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
manuel.eberl@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
- An analytic proof of the Prime Number Theorem
- The asymptotics of arithmetical functions such as the prime ω function, the divisor count $\sigma_0(n)$, 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, arithmetical function, Dirichlet series, prime number theorem, Dirichlet's theorem, zeta function, L functions

Digital Object Identifier 10.4230/LIPIcs.ITP.2019.16

Supplement Material The proof developments in the *Archive of Formal Proofs* (AFP) that this work refers to are listed in the bibliography. Additionally, a precise overview of what material from the book has been formalised and which theorems in the book correspond to which theorems in the formalisation can be found at 10.5281/zenodo.3262266.

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. Larry Paulson also started off the analytic proof of the Prime Number Theorem in Isabelle and allowed me to take over and replace it with a more high-level approach. I also thank Jeremy Avigad and Johannes Hölzl, who commented on a draft of this document, and the anonymous reviewers, who gave a number of helpful suggestions.

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, most of the book (and quite a bit of material that goes beyond the book) has been formalised:

- Chapters 1, 5, and 9 consist of fairly basic material (e. g. GCDs, congruences, Quadratic reciprocity), most of which was already available in the Isabelle/HOL library.
- The results from Chapters 2, 3, 4, and 6 have been formalised in their entirety.
- Chapters 10, 11, and 12 have been formalised with some omissions.
- For Chapters 7 and 13 (Dirichlet's Theorem and PNT), equivalent results have been formalised using a different approach.
- Chapters 8 and 14 have been skipped. The former is being actively worked on; the latter concerns number partitions and has little connection to the other material in the book.
- Various interesting results from other sources (e. g. Hildebrand's lecture notes [21]) that are not proven in Apostol's book have also been formalised.

For more precise information on this, see the supplementary material listed before.

I put particular focus on developing a usable library of Dirichlet series on one hand and concrete results about the distribution of primes on the other. As the development is much too large to be presented here in full, I will go through a high-level description of some of the most interesting material. Special attention will be given to parts where I encountered difficulties or chose a different route than Apostol did in his book. Proofs will only be given in the form of very brief sketches, e. g. when it is necessary in order to understand difficulties in formalising them. I would like to refer readers who are interested in the actual *proofs* either to my commented formalisation in the *Archive of Formal Proofs* (AFP) [13, 12, 15, 18, 16] or to the numerous excellent textbooks and lecture notes on the subject [2, 21, 7]. I chose not to show Isabelle code in this presentation since the main results are very close to mathematical notation (e. g. Re $s \geq 1 \Longrightarrow s \neq 1 \Longrightarrow$ zeta $s \neq 0$) and showing the Isabelle code would therefore not provide much additional insight.

Let me now give an outline of the sections to follow: Section 2 lists related work. Section 3 defines formal Dirichlet series and their connection to complex-analytic functions. Section 4 introduces multiplicative characters and Dirichlet characters. Section 5 builds on the Dirichlet series library to treat various L functions, such as the famous Riemann ζ function. Section 6 describes my formalisation of the Prime Number Theorem (PNT). Section 7 gives some more examples of interesting results that were formalised. 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.

▶ Remark 1. Any sum $\sum_p$ or product $\prod_p$ is to be understood to run over prime p only.

2 Related Work

The first formalisation of a result related to this work was that of the PNT in Isabelle/HOL by Avigad *et al.* [5] in 2007. They formalised the elementary Selberg–Erdős proof.[1] Carneiro formalised the same proof in Metamath [11].

Harrison developed the first (and until now only) formalisation of an analytic proof of the PNT in 3,600 lines [20] of HOL Light. He followed Newman's presentation, which I also did.[2]

[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.

[2] Paulson later ported Harrison's development to Isabelle/HOL, but the ported proofs were lengthy and not very readable, so he and I decided that it would be better to redo them in a more high-level style, which I did. Only a few small lemmas were kept.

Harrison also proved Dirichlet's Theorem [19] and I used some of the high-level structure of his development as an inspiration for mine. Moreover, formalisations of Bertrand's postulate exist by Harrison in HOL Light, by Théry in Coq [27], by Riccardi in Mizar [26], by Carneiro in Metamath [10], by Asperti and Ricciotti in Matita [4], and by Biendarra and Eberl in Isabelle/HOL [9].

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.

