A PVS Library on the Infinitude of Primes

Bruno Berto de Oliveira Ribeiro[1], Mariano M. Moscato[2⋆], Thaynara Arielly de Lima[3⋆⋆], and Mauricio Ayala-Rincón[1⋆⋆⋆]

[1] Universidade de Brasília, Exact Sciences Institute, Brasília D.F., Brazil
[2] Analytical Mechanics Associates Inc., Hampton, VA, U.S.A.
[3] Universidade Federal de Goiás, Institute of Mathematics and Statistics, Goiânia, Brazil

Abstract. This paper discusses the formalization in PVS of diverse proofs of the infinitude of primes. These proofs are developed using techniques taken from various areas of mathematics, such as set theory, algebra, analysis, number theory, and topology. The availability of such a variety of proofs is helpful as a didactic resource and aims to encourage mathematicians working in different areas to adopt interactive theorem provers as one of their everyday tools. The presented collection of formalizations follows the proofs selected by Erdös, Aigner, and Ziegler in their famous work "Proofs from THE BOOK," namely those based on Fermat numbers, Mersenne numbers and algebraic structures, topological properties, and the analysis of harmonic series. The paper discusses the differences between the informal proofs and the mechanical formalization and highlights the usefulness of distinguishing features of PVS to guide and facilitate the presented mechanization.

Keywords: Primes, Fermat Numbers, Mersenne Numbers, Harmonic Series, Theorem Proving, Algebraic Formalizations, PVS.

1 Introduction

Euclid's proof of the infinitude of primes [3] is a classic and highly illustrative result. As the concept of primality is typically presented in introductory math courses, this proof offers an excellent example of approaching problems involving infinity. Over the years, many mathematicians, such as Paul Erdös, have provided new proofs of this result, each drawing from different areas of mathematics. These proofs are not only valuable for showcasing the tools offered by such diverse fields, but they also serve as a reminder that mathematics is a profoundly interconnected discipline, where concepts and techniques from diverse branches often come together to solve fundamental problems.

In the context of formalizing mathematical knowledge, proof assistants offer invaluable tools to ensure rigor and correctness. They provide a structured and

⋆ NASA's System Wide Safety Project via RSES 80LARC23DA003.
⋆⋆ Project supported by FAPEG 202310267000223.
⋆⋆⋆ Project supported by CNPq Universal 409003/21-2 grants. The CNPq grant 313290/21-0 partially funded the author.

reliable approach to formalizing and verifying logical reasoning, ensuring that the proof is free of errors, ambiguities, and gaps. This work presents five alternative proofs of the infinitude of primes using the Prototype Verification System (PVS) [21]. These formalizations explore different proof techniques derived from various areas of mathematics, such as algebra, number theory, topology, and analysis. Each proof is constructed carefully to ensure logical consistency and rigor. The proofs are derived from those in "Proofs from THE BOOK" by Martin Aigner and Günter Ziegler [1], which offers six different proofs. Euclid's classical proof, the first in the mentioned book, is omitted here as it is already part of the NASA PVS Libraries, *NASALib*.[4] The presented mechanization relies on results from diverse libraries from NASALib and the PVS prelude. NASALib provides valuable abstractions for mathematical structures such as sets, groups, and Cartesian products.

Notably, this work does not assume the infinitude of primes beforehand, as circular reasoning is not accepted by proof assistants such as PVS. This kind of circularity can arise inadvertently in manual theorem proving when using a result much stronger than necessary. A notable example is using Gödel Completeness Theorem [14] to prove the Compactness Theorem. In "Proofs from THE BOOK," notation such as $p_1, p_2, p_3, \ldots$ is used for prime enumeration, but notice that this type of notation assumes the infinitude of primes beforehand.

One key aspect of this study is the identification and correction of notational errors and informalities in "Proofs from THE BOOK." PVS's robust type system helped to highlight and address these flaws, ensuring the proofs are precise and rigorous. Moreover, this work emphasizes the educational value of using PVS to formalize mathematical proofs. By breaking down the proofs into step-by-step procedures, this work not only demonstrates various formal proof techniques but also serves as a pedagogical resource. It offers readers the opportunity to learn how to structure and validate proofs within a proof assistant, fostering a deeper understanding of formal methods in mathematics. Thus, the mechanization of these proofs serves both as a study of mathematical reasoning and as a guide to using proof assistants effectively in diverse mathematical contexts.

1.1 Related work

A significant number of the needed theorems for fields such as algebra, number theory, analysis, and topology are already available as PVS formalizations in NASALib [4, 15, 19]. These theorems were imported when the code was initially set up, which greatly streamlined the work. This allows for a solid foundation, avoiding the need to prove basic results and instead focusing on more advanced or specific aspects of the problem at hand.

