Nine Chapters of Analytic Number Theory in Isabelle/HOL

Manuel Eberl
Technical University of Munich, Boltzmannstraße 3, Garching bei München, Germany
https://www21.in.tum.de/~eberlm
eberlm@in.tum.de

Abstract

In this paper, I present a formalisation of a large portion of Apostol's *Introduction to Analytic Number Theory* in Isabelle/HOL. Of the 14 chapters in the book, the content of 9 has been mostly formalised, while the content of 3 others was already mostly available in Isabelle before.

The most interesting results that were formalised are:

- The Riemann and Hurwitz ζ functions and the Dirichlet L functions
- Dirichlet's theorem on primes in arithmetic progressions
- The analytic proof of the Prime Number Theorem
- The asymptotics of arithmetical functions such as the prime ω function, the divisor functions $\sigma_x(n)$, and Euler's totient function $\varphi(n)$

2012 ACM Subject Classification Mathematics of computing → Mathematical analysis

Keywords and phrases Isabelle, theorem proving, analytic number theory, number theory, Dirichlet series, prime number theorem, Dirichlet's theorem, zeta function, L functions

Funding This work was supported by DFG grant NI 491/16-1. Part of it was conducted during a research visit in collaboration with the ALEXANDRIA project (ERC grant 742178).

Acknowledgements I would like to thank John Harrison for doing all the incredibly hard work of creating an extensive library of complex analysis in HOL Light – the first of its kind – and Larry Paulson and Wenda Li for porting it to Isabelle/HOL and extending it even further. Without these efforts, my work would not have been possible. I also thank Larry Paulson for starting off the analytic proof of the Prime Number Theorem in Isabelle (based on Harrison's development in HOL Light), which I later took over and mostly replaced by new material.

1 Introduction

The formalisation of Apostol's book in Isabelle/HOL started from the simple desire to have more properties about Euler's φ function available in the system. However, Apostol's style turned out to be very amenable to formalisation, and the subject matter was both of great interest as a basis for further development of number theory in Isabelle and as a case study for Isabelle's libraries on asymptotics and complex analysis. After 1.5 years of a highly part-time one-person effort, 9 of the 14 chapters are mostly formalised with 3 of the remaining ones mostly consisting of material that is already available in the Isabelle library.

The full development is much too large to be presented here. Thus, in the following sections, I will go through a high-level description of some of the most interesting material, with a particular focus on parts where I encountered difficulties or chose a different route than Apostol did in his book.

Let me give an outline of the sections to follow: Section 2 gives a brief overview of the material that was and was not formalised. Section 3 lists related work. Section 4 introduces multiplicative characters and Dirichlet characters. Section 5 defines formal Dirichlet series and their connection to complex-analytic functions. Section 6 builds on this to treat various L functions, such as the famous Riemann ζ function. Section 7 describes my formalisation

of the Prime Number Theorem (PNT). Section 8 gives an overview of the size of various parts of my formalisation and the effort involved in creating it. Lastly, in Section 9, some conclusions are drawn from this project.

2 Scope

Every theorem shown in this presentation was formalised in Isabelle. The developments are available either in the Isabelle library or in the *Archive of Formal Proofs* (AFP). Many additional results were also formalised but due to space constraints, I will not give an extensive list here. Instead, I will give a rough overview of which parts of Apostol's book have been formalised and which have not:

- Chapters 2, 3, 4, and 6 were completely formalised.
- Chapters 10, 11, and 12 were fully formalised with the exception of a few theorems.
- Chapter 7 (Dirichlet's theorem) was ignored since I have a different proof (using Newman's proof for the non-vanishing of $L(\chi, s)$ [20] and then following Harrison's formalisation [15]).
- Chapter 13 consists of Apostol's analytic proof of the PNT and some consequences of the PNT. The latter were formalised with one small exception; for the former, I follow a different approach described by Newman [20].
- The material from Chapters 1 and 5 and the first half of Chapter 9 was already present in the Isabelle library, or added to it independently by other people around the same time (most notably the Jacobi symbol and more material on the Legendre symbol by Daniel Stüwe). I merely filled some occasional gaps in these chapters.
- The second half of Chapter 9 was skipped since it is merely an example.
- Chapter 8 and the second half of Chapter 9 concern Gauss sums and induced Dirichlet characters. I skipped them and the small amount of material in other chapters that depends on them. I consider this future work.
- Chapter 14 (number partitions) was also not formalised at all. It is almost completely independent of the rest of the book. Some material on this is available in the AFP [5].

Of Apostol's examples, the more interesting ones (e. g. applications of the techniques that were developed) were typically formalised, whereas the less interesting ones (e. g. those that only served to illustrate a definition) were not. Uninteresting technical results that Apostol uses to derive another result that I obtained in a different way were also sometimes skipped.

Notably, I also formalised some results that Apostol does not treat but that seemed interesting to me or made the library more complete, e. g. on Pontryagin duality or formal exponentials and logarithms of Dirichlet series.

3 Related Work

The first formalisation of a result related to this work was that of the PNT in Isabelle/HOL by Avigad *et al.* [2] in 2007. They formalised the elementary Selberg–Erdős proof.[1] Carneiro formalised the same proof in Metamath [7].

[1] Unfortunately, this work was never submitted to the AFP and has not been maintained since then. At the time of writing this paper, the proofs are 12 years old; the formalisation comprises almost 27,000 lines, and many of them are unstructured proof scripts. Bringing them up to date to work with a modern version of Isabelle would be a massive undertaking. However, much of the more general material developed by Avigad *et al.* was moved to Isabelle's library, and for a considerable part of the remaining material, equivalent results are now already a part of the Isabelle library or my work anyway.

Harrison later developed the first (and until now only) formalisation of an analytic proof of the PNT in 3,600 lines [16] of HOL Light. He used Newman's presentation of the proof, which I also did. Harrison also proved Dirichlet's Theorem [15] and I used parts of his formalisation as a template for mine. Moreover, formalisations of Bertrand's postulate exist by Harrison in HOL Light, by Théry in Coq, by Riccardi in Mizar [21], by Carneiro in Metamath [6], by Asperti and Ricciotti in Matita [1], and by Biendarra and Eberl in Isabelle/HOL [4].

The big difference between these formalisations and the present one is that this one contains not just *one* result and the material required for it, but the majority of a textbook on the subject. Many proofs are much simpler and more 'high-level' through the use of *Dirichlet series* and Isabelle's advanced machinery for asymptotic reasoning.

4 Characters of a Finite Abelian Group

The first concept we shall explore is that of a *multiplicative character*, which will be needed to prove Dirichlet's theorem. For this section, let $G = (G, \otimes, 1)$ be a finite abelian group.

▶ **Definition 1** (Multiplicative character). *A* character *is a group homomorphism $\chi : G \to \mathbb{C}^\times$, i. e. $\chi(1) = 1$ and $\chi(a \otimes b) = \chi(a)\chi(b)$ for any $a, b \in G$. The character χ_0 that maps every element to 1 is called the* principal character*.*

For the necessary group theory, I use the `HOL-Algebra` library by Ballarin, which models a group as a record containing entries for the operation $\otimes$, the neutral element 1, and an explicit carrier set (which does not have to be the full type universe). The latter is necessary in HOL because notions such as subgroups cannot easily be expressed without explicit carrier sets. The fact that such a record indeed describes a group is then formalised as a *locale* [3] called *group*, which fixes such a record and assumes that all the usual group axioms hold.