3 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 2** (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 (we will mostly look at the complex case). 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 3** (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* $\operatorname{Re}(s) > \sigma_a$*, conditionally summable for* $\operatorname{Re}(s) \in (\sigma_c, \sigma_a)$*, and divergent for* $\operatorname{Re}(s) < \sigma_c$ *(where* $\operatorname{Re}(s)$ *denotes the real part of* s*). 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 for 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 converge. 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 aforementioned interplay of the formal and the analytical level:

One example of using formal Dirichlet series to derive an analytic result is this:

▶ **Theorem 4.** *Let* $\omega(n)$ *be the number of distinct prime factors of* n *and* $\mu(n)$ *the Möbius* μ *function, i. e.* $(-1)^{\omega(n)}$ *if* n *is square-free and 0 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 $\operatorname{Re}(s) > 1$ 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 [2]. Thus, it also holds analytically for $\operatorname{Re}(s) > 1$ so that we have $\zeta(2)M(2) = 1$ and therefore $M(2) = 1/\zeta(2)$, where $\zeta(2)$ – the famous *Basel problem* – has the well-known value $\pi^2/6$ [6]. ◀

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

▶ **Theorem 5** (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 $\mathrm{Re}(s_k) \longrightarrow \infty$ and $\forall k.\ f(s_k) = g(s_k)$, then $f(s)$ and $g(s)$ are equal as formal Dirichlet series.*

▶ Remark 6. In Isabelle, the condition on the existence of the sequence s_k is replaced by the following equivalent and more concise formulation using *filters* [22]:

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

The filter "f **going-to** F" is the contravariant image of F under f, i. e. "Re **going-to** at-top" describes the neighbourhood of complex numbers with "sufficiently large" real part.

The "$\exists_F\ x$ **in** F. $P(x)$" notation stands for "$P(x)$ holds frequently in F", i. e. the complement of P is not in the filter F. Less formally, one could say that $P(x)$ holds "again and again". In the case of "Re **going-to** at-top", this means that for any $C \in \mathbb{R}$, there exists an s with $\mathrm{Re}(s) \geq C$ for which the property is fulfilled.

▶ **Definition 7** (Truncation operator)**.** *For a Dirichlet series $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, let $T_m(f(s)) = \sum_{n=1}^{m} a_n n^{-s}$ 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 8.** $f(s) = g(s) \longleftrightarrow \forall m.\ T_m(f(s)) = T_m(g(s))$.

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 9.** *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 5. The question is how to show this if we do *not* know whether the series converge anywhere.

The key is to use Theorem 8 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 10. 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 11** (Pringsheim–Landau)**.** *Let $f(s)$ be a Dirichlet series with non-negative real coefficients and $\sigma_a \neq \pm\infty$. Then $f(s)$ has a singularity at σ_a.*

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

4 Characters of a Finite Abelian Group

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

▶ **Definition 12** (Multiplicative character). *A character is a group homomorphism $\chi : G \to \mathbb{C}^\times$, i. e. $\chi(1) = 1$ and $\chi(a \cdot b) = \chi(a)\chi(b)$ 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 $\cdot$, 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* [8] 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 13** (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 14** (Number of characters). $|\widehat{G}| = |G|$

In Isabelle, the proof is by induction on the subgroups of G, using a custom induction rule inspired by Apostol's proof. The idea here is to successively "adjoin" elements, i. e. for a subgroup H and some $x \in G \setminus H$, we form $\langle H; x\rangle$, the subgroup generated by $H \cup \{x\}$:

▶ **Lemma 15** (Induction on a group). *Let $G = (G, \cdot, 1)$ 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 all subgroups $H' \supseteq H$ and all $x \in G \setminus H'$, then $P(G)$ holds.*

I use this to show a stronger version of Theorem 14 that is just as easy to show:

▶ **Theorem 16** (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. By straightforward induction according to Lemma 15, using the bijection

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

in the induction step. ◀

Theorem 14 follows directly by taking $H = (\{1\}, \cdot, 1)$. Another useful corollary is this:

▶ **Corollary 17.** *For any $x \neq 1$, there exists a $\chi \in \widehat{G}$ such that $\chi(x) \neq 1$.*

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

▶ **Theorem 18** (Isomorphism to the double dual). *G is isomorphic to its double dual via the natural isomorphism $\nu : G \to \widehat{\widehat{G}}$, $\nu(x) = (\chi \mapsto \chi(x))$.*

This isomorphism is useful for the next properties:

▶ **Theorem 19** (Orthogonality relations). *For any $\chi \in \widehat{G}$ resp. $x \in G$, we have:*

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

Apostol's proof for (1) is very simple and straightforward to formalise. 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 thus (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 *could* 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 the dual of (1), with $\widehat{G}$ for G and $\nu(x)$ for χ. This requires only 6 lines of Isabelle code.

