s)\, ds = \frac{1}{2\pi i} \int_\gamma \frac{\mathrm{F}(s)}{s-b}\, ds. \qquad (32)$$

Here, we have applied lemma 2.8 to interchange limit and integral in the last step. Finally, recall that any function F satisfying equation (32) (Cauchy's formula) in $\mathrm{Int}(\gamma)$ is analytic there. A proof of this step: For all $b \in \mathrm{Int}(\gamma)$,

$$\begin{aligned} \frac{\mathrm{F}(b+h) - \mathrm{F}(b)}{h} &= \frac{1}{2\pi i h} \int_\gamma \mathrm{F}(s) \left(\frac{1}{s-b-h} - \frac{1}{s-b} \right) ds \\ &= \frac{1}{2\pi i} \int_\gamma \frac{\mathrm{F}(s)}{(s-b)(s-b-h)}\, ds, \end{aligned}$$

the h's cancel! In the last integral, the limit $h \to 0$ may be taken and gives the derivative. Strictly speaking, we would have to check for uniform convergence (as with the G_N above) to be able to apply lemma 2.8 again. □

Corollary 2.9
For all s with $\Re(s) > 1$,

$$\frac{d}{ds}\, \zeta(s) = \sum_{\mathbb{N}} \frac{\log(n)}{n^s}.$$

Problem: the real action takes place to the left of $\Re(s) = 1$. But our definition of the zeta function does not work there!

2.4 Analytic continuation of the Zeta Function

Further reading on this topic:

> Titchmarsh: ... Riemann zeta function
> (updated by Roger Heath-Brown).

Apostol is a little bit ponderous on this - he does the most general zeta function that he can.

An easy example: Consider the function

$$\mathrm{g}(s) = 1 + s + s^2 + \dots$$

The series converges for $|s| < 1$. Claim: g can be continued to a function which is analytic on the whole of $\mathbb{C}$ except for a simple pole at $s = 1$. Proof: For $|s| < 1$, $\mathrm{g}(s) = \frac{-1}{s-1}$. The latter expression is defined on $\mathbb{C}$ apart from a simple pole at $s = 1$ with residue -1. BUT: g is *not* defined by the series for $|s| \geq 1$. 12.2.99

Theorem 2.10
The Riemann zeta function is analytic on the whole of the complex plane with exception of a simple pole at $s = 1$, with residue 1.

Proof: In this section, we will only prove that there is an analytic continuation to the half-plane $\Re(s) > 0$. For this, we will see three methods of proof (theorem 2.10 will then be an immediate consequence of the functional equation which we will prove in chapter 3). The three methods are

1. Standard - the one you will find in the books.
2. A very elegant one, which you will do in exercise 16.
3. One which I do not claim to have invented - I rather think, it must be known to the experts. But I did not find it in the books.

1. The standard method: Use the ESF.
But be careful: ESF is about finite intervals!

$$\sum_{n=2}^{N} \frac{1}{n^s} = \int_1^N t^{-s}\, dt + \int_1^N \frac{-s\{t\}}{t^{s+1}}\, dt \tag{33}$$

The first term is

$$\left[\frac{t^{1-s}}{1-s}\right]_1^N = \frac{N^{1-s}}{1-s} - \frac{1}{1-s},$$

and since we suppose $\Re(s) > 1$, we get $N^{1-s} \to 0$ as N tends to infinity. The second term in equation (33) converges too, as N tends to infinity, since

$$\int_1^\infty \frac{|s|}{t^{\sigma+1}}\, dt < \infty$$

gives an upper bound. So we are justified in writing

$$\zeta(s) = 1 + \sum_{n=2}^{\infty} \frac{1}{n^s} = 1 - \frac{1}{1-s} - s\int_1^\infty \frac{\{t\}}{t^{1+s}}\, dt. \tag{34}$$

We claim: the integral in equation (34) represents an analytic function in the range $\Re(s) > 0$. By this claim, we get the analytic continuation of ζ to the half-plane $\Re(s) > 0$. There it is analytic, apart from a simple pole at $s = 1$ with residue 1.
Proof of claim: write

$$\mathrm{I}(s) = \sum_{n=1}^{\infty} \mathrm{f}_n(s), \tag{35}$$

where $\mathrm{f}_n(s) := \int_n^{n+1} \frac{\{t\}}{t^{s+1}}\, dt$. We will prove that for any $\delta > 0$,

- *a)* the series for $\mathrm{I}(s)$ converges uniformly on $\Re(s) > \delta$ and
- *b)* each f_n is analytic in the range $\Re(s) > \delta$.

Then we may apply theorem 2.7 to complete the proof that $\mathrm{I}(s)$ is analytic on $\Re(s) > 0$. As to a),

$$\begin{aligned}
\left|\mathrm{I}(s) - \sum_{n=1}^{N} \mathrm{f}_n(s)\right| &= \left|\sum_{n=N+1}^{\infty} \mathrm{f}_n(s)\right| \le \sum_{N+1}^{\infty} |\mathrm{f}_n(s)| \\
&\le \int_{N+1}^{\infty} \frac{1}{t^{\sigma+1}}\, dt = \left[\frac{t^{-\sigma}}{-\sigma}\right]_{N+1}^{\infty} \\
&= \frac{(N+1)^{-\sigma}}{\sigma},
\end{aligned}$$

and in absolute value, this is smaller than $\frac{1}{\delta(N+1)^\delta}$, so it tends to zero. And the bound depends on δ only, not on σ or s! This proves uniform convergence. As to claim b), consider the difference quotient

$$\frac{\mathrm{f}_n(s+h)-\mathrm{f}_n(s)}{h} = \frac{1}{h}\int_n^{n+1} \frac{\{t\}}{t^{s+1}}\left(\frac{1}{t^h}-1\right)\,dt. \tag{36}$$

Use a first-order Taylor approximation of the exponential:

$$\begin{aligned} t^{-h} &= e^{-h\log(t)} = 1 - h\log(t) + \mathrm{f}(h,t), \qquad \text{where} \\ \mathrm{f}(h,t) &= O((h\log(t))^2). \end{aligned} \tag{37}$$

Put this into equation (36):

$$\frac{1}{h}\left(\mathrm{f}_n(s+h)-\mathrm{f}_n(s)\right) = \int_n^{n+1} \frac{\{t\}}{t^{s+1}}\left(-\log(t)+\frac{1}{h}\mathrm{f}(h,t)\right)\,dt. \tag{38}$$

We can guess the derivative:

$$\left|\frac{1}{h}\left(\mathrm{f}_n(s+h)-\mathrm{f}_n(s)\right) + \int_n^{n+1}\frac{\{t\}}{t^{s+1}}\log(t)\,dt\right| \le \int_n^{n+1}\frac{1}{ht^{\sigma+1}}|\mathrm{f}(h,t)|\,dt. \tag{39}$$

The right-hand side tends to zero as $h\to 0$ by (37). This completes the first proof for the analytic continuation of the zeta function into $\Re(s)>0$. □

Why was it necessary to split the integral from 1 to ∞ into all these subintegrals? Answer: The Taylor approximation in (37) is only valid for bounded values of $h\log(t)$. If we had stuck to $\int_1^\infty$ all the way, t would be arbitrary and the quantity $h\log(t)$ would be unbounded. By the splitting of the integral, we had only to consider $t\in[n,n+1]$ for a *fixed* n.

These are treacherous waters!

3. GE's method: Has the additional benefit of giving a continuation to the whole of the complex plane (with exception of the simple pole at $s=1$). Consider

$$\int_1^\infty x^{-s}\,dx = \frac{-1}{1-s} = \frac{1}{s-1}.$$

Subtract this from zeta, to remove the pole! For $\Re(s) > 1$,

$$\begin{aligned}\zeta(s) - \frac{1}{s-1} &= \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{\infty} \int_n^{n+1} x^{-s}\, dx \\ &= \sum_{\mathbb{N}} \left(\frac{1}{n^s} - \int_0^1 (n+x)^{-s}\, dx \right) \\ &= \sum_{\mathbb{N}} \frac{1}{n^s} \left(1 - \int_0^1 \left(1 + \frac{x}{n}\right)^{-s} dx \right). \end{aligned} \tag{40}$$

The re-arrangement is ok, because the sums involved converge absolutely in $\Re(s) > 1$. Now assume that we have continued the zeta function to the domain $\Re(s) > 1-K$, for some integer $K \geq 0$. We want to continue it further to $\Re(s) > -K$. To do this, put $h := x/n$ and use a Taylor approximation of

$$\mathrm{f}_s(h) := (1+h)^{-s}$$

of order K. Recall that the Taylor polynomial of degree K for f_s in $h = 0$ is defined by

$$T_{\mathrm{f},s,K}(h) := \sum_{k=0}^{K} \frac{\mathrm{f}_s^{(k)}(0)}{k!} h^k. \tag{41}$$

(If you only want the continuation to $\Re(s) > 0$, think of $K = 1$: The Taylor polynomial for $(1 + x/n)^{-s}$ in this case is simply $1 - \frac{sx}{n}$, the error term is $O(n^{-2})$. Put this into equation (40), and you get a series convergent for $\Re(s) > 0$). We have to calculate higher derivatives of f_s in $h = 0$. They are given by equating $h = 0$ in

$$\mathrm{f}_s^{(k)}(h) = \frac{(-1)^k (s+k-1)(s+k-2) \cdot \ldots \cdot (s+1)s}{(h+1)^k}\, \mathrm{f}_s(h) \tag{42}$$

(it is easy to prove the relation (42) by induction on k). Since f_s is analytic in the neighbourhood of $h = 0$, we have an estimate for the error term:

$$|\mathrm{f}_s(h) - T_{\mathrm{f},s,K}(h)| \leq \frac{|\mathrm{f}_s^{(K+1)}(h')|}{(K+1)!} |h|^{K+1} \tag{43}$$

for some h' with $|h'| < |h|$. For bounded values of s, this is an $O(|h|^{K+1})$. Use the Taylor polynomial with $h = x/n$ in equation (40). We evaluate the inner integral first:

$$\int_0^1 \left(1+\frac{x}{n}\right)^{-s}\, dx = 1 + \sum_{k=1}^{K} \frac{\mathrm{f}_s^{(k)}(0)}{(k+1)!\, n^k} + O\left(\frac{1}{n^{K+1}}\right). \tag{44}$$

Putting this into equation (40) gives the nice identity

$$\begin{aligned} \zeta(s) - \frac{1}{s-1} &= -\sum_{k=1}^{K} \frac{(-1)^k (s+k-1)\cdot \ldots \cdot (s+1)s}{(k+1)!}\, \zeta(s+k) \\ &\quad + \sum_{n=1}^{\infty} \frac{1}{n^s} \int_0^1 T_{\mathrm{f},s,K}\left(\frac{x}{n}\right) - \left(1+\frac{x}{n}\right)^{-s}\, dx. \end{aligned} \tag{45}$$

The last sum converges by (43), and for all $s \neq 0, -1, -2, \ldots$ the values $\zeta(s+1), \zeta(s+2), \ldots, \zeta(s+K-1)$ are all defined by hypothesis, giving the continuation of the zeta function to $\Re(s) > -K$. In case $s = -m = 0, -1, -2, \ldots, 1-K$, one of the arguments of ζ in (45) becomes 1, but this is no problem, since the pole is cancelled out by the appropriate factor $(s+m)$ in the coefficient (the right-hand side of (45) has a removable singularity there).
Thus, we get an analytic continuation of the zeta function to

$$\Re(s) > -1, -2, \ldots,$$

in fact, to the whole of the complex plane! But in the next section, we will see a better method to achieve this: via the *functional equation*. □

Too late for beginning with the functional equation - here's a nice formula!