A character can then be defined as a locale that extends the *group* locale by fixing a function $\chi :: \alpha \to \mathbb{C}$ (where α is the type of the group elements) and assuming that the two homomorphism properties mentioned above hold for χ. For convenience, I only assume $\chi(1) \neq 0$ (from which $\chi(1) = 1$ easily follows) and I additionally require $\chi(x) = 0$ for any x not in the carrier of the group. The latter is to ensure *extensionality*, i. e. two characters are equal as HOL values iff they return the same result on every group element.

▶ **Definition 2** (Pontryagin dual group). *Denote the set of characters of G by $\widehat{G}$. Then $\widehat{G}$ forms a group $\widehat{G} := (\widehat{G}, \cdot, \chi_0)$ with point-wise multiplication and χ_0 as the identity. This group is called the* Pontryagin dual group *of G.*

▶ **Theorem 3** (Number of characters). $|\widehat{G}| = |G|$

Apostol shows this the following way: He notes that it clearly holds for the trivial group $\{1\}$ and that, if it holds for a subgroup H, it also holds for $\langle H; x\rangle$ where $\langle H; x\rangle$ is the smallest subgroup containing $H \cup \{x\}$. Since G is finite, we can reach G through this process in finitely many steps. In Isabelle, it is convenient to prove a custom induction rule for this kind of reasoning:

▶ **Lemma 4** (Induction on a group). *Let $G = (G, \otimes, 1)$ be a group and H some subgroup of G. Let P be some property on groups. If $P(H)$ holds and $P(H')$ implies $P(\langle H'; x\rangle)$ for any subgroup $H' \supseteq H$ and $x \in G \setminus H'$, then $P(G)$ holds.*

I use this to show a stronger version of Theorem 3 that is just as easy to show:

▶ **Theorem 5** (Number of character extensions). *Let H be a subgroup of G and $\chi \in \widehat{H}$. Let*

$$C(G) := \{\chi' \in \widehat{G} \mid \forall x \in H.\ \chi'(x) = \chi(x)\}$$

denote the set of characters on G that agree with χ on H. Then $|C(G)| \cdot |H| = |G|$, i. e. there are precisely $|G|/|H|$ ways to extend a character on H to a character on G.

Proof. We perform induction on G according to Lemma 4. The base case is trivial, so fix some $H' \supseteq H$ and $x \in G \setminus H'$. Let n be the index of x in H', i. e. the smallest $n \in \mathbb{N}_{>0}$ such that $x^n \in H'$. Then $|\langle H'; x\rangle| = n \cdot |H'|$. Moreover,

$$f : C(\langle H'; x\rangle) \to C(H') \times \{z \in \mathbb{C} \mid z^n = 1\}, \quad f(\chi) = (y \mapsto \chi(y), \chi(x))$$

is a bijection so that $|C(\langle H'; x\rangle)| = n \cdot |C(H')| \overset{\text{IH}}{=} n \cdot |H'|$. ◀

Theorem 3 follows directly by taking $H = (\{1\}, \otimes, 1)$. Another useful corollary is this:

▶ **Corollary 6.** *For any $x \neq 1$, there exists a $\chi \in \widehat{G}$ such that $\chi(x) \neq 1$.*

Next, we can prove a nice property that Apostol does not cover at all:

▶ **Theorem 7** (Isomorphism to the double dual). *G is isomorphic to its double dual via the natural isomorphism $\nu : G \to \widehat{\widehat{G}}$, $\nu(x) = (\chi \mapsto \chi(x))$.*

Proof. It is easy to check that ν is a homomorphism. By Corollary 6, $\ker(\nu) = \{1\}$, so it is injective. Since $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$, it is then also surjective. ◀

This isomorphism between is useful for the next properties:

▶ **Theorem 8** (Orthogonality relations). *For any $\chi \in \widehat{G}$ resp. $x \in G$, we have:*

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases} \quad (1) \qquad \sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} |G| & \text{if } x = 1 \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

Proof. Apostol's proof for (1) is very simple, so I omit it here. In order to show (2) from (1), Apostol represents the set of characters of G as a *character table* of G, i. e. a $|G| \times |G|$ complex matrix. If we denote this matrix by A, (1) shows that $AA^* = nI$ (where A^* is the conjugate transpose of A). By simple linear algebra, $A^*A = nI$ and therefore (2) follows.

Formalising this argument would have required importing Isabelle's linear algebra library and doing some tedious work to relate the matrix to the characters, so I chose another route. One *can* prove (2) relatively easily using the same induction principle as before in about 70 lines, but the easiest way is to simply use Pontryagin duality: (2) is, in fact, nothing but (1) with $G \to \widehat{G}$ and $\chi \to \nu(x)$. This requires only 6 lines of Isabelle code. ◀

▶ **Definition 9** (Dirichlet character). *A Dirichlet character χ for the modulus $m \in \mathbb{N}_{>1}$ is a character of the multiplicative group of the residue ring $\mathbb{Z}/m\mathbb{Z}$. For convenience, χ is represented as a periodic function of type $\mathbb{N} \to \mathbb{C}$ with period m, i. e. $\chi(k) = \chi(k \bmod m)$.*

5 Dirichlet Series

The central objects in analytic number theory are *Dirichlet series*. These are the main tools that set apart my approach to formalised number theory from that of previous formalisation work in multiplicative number theory like that by Avigad *et al.*, Harrison, and Carneiro.

▶ **Definition 10** (Formal Dirichlet series). *A formal series of the form* $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ *is called a Dirichlet series. Typically, the* a_n *are real or complex. The Dirichlet series over* $\mathbb{R}$ *or* $\mathbb{C}$ *form a commutative ring with the obvious choices for 0, 1, and addition. Multiplication is defined as* $(\sum_{n=1}^{\infty} a_n n^{-s}) \cdot (\sum_{n=1}^{\infty} b_n n^{-s}) = \sum_{n=1}^{\infty} (\sum_{k \cdot l = n} a_k b_l) n^{-s}$. *Also,* $\sum_{n=1}^{\infty} a_n n^{-s}$ *has a multiplicative inverse iff* $a_1 \neq 0$.

▶ **Theorem 11** (Convergence of Dirichlet series). *Each Dirichlet series has abscissæ of convergence* σ_c *and absolute convergence* σ_a *such that the infinite sum corresponding to it is absolutely summable for* $\Re s > \sigma_a$*, conditionally summable for* $\Re s \in (\sigma_c; \sigma_a)$*, and divergent for* $\Re s < \sigma_c$*. The* σ_c *and* σ_a *satisfy* $\sigma_c \leq \sigma_a \leq \sigma_c + 1$ *and may be* $\pm\infty$.

Much like formal power series (i. e. ordinary generating functions) for combinatorics, Dirichlet series are closely associated with number theory. Like generating functions, they are of great interest as mere formal objects, but when they converge, their interpretation as a complex-valued function is also enormously useful, as we will see.

Various formal analogues of analytic operations can be defined on formal Dirichlet series e. g. reciprocal, derivative, integral, $\exp(f(s))$, $\ln f(s)$, $f(s+s_0)$, $f(m \cdot s)$, and subseries. These have similar properties to their analytic counterparts (e. g. $\exp(f(s))' = f'(s)\exp(f(s))$) even when they do not convergece. When they do converge, they typically agree with their analytic counterparts. This allows one to prove properties of the analytic functions by reasoning on the formal level and vice versa.

There are 4,800 lines of material on formal Dirichlet series in my formalisation. This is far too much to show here, so I simply say that it contains all of Chapter 11 in Apostol's book and more, except for Sections 11.10 and 11.11. I will only show a few small examples that illustrate the afore-mentioned interplay of the formal and the analytical level:

One example of using a simple equality in the ring of formal Dirichlet series to derive an analytic result is this:

▶ **Theorem 12.** *Let* $\omega(n)$ *be the number of distinct prime factors of* n *and* $\mu(n)$ *the Möbius* μ *function, i. e.* 0 *if* n *is not square-free and* $(-1)^{\omega(n)}$ *otherwise. Then* $\sum_{n=1}^{\infty} \mu(n)/n^2 = 6/\pi^2$.