▶ **Definition 20** (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. $\chi(k) = \chi(k \bmod m)$.*

▶ Remark 21. Apostol's and my treatment of characters are quite elementary. There is an alternative, more group-theoretic view on this: It is straightforward to show that $\widehat{G_1 \times G_2} \simeq \widehat{G}_1 \times \widehat{G}_2$ and that $\widehat{C}_n \simeq C_n$ for cyclic groups C_n. Together with the *Fundamental Theorem of Finite Abelian Groups*, this implies a stronger variant of Theorem 14, namely $\widehat{G} \simeq G$. However, unlike with $\widehat{\widehat{G}} \simeq G$, the isomorphism is not natural and establishing it indeed requires the Fundamental Theorem, which is currently not available in `HOL-Algebra`. Since the formal proofs that were presented in this section are still reasonably short, I do not think this is a big problem.

5 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 $\mathrm{Re}(s) > 1$ and can be analytically or meromorphically continued to the entire complex plane.

▶ **Definition 22** (Riemann's ζ function). *For $\mathrm{Re}(s) > 1$, the Riemann ζ function is given by the Dirichlet series $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.*

▶ **Definition 23** (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 $\mathrm{Re}(s) > 1$ if $\chi = \chi_0$ and for $\mathrm{Re}(s) > 0$ if $\chi \neq \chi_0$.*

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

▶ **Theorem 24.** *Let $\Lambda(n)$ denote the von Mangoldt function. Then, if $\mathrm{Re}(s) > 1$:*

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

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

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

▶ **Theorem 25** (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 26** (Hurwitz's ζ function)**.** *Let $a \in \mathbb{R}_{>0}$ and $\mathrm{Re}(s) > 1$. Then $\zeta(s,a)$ is given by the (non-Dirichlet) series $\zeta(s,a) = \sum_{n=0}^{\infty} (n+a)^{-s}$.*

Apostol only considers $\zeta(s,a)$ for $a \in (0,1]$ since some results only hold for $a \leq 1$ and the case of $a > 1$ can be reduced to $a \in (0,1]$. It is, however, useful to allow also $a \geq 1$ – e. g. in Newman's proof of the PNT, as noted already by Harrison [20].

▷ Claim 27. $\zeta(s,a)$ can be continued analytically to $\mathbb{C} \setminus \{1\}$ with a simple pole at $s = 1$. Both Riemann's ζ function and the Dirichlet L functions can easily be expressed in terms of $\zeta(s,a)$, so that a continuation for Hurwitz's ζ also yields continuations for the other two [2].

The main question now is therefore how to construct the continuation of $\zeta(s,a)$.

5.1 Analytic Continuation of Hurwitz's ζ Function

Apostol constructs the continuation using an integral along an infinite contour. I did formalise this eventually (see Theorem 36), but when I first defined $\zeta(s,a)$ in Isabelle, this approach seemed quite daunting to me, so I chose another route that seems to be folklore [2, 24] and that I discovered independently: Since $\zeta(s,a)$ is defined for $\mathrm{Re}(s) > 1$ by an infinite sum $\sum_{n=0}^{\infty}(n+a)^{-s}$ and the corresponding improper integral $\int_0^{\infty}(x+a)^{-s}\,\mathrm{d}x$ is easy to compute, the Euler–MacLaurin summation formula [14] suggests itself. Applying it, 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. $P_k(t) = B_k(t - \lfloor t \rfloor)$.

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 non-obvious term is the integral in the last summand. Leibniz's rule shows that the definite integral $\int_0^b$ is analytic in s, and an integral version of the Weierstraß M-test then shows that the improper integral $\int_0^{\infty}$ is uniformly convergent and therefore analytic in s for $\mathrm{Re}(s) > -2N$.

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

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

This means that two functions $\mathit{prezeta}_M$ and $\mathit{prezeta}_N$ will always agree on $\mathrm{Re}(s) > 1$, and by analytic continuation they will then also agree on their entire domain, i. e. for all s with $\mathrm{Re}(s) > -2\max(M,N)$. 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:

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

This function is entire and agrees with any of the $\mathit{prezeta}_N(s,a)$ for all s with $\mathrm{Re}(s) > -2N$. Thus, it is an analytic continuation of the left-hand side of (3) so that we can simply define

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

to obtain the Hurwitz ζ function on all of $\mathbb{C} \setminus \{1\}$. For convenience, I choose $\zeta(1,a) = 0$ as is often done in HOL-based systems (cf. $\Gamma(-n)$ for $n \in \mathbb{N}$ in Isabelle/HOL and HOL Light). The advantage of the Euler–MacLaurin approach is that it is simple to implement 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 28** (Special values of ζ). *For any $n \in \mathbb{N}_{\geq 0}$, we have:*

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

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 the Basel problem $\zeta(2) = \pi^2/6$.