Theorem 2.11
If $s = \sigma + it$, $\sigma > 1$, then

$$\log(\zeta(s)) = s \int_2^{\infty} \frac{\pi(x)}{x(x^s - 1)}\, dx.$$

Proof: See exercise 29, hint: You will obtain a sum over all primes. Convert this to a sum over all natural numbers using

$$\pi(n) - \pi(n-1) = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

In Q19 (MAPLE): Change mod to abs. Q 7,8,9,10,13,14 in by Fri wk 5.

3 The Functional Equation

15.2.99

3.1 The Gamma Function

It is amazing how the Gamma function helps us to understand the zeta function.

Definition 3.1
For every s with $\Re(s) > 0$, the integral

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

exists and is called the Gamma function $\Gamma(s)$.

The integral exists in this range by comparison with the real Gamma function, see MTH2A32. We claim: Γ is analytic in $\Re(s) > 0$.
The proof is left as an exercise - proceed along the following steps:

I : $\Gamma(s) = \sum_0^\infty \Gamma_n(s)$, where $\Gamma_n(s) := \int_n^{n+1} e^{-t} t^{s-1}\, dt$,
II : $\sum_0^N \Gamma_n(s) \to \Gamma(s)$
uniformly on $\Re(s) > \delta$, for any fixed $\delta > 0$,
III : Prove that Γ_n is analytic.

All these steps are very similar to the argument for $\int_0^\infty \frac{\{t\}}{t^{s+1}}\, dt$. Later on, another (better) proof will be given.

Proposition 3.2
The Gamma function has the following properties:

1. For all s with $\Re(s) > 0$,

$$\Gamma(s+1) = s\Gamma(s).$$

2. For all integers $N \geq 0$,

$$\Gamma(N+1) = N!.$$

Proof of 1:

$$\Gamma(s+1) = \int_0^\infty e^{-t} t^s\, dt = [-e^{-t} t^s]_0^\infty + s \int_0^\infty e^{-t} t^{s-1}\, dt.$$

The bracket term vanishes at $t = 0$ because $\Re(s) > 0$. Item 2. follows from 1. by induction together with $\Gamma(1) = 1$. $\square$

Now write

$$\Gamma(s) = \frac{1}{s}\Gamma(s+1). \tag{46}$$

The right-hand side is defined for $\Re(s) > -1$ apart from $s = 0$, where it has a simple pole with residue $\Gamma(1) = 1$. Iterate this:

$$\Gamma(s) = \frac{1}{s(s+1)}\Gamma(s+2). \tag{47}$$

The right-hand side of (47) is defined for $\Re(s) > -2$, apart from $s = 0, -1$, where we have simple poles again. In this way, we can continue the Gamma function to the whole plane, where it is analytic apart from simple poles at $0, -1, -2, \ldots$.
Our goal throughout this chapter will be the following theorem:

Theorem 3.3 (THE Functional Equation)
Define

$$\mathrm{F}(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

known to exist for $\Re(s) > 0$. Then F satisfies the functional equation

$$\mathrm{F}(1-s) = \mathrm{F}(s).$$

Corollary 3.4
1. F is analytic in the whole complex plane apart from poles at 1 and 0.
2. If we know that Γ never vanishes, then ζ can be continued to the whole plane, where it is analytic apart from a simple pole at $s = 1$.

For we can expand theorem 3.3, giving

$$\begin{aligned} \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) &= \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s), \\ \zeta(1-s) &= \frac{\pi^{-s+\frac{1}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)}{\Gamma\left(\frac{1-s}{2}\right)}. \end{aligned} \tag{48}$$

Example: We know that Γ has a simple pole at $-m$ for $m \in \mathbb{N}$. So, for all $m \in \mathbb{N}$,

$$\zeta(-2m) = 0 \tag{49}$$

(we have $1 - s = -2m \iff s = 2m + 1$, we know $\zeta \neq 0$ for $\Re(s) > 1$ by the Euler product expansion and we assumed $\Gamma \neq 0$ everywhere). The case $1 - s = 0$, i. e. $s = 1$ is different: There, the right-hand side has a simple pole in the numerator too (in ζ), cancelling the one in Γ. Thus ζ is analytic and nonzero in $s = 0$. Picture: By the functional equation, all we need to know is the values of ζ for $\Re(s) \geq 1/2$. We found $\zeta(-2m) = 0$ for all $m \in \mathbb{N}$. There are no more zeros of ζ with $\Re(s) < 0$, because Γ has no other poles (just look at equation (48)). Also, $\zeta(s) \neq 0$ for $\Re(s) > 1$ because of the Euler product expansion (see remark 2.2). So any other zero of ζ must lie in the 'critical strip' $0 \leq \Re(s) \leq 1$.
Riemann stated without proof that

> all zeros of ζ in the critical strip have $\Re(s) = 1/2$ (the 'Riemann Hypothesis').

This has not been proved yet. A very important unsolved problem - see the talk by Michael Berry, FRS. All the zeros found thus far lie on the line $\Re(s) = 1/2$, and they are all simple.

3.2 Fourier Analysis

For the proof of the functional equation - theorem 3.3 - we will need some Fourier analysis.

Definition 3.5
The *Schwartz space* $\mathbb{S}$ is the set of functions $\mathrm{f} : \mathbb{R} \to \mathbb{C}$ which are infinitely differentiable, and whose derivatives $\mathrm{f}^{(n)}$ (including $\mathrm{f}^{(0)} = f$) all satisfy

$$(1 + |x|)^m \, \mathrm{f}^{(n)} = O(1) \tag{50}$$

for all $m \in \mathbb{N}$. The bound may depend upon m and n. Example: $e^{-x^2} \in \mathbb{S}$. Note that $\mathbb{S}$ is a complex vector space, and that all functions $\mathrm{f} \in \mathbb{S}$ are integrable:

$$\left| \int_{\mathbb{R}} \mathrm{f}(x) \, dx \right| \leq \int_{\mathbb{R}} |\mathrm{f}(x)| \, dx \leq C \int_{\mathbb{R}} \frac{1}{(1 + |x|)^2} \, dx$$

(take $n = 0$ and $m = 2$ in equation (50)). Now define for all $\mathrm{f} \in \mathbb{S}$ the *Fourier transform of* f by

$$\hat{\mathrm{f}}(y) := \int_{\mathbb{R}} \mathrm{f}(x) \exp(-2\pi i x y)\, dx.$$

This integral exists for the same reason as above:

$$|\hat{\mathrm{f}}(y)| \leq \int_{\mathbb{R}} |\mathrm{f}| < \infty,$$

in fact $\hat{\mathrm{f}} \in \mathbb{S}$ again (apply equation (50) with $m + n$ to get the bound for $\hat{\mathrm{f}}^{(n)}$). Thus $\mathrm{f} \to \hat{\mathrm{f}}$ is a linear map from $\mathbb{S}$ to $\mathbb{S}$.
Periodicity: A function g on $\mathbb{R}$ is *periodic* if $\mathrm{g}(x) = \mathrm{g}(x + m)$ for all $m \in \mathbb{Z}$ and for all $x \in \mathbb{R}$. Suppose g is periodic and piecewise continuous. Then its *k-th Fourier coefficient* is defined for $k \in \mathbb{Z}$ as

$$c_k := \int_0^1 \mathrm{g}(x) e^{-2\pi i k x}\, dx.$$

Lemma 3.6
If g is periodic and differentiable infinitely often, then there exists $C > 0$, 16.2.99
depending only upon g, such that

$$|c_k| \leq \frac{C}{k^2}$$

for all $k \neq 0$.

Proof: Integrate by parts!

$$c_k \;=\; \left[\frac{-e^{-2\pi i k x}\mathrm{g}(x)}{2\pi i k}\right]_0^1 + \int_0^1 \frac{-e^{-2\pi i k x}\mathrm{g}'(x)}{2\pi i k}\, dx.$$

Now the bracket term vanishes because g is periodic. Integrate by parts again, so that k^2 appears in the denominator, then estimate the exponential by 1. Put $C = \int_0^1 |g''| dx/(4\pi^2)$. □

Theorem 3.7
Any function g which is periodic and differentiable infinitely often has a Fourier series expansion

$$\mathrm{g}(x) = \sum_{k \in \mathbb{Z}} c_k e^{2\pi i k x}$$

which is uniformly convergent.

Proof that the Fourier series converges uniformly: Call G the Fourier series of g, and apply lemma 3.6.

$$\left| \mathrm{G}(x) - \sum_{k=-n}^{n} c_k e^{2\pi i k x} \right| \leq C \sum_{|k|>n} \frac{1}{k^2},$$

where the last sum tends to zero independent of x (the constant C depends only on g). The equality $\mathrm{g}(x) = \mathrm{G}(x)$ for all $x \in [0,1]$ is not so easy to prove. Since this is not really part of the course, the proof is done in Appendix **??**. □

Theorem 3.8 (Poisson Summation Formula - PSF)
Suppose f belongs to the Schwartz space (see definition 3.5. Then

$$\sum_{\mathbb{Z}} \mathrm{f}(m) = \sum_{\mathbb{Z}} \hat{\mathrm{f}}(m).$$

Proof: Let

$$\mathrm{g}(x) := \sum_{\mathbb{Z}} \mathrm{f}(x+m).$$

Clearly g is periodic. But g is also differentiable infinitely often:

$$\left| \sum_{|m|>N} \mathrm{f}^{(n)}(m) \right| \leq \sum_{|m|>N} \left| \mathrm{f}^{(n)}(m) \right| \leq C \sum_{|m|>N} \frac{1}{(1+|x+m|)^2},$$

where the last series tends to zero independent of x. So the n-th derivatives of the partial sums converge uniformly, for all $n \geq 0$. Now we cannot use theorem 2.7, since the f_n are not necessarily analytic. But we can use lemma 2.8: Let γ be the real interval $[1, x]$, let the functions G_N be the partial sums of the derivatives $\mathrm{f}_n{}'$ and use the fundamental theorem of calculus:

$$\frac{\mathrm{d}}{\mathrm{d}x} \int_0^x \mathrm{G}_N(t)\, dt = \mathrm{G}_N(x) - \mathrm{G}_N(0).$$

Here, the integral converges to $\mathrm{g}(x) - \mathrm{g}(0)$ as $N \to \infty$. (and similarly for higher derivatives, using induction). Therefore g is n times differentiable and its n-th derivative is the limit of that of the partial sums. So we may do Fourier analysis!