Proof. Consider the formal series $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$ and $M(s) := \sum_{n=1}^{\infty} \mu(n) n^{-s}$. It is clear that they both converge absolutely for $\Re s > 1$ by the comparison test. It is easy to show $\sum_{d|n} \mu(d) = [n = 1]$, i. e. $\zeta(s)M(s) = 1$ holds formally. Thus, it also holds analytically for $\Re s > 1$ so that we have $\zeta(2)M(2) = 1$ and therefore $M(2) = 1/\zeta(2)$, where $\zeta(2)$ has the well-known value $\pi^2/6$. ◀

The following theorem allows us to transfer an analytic equality to the formal level:

▶ **Theorem 13** (Uniqueness of Dirichlet series). *Let* $f(s) = g(s)$ *be two formal Dirichlet series whose abscissa of convergence is* $< \infty$*. If there exists a sequence* s_k *with* $\Re s_k \longrightarrow \infty$ *and* $\forall k.\ f(s_k) = g(s_k)$*, then* $f(s)$ *and* $g(s)$ *are equal as formal Dirichlet series.*

▶ Remark 14. In Isabelle, the condition on the existence of the sequence s_k is replaced by the following equivalent and more concise formulation using *filters* [18]:

$$\exists_F\ s \textbf{ in } \Re \textbf{ going-to } \text{at-top}.\ f(s) = g(s)$$

Here, the '$\exists_F\, x$ **in** F. $P(x)$' notation stands for 'frequently', i. e. the complement of P is not in the filter F. The filter 'f **going-to** F' is the contravariant image of F under f.

▶ **Definition 15** (Truncation operator)**.** *For a Dirichlet series $f(s) = \sum_{n=1}^{\infty} a_n s^{-n}$, let $T_m(f(s)) = \sum_{n=1}^{m} a_n s^{-n}$ denote the m-th order truncation of $f(s)$. The result is a Dirichlet polynomial, i. e. a Dirichlet series with only finitely many non-zero coefficients.*

▶ **Theorem 16.** $f(s) = g(s) \longleftrightarrow \forall m.\ T_m(f(s)) = T_m(g(s))$.

The following is an instance where these theorems are used to avoid a lot of complicated reasoning on the formal level by leveraging a result on the analytic level:

▶ **Theorem 17.** *For any (not necessarily convergent) Dirichlet series $f(s)$ and $g(s)$, we have* $\exp(f(s) + g(s)) = \exp(f(s)) \exp(g(s))$.

Proof. It is clear that the result holds analytically whenever the series converge, so if the series have a non-empty half-plane of convergence, they must be equal by Theorem 13. The question is how to show this if we do *not* know whether the series converge anywhere.

The key is to use Theorem 16 together with $T_m(\exp(h(s))) = T_m(\exp(T_m(h(s))))$. This allows us to assume w. l. o. g. that the series in question are Dirichlet polynomials and therefore converge everywhere. ◀

▶ Remark 18. This technique of showing an equality on Dirichlet series by showing that it holds for all Dirichlet polynomials works if the two sides of the equation in question are continuous functions w. r. t. the topology on formal Dirichlet series, i. e. each coefficient of the result only depends on finitely many coefficients of the input. The topological structure of Dirichlet series was not formalised yet, but this is a useful fact to keep in mind.

The following is another important theorem connecting a series with the function it defines that we will use later:

▶ **Theorem 19** (Pringsheim–Landau)**.** *Let $f(s)$ be a Dirichlet series with non-negative real coefficients and $\sigma_a \in \mathbb{R}$. Then $f(s)$ has a singularity at σ_a.*

Conversely, if $f(s)$ has an an analytic continuation to some half-plane $\{s \mid \Re s > c\}$, then $\sigma_a \leq c$. In particular, if $f(s)$ is entire, the series must converge everywhere.

Lastly, purely on the formal level, the following is a representative example of a whole variety of interesting asymptotic results: For $\sigma_0(n)$ (the number of divisors of n), the trivial equality of formal Dirichlet series $\sum_{n=1}^{\infty} \sigma_0(n) n^{-s} = \zeta(s)^2$ implies:

▶ **Theorem 20.** $d(n) = x \ln x + (2\gamma - 1)x + O(\sqrt{x})$ *for the Euler–Mascheroni constant γ.*

6 The L Functions

In this section, we will look at four functions from the class of L functions: Riemann's ζ function, Dirichlet's L function, Hurwitz's ζ function, and the periodic ζ function. These are all complex-valued functions that are defined by an infinite sum for $\Re s > 1$ and can be analytically or meromorphically continued to the entire complex plane.

▶ **Definition 21** (Riemann's ζ function)**.** *For $\Re s > 1$, the Riemann ζ function is given by the Dirichlet series $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.*

▶ **Definition 22** (Dirichlet L functions)**.** *Let χ be a Dirichlet character for the modulus $m > 0$. Then $L(s, \chi)$ is given by the Dirichlet series $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$ for $\Re s > 1$ if $\chi = \chi_0$ and for $\Re s > 0$ if $\chi \neq \chi_0$.*

We immediately get the following properties for free from the Dirichlet series library:

▶ **Theorem 23.** *Let $\Lambda(n)$ denote the von Mangoldt function. Then, if $\Re s > 1$:*

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} \qquad \zeta'(s) = -\sum_{n=1}^{\infty} \frac{\ln n}{n^s} \qquad \ln \zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\ln n \cdot n^s}$$

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}} \qquad L'(s,\chi) = -\sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n^s} \qquad \ln L(s,\chi) = \sum_{n=2}^{\infty} \frac{\chi(n)\Lambda(n)}{\ln n \cdot n^s}$$

However, $\zeta(s)$ and $L(s,\chi)$ can be defined on a larger domain:

▶ **Theorem 24** (Analytic continuation of $\zeta(s)$ and $L(s,\chi)$)**.**

1. *$\zeta(s)$ can be continued to an analytic function on $\mathbb{C} \setminus \{1\}$ with a simple pole at $s = 1$.*
2. *For non-principal χ, $L(s,\chi)$ can be continued to an entire function.*
3. *For $\chi = \chi_0$, we have $L(s,\chi_0) = \zeta(s) \cdot \prod_{p|m}(1-p^{-s})$, i. e. $L(s,\chi_0)$ is equal to $\zeta(s)$ up to an entire factor and is therefore also analytic on $\mathbb{C} \setminus \{1\}$ with a simple pole at $s = 1$.*

The difficult part here is to actually construct the analytic continuations. To do this uniformly and without duplication of work, Newman uses a generalisation of $\zeta(s)$:

▶ **Definition 25** (Hurwitz's ζ function)**.** *Let $a \in \mathbb{R}_{>0}$ and $\Re s > 1$. Then $\zeta(s,a)$ is given by the (non-Dirichlet) series $\zeta(s,a) = \sum_{n=0}^{\infty} (n+a)^{-s}$.*

▷ Claim 26. Like the Riemann ζ function, the Hurwitz ζ function can be continued to an analytic function on $\mathbb{C} \setminus \{1\}$ with a simple pole at $s = 1$, and by letting $a = 1$, we recover the Riemann ζ function on its full domain so that an analytic continuation for Hurwitz's ζ also gives us one for Riemann's ζ.