Euclid's classic proof of the infinitude of primes has been formalized in various proof assistants, each presenting different approaches. One notable collection of such formalizations can be found in the "Formalizing 100 Theorems"

[4] See https://github.com/nasa/pvslib/blob/master/numbers/infinite_primes.pvs.

project [26], where formalizations on eleven different proof assistants are referenced. The usual strategies employed in these formalizations often revolve around two key techniques. One approach uses the product of primes plus one variant of Euclid's proof, as seen in proofs formalized in systems like Naproche [17] and the NASALib itself. The other approach employs a factorial plus one method, which is used in the Isabelle/HOL and Coq proofs.

In addition to classical Euclid's proof of the infinitude of primes, other proofs have been developed using different proof assistants, such as those found in Isabelle. Such proofs are Fürstenberg's topological proof [9] and another involving the zeta function [8]. The topology-based proof is simpler to formalize, as it relies on fewer mathematical structures compared to other proofs in "Proofs from THE BOOK" ("THE BOOK," for short), leaving less room for alternative approaches. As a result, the existing formalization differs primarily in how it is handled by different proof assistants rather than in the structure of the proof itself. However, it remains valuable to include this proof in the presented formalization, as it offers an opportunity to showcase the topology library from NASALib. On the other hand, the proof of the zeta function, which is also presented in "THE BOOK" and will be covered here as well, diverges more from ours since it takes a more complex analytical approach, such as using the analytic continuation of the zeta function and then employing the divergence at $s = 1$ to prove the infinitude of primes.

While the primary focus of this paper is on the first topic of "THE BOOK," which addresses the infinitude of primes, it is also worth noting that there are other formalizations in "THE BOOK" beyond this first topic. These include proofs of the irrationality of certain numbers [22] and Fermat's two-square theorem [5].

1.2 Main contributions

The main contributions of this work are:

- The formalization in PVS of five additional proofs for the infinitude of primes, which can be presented as applications of the results from various NASALib's libraries, such as `ints`, `algebra`, `analysis`, and `topology`.
- The discussion and formalization of omitted details in "Proofs from THE BOOK."
- A new approach for the standard prime factorization theorem in NASALib and general structure specification.
- Several improvements in the `algebra` library, such as the $\mathbb{Z}/p\mathbb{Z}$ coset manipulation and type-checking related problems.
- Minor improvements in the manipulation of integer expressions in PVS, especially related to the *gcd* function.

1.3 Organization

Section 2 sketches the informal proofs that guide the formalization presented in this paper. Section 3 discusses aspects of the formalizations, focusing on the

two more interesting proofs in terms of the usage of distinguishing typing features provided by PVS and the level of difficulty involved in their mechanical verification. Section 4 concludes the paper by providing some final remarks, also providing quantitative data, and discussing possible lines of future work. The paper includes hyperlinks to specific points of the formalization, which are properly marked using this symbol. An appendix includes details of the proofs.

2 Brief Description of the Informal Proofs

This section briefly describes the proofs addressed in the presented formalization. In the following, the set of prime numbers is denoted by $\mathbb{P}$.

2.1 Fermat numbers

The second proof detailed in [1] uses number theory [16]. More precisely, it uses the infinitude of the Fermat numbers [23]. The Fermat numbers are of the form:

$$F_n = 2^{2^n} + 1, \text{ where } n \in \mathbb{Z}_{\geq 0}$$

The main idea guiding the proof is to show that Fermat numbers are pairwise relative primes. In other words, each Fermat number must have at least one distinct prime divisor. Since it is possible to find infinitely many Fermat numbers, it follows that there must be infinitely many prime numbers. Since NASALib and the PVS prelude provide a strong set of theorems in number theory, this proof turned out to be one of the shortest.

2.2 Mersenne Numbers

The third proof uses the Mersenne numbers [23], which are defined as $M_n = 2^n - 1$, $n \in \mathbb{Z}_{\geq 0}$. In this proof, n is restricted to the set of prime numbers and is denoted by p. The main idea of the proof is to show that there exists a prime divisor q of M_p, such that q is greater than p. If there were finite primes, there must exist a maximum prime p_{max}. This is a contradiction since one can find a greater prime from the set of divisors of $M_{p_{max}}$.

The approach followed in "Proofs from THE BOOK" is based on abstract algebra, using Lagrange's Theorem [18] and the fact that $\mathbb{Z}_q \setminus \{0\}$ is a group under multiplication. The proof is structured as described below.