Let c_k be the k-th Fourier coefficient of g, so by theorem 3.7

$$\mathrm{g}(x) = \sum_{k\in\mathbb{Z}} c_k e^{2\pi ikx}, \qquad \mathrm{g}(0) = \sum_{k\in\mathbb{Z}} c_k. \tag{51}$$

On the other hand,

$$\begin{aligned} c_k &= \int_0^1 \mathrm{g}(x)e^{-2\pi ikx}\,dx = \int_0^1 \sum_{m\in\mathbb{Z}} \mathrm{f}(x+m)e^{-2\pi ikx}\,dx \\ &= \sum_{m\in\mathbb{Z}} \int_0^1 \mathrm{f}(x+m)e^{-2\pi ikx}\,dx. \end{aligned}$$

This interchange of sum and integral is justified, because the series for g converges uniformly (lemma 2.8 again). We multiply each summand by a factor of $e^{-2\pi ikm} = 1$:

$$\begin{aligned} c_k &= \sum_{m\in\mathbb{Z}} \int_0^1 \mathrm{f}(x+m)e^{-2\pi ik(x+m)}\,dx = \int_{\mathbb{R}} \mathrm{f}(x)e^{-2\pi ikx}\,dx \\ &= \hat{\mathrm{f}}(k). \end{aligned}$$

Now use equation (51):

$$\sum_{m\in\mathbb{Z}} \mathrm{f}(m) = \mathrm{g}(0) = \sum_{k\in\mathbb{Z}} c_k = \sum_{k\in\mathbb{Z}} \hat{\mathrm{f}}(k).$$

This completes the proof of the Poisson summation formula. □

Lemma 3.9
If $\mathrm{f}(y) = e^{-\pi y^2}$, then $\hat{\mathrm{f}}(y) = \mathrm{f}(y)$.

Proof:

$$\hat{\mathrm{f}}(y) = \int_{\mathbb{R}} e^{-\pi y^2} e^{-2\pi ikxy}\,dx.$$

The idea is to complete the square:

$$-\pi(x^2 + 2ixy) = -\pi[(x+iy)^2 + y^2].$$

So the Fourier transform of f is

$$\hat{\mathrm{f}}(y) = e^{-\pi y^2} \int_{\mathbb{R}} e^{-\pi(x+iy)^2}\, dx.$$

Call I(y) the integral $\int_{\mathbb{R}} \exp(-\pi(x+iy)^2)\, dx$. We know that I(0) is One. What happens if $y \neq 0$? Fix some large N and consider the following paths:

$$\begin{array}{ll} \gamma_1 := [-N, N], & \gamma_2 := [N, N+yi], \\ \gamma_3 := [N+yi, -N+yi], & \gamma_4 := [-N+yi, -N]. \end{array}$$

Put $\gamma := \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$ (a rectangle). Since $e^{-\pi z^2}$ is an analytic function in the whole of the complex plane, we have for any N

$$\int_{\gamma} e^{-\pi z^2}\, dz = 0.$$

Now as $N \to \infty$, the integral of $e^{-\pi z^2}$ over γ_1 tends to I(0) = 1, the integral over γ_3 tends to $-\mathrm{I}(y)$ and the integrals over γ_2 and γ_4 both tend to 0, by the standard estimate. This completes the proof of lemma 3.9. □

> Could we make up an argument involving only real integrals? Sure, we could have sin and cos and real part etc etc. But I do not see at all how this could work - certainly some clever tricks would be necessary. No chance that it would be more elegant than complex integration.

3.3 The Theta Function

Theorem 3.10
Define for real $y > 0$ the theta function by

$$\theta(y) := \sum_{\mathbb{Z}} e^{-n^2 \pi y}.$$

Then

$$\theta\left(\frac{1}{y}\right) = \sqrt{y}\, \theta(y). \tag{52}$$

Proof: This is not obvious! Does not even look possible. But it really makes the functional equation for the zeta function work.
Note that the series defining θ converges uniformly in the range $y > \delta$ for any fixed $\delta > 0$ (see also exercise 30). Fix some real $b > 0$ and define with our old friend f of lemma 3.9

$$\mathrm{f}_b(y) := \mathrm{f}(by) = e^{-\pi b^2 y^2}.$$

Of course f_b is in the Schwartz space, so we may apply the Poisson summation formula 3.8

$$\sum_{\mathbb{Z}} \mathrm{f}_b(n) = \sum_{\mathbb{Z}} \hat{\mathrm{f}}_b(n). \tag{53}$$

What is $\hat{\mathrm{f}}_b(y)$?

$$\hat{\mathrm{f}}_b(y) = \int_{\mathbb{R}} \mathrm{f}_b(x) e^{-2\pi i x y}\, dx = \int_{\mathbb{R}} \mathrm{f}(bx) e^{-2\pi i x y}\, dx. \tag{54}$$

Now put $u := bx$, so $dx = \frac{1}{b} du$: Equation (54) becomes

$$\hat{\mathrm{f}}_b(y) = \frac{1}{b} \int_{\mathbb{R}} \mathrm{f}(u) e^{-2\pi i u \frac{y}{b}}\, du = \frac{1}{b} \hat{\mathrm{f}}\left(\frac{y}{b}\right). \tag{55}$$

We apply lemma 3.9 to this equation, so

$$\hat{\mathrm{f}}_b(y) = \frac{1}{b} \mathrm{f}\left(\frac{y}{b}\right). \tag{56}$$

Put this result into equation (53) and insert the definition of f again:

$$\sum_{\mathbb{Z}} e^{-\pi b^2 m^2} = \frac{1}{b} \sum_{\mathbb{Z}} e^{-\pi \frac{m^2}{b^2}}.$$

Finally, put $b := \sqrt{y}$ and the functional equation for θ emerges. □

Now we are ready for the proof of theorem 3.3! We begin with 19.2.99

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty e^{-x} x^{\frac{s}{2}-1}\, dx = \int_0^\infty e^{-x} x^{\frac{s}{2}}\, \frac{dx}{x}. \tag{57}$$

So, in the domain $\Re(s) > 1 + \delta$,

$$\mathrm{F}(s) = \pi^{-\frac{s}{2}} \sum_{n\in\mathbb{N}} \int_0^\infty n^{-s} e^{-x} x^{\frac{s}{2}}\, \frac{dx}{x}. \tag{58}$$

Next, replace x by $\pi n^2 y$ in the integral. This means $dx/x = dy/y$, and we get after some cancelling

$$\mathrm{F}(s) = \int_0^\infty \sum_{n\in\mathbb{N}} e^{-\pi n^2 y} y^{\frac{s}{2}} \frac{dy}{y}. \tag{59}$$

The interchange of integral and sum is ok, because the series for the zeta function converges uniformly on $\Re(s) > 1 + \delta$. Define

$$\mathrm{g}(y) := \sum_{n\in\mathbb{N}} e^{-\pi n^2 y} = \frac{\theta(y) - 1}{2}. \tag{60}$$

Split the integral in equation (59):

$$\mathrm{F}(s) = \int_1^\infty y^{\frac{s}{2}} \mathrm{g}(y) \frac{dy}{y} + \int_0^1 y^{\frac{s}{2}} \mathrm{g}(y) \frac{dy}{y}. \tag{61}$$

In the second integral, change y to $z = y^{-1}$. Thus it becomes an integral from ∞ to 1, and $dz/z = -dy/y$ (this minus sign goes into reversing the boundaries):

$$\mathrm{F}(s) = \int_1^\infty y^{\frac{s}{2}} \mathrm{g}(y) \frac{dy}{y} + \int_1^\infty z^{-\frac{s}{2}} \mathrm{g}(z^{-1}) \frac{dz}{z}. \tag{62}$$

Now our preparations come into play: By theorem 3.10, which we proved using the Poisson summation formula, theorem 3.8

$$\begin{aligned} \mathrm{g}(y^{-1}) &= \frac{\theta(y^{-1}) - 1}{2} = \frac{\sqrt{y}\,\theta(y) - 1}{2} \\ &= \frac{\sqrt{y}\,(\theta(y) - 1) + \sqrt{y} - 1}{2} = \sqrt{y}\,\mathrm{g}(y) + \frac{\sqrt{y} - 1}{2}. \end{aligned} \tag{63}$$

Put this into equation (62)

$$\begin{aligned} \mathrm{F}(s) &= \int_1^\infty y^{\frac{s}{2}} \mathrm{g}(y) \frac{dy}{y} + \int_1^\infty y^{\frac{1-s}{2}} \mathrm{g}(y) \frac{dy}{y} \\ &\quad + \frac{1}{2} \int_1^\infty y^{-\frac{s}{2}} \left(y^{\frac{1}{2}} - 1 \right) \frac{dy}{y}. \end{aligned} \tag{64}$$

We evaluate the third integral I_3 in equation (64):

$$\begin{aligned} 2\mathrm{I}_3 &= \int_1^\infty y^{-\frac{1+s}{2}} - y^{-\frac{2+s}{2}} \, dy = \left[\frac{y^{\frac{1-s}{2}}}{\frac{1-s}{2}} - \frac{y^{-\frac{s}{2}}}{-\frac{s}{2}} \right]_1^\infty \\ &= 2 \left(\frac{-1}{1-s} - \frac{1}{s} \right) = 2 \left(\frac{1}{s-1} - \frac{1}{s} \right). \end{aligned} \tag{65}$$

Claim: For all $z \in \mathbb{C}$, the function

$$\mathrm{G}(z) = \int_1^\infty y^z \mathrm{g}(y) \, dy \qquad (*)$$

is analytic. Assuming that this is true, we have by equations (64) and (65)

$$\mathrm{F}(s) = \mathrm{G}\left(\frac{s}{2} \right) + \mathrm{G}\left(\frac{1-s}{2} \right) + \frac{1}{s-1} - \frac{1}{s}.$$

which shows that F is analytic for all $s \in \mathbb{C}$ apart from simple poles at $s = 1$ and $s = 0$, *and it completes the proof of theorem 3.3*!
So let us prove the claim $(*)$: Write $\mathrm{G}(z) = \sum_{n \in \mathbb{N}} \mathrm{G}_n(z)$, where

$$\mathrm{G}_n(z) := \int_n^{n+1} y^z \mathrm{g}(y) \, dy.$$

We will prove that the G_n are all analytic functions on all of $\mathbb{C}$. Consider the difference quotient for $\mathrm{G}_n(z)$ (exactly as in the standard proof for the analytic continuation of zeta):

$$\frac{1}{h} \int_n^{n+1} y^z \left(y^h - 1 \right) \mathrm{g}(y) \, dy = \frac{1}{h} \int_n^{n+1} y^z \mathrm{g}(y) (1 + h \log(y) + \rho(h, y) - 1) \, dy$$

where $\rho(h, y) = O(h^2)$ for bounded values of y. So one may divide by h and take the limit $h \to 0$.