▶ **Theorem 29** (Integral representation for $\zeta(s,a)$). *For any s with $\mathrm{Re}(s) > 1$, we have:*

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

5.2 The Non-Vanishing of $\zeta(s)$ and $L(s,\chi)$ for $\mathrm{Re}(s) = 1$

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

▶ **Theorem 30.** *For any s with $\mathrm{Re}(s) \geq 1$, we have $\zeta(s) \neq 0$ and $L(s,\chi) \neq 0$.*

The case of $\mathrm{Re}(s) > 1$ is a simple consequence of the Euler product formula for $\zeta(s)$ and $L(s,\chi)$ (cf. Theorem 24); the difficult part is the case $\mathrm{Re}(s) = 1$. For this, I formalised the very simple proof presented by Newman [25], whose key ingredient is the aforementioned Pringsheim–Landau theorem (see Theorem 11). This proof is stunningly short and its high-level reasoning translates well to Isabelle/HOL now that a library of Dirichlet series is available. The gain is most striking for the Dirichlet L function, where Apostol's proof only treats the case of $s = 1$, and even 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.

5.3 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 31** (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 32** (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 33** (Periodic ζ function)**.** *For $\mathrm{Re}(s) > 1$, 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 34. $F(s,a)$ is called *periodic* because $F(s,a+n) = F(s,a)$ for any integer n. For non-integer a, the above series converges for $\mathrm{Re}(s) > 0$ and can be continued to an entire function. For integer a, it is simply the Riemann ζ function.

Apostol does not discuss the analytic continuation of $F(s,a)$ at all, but it seemed useful to me to do this nonetheless. The strategy I used to construct the continuation of $F(s,a)$ for non-integer a is somewhat interesting: Theorem 32 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 35.** *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 32 for $\mathrm{Re}(s) > 1$ (where F is simply given by its Dirichlet series).
2. Use this to show Theorem 35 for $\mathrm{Re}(s) > 1$.

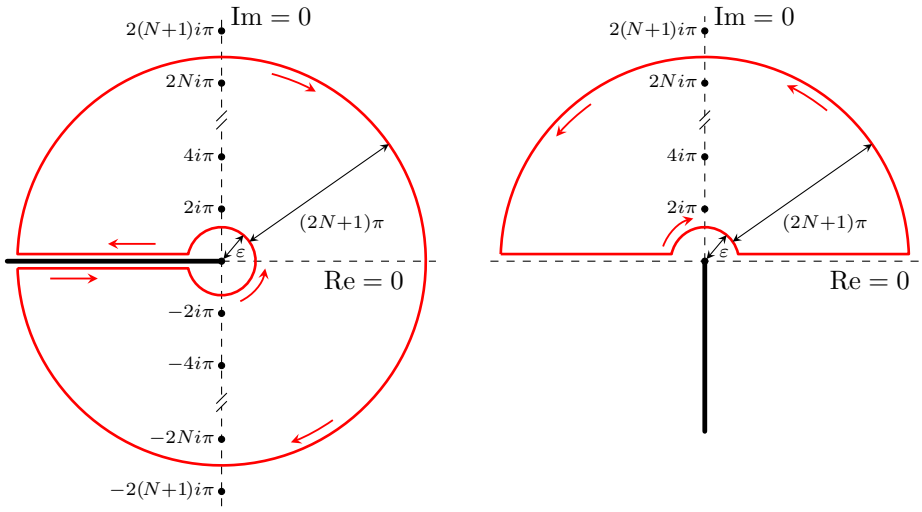


Figure 1 Apostol's integration contour and my modified version for proving Hurwitz's formula ($\varepsilon < 2\pi$). The black dots are the poles of the integrand; the thick black line is its branch cut. Note that in both cases, the line segments of the contour lie *on* the real axis despite the small gap in the illustration.

3. Use the right-hand side of Theorem 35 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 $\mathrm{Re}(s) > 0$ 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

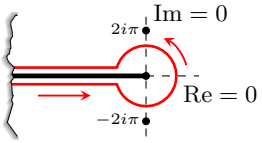
$$F(0,a) := \lim_{s\to 0} F(s,a) = \frac{i}{2\pi}\big(\mathrm{prezeta}(1,a) - \mathrm{prezeta}(1,1-a) + \ln(1-q) - \ln q\big) - \frac{1}{2}\,.$$

5. Extend the validity of Theorems 32 and 35 to their full domains by analytic continuation.

The only difficult part here is the first step, which we shall look at now. First of all, we require the contour integral representation for $\zeta(s,a)$ mentioned in Section 5.1:

▶ **Theorem 36.** *For any $s \in \mathbb{C} \setminus \{1\}$, we have*

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



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

Proof. Due to analytic continuation, we can assume $\mathrm{Re}(s) > 1$ w. l. o. g. By homotopy, all contours with a radius $\varepsilon < 2\pi$ yield the same result. Letting $\varepsilon \to 0$, the contribution of the circle vanishes and the $\int_{\circlearrowleft}$ becomes the $\int_0^\infty$ from Theorem 29. ◀

▶ Remark 37. Note that in order to even state this theorem formally, one needs to make the limit inherent in this "improper contour integral" explicit. I chose to decompose the integral as $\int_{\circlearrowleft} = \int_{\curvearrowleft} - \int_{\curvearrowright}$. The two line segments can then be written as Lebesgue integrals $\int_0^{-\infty}$, leaving only two finite circular arcs as the remainder. There is yet another subtlety hidden in this integral that will be discussed in Section 5.3.1.

The proof of Hurwitz's formula for $\mathrm{Re}(s) > 1$ then proceeds by computing this contour integral in a different way using the Residue Theorem. To do this, we first need to approximate it by an integral over a *finite* contour $C_{N,\varepsilon}$ such that $\int_{C_{N,\varepsilon}} \longrightarrow \int_{\text{⊨○}}$ as $N \to \infty$. Figure 1 shows Apostol's choice for $C_{N,\varepsilon}$. Applying the Residue Theorem to this, we get

$$\frac{1}{2i\pi} \int_{C_{N,\varepsilon}} \frac{z^{-s} e^{az}}{1 - e^z} \,\mathrm{d}z = \sum_{z_0} \mathrm{ind}_{C_{N,\varepsilon}}(z_0) \operatorname*{Res}_{z=z_0} \frac{z^{-s} e^{az}}{1 - e^z} \tag{4}$$

where the sum on the right-hand side extends over all the singularities of the integrand (represented by black dots in Figure 1). We can now let $N \to \infty$ so that the contribution of the outer circle vanishes. The integral on the left-hand side is then simply a $\int_{\text{⊨○}}$, which is equal to $\zeta(s, a)/\Gamma(s)$ by Theorem 36, and winding number on the right-hand side -1 for every non-zero pole z_0. Evaluating this sum, we find that it indeed equals $\frac{i^{-s}}{(2\pi)^s} F(s, a) + \frac{i^s}{(2\pi)^s} F(s, -a)$, which concludes the proof of Hurwitz's formula for $\mathrm{Re}(s) > 1$. ⌟

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 36). 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. Side conditions like the analyticity of the integrand, on the other hand, can be solved mostly automatically using Isabelle's general-purpose automation together with specialised theorem collections like `analytic_intros`.

Some aspects of the formal proofs of these statements deserve more attention, and we will discuss them now.

5.3.1 Branch Cuts

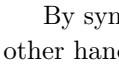
In both theorems, the term z^{-s} is a multi-valued function. It is defined in Isabelle as $e^{-s \ln z}$ where ln is the standard branch of the logarithm, which has a branch cut on the negative real axis. The two lines of Apostol's contour lie directly on this cut, taking different branches of the logarithm (indeed, if they did not, they would simply cancel each other). This makes sense formally 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.

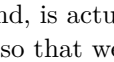
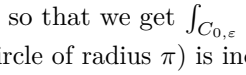
My first idea to circumvent this problem was to resort to some kind of limiting argument by placing the two horizontal lines not directly on the real axis, but some ε above (resp. below) it. However, this would likely have been a very tedious argument to do in Isabelle. I therefore decided to again cut the contour into two halves, similarly to Remark 37. When their integrals are added together, we recover Apostol's contour integral. Due to symmetry, it is actually again enough to look at the upper half (cf. the right part of Figure 1), as the lower one follows by conjugation.

For this upper contour ⌒, we can now 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 $\widetilde{\ln}\, z := \ln(-iz) + \frac{1}{2} i\pi$, whose branch cut lies on the negative imaginary axis, safely away from our contour. I also reversed the contour so that the winding numbers are all 1.

5.3.2 Homotopy

The proof of Theorem 36 uses the fact that the integral along ⊨○ is invariant for all radii $\varepsilon < \pi$. This is because all of these contours are homotopic, i. e. they can be continuously deformed into one another without crossing any of the singularities of the integrand. However, proving that this is the case turned out to be very tedious in Isabelle because there are almost no library theorems that help showing that two composite paths are homotopic.