▶ **Theorem 27** (Expressing $L(s,\chi)$ in terms of $\zeta(s,a)$)**.** *For any Dirichlet character χ modulo m, we have for all s with $\Re s > 1$: $L(s,\chi) = m^{-s} \sum_{k=1}^{m} \chi(k)\zeta(s,k/m)$*

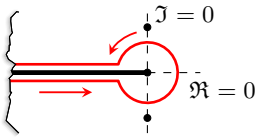
Due to Claim 26, the right-hand side constitutes an analytic continuation of $L(s,\chi)$ to all of $\mathbb{C} \setminus \{1\}$. All that remains now is to handle the removable singularity at 1 for non-principal χ, for which we can simply evaluate the Dirichlet series for $L(s,\chi)$ directly since it converges for all $\Re s > 0$. The main question now is therefore how to construct $\zeta(s,a)$.

6.1 Analytic Continuation of Hurwitz's ζ Function

Apostol constructs the continuation using the following result:

▶ **Theorem 28.** *For $\Re s > 1$, we have*

$$\zeta(s,a) = \frac{\Gamma(1-s)}{2i\pi} \int_C \frac{z^{s-1}e^{az}}{1-e^z}\, dz \qquad \text{where } C =$$



if the inner circle has radius $r < 2\pi$.[2] *This continues $\zeta(s,a)$ analytically to $\mathbb{C} \setminus \{1\}$.*

[2] There is a subtlety hidden in this integral that will be discussed in Section 6.3.1.

In Isabelle, contour integrals are only defined for finite contours, so this 'improper contour integral' has to be expressed as the sum of a contour integral along the circular part and two Lebesgue integrals $\int_r^\infty$. Formalising this theorem seemed somewhat daunting to me at the time, which is why I chose another route[3]: Applying the Euler–MacLaurin summation formula [10] to the sum in the definition of $\zeta(s,a)$ for $\Re s > 1$, we obtain

$$\sum_{n=0}^{\infty}(s+a)^{-n} - \frac{a^{1-s}}{s-1} = \frac{a^{-s}}{2} + \sum_{i=1}^{N}\frac{B_{2i}}{(2i)!}\,a^{-s-2i+1}\,s^{\overline{2i-1}} + \frac{(-1)^{2N}\,s^{\overline{2N+1}}}{(2N+1)!}\int_0^\infty P_{2N+1}(t)\cdot(t+a)^{-s-2N-1}\,\mathrm{d}t \tag{3}$$

where $s^{\overline{k}}$ denotes the rising factorial, B_k is the k-th Bernoulli number, and $P_k(t)$ is the periodic version of the Bernoulli polynomial $B_k(t)$, i. e. $P_k(t) = B_k(t - \lfloor t \rfloor)$.

One can see with some effort that the right-hand side is now actually analytic on a larger domain: all terms except the last one are clearly entire functions in s; the only problematic term is the integral in the last summand. Leibniz's rule shows that the integral is analytic on compact intervals $[0;b]$, and an integral version of the Weierstraß M-test shows that the indefinite integral is uniformly convergent and therefore analytic for $\Re s > -2N$.

Let us write $\mathit{prezeta}_N(s,a)$ for the right-hand side. This is then a function in s that is analytic for $\Re s > -2N$ and that also fulfils

$$\mathrm{prezeta}_N(s,a) = \sum_{n=0}^{\infty}(s+a)^{-n} - \frac{a^{1-s}}{s-1} \qquad \text{for } \Re s > 1\ .$$

This means that two functions $\mathit{prezeta}_M$ and $\mathit{prezeta}_N$ will always agree on $\Re s > 1$, and by analytic continuation they will then also agree on their entire domain, i. e. for all s with $\Re s > -2\max(M,N)$. We can therefore define a full analytic continuation to all of $\mathbb{C}$ by choosing N 'big enough' for each input, i. e. we define:

$$\mathrm{prezeta}(s,a) := \mathrm{prezeta}_{\max(0,1-\lceil \Re s/2\rceil)}(s,a)$$

It is then easy to show that this function is entire and agrees with any of the $\mathit{prezeta}_N(s,a)$ for all s with $\Re s > -2N$. In particular, it is an analytic continuation of the left-hand side of (3) so that we can now simply define

$$\zeta(s,a) := \mathrm{prezeta}(s,a) + \frac{a^{1-s}}{s-1}$$

to obtain a valid definition of the Hurwitz ζ function on all of $\mathbb{C}\setminus\{1\}$. The advantage of this approach is that it is fairly simple to implement in Isabelle because all of the 'heavy lifting' has already been done in the AFP entry on the Euler–MacLaurin formula.

Various basic properties of the Hurwitz and Riemann ζ functions then follow in a straightforward way, of which I show some notable ones here:

▶ **Theorem 29** (Special values of ζ). *For any $n \in \mathbb{N}_{\geq 0}$, we have:*

$$\zeta(a,-n) = -\frac{B_{n+1}(a)}{n+1} \qquad \zeta(-n) = -\frac{B_{n+1}}{n+1} \qquad \zeta(2n) = \frac{(-1)^{n+1}\cdot B_{2n}\cdot(2\pi)^{2n}}{2(2n)!}$$

[3] I eventually proved it anyway since it is required for the proof of Hurwitz's formula (see Section 6.3), but I do not use it to define $\zeta(s,a)$.

where $B_n = B_n(1)$ are the Bernoulli numbers with $B_1 = \frac{1}{2}$. In particular, this implies the famous $\zeta(-1) = -\frac{1}{12}$ and $\zeta(2) = \pi^2/6$.

▶ **Theorem 30** (Integral representation for $\zeta(s,a)$)**.** *For any s with $\Re s > 1$, we have:*

$$\Gamma(s)\zeta(s,a) = \int_0^\infty \frac{t^{s-1}e^{-at}}{1-e^{-t}}\,dt$$

6.2 The Non-Vanishing of $\zeta(s)$ and $L(s,\chi)$ for $\Re s = 1$

The following is a core ingredient in the Prime Number Theorem and Dirichlet's Theorem:

▶ **Theorem 31.** *For any s with $\Re s \geq 1$, we have $\zeta(s) \neq 0$ and $L(s,\chi) \neq 0$.*

Proof. The case of $\Re s > 1$ is a simple consequence of the Euler product formula for $\zeta(s)$ and $L(s,\chi)$ (cf. Theorem 23); the difficult part is the case $\Re s = 1$. A very simple proof of this is presented by Newman [20]. Very briefly, it works like this for $\zeta(s)$:

Suppose $\zeta(1+\tau i) = 0$ for $\tau \neq 0$. By $\zeta(\overline{s}) = \overline{\zeta(s)}$, it follows that $\zeta(1-\tau i) = 0$ as well. If we form $\zeta(s)\zeta(s+\tau i)$, the simple pole of $\zeta(s)$ at $s = 1$ is cancelled by the zero of $\zeta(s+\tau i)$. By analogous reasoning, $f(s) := \zeta(s)^2\zeta(s+\tau i)\zeta(s-\tau i)$ has only removable singularities and is therefore entire.

We now leave the world of analytic complex functions for a moment and go to formal Dirichlet series. Using $\ln\zeta(s) = \sum_{n=1}^\infty \Lambda(n)/\ln n \cdot n^{-s}$, it is easy to see that

$$\ln f(s) = \sum_{n=1}^\infty \frac{2(1+\cos(a\ln k))\Lambda(n)/\ln n}{n^s}$$

as a formal Dirichlet series. These coefficients are obviously non-negative, which implies that those of $\exp(\ln f(s)) = f(s)$ are as well.