Next, we want to prove that the partial sums of the G_n converge uniformly on a suitable domain. Consider z in the half-plane $\Re(z) < K$ for some fixed K. There

$$\left| \int_N^\infty y^z \mathrm{g}(y)\, dy \right| \leq \int_N^\infty y^K |\mathrm{g}(y)|\, dy. \tag{66}$$

Now we estimate $|\mathrm{g}(y)|$:

$$|\mathrm{g}(y)| = \sum_{n \in \mathbb{N}} e^{-\pi n^2 y} \leq \sum_{n=1}^{\infty} e^{-\pi n y} = \frac{e^{-\pi y}}{1 - e^{-\pi y}}.$$

The denominator is clearly bounded below for $1 < y$, so the right-hand side of inequality (66) is finite for e. g. $N = 1$. As an immediate consequence, the integrals from N to infinity must tend to zero, and all this was independent of s. Now we may apply theorem 2.7 and deduce that G is analytic on the half-plane $\Re(s) < K$. Since K was arbitrary, G is analytic on the whole complex plane. □

3.4 The Gamma Function Revisited

22.2.99

We have seen that ζ and Γ go together like Laurel & Hardy, Batman & Robin, or Hardy & Wright. We need to know properties of Γ (e. g. $\Gamma(s) \neq 0$ for all s) in order to understand ζ better.

Theorem 3.11 (W like Weierstrass)
Define a function f(s) by

$$\mathrm{f}(s) = se^{\gamma s} \prod_1^\infty \left[\left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}} \right] \tag{67}$$

where γ is the EULER-MASCHERONI constant. Then f(s) is an analytic function on the whole of the complex plane, and it has zeros in $0, -1, -2, -3, \ldots$ *only.*

Proof of theorem W:
Consider the function

$$\mathrm{g}(s) := \sum_1^\infty \mathrm{g}_n(s) := \sum_1^\infty \left[\log\left(1 + \frac{s}{n}\right) - \frac{s}{n} \right]. \tag{68}$$

Each g_n is analytic away from $-1, -2, -3, \ldots$. We want to prove that the series of the g_n converges uniformly on $\{s \in \mathbb{C} : \ |s| < K\}$ for every fixed $K > 0$. Choose $N > 2K$, so for all $n \geq N$, $|s/n| \leq 1/2$, and

$$\log\left(1 + \frac{s}{n}\right) = \frac{s}{n} - \frac{1}{2}\left(\frac{s}{n}\right)^2 + \frac{1}{3}\left(\frac{s}{n}\right)^3 - \ldots$$

Thus we can estimate $\mathrm{g}_n(s)$ for all these s and n:

$$\begin{aligned} |\mathrm{g}_n(s)| &\leq \frac{1}{2}\left|\frac{s}{n}\right|^2 + \frac{1}{3}\left|\frac{s}{n}\right|^3 + \ldots \\ &\leq \frac{|s|^2}{n^2} \frac{1}{1 - \frac{|s|}{n}} \leq 2\frac{|s|^2}{n^2} < \frac{2K^2}{n^2}. \end{aligned}$$

We can sum this for $n = N$ to infinity:

$$\left| \sum_{n=N}^\infty \mathrm{g}_n(s) \right| \leq \sum_N^\infty \frac{2K^2}{n^2},$$

and the latter is arbitrarily small if N is large, as the tail end of a convergent series. So the series of the analytic functions $\mathrm{g}_n(s)$ converges uniformly on $|s| < K$ for arbitrary K. By theorem 2.7, we deduce that the limit $\mathrm{g}(s)$ is analytic for all s not equal to $-1, -2, -3, \ldots$. The same holds for

$$\exp(\mathrm{g}(s)) = \prod_1^\infty \left[\left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}} \right].$$

After multiplying this by $se^{\gamma s}$, we see that $\mathrm{f}(s)$ is an analytic function away from $-1, -2, -3, \ldots$ It is clear that f has zeros in all these points, so that $\log(\mathrm{f}(s))$ has a singularity there. Conversely, for all s away from these obvious zeros, we have shown that $\log(\mathrm{f}(s))$ is analytic, so that f cannot be zero elsewhere. Finally, for some fixed $m \in \mathbb{N}$, consider the infinite product defining f without the factor corresponding to $n = m$. The same estimates as above show that the log of this is analytic in $s = -m$, so f is analytic in $s = -m$ as well. □

Corollary 3.12
The zeros of f as in theorem 3.11 are all simple, and the function

$$\frac{1}{\mathrm{f}(s)} = \frac{1}{s} e^{-\gamma s} \prod_1^\infty \left(1 + \frac{s}{n}\right)^{-1} e^{\frac{s}{n}}$$

is analytic on $\mathbb{C}$ apart from simple poles at $0, -1, -2, \ldots$. The function $1/\mathrm{f}$ has no zeros at all (because f has no poles).

Theorem 3.13 (E like Euler)
For all $s \neq 0, -1, -2, \ldots$ holds

$$\frac{1}{\mathrm{f}(s)} = \frac{1}{s} \prod_1^\infty \left[\left(1 + \frac{1}{n}\right)^s \left(1 + \frac{s}{n}\right)^{-1} \right].$$

Proof: We insert the definition of the Euler constant γ.

$$\begin{aligned}
\mathrm{f}(s) &= s \lim_{m\to\infty} e^{s(1+\frac{1}{2}+\ldots+\frac{1}{m}-\log(m))} \lim_{N\to\infty} \prod_1^N \left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}} \\
&= s \lim_{m\to\infty} e^{s(1+\frac{1}{2}+\ldots+\frac{1}{m}-\log(m))} \prod_1^m \left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}} \\
&= s \lim_{m\to\infty} m^{-s} \prod_{n=1}^m \left(1 + \frac{s}{n}\right). \qquad (69)
\end{aligned}$$

Now comes a little rabbit out of a hat: Write m in a complicated way!

$$m = \left(1+\frac{1}{1}\right)\left(1+\frac{1}{2}\right)\cdot\ldots\cdot\left(1+\frac{1}{m-1}\right). \tag{70}$$

Insert this into equation (69) and use the fact that for all s

$$\lim_{m\to\infty}\left(1+\frac{1}{m}\right)^s = 1. \tag{71}$$

Thus equation (69) becomes

$$\begin{aligned}
\mathrm{f}(s) &= s\lim_{m\to\infty}\prod_{n=1}^{m-1}\left(1+\frac{1}{n}\right)^{-s}\prod_{n=1}^{m}\left(1+\frac{s}{n}\right)\\
&= s\lim_{m}\left(1+\frac{1}{m}\right)^s\prod_{1}^{m}\left(1+\frac{1}{n}\right)^{-s}\left(1+\frac{s}{n}\right)\\
&= s\lim_{m}\prod_{1}^{m}\left(1+\frac{1}{n}\right)^{-s}\left(1+\frac{s}{n}\right). \qquad (72)
\end{aligned}$$

Now invert both sides, and the proof of theorem E is complete. □

Corollary 3.14
For all $s\in\mathbb{C}$ holds

$$\frac{1}{\mathrm{f}(s)} = \lim_{m\to\infty}\frac{1\cdot 2\cdot\ldots\cdot(m-1)m^s}{s(s+1)\cdot\ldots\cdot(s+m-1)}.$$

Proof: By theorem E, for $s\neq 0,-1,-2,\ldots$

$$\begin{aligned}
\frac{1}{\mathrm{f}(s)} &= \lim_{m}\frac{1}{s}\prod_{1}^{m-1}\left(1+\frac{1}{n}\right)^s\left(1+\frac{s}{n}\right)^{-1}\\
&= \lim_{m}\frac{1}{s}\frac{(1+1)^s\left(1+\frac{1}{2}\right)^s\ldots\left(1+\frac{1}{m-1}\right)^s}{\left(1+\frac{s}{1}\right)\ldots\left(1+\frac{s}{m-1}\right)}\\
&= \lim_{m}\frac{1}{s}\frac{(1+1)2(\left(1+\frac{1}{2}\right)^s\ldots(m-1)\left(1+\frac{1}{m-1}\right)^s}{(1+s)(2+s)\ldots(m-1+s)}
\end{aligned}$$

where we have just expanded the fraction by $2 \cdot 3 \cdot \ldots \cdot (m-1)$. Now collect the integers in the numerator into one product, and the other factors into a product

$$\prod_{n=1}^{m-1} \left(1 + \frac{1}{n}\right)^s = m^s$$

by the trick we did in equation (70). This completes the proof of the corollary. □

Theorem 3.15
For all s such that $\Re(s) > 0$, 23.2.99

$$\frac{1}{\mathrm{f}(s)} = \Gamma(s) = \int_0^\infty e^{-t} t^{s-1}\, dt. \tag{73}$$

Thus, we have three representations of the Gamma function - the definition, and the ones given in theorems W and E. And they are all useful!