I circumvented this problem in the following way: First of all, I restricted myself to $\varepsilon < \pi$.[3] Next, since the line segments extending from $-\pi$ to $-\infty$ are the same for all ε, we can ignore them and focus on the finite subcontour . It can be seen that  .

By symmetry, it is enough to show that  is invariant under changes of ε. This, on the other hand, is actually a corollary of (4): If we let $N := 0$, the sum on the right-hand side vanishes so that we get  for all ε. Since  and  (a half circle of radius π) is independent of ε, it follows that  is indeed the same for all ε.

Effectively, this replaces the homotopy argument (which is intuitively obvious for humans and not mentioned at all by Apostol) with a much "heavier" invocation of the Residue Theorem – but since we already applied the Residue Theorem anyway, all that work is already done.

5.3.3 Winding Numbers

The evaluation of the winding numbers $\text{ind}_{C_{N,\varepsilon}}(z_0)$ is also easy for a human: the contour $C_{N,\varepsilon} =$  *clearly* winds counter-clockwise once around each pole $2ni\pi$ with $0 < n \leq N$, and all the other poles are *clearly* completely outside the contour. Proving these things in a theorem prover, on the other hand, is notoriously difficult [20], especially for a more complicated contour like this.

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 $C_{N,\varepsilon}$, so the winding number for these points must be 0. Moreover, $C_{N,\varepsilon}$ 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 weigh 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 [23]. It is based on computing 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 numbers are 1 with a mere 18 lines of proof code.

6 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:

[3] This restriction could easily be lifted by allowing arbitrary radii in (4) instead of just $(2N+1)\pi$.

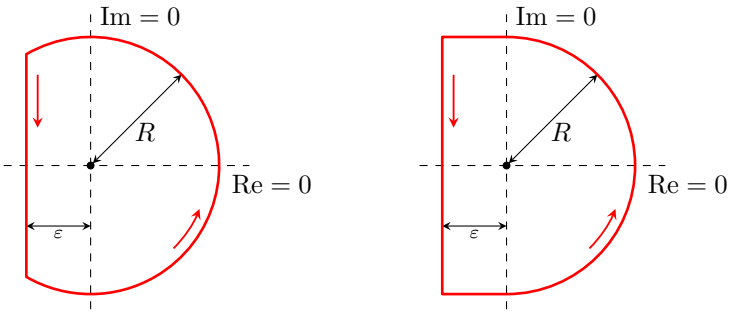


Figure 2 Newman's integration contour in his proof of Ingham's Tauberian theorem and Harrison's modified version. The dot in the middle is the pole of the integrand at the origin.

▶ **Definition 38.**

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

$\pi(x)$ 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 39.** *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:*

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

Most of these 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 implies $\vartheta(x) \sim x$ fairly directly as we shall see. The key ingredient is a Tauberian theorem first proven by Ingham, which we will discuss now.

6.1 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 40** (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 $\operatorname{Re}(s) > \sigma$. If $f(s)$ is analytic on the larger set $\operatorname{Re}(s) \ge \sigma$, then F also converges to $f(s)$ for all $\operatorname{Re}(s) \ge \sigma$.*

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 aforementioned typical problems of complex analysis in Isabelle, namely having to prove many side conditions such as the geometry of the integration contours. The winding numbers, on the other hand, are unproblematic this time since the contours are very simple.

6.2 An Overview of the Remainder of Newman's Proof

Recall that our main objective was to prove

$$\mathfrak{M}(x) \sim \ln x + c + o(1)\ . \tag{5}$$

The starting point is Mertens' First Theorem, which I prove following e. g. Hildebrand [21]:

▶ **Theorem 41** (Mertens' First Theorem)**.** $\mathfrak{M}(x) = \ln x + O(1)$

To then show (5) 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 $\mathrm{Re}(s) > 1$. Rearrangement yields

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

and further rearrangements show

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

for some function $A(s)$ that is analytic for $\mathrm{Re}(s) > \frac{1}{2}$. Moreover, $\zeta'(s)/\zeta(s)$ is analytic for $\mathrm{Re}(s) \geq 1$, $s \neq 1$ due to the non-vanishing of $\zeta(s)$ in that domain (cf. Theorem 30).