Combining these two facts with the Pringsheim–Landau theorem, we obtain that $f(s)$ converges *everywhere*. This outrageous claim is then easy to refute: if $f(s) = \sum_{n=1}^\infty a_n n^{-s}$ were to converge everywhere, then so would the subseries $g(s) := \sum_{k=0}^\infty a_{2^k}\left(2^k\right)^{-s}$ with the analytic continuation

$$g(s) = \frac{1}{(1-2^{-s})^2}\cdot\frac{1}{1-2^{-s-\tau i}}\cdot\frac{1}{1-2^{-s+\tau i}}$$

for $\Re s > 0$. However, it is clear that the right-hand tends to ∞ as $s \to 0$ along the positive real axis. On the other hand, since its series converges everywhere, $g(s)$ is entire and must tend to a finite limit as $s \to 0$. This is a contradiction. ◀

With small adjustments, the same argument applies to $L(s,\chi)$ for $\chi \neq \chi_0$ with modulus m:

- We replace ζ in the above proof by $h(s) := \prod_\chi L(s,\chi)$ where the product extends over all characters with modulus m.
- Instead of taking the subseries of powers of 2, we now take the subseries of powers of some prime $p > m$.

The above proofs are stunningly short and simple. The gain is most striking for the Dirichlet L function, where Apostol's proof only treats the case of $s = 1$, but that proof is still more complicated than Newman's and involves lengthy complicated 'Big-O' reasoning. Indeed, in a first version of the formalisation, I formalised Apostol's proof, but it was considerably longer and messier than the new version – with the added bonus that the new one is also more general.

Harrison also only proves $L(1,\chi) \neq 0$ – indeed, he does not define $L(s,\chi)$ at all; he defines only $L(1,\chi)$ since that is all that is required for Dirichlet's theorem. Despite this and the much higher verbosity of structured Isabelle proofs compared to HOL Light, his proof is longer than mine. The reason for this is that his proof is very elementary and uses very little library material while mine builds on a large library of Dirichlet series. However, I think that the comparison is still not entirely unjustified since all of this material is sufficiently general to be called 'library material' (as opposed to technical lemmas specifically designed for this one proof), and building sufficiently large and general libraries to make proofs like this cleaner and easier is, after all, one of our goals in formalisation.

6.3 Hurwitz's Formula

More as a challenge to myself and the Isabelle libraries, I chose to formalise another non-trivial property of the ζ functions:

▶ **Theorem 32** (Reflection formula for $\zeta(s)$)**.** *For $s \notin \{0,1\}$, we have:*

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

Note that while $\Gamma(s)$ has poles at $s \in \mathbb{Z}_{\leq 0}$, its reciprocal $1/\Gamma(s)$ is entire, so the formula holds even for $s \in \mathbb{Z}_{<0}$.

This formula is a corollary of a more general one for $\zeta(s,a)$ known as *Hurwitz's formula*:

▶ **Theorem 33** (Hurwitz's formula)**.** *Let $a \in (0;1)$ and $s \in \mathbb{C} \setminus \{0\}$ with $a \neq 1 \vee s \neq 1$. Then:*

$$\frac{1}{\Gamma(s)} \cdot \zeta(1-s,a) = (2\pi)^{-s}\big(i^{-s}F(s,a) + i^{s}F(s,-a)\big)$$

Here, $F(s,a)$ is the *periodic ζ function*, which we still have to define:

▶ **Definition 34** (Periodic ζ function)**.** *For $\Re s > 1$, the periodic ζ function $F(s,a)$ is given by the Dirichlet series $F(s,a) = \sum_{n=1}^{\infty} e^{2i\pi na} n^{-s}$.*

▷ Claim 35. $F(s,a)$ is called *periodic* because $F(s,a+n) = F(s,a)$ for any integer n. For non-integer a, the above series converges for $\Re s > 0$ and can be continued to an entire function. For integer a, it is simply the Riemann ζ function.

The strategy I used to construct this analytic continuation of $F(s,a)$ for non-integer a is somewhat interesting: Theorem 33 can be rearranged to give a formula that expresses $F(s,a)$ in terms of $\zeta(1-s,a)$ and $\zeta(1-s,1-a)$:

▶ **Theorem 36.** *Let $a \in (0;1)$ and $s \in \mathbb{C} \setminus \mathbb{N}$. Then:*

$$F(s,a) = i(2\pi)^{s-1}\Gamma(1-s)\big(i^{-s}\zeta(1-s,a) - i^{s}\zeta(1-s,1-a)\big)$$

We therefore proceed like this (assuming w. l. o. g. $a \in (0;1)$):

1. Show Theorem 33 for $\Re s > 1$ (where F is simply given by its Dirichlet series).
2. Use this to show Theorem 36 for $\Re s > 1$.
3. Use the right-hand side of Theorem 36 as the definition of $F(s,a)$ for $s \notin \mathbb{N}$. Compatibility with the Dirichlet series definition follows by analytic continuation.
4. Since the Dirichlet series definition covers $\Re s > 0$ and the new definition covers $\mathbb{C} \setminus \mathbb{N}$, the only point left is $s = 0$, which is a removable singularity that can be eliminated via

$$F(0,a) := \lim_{s \to 0} F(s,a) = \frac{i}{2\pi}\big(\text{prezeta}(1,a) - \text{prezeta}(1,1-a) + \ln(1-q) - \ln q\big) - \frac{1}{2}\,.$$

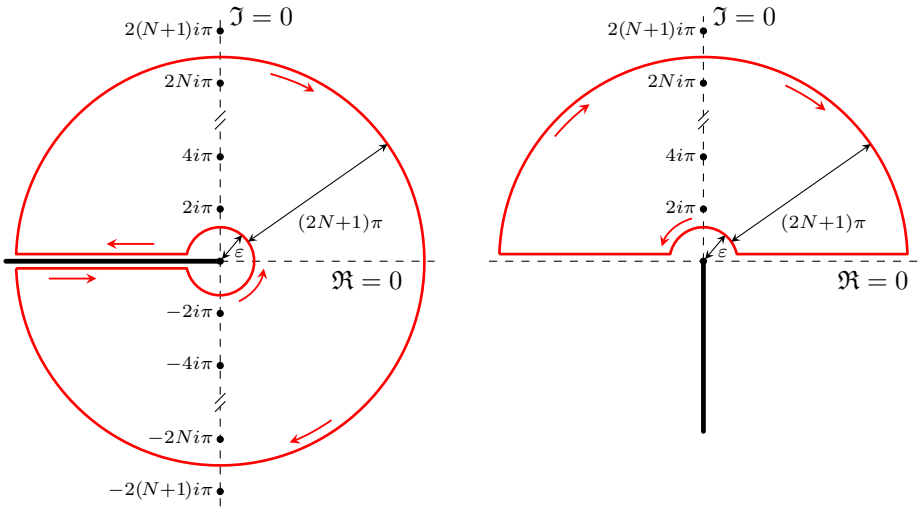


Figure 1 Apostol's integration contour and my modified version for proving Hurwitz's formula. The black dots are the poles of the integrand; the thick black line is its branch cut. Note that in both cases, the line segments of the contour lie *on* the real axis despite the small gap in the illustration.

5. Extend the validity of Theorems 33 and 36 to their full domains by analytic continuation.

The only difficult part here is the first step, which we shall look at now:

Proof. Apostol's proof uses the afore-mentioned contour integral representation for $\zeta(s, a)$ (see Theorem 28). He uses a finite version γ_N of the Hankel contour obtained by cutting of the lines extending to infinity at a finite radius $(2N+1)\pi$ and connecting the ends with a circle (see Figure 1). Applying the Residue theorem to this contour gives us:

$$\frac{1}{2i\pi}\int_{\gamma_N} \frac{z^{-s}e^{az}}{1-e^z}\,\mathrm{d}z = \sum_{z_0 \text{ is a pole}} \mathrm{ind}_{\gamma_N}(z_0)\cdot \operatorname*{Res}_{z=z_0}\left(\frac{z^{-s}e^{az}}{1-e^z}\right).$$

As $N \to \infty$, the contribution of the outer circle vanishes so that the integral on the left-hand side converges to the integral in Theorem 28 for $s \to 1-s$ and thus the left-hand side tends to $\zeta(1-s,a)/\Gamma(s)$.