Proof of theorem 3.15: Define for integers $n \in \mathbb{N}$

$$\Gamma_n(s) := \int_0^n \left(1 - \frac{t}{n}\right)^n t^{s-1}\, dt.$$

Evaluate $\Gamma_n(s)$ by integrating by parts and a substitution $t = u\tau$, which means $dt = u\, d\tau$.

$$\begin{aligned}
\Gamma_n(s) &= n^s \int_0^1 (1-\tau)^n \tau^{s-1}\, d\tau \\
&= n^s \left[(1-\tau)^n \frac{\tau^s}{s}\right]_0^1 + \frac{n^s n}{s} \int_0^1 (1-\tau)^{n-1} \tau^s\, d\tau \\
&= \frac{n^s n(n-1)}{s(s+1)} \int_0^1 (1-\tau)^{n-2} \tau^{s+1}\, d\tau = \ldots \\
&= \frac{n^s n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1}{s(s+1) \cdot \ldots \cdot (s+n)}.
\end{aligned}$$

Now let n tend to infinity, and use the corollary 3.14 which shows

$$\lim_n \Gamma_n(s) = \frac{1}{\mathrm{f}(s)}. \tag{74}$$

To complete the proof of theorem 3.15, we want to prove

$$\lim_n \Gamma_n(s) = \Gamma(s). \tag{75}$$

This is plausible, because

$$\lim_n \left(1 - \frac{t}{n}\right)^n = e^{-t} \tag{76}$$

for all t (to prove this, just take logs, replace $1/n$ by h, and apply l'Hopital's rule). BUT to apply equation (76) to our problem, an exchange of limit and integral is required! We must prove

$$\lim_n \int_0^n \left[e^{-t} - \left(1 - \frac{t}{n}\right)^n \right] t^{s-1}\, dt = 0. \tag{77}$$

So we estimate the integrand in equation (77):

$$\left| t^{s-1} \left(e^{-t} - \left(1 - \frac{t}{n}\right)^n \right) \right| = t^{\sigma-1} \left| e^{-t} - \left(1 - \frac{t}{n}\right)^n \right|. \tag{78}$$

We need the following estimate:

$$\left| e^{-t} - \left(1 - \frac{t}{n}\right)^n \right| \leq \frac{t^2 e^{-t}}{n} \tag{79}$$

for all $t \in [0, n]$. Prove this as an exercise, or see Whittaker & Watson, A Course in Modern Analysis - one of the all-time classics! Assuming this estimate, we get

$$\int_0^n t^{\sigma-1} \left| e^{-t} - \left(1 - \frac{t}{n}\right)^n \right| \, dt \leq \frac{1}{n} \int_0^\infty e^{-t} t^{\sigma+1}\, dt = \frac{\Gamma(\sigma+2)}{n}, \tag{80}$$

which obviously tends to zero (note that the convergence is even uniform for bounded s, although we do not need this here). □

Corollary 3.16
For all $s \in \mathbb{C}$, s not in $\mathbb{N}$, we have

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

Proof: By theorem W,

$$\begin{aligned} \Gamma(s)\Gamma(-s) &= \frac{-1}{s^2} \prod_1^\infty \left(1 + \frac{s}{n}\right)^{-1} e^{-\frac{s}{n}} \prod_1^\infty \left(1 - \frac{s}{n}\right)^{-1} e^{\frac{s}{n}} \\ &= \frac{-1}{s^2} \prod_1^\infty \left(1 - \frac{s^2}{n^2}\right)^{-1} = \frac{-\pi}{s \sin(\pi s)} \end{aligned}$$

using the formula

$$\sin(\pi s) = \pi s \prod_1^\infty \left(1 - \frac{s^2}{n^2}\right). \tag{81}$$

Now the corollary follows, because $-s\Gamma(-s) = \Gamma(1-s)$. □

Instead of proving formula (81), we do an application: Look at

$$\sin(\pi s) = \pi s - \frac{(\pi s)^3}{6} + \dots \tag{82}$$

By equation (81), this is equal to

$$\begin{aligned} &\pi s \left(1 - s^2 \left(\frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \dots\right) + \dots\right) \\ &= \pi s - \pi s^3 \sum_1^\infty \frac{1}{n^2} + \dots \end{aligned}$$

Comparing the coefficient at s^3 with that of equation (82), we have proved

$$\sum_{n=1}^\infty \frac{1}{n^2} = \frac{\pi^2}{6}.$$

See also exercise 20, proving that $\zeta(2k)$ is a rational multiple of π^{2k}. In contrast to this, we know very little about the values $\zeta(3),\ \zeta(5), \dots$
Apery proved only in 1978 that $\zeta(3) \notin \mathbb{Q}$. See the article 'A Proof that Euler Missed' by A. van der Poorten (Mathematical Intelligencer 1979) or 'Roger Apéry et l'irrationnel' by Michel Mendes-France. For information on the computational evidence for the Riemann Hypothesis, see A. Odlyzko's homepage

http:// www.research.att.com/ awo

or the article 'Primes, Quantum Chaos and Computers' by A. Odlyzko (Number Theory, NRC(1993), 35-46.

Theorem 3.17
Define $N(T)$ to be the number of zeros of the Riemann zeta function up to height T,

$$N(T) := \#\{s \in \mathbb{C} :\ 0 \le \Re(s) \le 1,\ \zeta(s) = 0,\ 0 < \Im(s) < T\}.$$

We do not know a formula for each individual zero, but we know an asymptotic formula:

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

We will prove this later, perhaps. Note however, that the proof makes use of Stirling's general formula

$$\log(\Gamma(s)) = -s + \left(s - \frac{1}{2}\right)\log(s) + O_\delta(1), \tag{83}$$

provided $|\mathrm{Arg}(s)| < \pi - \delta$.

Figure 3: Primes modulo 4

$\mathbf{p \equiv 1}$	(mod **4**)		5			13	17			29		37	41
$\mathbf{p \equiv 3}$	(mod **4**)	3		7	11			19	23		31		

4 Primes in an Arithmetic Progression

26.2.99

We start off with two elementary results, then give more sophisticated proofs of them, suggesting a general method. The algebraic requirements to this method are characters of abelian groups, the analytic part is a non-vanishing statement about L-functions. The culminating point is DIRICHLET's general Theorem 4.3 in section 4.2.

4.1 Two Elementary Propositions

Consider all the primes congruent to 1 modulo four (see figure 3, first row) resp. congruent to three modulo four (second row). We might guess that there are infinitely many primes of each type.

Proposition 4.1
There are infinitely many primes congruent to three modulo four.

Proof 1: This proceeds like the first proof for the infinity of prime numbers. Suppose that the proposition is false, and there are only r such primes $p_1, \ldots, p_r$. Define

$$N := (p_1 \cdot \ldots \cdot p_r)^2 + 2.$$

Since $p_1^2 \equiv \ldots \equiv p_r^2 = 1 \pmod 4$, we have $N \equiv 3 \pmod 4$. Now N decomposes into prime factors,

$$N = q_1 \cdot \ldots \cdot q_k,$$

which must all be odd. So they are all congruent to 1 or 3 modulo four. At least one of the primes q_i must be congruent to 3, since otherwise N would be congruent to 1. So q_i is one of $p_1, \ldots, p_r$ and divides N and $N-2$, hence divides 2, a contradiction. □

Proposition 4.2
There are infinitely many primes congruent to 1 modulo four.

Proof: This proof is slightly different. Rather than deriving a contradiction, we will show that for any given $N > 1$, there exists a prime congruent to 1 modulo four and greater than N. Given $N > 1$, define

$$M := (N!)^2 + 1. \tag{84}$$

Clearly, M is odd. Let p be the smallest prime factor of M, then clearly $p > N$. We claim $p \equiv 1 \pmod 4$ (which completes the proof of the proposition, since N was arbitrary). To prove the claim, transform (84) into

$$(N!)^2 = M - 1 \equiv -1 \pmod p. \tag{85}$$

Since p divides M, p is odd, and we may raise equation (85) to the $(p-1)/2$th power:

$$(N!)^{p-1} \equiv (-1)^{\frac{p-1}{2}}. \tag{86}$$

Now by Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod p$ for all $a \not\equiv 0 \pmod p$. So $(p-1)/2$ must be even, proving the claim. □

Consider $p \equiv 5 \pmod 6$: One can prove that there are infinitely many such primes in a way similar to the proof of Proposition 4.1. Use reasoning by absurdity and

$$N := 2 \cdot 3 \cdot \ldots \cdot p_r + 5.$$

What do you take for primes $p \equiv 1 \pmod 6$ (only for 1 and 5 modulo 6, there is a chance of infinitely many primes)? Exercise.

Isn't this nice?? **NO!**

The results are nice, but the proofs are awkward. We would like to have a general principle for proving such results.

4.2 A New Method of Proof

We will re-do the proofs of Propositions 4.1 and 4.2 along the lines of proof 2 for the infinity of primes. Consider for odd $n \in \mathbb{N}$ the function

$$\mathrm{c}_1(n) := \frac{1+(-1)^{\frac{n-1}{2}}}{2} = \begin{cases} 1 & \text{for } n \equiv 1 \pmod 4 \\ 0 & \text{for } n \equiv 3 \pmod 4 \end{cases} \tag{87}$$

This is a gadget for picking out a particular congruence class. Later, we will compare this fact with orthogonality relations for characters of abelian groups. Using the gadget, for real $\sigma > 1$,

$$\begin{aligned} \sum_{p \equiv 1 \bmod 4} \frac{1}{p^\sigma} &= \frac{1}{2} \sum_{\text{odd } p} \frac{\mathrm{c}_1(p)}{p^\sigma} \\ &= \frac{1}{2} \sum_{\text{odd } p} \frac{1}{p^\sigma} + \frac{1}{2} \sum_{\text{odd } p} \frac{(-1)^{\frac{p-1}{2}}}{p^\sigma}. \end{aligned} \tag{88}$$

The rearrangement here is ok, because the series involved converge absolutely. The first summand on the right of equation (88) tends to infinity as $\sigma \to 1$ (see theorem 1.5). We claim that the second summand converges for $\sigma \to 1$. $(*)$ This implies that the left hand side of (88) tends to infinity, and we conclude that there must be infinitely many primes over which the summation runs. Also, using a similar gadget,

$$\mathrm{c}_3(n) := \frac{1-(-1)^{\frac{n-1}{2}}}{2} = \begin{cases} 0 & \text{for } n \equiv 1 \pmod 4 \\ 1 & \text{for } n \equiv 3 \pmod 4 \end{cases}, \tag{89}$$

we get the existence of infinitely many primes $p \equiv 3 \pmod 4$ in *very much the same way*!

Nice!

The biggest payoff is that the argument can be made to work in complete generality. At the end of this chapter, we will have proved the following theorem:

Theorem 4.3 (Dirichlet) If $a \in \mathbb{N}$ and $q \in \mathbb{N}$ are coprime, then there are infinitely many primes p such that

$$p \equiv a \pmod q.$$

Note that this is the most general result we could hope for. If a and q are not coprime, every number $n \equiv a \pmod{q}$ will be divisible by $\gcd(a,q) > 1$, so there can only be finitely many such primes.