Putting everything together, we obtain that $f(s)$ can be continued analytically to $\mathrm{Re}(s) \geq 1$ 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 $\mathrm{Re}(s) \geq 1$ and has the Dirichlet series

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

Applying Theorem 40, we deduce that this series converges for $\mathrm{Re}(s) \geq 1$. For $s = 1$, this means that $\sum_{n=1}^{\infty} \frac{a_n}{n}$ is summable. Next, Newman proves the following lemma:

▶ **Lemma 42.** *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 (5) 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 $\mathrm{Re}(s) > \frac{1}{2}$ 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 [17].
- 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 [17] for real-valued functions.
- The proof of Lemma 42 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 [20] 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 $\mathfrak{M}(x)$:

$$\vartheta(x) = x\mathfrak{M}(x) - \int_2^x \mathfrak{M}(t)\,\mathrm{d}t \tag{6}$$

Substituting (5) into (6) yields, in a straightforward way,

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

and thus the desired $\vartheta(x) \sim x$. I find it likely that this is what Newman had in mind. ◀

7 Various Other Interesting Results

In this last section, I will give a few examples of other interesting number-theoretic results that I have formalised. The proofs were all fairly straightforward and there is not much to be said about them, but they are worth mentioning nonetheless.

▶ **Theorem 43** (Dirichlet's Theorem). *Let $m > 0$ and $gcd(k, m) = 1$. Then there are infinitely many primes congruent k modulo m.*

▶ **Theorem 44** (Elementary bounds for $\pi(x)$ and p_n)**.** *For any $x \geq 2$ and $n > 0$, we have:*

$$\frac{1}{6}\frac{x}{\ln x} < \pi(x) < 3(e^{-1} + \ln 2)\frac{x}{\ln x} \qquad \text{and} \qquad \frac{139}{443} n \ln n \leq p_{n-1} < 12(n \ln n + n \ln(12/e))$$

In particular, this implies $\pi(x) \in \Theta(x/\ln x)$ and $p_n \in \Theta(n \ln n)$. All of this can be derived without the PNT (hence "elementary" results).

▶ **Theorem 45** (Mertens' three theorems)**.**

- $-1 - 9\pi^{-2} < \mathfrak{M}(n) - \ln n \leq \ln 4$ *for all $n > 0$ and thus* $|\mathfrak{M}(n) - \ln n| < 2$.
- $|(\sum_{p \leq x} 1/p) - \ln\ln x - M| \leq 4/\ln x$ *for all $x \geq 2$ and thus* $\sum_{p \leq x} 1/p = \ln\ln x + M + O(1/\ln x)$ *where M is the Meissel–Mertens constant.*
- $\prod_{p \leq x}(1 - 1/p) = C/\ln x + O(\ln^{-2} x)$ *for some constant $C > 0$.*

Typically, number-theoretic functions that talk about a *single* integer such as $\varphi(n)$ and $\sigma_0(n)$ oscillate heavily and therefore have no nice asymptotics like $\pi(x) \sim x \ln x$. However, their *averages* (i. e. $\sum_{n \leq x} \varphi(n)$) are often more well-behaved:

▶ **Theorem 46** (Averages of arithmetical functions)**.**

- *Let $S(x)$ denote the number of square-free integers $\leq x$. Then $S(x) = \frac{6}{\pi^2}x + O(\sqrt{x})$, i. e. $6/\pi^2 \approx 60.8\,\%$ of integers are square-free.*
- *Euler's totient function φ fulfils $\sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2}x^2 + O(x \ln x)$, i. e. on average, an integer n has $\frac{3}{\pi^2}n$ numbers $\leq n$ that are coprime to it ($\approx 30.4\,\%$).*
- *The divisor function σ_0 fulfils $\sum_{n \leq x} \sigma_0(n) = x \ln x + (2\gamma - 1)x + O(\sqrt{x})$ where $\gamma \approx 0.5772$ is the Euler–Mascheroni constant, i. e. on average, an integer n has $\ln n + 2\gamma - 1$ divisors.*
- $\sum_{n \leq x} \sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1} x^{\alpha+1} + O(R(x))$ *for $\alpha > 0$ where $R(x) = x \ln x$ if $\alpha = 1$ and $R(x) = x^{\max(1,\alpha)}$ otherwise.*
- $\sum_{n \leq x} \sigma_{-\alpha}(n) = \zeta(\alpha + 1)\, x + O(R(x))$ *for $\alpha > 0$ where $R(x) = \ln x$ if $\alpha = 1$ and $R(x) = x^{\max(0,1-\alpha)}$ otherwise.*

Lastly, the following are interesting consequences that follow relatively easily from the PNT:

▶ **Corollary 47.**

- *For each $c > 1$, there exists an x_0 s. t. all intervals $(x, cx]$ with $x \geq x_0$ contain a prime.*
- *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 $C \in \mathbb{R}_{>0}$*

The last three statements perhaps deserve some more explanation: They give asymptotic bounds for $\omega(n)$, $\sigma_0(n)$, and $\varphi(n)$. For instance, $\omega(n) < c \ln n / \ln\ln n$ for all sufficiently large n if $c > 1$, but $\omega(n) > c \ln n / \ln\ln n$ for infinitely many n if $c < 1$. Thus, $\ln n / \ln\ln n$ is the best possible upper bound of that shape for $\omega(n)$ (and analogously for the other two).