The poles of the integrand are at $2ni\pi$ for $n \in \mathbb{Z} \setminus \{0\}$. The winding numbers are 1 for all poles with $|n| \leq N$ and 0 otherwise. At each pole, the integrand is of the form $f(z)/g(z)$ where f is analytic and g has a simple zero, so we can simply compute the residues as $f(2ni\pi)/g'(2ni\pi)$. Thus, the right-hand side simplifies to

$$\frac{i^{-s}}{(2\pi)^s}\sum_{n=1}^{N}\frac{e^{2ni\pi a}}{n^s} + \frac{i^s}{(2\pi)^s}\sum_{n=1}^{N}\frac{e^{-2ni\pi a}}{n^s} \xrightarrow{N\to\infty} \frac{i^{-s}}{(2\pi)^s}F(s,a) + \frac{i^s}{(2\pi)^s}F(s,-a).$$

This concludes the proof of Hurwitz's formula for $\Re s > 1$. ◀

The formalisation of the proof was fairly routine. It is, however, quite large and tedious, containing almost 1,000 lines of proof code compared to 6.5 pages in Newman's book (both including the proof of Theorem 28). This seems to be a common pattern in Isabelle proofs using the Residue theorem and it is likely due to the many side conditions that need to be shown, many of which are of geometric nature and thus much easier to explain to a human

than to a theorem prover. There are, however, also occasional encouraging surprises: For example, some side conditions consist of showing that certain indefinite integrals exist. For the integral

$$\int_\varepsilon^\infty \frac{x^y e^{-ax}}{1-e^{-x}}\,\mathrm{d}x \qquad \text{for } \varepsilon > 0,\ a > 0$$

this proof is a mere 17 lines thanks to the fact that the asymptotic estimate $\frac{x^y e^{-ax}}{1-e^{-x}} \in O(e^{-\frac{1}{2}ax})$ can be proven fully automatically by Isabelle's `real_asymp` tactic, making the Isabelle proof of this particular statement even shorter than Apostol's proof in his book.

Two aspects of the formal proof deserve more attention, and we will discuss them now.

6.3.1 Branch Cuts

The term z^{-s} is a multi-valued function. It is defined in Isabelle as $e^{-s \ln z}$ where ln is the standard branch of the logarithm, which has a branch cut on the negative real axis. Two parts of Apostol's contour lie directly on this cut, taking different branches of the logarithm. This is unproblematic when considering the integrand as a multi-valued function in the sense of a Riemann surface, but we do not have any of this analytic machinery in Isabelle.

My first idea to circumvent this problem was to resort to some kind of limiting argument by placing the two horizontal lines not directly on the real axis, but some ε above (resp. below) it. However, this would likely have been a very tedious argument to do rigorously. I therefore decided to instead cut the contour in two halves. When their integrals are added together, we recover Apostol's contour integral. Due to symmetry, it is actually enough to look at the upper half (see Figure 1), as the lower one follows by conjugation.

For the upper contour, it is now clear that we can integrate over the same branch of the logarithm everywhere. In order to avoid the branch cut of the standard logarithm, I use a different branch $\widehat{\ln} z := \ln(-iz) + \frac{1}{2}i\pi$, whose branch cut lies on the negative imaginary axis, safely away from our contour (see Figure 1).

6.3.2 Winding Numbers

The evaluation of the winding numbers is easy for a human: the contour *clearly* winds counterclockwise around each pole with $|n| \leq N$, and all the other poles are clearly completely outside the contour. Proving these things in a theorem prover, especially for a more complicated contour such as this one, is notoriously difficult [16]. To show that the poles outside the contour really do lie outside (i. e. have winding number 0), I use simple geometric arguments: for the branch cut on the negative imaginary axis, one can draw a vertical line from each point to $-i\infty$ without crossing γ_N, so the winding number for these points must be 0. Moreover, γ_N is contained in a ball of radius $(2N+1)\pi$, which is a convex set that does not contain any of the poles with $n > N$. Thus, these poles must also have winding number 0.

The more difficult part is to show that the winding number for the points inside the contour is 1. Geometric arguments for this are difficult. One approach would be to show that the contour is a closed simple curve (which implies that the winding number must be either -1, 0, or 1) and then analyse the contributions of the four different parts of the curve to show that the overall value must be positive, thus 1. However, to avoid having to do this work, I instead use Li's framework for computing Winding numbers in Isabelle [19]. It uses Cauchy indices and comes with some setup to handle combinations of line segments and circular arcs almost automatically, allowing me to prove that the winding number is 1 with a mere 18 lines of proof code.

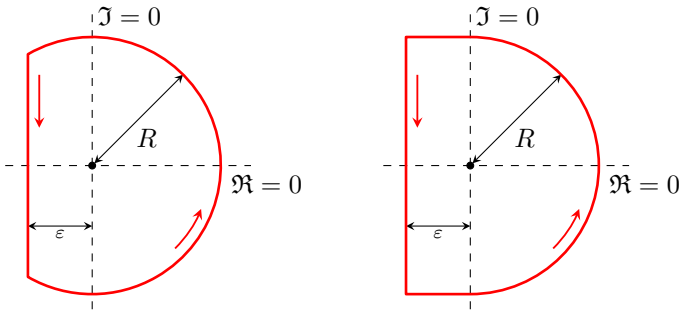


Figure 2 Newman's integration contour in his proof of Ingham's Tauberian theorem and Harrison's modified version. The dot in the middle is the pole of the integrand at the origin.

7 The Prime Number Theorem

The formal statement of the PNT is simply the asymptotic estimate $\pi(x) \sim x \ln x$, where $\pi(x)$ is the number of prime numbers $\leq x$. I will now explain, in a high-level way, how the formalised proof works. First of all, let us define the following functions related to primes:

▶ **Definition 37.**

$$\pi(x) = \sum_{p \leq x} 1 = |\{p \mid p \text{ prime} \wedge p \leq x\}| \qquad p_n = \text{the } n\text{-th prime number } (p_0 = 2)$$
$$\vartheta(x) = \sum_{p \leq x} \ln p \qquad \mathfrak{M}(x) = \sum_{p \leq x} \ln p/p$$
$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{p^k \leq x} \ln p \qquad M(x) = \sum_{n \leq x} \mu(n)$$

$\pi(x)$ is usually called the 'prime-counting function'. $\vartheta(x)$ and $\psi(x)$ are the first and the second Chebyshev function. $\mu(n)$ is the Möbius μ function. $\mathfrak{M}(x)$ is a non-standard notation I adopted; the function that it denotes is related to Mertens' first theorem and a key part in Newman's proof of the PNT.

▶ **Theorem 38.** *The following are all equivalent formulations of the PNT, i. e. given one of them, it is fairly easy to show the other ones by elementary means:*

$$\pi(x) \sim x/\ln x \quad \pi(x) \ln \pi(x) \sim x \quad p_n \sim n \ln n \quad \vartheta(x) \sim x \quad \psi(x) \sim x \quad M(x) \in o(x)$$

Proof. Omitted; see Chapter 4 in Apostol's presentation. Most equivalence proofs are quite short, both on paper and in Isabelle. ◀

Newman's approach to prove the PNT is then to prove $\mathfrak{M}(x) = \ln x + c + o(1)$, which directly implies $\vartheta(x) \sim x$. The key ingredient is a Tauberian theorem first proven by Ingham, which we will discuss now.