For the moment, let us pursue the aim of another proof of Proposition 4.2, since all the essentials of DIRICHLET's proof become apparent there already. We still have to prove the claim $(*)$. To do this, define two functions $\chi, \chi_0 : \mathbb{N} \to \{-1, 0, 1\}$ by

$$\begin{aligned} \chi(n) &= \begin{cases} 0 & \text{if } n \text{ even} \\ (-1)^{\frac{n-1}{2}} & \text{if } n \text{ odd} \end{cases} \\ \chi_0(n) &= \begin{cases} 0 & \text{if } n \text{ even} \\ 1 & \text{if } n \text{ odd} \end{cases} \end{aligned} \tag{90}$$

Then define complex functions

$$\mathrm{L}(s, \chi) := \sum_{n \in \mathbb{N}} \frac{\chi(n)}{n^s} \tag{91}$$

and similarly $L(s, \chi_0)$. Such functions are called L-functions and are a special kind of Dirichlet series. Clearly, the series defining $L(s, \chi)$ and $L(s, \chi_0)$ converge absolutely for all s with $\Re(s) > 1$.

Lemma 4.4
The series $L(s, \chi)$ converges for $s = 1$, and

$$L(1, \chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \ldots = \frac{\pi}{4}.$$

Proof: Consider the integral

$$\int_0^1 \frac{dt}{1+t^2} = [\tan^{-1}(t)]_0^1 = \frac{\pi}{4}. \tag{92}$$

Substitute into this integral the expansion

$$\frac{1}{1+t^2} = \sum_{n=0}^{\infty} \frac{1}{(-t^2)^n} \tag{93}$$

which converges for all $0 \leq t < 1$. Fix any $0 < x < 1$, then the series in (93) converges uniformly for $0 \leq t \leq x$. We have for all $0 < x < 1$

$$\begin{aligned} \mathrm{f}(x) = \int_0^x \frac{dt}{1+t^2} &= \sum_{n=1}^{\infty} \int_0^x (-t^2)^n \, dt \\ &= \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} x^{2n+1}, \end{aligned} \tag{94}$$

because there we may interchange integration and summation thanks to the uniform convergence. Now, we may take the limit $x \to 1$ thanks to Abel's Limit theorem (a nice special feature of power series - see Appendix B, since this is rather a theorem of Calculus). For $x \to 1$, we get $L(1, \chi)$ on the right-hand side, and the integral in (92), $\mathrm{f}(1) = \pi/4$ on the left-hand side. □

Lemma 4.5
The functions χ and χ_0 are completely multiplicative (see definition 1.19).

Proof: Check all cases for m and n modulo 4 in $\chi(mn) = \chi(m)\chi(n)$ resp. the same for χ_0. □

Now recall the Euler expansion for the zeta function, equation (11). Since χ and χ_0 are completely multiplicative, we get in exactly the same way (see Theorem 2.1) an Euler expansion of $L(\sigma, \chi)$ and $L(\sigma, \chi_0)$:

$$\begin{aligned} L(\sigma, \chi) &= \prod_{\text{odd } p} \left(1 - \frac{\chi(p)}{p^\sigma}\right)^{-1} \\ L(\sigma, \chi_0) &= \prod_{\text{odd } p} \left(1 - \frac{1}{p^\sigma}\right)^{-1} \end{aligned} \tag{95}$$

As in proof 2 for the existence of infinitely many primes, take logs of the two equations (95):

$$\begin{aligned} \log L(\sigma, \chi) &= -\sum_{\text{odd } p} \log\left(1 - \frac{\chi(p)}{p^\sigma}\right) = \sum_{\text{odd } p} \frac{\chi(p)}{p^\sigma} + O(1), \\ \log L(\sigma, \chi_0) &= -\sum_{\text{odd } p} \log\left(1 - \frac{1}{p^\sigma}\right) = \sum_{\text{odd } p} \frac{1}{p^\sigma} + O(1). \end{aligned} \tag{96}$$

Now add up (see equation (88)): 1.3.99

$$\begin{aligned}\log(L(\sigma,\chi_0)\cdot L(\sigma,\chi)) &= \sum_{\text{odd } p}\frac{1+\chi(p)}{p^\sigma}+O(1)\\ &= 2\sum_{p\equiv 1 \bmod 4}\frac{1}{p^\sigma}+O(1). \qquad (97)\end{aligned}$$

What is the behaviour of the left-hand side as σ tends to 1 from above?

$$\begin{aligned}L(\sigma,\chi) &\to \frac{\pi}{4}\neq 0\\ L(\sigma,\chi_0) &= \left(1-\frac{1}{2^\sigma}\right)\sum_n\frac{1}{n^\sigma}\to\infty.\end{aligned}$$

The terms $O(1)$ in (96) are still $O(1)$ for $\sigma\to 1$, so we conclude

$$\sum_{p\equiv 1 \bmod 4}\frac{1}{p^\sigma}\to\infty$$

for $\sigma\to 1$. This completes the second proof of Proposition 4.2. Had we subtracted instead of added the two equations (96), we would have got a proof that

$$\sum_{p\equiv 3 \mod 4}\frac{1}{p^\sigma}$$

diverges for $\sigma\to 1$ and hence another proof of Proposition 4.1. □

Another case: Congruences modulo 3. Consider the functions

$$\begin{aligned}\chi_0(n) &:= \begin{cases}1 & \text{if } 3\not| n\\ 0 & \text{if } 3|n\end{cases}\\ \chi(n) &:= \begin{cases}1 & \text{if } n\equiv 1 \pmod 3\\ -1 & \text{if } n\equiv 2 \pmod 3\\ 0 & \text{if } n\equiv 0 \pmod 3\end{cases} \qquad (98)\end{aligned}$$

As in the previous example, the functions c_1 and c_2 picking out a particular congruence class can be rewritten using χ and χ_0.

$$\begin{aligned}\mathrm{c}_1(n) &:= \frac{1}{2}(\chi_0(n)+\chi(n)) = \begin{cases}1 & \text{if } n\equiv 1 \pmod 3\\ 0 & \text{otherwise and}\end{cases}\\ \mathrm{c}_2(n) &:= \frac{1}{2}(\chi_0(n)-\chi(n)) = \begin{cases}1 & \text{if } n\equiv 2 \pmod 3\\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

Then define functions

$$L(\sigma, \chi) := \sum_n \frac{\chi(n)}{n^\sigma}$$

and similarly $L(\sigma, \chi_0)$. As in the previous example, χ and χ_0 are completely multiplicative, hence $L(\sigma, \chi)$ and $L(\sigma, \chi_0)$ have an Euler product expansion. Moreover,

$$L(\sigma, \chi_0) = \sum_{3 \not| n} \frac{1}{n^\sigma} = \left(1 - \frac{1}{3^\sigma}\right) \zeta(\sigma)$$

tends to infinity as σ tends to 1. We have all the ingredients to repeat the second proof of Proposition 4.2 in this case *but one*: We do not yet know whether

$$L(1, \chi) \neq 0. \tag{99}$$

If we knew this, we could proceed exactly as before - the key step is

$$\log(L(\sigma, \chi_0) \cdot L(\sigma, \chi)) = 2 \sum_{p \equiv 1 \pmod 3} \frac{1}{p^\sigma} + O(1)$$

As long as we do not know the fact (99), the left-hand side might have a limit as σ tends to 1. We will prove (99) only in section (4.5), as part of a general result. But let us put on record: If we want to prove results like Proposition 4.2 along the lines of the second proof, there are two things we need to get to grips with:

1. A machinery for pulling out a particular congruence class via multiplicative functions (see sections 4.3, 4.4).

2. A non-vanishing statement about L-functions at $\sigma = 1$ (see section 4.5).

4.3 Characters of Finite Abelian Groups

In this section, we want to deal with Problem 1 from the preceding section. Consider the example $n = 5$. Define the functions

$$\begin{aligned} \chi_0(n) &:= \begin{cases} 1 & \text{if } n \not\equiv 0 \pmod 5 \\ 0 & \text{if } 5|n \end{cases} \\ \chi(n) &:= \begin{cases} i & \text{if } n \equiv 2 \pmod 5 \\ -1 & \text{if } n \equiv 4 \pmod 5 \\ -i & \text{if } n \equiv 3 \pmod 5 \\ 1 & \text{if } n \equiv 1 \pmod 5 \\ 0 & \text{if } n \equiv 0 \pmod 5 \end{cases} \end{aligned} \tag{100}$$

Now check that

$$\frac{1}{4}(\chi_0(n) + \chi(n) + \chi^2(n) + \chi^3(n)) \;=\; \mathrm{c}_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 5 \\ 0 & \text{otherwise} \end{cases}$$

What if you want to pull out the congruence class $n \equiv 2 \pmod 5$? We need a general set-up. Recall that in the ring $\mathbb{Z}/n$, the units are $U(\mathbb{Z}/n) = \{k \bmod n : \ (k, n) = 1\}$ (see section 1.3). This is a group under multiplication. E. g. if $n = 5$, $U(\mathbb{Z}/5) = \{1, 2, 3, 4\}$ is a cyclic group, generated by e. g. $2 \bmod 5$. The multiplication table of $U(\mathbb{Z}/5)$ is

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

So $U(\mathbb{Z}/5) \cong \{1, i, -1, -i\}$.

Definition 4.6
Suppose G is a finite abelian group. A *character of* G is a homomorphism

$$\chi : \ G \to (\mathbb{C}^*, \cdot)$$

(the multiplicative group $\mathbb{C}^*$ is $\mathbb{C} - \{0\}$ equipped with the usual multiplication $\cdot$). By convention, we will write all finite groups multiplicatively in this section - hence the identity will be written as 1_G or 1. For any group, the map

$$\chi_0 : \ G \to \mathbb{C}^*, \ \chi_0(g) := 1$$

is a character, called the *trivial character*.

Lemma 4.7
If χ is a character of the finite abelian group G, then $\chi(1_G) = 1$ and $\chi(g)$ is a root of unity, i. e. $\chi(g)^n = 1$ for some n depending on g. In particular, $|\chi(g)| = 1$ ($\chi(g)$ lies on the unit circle).

Proof: Clearly $\chi(1_G) = \chi(1_G \cdot 1_G) = \chi(1_G)\chi(1_G)$. Then divide by the nonzero number $\chi(1_G)$. As to the second statement, we use the fact that for every $g \in G$ there exists $n \in \mathbb{N}$ such that $g^n = 1_G$. This implies $\chi(g)^n = \chi(g^n) = \chi(1_G) = 1$. □

Example: $G = C_n = \langle g \rangle$. If it helps you, $G \cong (\mathbb{Z}/n, +)$, an *additive* group - but if it doesn't, just forget it. Since $g^n = 1$, $\chi(g)^n = 1$ and $\chi(g)$ must be a n-th root of unity *for this particular* n! Any of the n different n-th roots of unity can occur as $\chi(g)$, and of course $\chi(g)$ determines all the values of χ on G, since G is generated by g. So there are n distinct characters of G. We can label the characters of G with labels $0, 1, \ldots, n-1$ as follows:

$$\begin{aligned} \chi_k \qquad \text{is determined by } \chi_k(g) &= e^{\frac{2\pi i k}{n}} \\ \text{so } \chi_k(g^m) &= e^{\frac{2\pi i k m}{n}}. \end{aligned} \tag{101}$$

Theorem 4.8
Let G be a finite abelian group. Then the characters of G form a group under multiplication,

$$(\chi \cdot \psi)(g) := \chi(g)\psi(g),$$

denoted $\hat{G}$. The identity in $\hat{G}$ is the trivial character. The group $\hat{G}$ is isomorphic to G. In particular, any finite abelian group G of order n has exactly n distinct characters.