As for the other direction, recall that $\omega(p) = 1$, $\sigma_0(p) = 2$, and $\varphi(p) = p - 1$. Therefore, the above results show that $\omega(n)$ oscillates between 1 and $\ln n / \ln\ln n$, $\sigma_0(n)$ oscillates between 2 and $2^{\ln n / \ln\ln n}$, and $\varphi(n)$ oscillates between $Cn/\ln\ln n$ and $n - 1$.

8 Size of the Formalisation

The formalised material is spread over five AFP entries [13, 12, 15, 18, 16]. 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.

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 small 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 hope:

1. applying the Residue Theorem
2. geometric properties of integration contours
3. manipulating nested infinite sums
4. establishing homotopy of concrete composite paths
5. reasoning about cancellation of poles

For the first three items, 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.

Item 4 could probably be addressed by providing more library results about homotopy.

Item 5 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 [17]. 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.

A related issue is that reasoning with asymptotic expansions like $f(x) = x^2 + \ln x + O(1/x)$ can be tedious in Isabelle/HOL. They *can* be written as $f =o\ (\lambda x.\ x\hat{}2 + \ln x)\ +o\ O(\lambda x.\ 1/x)$, but there is currently little support for working with them. Affeldt *et al.* [1] demonstrated an approach for this in Coq that could possibly be adapted to Isabelle/HOL.

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.

There is already work in progress on formalising the remaining parts of Apostol's book. After that, a natural continuation would be to focus on the second volume of Apostol's book, which is called *Modular Functions and Dirichlet Series in Number Theory* [3]. This would be another big step in formalising the essential tools of modern number theory in a theorem prover.

References

1 Reynald Affeldt, Cyril Cohen, and Damien Rouhling. Formalization Techniques for Asymptotic Reasoning in Classical Analysis. *J. Formalized Reasoning*, 11(1):43–76, 2018. doi:10.6092/issn.1972-5787/8124.

2 Tom M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, 1976. doi:10.1007/978-1-4757-5579-4.

3 Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*, volume 41 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1990. doi:10.1007/978-1-4612-0999-7.

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

5 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.

6 Raymond Ayoub. Euler and the zeta function. *The American Mathematical Monthly*, 81(10):1067–1086, 1974. doi:10.2307/2319041.

7 Joseph Bak and Donald J. Newman. *Complex Analysis*. Undergraduate Texts in Mathematics. Springer New York, 1999.

8 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.

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

10 Mario Carneiro. Arithmetic in Metamath, Case Study: Bertrand's Postulate. *CoRR*, abs/1503.02349, 2015. arXiv:1503.02349.

11 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.

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

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

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

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

16 Manuel Eberl. Elementary Facts About the Distribution of Primes. *Archive of Formal Proofs*, February 2019. , Formal proof development. URL: http://isa-afp.org/entries/Prime_Distribution_Elementary.html.

17 Manuel Eberl. Verified Real Asymptotics in Isabelle/HOL. Draft available at https://www21.in.tum.de/~eberlm/real_asymp.pdf, 2019.

18 Manuel Eberl and Lawrence C. Paulson. The Prime Number Theorem. *Archive of Formal Proofs*, September 2018. , Formal proof development. URL: http://isa-afp.org/entries/Prime_Number_Theorem.html.

19 John Harrison. A formalized proof of Dirichlet's theorem on primes in arithmetic progression. *Journal of Formalized Reasoning*, 2(1):63–83, 2009. doi:10.6092/issn.1972-5787/1558.

20 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(3):243–261, October 2009. doi:10.1007/s10817-009-9145-6.

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

22 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.

23 Wenda Li and Lawrence C. Paulson. Evaluating Winding Numbers and Counting Complex Roots through Cauchy Indices in Isabelle/HOL. *CoRR*, abs/1804.03922, 2018. arXiv:1804.03922.

24 M. Ram Murty and Marilyn Reece. A simple derivation of $\zeta(1-K) = -B_K/K$. *Funct. Approx. Comment. Math.*, 28:141–154, 2000. doi:10.7169/facm/1538186691.

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

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

27 Laurent Théry. Proving Pearl: Knuth's Algorithm for Prime Numbers. In David Basin and Burkhart Wolff, editors, *Theorem Proving in Higher Order Logics*, pages 304–318, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg. doi:10.1007/10930755_20.