7.1 Ingham's Tauberian Theorem

A Tauberian theorem is a theorem that allows one to show – under certain conditions – that a series converges in some region if the function that it defines exists there. In our case, Ingham's theorem allows us to show that certain Dirichlet series converge not just to the right of the abscissa of convergence, but *on it* as well. The precise statement is as follows:

▶ **Theorem 39** (Ingham's Tauberian theorem)**.** *Let $F(s) = \sum a_n n^{-s}$ be a Dirichlet series with $a_n \in O(n^{\sigma-1})$ for some $\sigma \in \mathbb{R}$. Then F converges to an analytic function $f(s)$ for $\Re s > \sigma$. If $f(s)$ is analytic on the larger set $\Re s \geq \sigma$, then F also converges to $f(s)$ for all $\Re s \geq \sigma$.*

One can w. l. o. g. assume $\sigma = 1$. Newman then proves the theorem by applying the Residue theorem twice, once to a circle around 0 with a vertical cut-off line to the left of the origin, close to the abscissa of convergence (see Figure 2) and once to a full circle around the origin.

My formal proof follows Newman's argument very closely, but like Harrison, I use a modified version of Newman's contour: a semicircle plus a rectangle (see Figure 2). The value of the integral is the same in both cases since the two contours are homotopic, but the bounding of the contributions of the various parts of the contour is different.

The reason why I picked Harrison's contour over Newman's is that I could not understand how Newman's bounding of the different contributions fits to his contour, and it seems likely that this is also the reason why Harrison altered the contour in the first place. Additionally, the shape of the inside of Harrison's contour is somewhat easier to describe.

The formal proof is quite short (roughly 500 lines) and was – apart from the issue I just mentioned – very straightforward to write. However, it again suffers from the afore-mentioned typical problems of complex analysis in Isabelle, namely having to prove many side conditions such as analyticity and the geometry of the integration contours. The winding numbers, on the other hand, are unproblematic this time since the contours are very simple.

7.2 An Overview of the Remainder of Newman's Proof

Recall that our main objective was to prove

$$\mathfrak{M}(x) \sim \ln x + c + o(1)\ . \tag{4}$$

The starting point is Mertens' First Theorem, which is easy to prove following e. g. Hildebrand [17]:

▶ **Theorem 40** (Mertens' First Theorem)**.** $\mathfrak{M}(x) = \ln x + O(1)$

To then show (4) from this, Newman defines the Dirichlet series $f(s) := \sum_{n=1}^{\infty} \mathfrak{M}(n) n^{-s}$. Since $\mathfrak{M}(n) - \ln n$ is bounded, $f(s)$ converges absolutely for $\Re s > 1$. Rearrangement yields

$$f(s) = \sum_p \frac{\ln p}{p} \zeta(s, p) \qquad \text{for } \Re s > 1$$

and further rearrangements show

$$f(s) = \frac{A(s) - \zeta'(s)/\zeta(s)}{s-1} \qquad \text{for } \Re s > 1$$

for some function $A(s)$ that is analytic for $\Re s > \frac{1}{2}$. Moreover, $\zeta'(s)/\zeta(s)$ is analytic for $\Re s \geq 1$, $s \neq 1$ due to the non-vanishing of $\zeta(s)$ in that domain (cf. Theorem 31).

Putting everything together, we obtain that $f(s)$ can be continued analytically to $\Re s \geq 1$ except for a double pole at $s = 1$. As Newman states, this double pole can be turned into a simple pole by adding $\zeta'(s)$, and that simple pole can then be eliminated by subtracting a suitable multiple of $\zeta(s)$, yielding a function $g(s) := f(s) + \zeta'(s) - c\,\zeta(s)$ that is analytic for $\Re s \geq 1$ and has the Dirichlet series

$$g(s) = \sum_{n=1}^{\infty} \underbrace{(\mathfrak{M}(n) - \ln n - c)}_{=:\, a_n} n^{-s}\ .$$

Applying Theorem 39, we deduce that this series converges for $\Re s \geq 1$. For $s = 1$, this means that $\sum_{n=1}^{\infty} \frac{a_n}{n}$ is summable. Next, Newman proves the following lemma:

▶ **Lemma 41.** *Let $a_n : \mathbb{N} \to \mathbb{R}$ be non-decreasing and $\sum_{n=0}^{\infty} \frac{a_n}{n}$ be summable. Then $a_n \longrightarrow 0$.*

Applied to our a_n from before, we get $\mathfrak{M}(n) - \ln n \longrightarrow c$. From this, the slightly stronger version on real numbers (4) follows easily by noting that $\ln x - \ln \lfloor x \rfloor \longrightarrow 0$.

There were no major difficulties in formalising any of this. However, some parts deserve a few comments:

- The rearrangements leading to the analytic continuation of $f(s)$ involve changing the order of summation in nested infinite sums. To do this, I used Isabelle's library for absolutely summable families. This makes the arguments nice to formalise, but the library has the problem of having a function for the *value* of an infinite sum and for its *existence*. Any rearrangement of sums therefore has to be done twice, once for the value of the sum and once for its summability. Similar problems occur in Isabelle with nested integrals and it is not clear if and how this can be avoided in a HOL-based theorem prover.
- Showing that $A(s)$ is indeed analytic for $\Re s > \frac{1}{2}$ was a surprisingly easy application of the *Weierstraß M test* with the bounding series $M_n := \ln n(Cn^{-x-1} + n^{-x}(n^x - 1)^{-1})$. The proof obligation that M_n be summable can be solved by showing $M_n \in O(n^{-1-\varepsilon})$ with a suitable $\varepsilon > 0$, and this can be shown by Isabelle's automation for real limits [13].
- The pole cancellation argument showing that $g(s)$ is analytic is about 86 lines long, which is not too long, but still longer than one might expect given that it is obvious considering the Laurent series expansions of the functions involved. This is due to the fact that there is currently no theory of Laurent series expansions in Isabelle yet. In the future, this entire argument could potentially be automated by computing Laurent series expansions for meromorphic functions similarly to how Isabelle's automation already computes Multiseries expansions [13] for real-valued functions.
- The proof of Lemma 41 is very technical and tedious, but it seems to me that this is the case in Newman's paper presentation as well.

The last remaining step, showing that $\mathfrak{M}(x) - \ln x \longrightarrow c$ implies $\vartheta(x) \sim x$, is left as an exercise to the reader by Newman. Harrison was not quite sure what Newman meant and proceeded to prove a number of very technical and ad-hoc lemmas that I find very difficult to follow. Therefore, instead of attempting to port Harrison's proof, I followed Newman's hint in the book and used Abel's summation formula to write $\vartheta(x)$ in terms of $\mathfrak{M}(x)$:

$$\vartheta(x) = x\mathfrak{M}(x) - \int_2^x \mathfrak{M}(t)\,\mathrm{d}t \tag{5}$$

Substituting (4) into (5) yields

$$\begin{aligned}\vartheta(x) &= x\ln x + cx + o(x) - \int_2^x \ln t + c + o(1)\,\mathrm{d}t \\ &= x\ln x + cx + o(x) - (x\ln x - x + cx + o(x)) = x + o(x)\end{aligned}$$

and thus the desired $\vartheta(x) \sim x$. ◀

▶ **Corollary 42** (Elementary consequences of the PNT)**.**

- *For each $c > 1$, the interval $(x, cx]$ contains a prime for sufficiently large x.*
- *The fractions of the form p/q for prime p, q are dense in $\mathbb{R}_{>0}$.*
- $\operatorname{lcm}(1, \ldots, n) = \exp(x + o(x))$
- $\limsup_{n\to\infty} \omega(n) \ln\ln n / \ln n = 1$
- $\limsup_{n\to\infty} \ln \sigma_0(n) \ln\ln n / \ln n = \ln 2$
- $\liminf_{n\to\infty} \varphi(n) \ln\ln n / n = C$ *for some* $C > 0$

8 Size and Effort of the Formalisation

The material that was formalised is spread over five entries in the *Archive of Formal Proofs* [9, 8, 11, 14, 12]. They have a combined size of roughly 25,000 lines of Isabelle code, with the two largest single files by far being those on the analytic properties of Dirichlet series and the properties of the ζ functions. The largest single proof by a large margin is that of Hurwitz's formula and the contour integral form of $\zeta(s, a)$ with roughly 1,000 lines.