Remark 4.9
This is a lens, and through it you see into the 'world of duality'. Think of this one day: What would happen if you took $G = \mathbb{Z}$ - what is

$$\hat{\mathbb{Z}} := \{\text{homomorphisms } \mathbb{Z} \to \text{unit circle}\}?$$

What if you took $G =$ unit circle? The answer is: Fourier Analysis!

Proof of Theorem 4.8: Use the Structure Theorem for finite abelian groups, 2.3.99
which says that G is isomorphic to a product of cyclic groups.

$$G \cong \prod_{j=1}^{k} C_{n_j}.$$

Choose a generator g_j for each of the factors C_{n_j} and define characters on G by

$$\chi^{(j)}(*, \ldots, *, g_j, *, \ldots, *) := e^{\frac{2\pi i}{n_j}},$$

i. e. ignore all entries except the j-th, and there use the same definition as in the Example above. Then the characters $\chi^{(1)}, \ldots, \chi^{(k)}$ generate a subgroup of $\hat{G}$ which is isomorphic to G: Each $\chi^{(j)}$ generates a cyclic group of order n_j, and this group has trivial intersection with the span of all the other $\chi^{(i)}$'s, since all characters in the latter have value 1 at g_j. Likewise, for any given character of G, it is easy to write down a product of powers of the $\chi^{(j)}$ which coincides with χ on the generators g_j, hence on all of G. □

Corollary 4.10
Let G be a finite abelian group. For any $1 \neq g \in G$, there exists $\chi \in \hat{G}$ such that $\chi(g) \neq 1$.

Proof: Looking again at the proof of Theorem 4.8, we may write $g = (*, \ldots, *, g_j^r, *, \ldots, *)$ with some entry $g_j^r \neq 1$, i. e. $0 < r < n_j$. Then $\chi^{(j)}(g) = e^{\frac{2piir}{n_j}} \neq 1$. □

Theorem 4.11
Let G be a finite abelian group. Then for all elements $h \in G$ and all characters $\psi \in \hat{G}$ hold the identities

$$\sum_{g \in G} \psi(g) = \begin{cases} |G| & \text{if } \psi = \chi_0 \\ 0 & \text{if } \psi \neq \chi_0 \end{cases} \tag{102}$$

$$\sum_{\chi \in \hat{G}} \chi(h) = \begin{cases} |G| & \text{if } h = 1 \\ 0 & \text{if } h \neq 1 \end{cases}. \tag{103}$$

These identities are known as *orthogonality relations for group characters.*

Proof of the first assertion: The case $\psi = \chi_0$ is trivial, so assume $\psi \neq \chi_0$. There must exist an element $h \in G$ such that $\psi(h) \neq 1$. Then

$$\psi(h) \sum_{g \in G} \psi(g) \;\; = \;\; \sum_{g \in G} \psi(gh) = \sum_{g \in G} \psi(g),$$

because multiplication by h only permutes the summands. But this equation can only be true if $\sum_{g \in G} \psi(g) = 0$. Now for the second assertion, assume $h \neq 1$. By the Corollary 4.10, there exists some character $\psi \in \hat{G}$ such that $\psi(h) \neq 1$. We play the same game:

$$\psi(h) \sum_{\chi \in \hat{G}} \chi(h) \;\; = \;\; \sum_{\chi \in \hat{G}} (\psi \cdot \chi)(h) = \sum_{\chi \in \hat{G}} \chi(h),$$

since multiplication by ψ only permutes the elements of $\hat{G}$, and again this can only be true if $\sum_{\chi \in \hat{G}} \chi(h) = 0$. □

Corollary 4.12
For all $g, h \in G$, we have

$$\sum_{\chi \in \hat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} |G| & \text{if } g = h \\ 0 & \text{if } g \neq h \end{cases}$$

Proof: Note that

$$\chi(h^{-1}) = \chi(h)^{-1} = \overline{\chi(h)},$$

since $\chi(h)$ is on the unit circle. Then use Theorem 4.11 with gh^{-1} in place of h. □

This is the gadget in its ultimate version! As an example, take $G = U(\mathbb{Z}/5) \cong C_4$. Here is a table of all the characters.

	χ_0	χ_1	χ_2	χ_3
1	1	1	1	1
2	1	i	-1	$-i$
4	1	-1	1	-1
3	1	$-i$	-1	i

(104)

Note that we have written the elements of $U(\mathbb{Z}/5)$ in an unusual ordering - this is given by $2^0, 2^1, 2^2, 2^3$. The character values behave likewise. Note also $\chi_1^2 = \chi_2$ and $\chi_1^3 = \chi_3 = \chi_1^{-1}$. We have used earlier

$$\chi_0(n) + \chi_1(n) + \chi_2(n) + \chi_3(n) = 4\mathrm{c}_1(n)$$

which is just the case $h = 1$ of the corollary 4.12. We asked then, what about $\mathrm{c}_2(n)$ (1 if n congruent to 2 and 0 otherwise)? The corollary says take $h = 2$, and we get

$$\chi_0(n) - i\chi_1(n) - \chi_2(n) + i\chi_3(n) = 4\mathrm{c}_2(n).$$

Check the cases!

Remark 4.13
If you remember something about Fourier Analysis - this is really like Fourier Analysis, only nicer. The rule

$$\frac{1}{|G|}\sum_{h\in G} \mathrm{f}(g)\overline{\mathrm{g}(h)}$$

is an inner product on the vector space of all functions on G, and the characters form a complete orthonormal set. There are no worries about convergence, integrability ... And in particular, *any* complex function on G can be written as linear combination of the characters.

4.4 Dirichlet characters and L-functions

Definition 4.14
Given $1 < q \in \mathbb{N}$, consider $G := U(\mathbb{Z}/q)$ and a character $\chi \in \hat{G}$. Extend χ to a function X on $\mathbb{N}$ by setting

$$X(n) := \begin{cases} \chi(n \bmod q) & \text{if } n \text{ coprime to } q \\ 0 & \text{otherwise} \end{cases} \tag{105}$$

Then the function X is called a *Dirichlet character modulo q*. Note that this is a slight abuse of language - it is not meant to say that $\mathbb{N}$ were a group. However, we will even write χ instead of X for the Dirichlet character associated to χ. In the same way, for any $a \in G$, we can extend the function

$$\mathrm{c}_a(b) := \begin{cases} 1 & \text{if } b = a \\ 0 & \text{otherwise} \end{cases} \tag{106}$$

to a periodic function on $\mathbb{N}$, which will also be written as c_a. Finally, associate to each Dirichlet character χ the function

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

called the *L-function of* χ.

Example: Take the trivial character χ_0 of $U(\mathbb{Z}/4)$. The associated Dirichlet character is just the function χ_0 that we used in the second proof of Propositions 4.2 and 4.1. And the functions c_1 and c_3 that we used there are extensions of functions on $U(\mathbb{Z}/4)$ as in (106). Same thing for the L-functions - the notation has been carefully chosen to be consistent.

Proposition 4.15
A Dirichlet character is completely multiplicative, and the associated L-function has an Euler product expansion.

Proof: Let χ be a Dirichlet character modulo q. If two integers m, n are given, and at least one of them is not coprime to q, then neither is the product mn. So $\chi(mn) = 0 = \chi(m)\chi(n)$. If on the other hand, both m and n are coprime to q, then $(m \bmod q) \cdot (n \bmod q) = (mn \bmod q)$ by definition, and because χ in the original sense is a group character, we have $\chi(mn) = \chi(m)\chi(n)$. The existence of an Euler product expansion follows then directly from Theorem 2.1. Since $\chi(p) = 0$ for all p dividing q, we get

$$L(s,\chi) = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{p \not| q} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \tag{107}$$

□

Clearly the L-functions converge for $\Re(s) > 1$, by comparison with the Riemann zeta function. Now let us see how these L-functions can be marshalled to prove Dirichlet's Theorem about primes in an arithmetic progression.

By Theorem 2.1 which gives the Euler product expansion, $L(s,\chi) \neq 0$ for $\Re(s) > 1$. So we may take logs in (107) and expand the log:

$$\begin{aligned} \log L(s,\chi) &= -\sum_{p \nmid q} \log\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{p \nmid q} \sum_{m=1}^{\infty} \frac{1}{m} \frac{\chi(p^m)}{p^{sm}} \\ &= \sum_{p \nmid q} \frac{\chi(p)}{p^s} + O(1) \end{aligned} \tag{108}$$

as before. For a given congruence class $a \bmod q$, with a coprime to q, multiply both sides by $\overline{\chi(a)}$ and sum over all $\chi \in \widehat{U(\mathbb{Z}/q)}$ resp. the associated Dirichlet characters. We get

$$\sum_{\chi} \overline{\chi(a)} \log L(s,\chi) = \sum_{\chi} \overline{\chi(a)} \sum_{p \nmid q} \frac{\chi(p)}{p^s} + O(1) \tag{109}$$

Since the series on the right converges absolutely, we may interchange summations. By corollary 4.12

$$\sum_{\chi} \overline{\chi(a)} \chi(p) = \begin{cases} \phi(q) & \text{if } p = a \pmod q \\ 0 & \text{otherwise.} \end{cases}$$

There, $\phi(q) = |U(\mathbb{Z}/q)|$ by definition (the Euler phi function, see (19) in section 1.3). We have proved now

$$\sum_{\chi} \overline{\chi(a)} \log L(s,\chi) = \phi(q) \sum_{p \equiv a \bmod q} \frac{1}{q^s} + O(1). \tag{110}$$

Now drumroll please! Let $s \to 1$. We claim

i) The L-function $L(s,\chi_0)$ has a simple pole at $s = 1$.

ii) For all $\chi \neq \chi_0$, the L-function $L(\chi,s)$ has a nonzero limit as $s \to 1$.

Once these claims are proved, we know that the left-hand side in (110) tends to infinity as $s \to 1$. For the right-hand side, this means that there must be infinitely many summands. This will complete the proof of Dirichlet's Theorem.