With the exception of a few minor results, the work presented here was done in 1.5 years by one person – however, the work was not done continuously, but sporadically whenever I found time for it. The total amount of time that went into it is therefore difficult to measure. As a point of reference, the formalisation of Newman's proof of the Prime Number Theorem (with all the components such as Dirichlet series and the ζ function already in place) comprises 3300 lines and took 6 days of full-time work. However, I used two lemmas that had previously been ported from Harrison's HOL Light formalisation by Paulson. Considering this, a time frame of 7 days for proving the Prime Number Theorem seems reasonable. Based on this, a total effort of 4–6 person-months for the entire work seems realistic.

The formalisation proceeded smoothly and without major difficulties, although some aspects of it stand out as considerably more painful than one might anticipate:

- applying the Residue Theorem
- geometric properties of integration contours
- manipulating nested infinite sums
- reasoning about cancellation of poles

For the first three points, it is not clear to me if and how this can be improved – or if, perhaps, there is simply an inherent difficulty in doing such things formally. The last point, on the other hand, could be easily managed by building a tactic to automatically compute Laurent series expansions for meromorphic functions, similar to the existing one for Multiseries expansions of real functions. [13] This would be an interesting project for the future. Extending the limit automation to use not just full asympotic expansions but also partial asymptotic information (such as $\vartheta(x) \sim x$) would also occasionally eliminate some tedious manual work.

9 Conclusion

I formalised a large portion of a mathematical textbook on an advanced topic, namely Analytic Number Theory. While some results from this field have been formalised before (such as Dirichlet's Theorem and the Prime Number Theorem), they typically tried to obtain a short route to the result without building an actual library of Analytic Number Theory.

In my opinion, this work demonstrates the following:

- Formalising an entire mathematical textbook in a modern theorem prover *can* be feasible with a moderate amount of effort.
- Good and extensive libraries (e. g. on complex analysis and Dirichlet series) can yield short, clear, and high-level proofs of 'high-profile' results like the Prime Number Theorem.
- Specialised tools (e. g. for proving limits or computing winding numbers) are invaluable, as they can take care of tedious and uninteresting parts of the proofs and 'close the gap' between what is obvious to a human mathematician and what is easy to do in the system.

References

1 Andrea Asperti and Wilmer Ricciotti. A proof of Bertrand's postulate. *Journal of Formalized Reasoning*, 5(1):37–57, 2012. URL: https://jfr.unibo.it/article/view/3406, doi:10.6092/issn.1972-5787/3406.

2 Jeremy Avigad, Kevin Donnelly, David Gray, and Paul Raff. A formally verified proof of the prime number theorem. *ACM Trans. Comput. Logic*, 9(1), December 2007. doi:10.1145/1297658.1297660.

3 Clemens Ballarin. Locales: A module system for mathematical theories. *Journal of Automated Reasoning*, 52(2):123–153, 2014. doi:10.1007/s10817-013-9284-7.

4 Julian Biendarra and Manuel Eberl. Bertrand's postulate. *Archive of Formal Proofs*, January 2017. http://isa-afp.org/entries/Bertrands_Postulate.html, Formal proof development.

5 Lukas Bulwahn. Cardinality of number partitions. *Archive of Formal Proofs*, January 2016. http://isa-afp.org/entries/Card_Number_Partitions.html, Formal proof development.

6 Mario Carneiro. Arithmetic in Metamath, case study: Bertrand's postulate. *CoRR*, abs/1503.02349, 2015. URL: http://arxiv.org/abs/1503.02349, arXiv:1503.02349.

7 Mario Carneiro. Formalization of the prime number theorem and Dirichlet's theorem. In *Proceedings of the 9th Conference on Intelligent Computer Mathematics (CICM 2016)*, pages 10–13, 2016. URL: http://ceur-ws.org/Vol-1785/F3.pdf.

8 Manuel Eberl. Dirichlet L-functions and Dirichlet's theorem. *Archive of Formal Proofs*, December 2017. http://isa-afp.org/entries/Dirichlet_L.html, Formal proof development.

9 Manuel Eberl. Dirichlet series. *Archive of Formal Proofs*, October 2017. http://isa-afp.org/entries/Dirichlet_Series.html, Formal proof development.

10 Manuel Eberl. The Euler–MacLaurin formula. *Archive of Formal Proofs*, March 2017. http://isa-afp.org/entries/Euler_MacLaurin.html, Formal proof development.

11 Manuel Eberl. The Hurwitz and Riemann ζ functions. *Archive of Formal Proofs*, October 2017. http://isa-afp.org/entries/Zeta_Function.html, Formal proof development.

12 Manuel Eberl. Elementary facts about the distribution of primes. *Archive of Formal Proofs*, February 2019. http://isa-afp.org/entries/Prime_Distribution_Elementary.html, Formal proof development.

13 Manuel Eberl. Verified real asymptotics in Isabelle/HOL. Draft available at https://www21.in.tum.de/~eberlm/real_asymp.pdf, 2019.

14 Manuel Eberl and Lawrence C. Paulson. The prime number theorem. *Archive of Formal Proofs*, September 2018. http://isa-afp.org/entries/Prime_Number_Theorem.html, Formal proof development.

15 John Harrison. A formalized proof of Dirichlet's theorem on primes in arithmetic progression. *Journal of Formalized Reasoning*, 2(1):63–83, 2009.

16 John Harrison. Formalizing an analytic proof of the Prime Number Theorem (dedicated to Mike Gordon on the occasion of his 60th birthday). *Journal of Automated Reasoning*, 43:243–261, 2009.

17 A. J. Hildebrand. Introduction to analytic number theory (lecture notes). https://faculty.math.illinois.edu/~hildebr/ant/.

18 Johannes Hölzl, Fabian Immler, and Brian Huffman. Type classes and filters for mathematical analysis in Isabelle/HOL. In Sandrine Blazy, Christine Paulin-Mohring, and David Pichardie, editors, *Interactive Theorem Proving*, volume 7998 of *Lecture Notes in Computer Science*, pages 279–294. Springer Berlin Heidelberg, 2013. doi:10.1007/978-3-642-39634-2_21.

19 Wenda Li and Lawrence C. Paulson. Evaluating winding numbers and counting complex roots through Cauchy indices in Isabelle/HOL. *CoRR*, abs/1804.03922, 2018. URL: http://arxiv.org/abs/1804.03922.

20 Donald J. Newman. *Analytic number theory*. Number 177 in Graduate Texts in Mathematics. Springer, 1998. doi:10.1007/b98872.

21 Marco Riccardi. Pocklington's theorem and Bertrand's postulate. *Formalized Mathematics*, 14:47–52, 01 2006. doi:10.2478/v10037-006-0007-y.