The first claim is quite easy to prove: 5.3.99

$$L(s,\chi_0) = \prod_{p \not| q} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p|q} \left(1 - \frac{1}{p^s}\right) \zeta(s), \tag{111}$$

and we know that ζ has a simple pole at $s = 1$. The second claim is horribly difficult to prove!

A last remark before we embark on this. Looking back at figure 3, one might have guessed that both congruence classes of primes modulo four contain 'about' the same number of primes up to a given bound. This is true in complete generality. For all a coprime to q,

$$\lim_{T\to\infty} \frac{\#\{p \equiv a \pmod q,\ p \leq T\}}{\#\{p \leq T\}} \to \frac{1}{\phi(q)}. \tag{112}$$

Note that the limit is independent of a. This can be proved by a slight refinement of the methods given in this chapter.

4.5 Analytic continuation of L-functions and Abel's Summation Formula

In this section, we will not only complete the proof of Dirichlet's Theorem 4.3. On the way, we will see Abel's Summation Formula and and the analytic continuation of L-functions to the half-plane $\Re(s) > 0$.

Theorem 4.16 (Abel)
Let $\mathrm{a}(n)$ be an arithmetical function and define $\mathrm{A}(x) := \sum_{n \le x} \mathrm{a}(n)$. Let $\mathrm{f}: [y, x] \to \mathbb{C}$ be differentiable with continuous derivative. Then

$$\sum_{x < n \le y} \mathrm{a}(n)\mathrm{f}(n) = \mathrm{A}(y)\mathrm{f}(y) - \mathrm{A}(x)\mathrm{f}(x) - \int_x^y \mathrm{A}(t)\mathrm{f}'(t)\, dt. \tag{113}$$

Proof: Assume $x, y \in \mathbb{N}$ are integral for ease, $m = y$ and $k = x$. So the left-hand side of (113) is

$$\begin{aligned} \sum_{n=k+1}^{m} \mathrm{a}(n)\mathrm{f}(n) &= \sum_{n=k+1}^{m} (\mathrm{A}(n) - \mathrm{A}(n-1))\mathrm{f}(n) \\ &= -\sum_{n=k+1}^{m} \mathrm{A}(n-1)(\mathrm{f}(n) - \mathrm{f}(n-1)) + \mathrm{A}(m)\mathrm{f}(m) - \mathrm{A}(k)\mathrm{f}(k). \end{aligned}$$

This is rather like integration by parts - sums instead of integrals, taking differences instead of differentiating. And there are some terms coming from the boundary of the summation interval, too! Note that we did not use the hypothesis that f be differentiable up to now. But we are not finished yet. Using $\mathrm{A}(t) = \mathrm{A}(n)$ for all $t \in [n, n+1[$, we get

$$\mathrm{A}(n-1)(\mathrm{f}(n) - \mathrm{f}(n-1)) = \mathrm{A}(n-1) \int_{n-1}^{n} \mathrm{f}'(t)\, dt = \int_{n-1}^{n} \mathrm{A}(t)\mathrm{f}'(t)\, dt.$$

Sum this from $n = k+1$ to $n = m$ to get the statement of the theorem. □

Apply this formula to $\mathrm{a}(n) := \chi(n)$ (χ a Dirichlet character modulo q, but not the trivial character) and $\mathrm{f}(t) := t^{-s}$. We have $\sum_{n=k}^{k+q-1} \chi(n) = 0$ for all $k \in \mathbb{N}$. Hence $\mathrm{A}(x) = O(1)$, in fact $|A(x)| \le \phi(q)$ for all x. Abel's summation formula gives

$$\sum_{1 < n \le y} \frac{\chi(n)}{n^s} = \frac{\mathrm{A}(y)}{y^s} - 1 + s \int_1^y \frac{\mathrm{A}(t)}{t^{s+1}}\, dt. \tag{114}$$

The integral on the right-hand side of equation (114) can be split into integrals from 1 to 2, from 2 to 3 and so on. The series of these integrals converges uniformly for $\Re(s) > \delta$, with any fixed $\delta > 0$, hence we may let $y \to \infty$. And each of these integrals is an analytic function of s for $\Re(s) > 0$. Hence the function $L(s, \chi)$ is analytic in this domain by Theorem 2.7. This argument is in fact the same that we used in one of the proofs of the analytic continuation of the zeta function.
We will now finally prove $L(s, \psi) \neq 0$ for $s = 1$. Consider first the case that ψ is a non-real Dirichlet character, i. e. not all $\psi(n)$ are ± 1. Consider for $\sigma > 1$

$$\begin{aligned} \log \prod_{\chi} L(\sigma, \chi) &= \sum_{\chi} \log L(\sigma, \chi) = -\sum_{\chi} \sum_{p \nmid q} \log \left(1 - \frac{\chi(p)}{p^s}\right) \quad (115) \\ &= \sum_{\chi} \sum_{p \nmid q} \sum_{m} \frac{\chi(p)^m}{m p^{\sigma m}}. \end{aligned}$$

Suppose $L(1, \psi) = 0$. Then we must also have $L(1, \bar{\psi}) = 0$. By hypothesis, $\psi \neq \bar{\psi}$, and both ψ and $\bar{\psi}$ appear in the product over all characters in (115). As σ tends to 0, the simple pole of $L(s, \chi_0)$ is doubly cancelled by the zeros in $L(s, \psi)$ and $L(s, \bar{\psi})$, hence the product must tend to 0 and the logarithm in (115) to $-\infty$. But the right-hand side of (115) is always nonnegative! This follows from $\sum_{\chi} \chi(p^m) = 0$ or $\phi(q)$ (see Theorem 4.11). This is a contradiction, and we have proved $L(1, \psi) \neq 0$ in the case that ψ is not real.

The case that ψ is real, i. e. $\psi(n) = \pm 1$ for all $n \in \mathbb{N}$, is rather more complicated. Suppose again $L(1, \psi) = 0$. Then $\zeta(s)L(s, \psi)$ must be analytic in the half-plane $\Re(s) > 0$. Write $\mathrm{F}(s) := \zeta(s)L(s, \psi)$ as Dirichlet series (see Application 1.27), 8.3.99

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

where the function $\mathrm{f} := \psi * \mathrm{u}$ is defined by

$$\mathrm{f}(n) = (\psi * \mathrm{u})(n) = \sum_{d|n} \psi(d).$$

Lemma 4.17

Define another arithmetical function g by

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

Then $\mathrm{f}(n) \geq \mathrm{g}(n)$ for all $n \in \mathbb{N}$.

Proof of the Lemma: Note that both f and g are multiplicative arithmetical functions. So it is enough to consider the case $n = p^k$, a prime power. We have

$$\mathrm{f}(p^k) = 1 + \psi(p) + \cdots + \psi(p)^k = \begin{cases} 1 & \text{if } \psi(p) = 0 \\ k+1 & \text{if } \psi(p) = 1 \\ 0 & \text{if } \psi(p) = -1 \text{ and } k \text{ odd} \\ 1 & \text{if } \psi(p) = -1 \text{ and } k \text{ even.} \end{cases}$$

Clearly then $\mathrm{f}(n) \geq 0$ for all n. This settles already the claim of the lemma in the case that n is not a square. If n is a square, the exponent of each prime in n is even, and we get $\mathrm{f}(n) \geq 1$ by looking at the table above. This completes the proof of Lemma 4.17. □

Back to the main proof: Fix $0 < r < 3/2$. Since F is analytic in half-plane $\sigma > 0$, look at Taylor expansion of F about $s = 2$.

$$\mathrm{F}(2-r) = \sum_{\nu=1}^{\infty} \frac{\mathrm{F}^{(\nu)}(2)}{\nu!}(-r)^\nu,$$

where the ν-th derivative $\mathrm{F}^{(\nu)}(2)$ is given by

$$\mathrm{F}^{(\nu)}(2) = \sum_{n=1}^{\infty} \mathrm{f}(n) \frac{(-\log n)^\nu}{n^2}. \tag{116}$$

We will prove later that the Dirichlet series for F converges uniformly for $\sigma > 0$, so that we may indeed differentiate term by term. Now consider a general summand of the Taylor expansion.

$$\begin{aligned} \frac{\mathrm{F}^{(\nu)}(2)}{\nu!}(-r)^\nu &= \frac{r^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{\mathrm{f}(n)(\log n)^\nu}{n^2} \geq \frac{r^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{\mathrm{g}(n)(\log n)^\nu}{n^2} \\ &= \frac{r^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{1 \cdot (\log(n^2))^\nu}{n^4} = \frac{(-2r)^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{(-\log(n))^\nu}{n^4} \\ &= \frac{(-2r)^\nu}{\nu!} \zeta^{(\nu)}(4). \end{aligned}$$

Use this inequality for all terms of the Taylor expansion of F.

$$\mathrm{F}(2-r) \geq \sum_{\nu=0} \frac{(-2r)^\nu}{\nu!} \zeta^{(\nu)}(4) = \zeta(4-2r). \tag{117}$$

Then let $r \to 3/2$. The right-hand side of equation (117) tends to infinity, since ζ has a pole at $s = 1$. The left-hand side is bounded because F(s) is analytic for $s > 0$, a contradiction.
We still have to prove our claim that the Dirichlet series for F does converge uniformly for all $s > 0$. Look again at equation (116) and plug it into the Taylor series for F about $s = 2$.

$$\mathrm{F}(2-r) = \sum_{\nu=0}^{\infty} \frac{1}{\nu!} r^\nu \sum_{n=1}^{\infty} \mathrm{f}(n) \frac{(\log n)^\nu}{n^2}.$$

Note that the minus sign of $-r$ cancels with that in the derivative, so that all terms are positive. Hence we may interchange the summations,

$$\mathrm{F}(2-r) = \sum_{n=1}^{\infty} \frac{\mathrm{f}(n)}{n^2} \sum_{\nu=0}^{\infty} \frac{1}{\nu!} (r \log n)^\nu \tag{118}$$

and this sum converges for all r with $|r| < 2$, because by our assumption, $\mathrm{F}(s)$ is analytic in the whole half-plane $\Re(s) > 0$. The inner sum in equation (118) is just $e^{r \log n} = n^r$. So equation (118) becomes

$$\mathrm{F}(2-r) = \sum_{n=1}^{\infty} \frac{\mathrm{f}(n)}{n^{2-r}}. \tag{119}$$

The right-hand side converges for all $r < 2$, and if we substitute $s = 2 - r$, we get just the Dirichlet series for F back again, which converges for all $s > 0$. Since any Dirichlet series convergent for all $s > s_0$ converges *uniformly* in that domain, the proof is complete. □