1. Let p be an arbitrary prime and q be one prime factor of $M_p = 2^p - 1$. Notice that q must be odd since $2^p - 1$ is odd.
2. Since q divides $2^p - 1$, this implies that $2^p \equiv 1 (\text{mod } q)$. The number p is a prime; thus, it must be the order of the element $\overline{2}$ in $\mathbb{Z}_q \setminus \{0\}$. Otherwise, there would be $r \in \mathbb{N}, 1 < r < p$, which divides p.
3. An element $\overline{a} \in \mathbb{Z}_q \setminus \{0\}$ of order n generates a subgroup $\langle \overline{a} \rangle = \{\overline{a}^i : i \in \mathbb{Z}_{\geq 0}\}$ with cardinality $|\langle \overline{a} \rangle| = n$. By applying Lagrange's Theorem, $|\langle \overline{2} \rangle| = p$ divides $|\mathbb{Z}_q \setminus \{0\}| = q - 1$.
4. Assume there exists a maximum prime p_{max}. Thus, there exists $q \in \mathbb{P}$ such that $p_{max} \mid q - 1$. Consequently, $p_{max} \leq q - 1$, and $p_{max} < q$, which is a contradiction. Therefore, there are infinitely many primes.

2.3 Euler Product Formula and Cauchy Equality

The structure of the manual proof can be divided into the following steps.

1. Let $\pi(n)$ be the prime-counting function that counts the number of prime numbers smaller than or equal to n. Suppose there exists an enumeration of $\mathbb{P}$ in increasing order.
2. The harmonic numbers can be underestimated with natural logarithms as
$$\log(n) \leq H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$
3. The product of a geometric series of inverse prime numbers less than or equal to n is equal to another series that contains every $\frac{1}{k}$ from $H_n = 1+\frac{1}{2}+\ldots+\frac{1}{n}$:
$$H_n \leq \prod_{i=1}^{\pi(n)} \sum_{k=0}^{\infty} \frac{1}{p_i^k} = \sum_{\substack{k \in \mathbb{Z}_{>0}, \\ k=1 \ \vee \ \exists p \in \mathbb{P}, \\ (p \leq n \ \wedge \ p \mid k)}} \frac{1}{k}$$
4. For each prime number p_i, the geometric series $\sum_{k=0}^{\infty} \frac{1}{p_i^k}$ converges to $\frac{p_i}{p_i - 1}$. Also, $p_i \geq i + 1$, which implies that $\frac{p_i}{p_i - 1} \leq \frac{i+1}{i}$. Consequently,
$$\prod_{i=1}^{\pi(n)} \sum_{k=0}^{\infty} \frac{1}{p_i^k} = \prod_{i=1}^{\pi(n)} \frac{p_i}{p_i - 1} \leq \prod_{i=1}^{\pi(n)} \frac{i+1}{i} = \pi(n) + 1$$
5. By arranging inequalities, $\log(n) \leq \pi(n) + 1$. Since the natural logarithmic function is strictly increasing, the sequence generated by the π function diverges, which means that $\mathbb{P}$ is infinite.

2.4 Fürstenberg's Topological Proof

Hillel Fürstenberg introduced this elegant proof as a 12-line note in the section on Mathematical Notes of the American Mathematical Monthly in 1995 [12]. This non-traditional approach builds a topology [20] on integer numbers. The structure of this proof can be divided into the following parts.

1. Given $a, b \in \mathbb{Z}$, where $b > 0$, define the family of sets $N_{a,b} = \{a + bn : n \in \mathbb{Z}, b > 0\}$.
2. A set $O \subseteq \mathbb{Z}$ is called open whether $O = \emptyset$ or for every element $a \in O$, there exists some $b \in \mathbb{Z}, b > 0$ with $N_{a,b} \subseteq O$. As usual in topology, a closed set is defined as a complement of an open set in $\mathbb{Z}$.
3. By definition, the union of two open sets $O_1 \cup O_2$ is another open set. Also, the intersection of two open sets is also an open set: if $a \in O_1 \cap O_2$, thus there exist $b_1 > 0$ and $b_2 > 0$, such that $N_{a,b_1} \subseteq O_1$ and $N_{a,b_2} \subseteq O_2$; consequently, $N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Therefore, such open sets induce a well-defined topology.

4. For any $a, b \in \mathbb{Z}$, $b > 0$, $N_{a,b}$ is open. Also, notice that $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$. Since $N_{a,b}$ is the complement of the open set $\bigcup_{i=1}^{b-1} N_{a+i,b}$, thus $N_{a,b}$ is a closed set.
5. If O is a nonempty open set then O is infinite, since $N_{a,b} \subseteq O$ for some $b > 0$.
6. Every $n \in \mathbb{Z} \setminus \{-1, 1\}$ has a prime divisor p, which implies that $n \in N_{0,p}$. Consequently, $\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}$.
7. If $\mathbb{P}$ is finite, then $\mathbb{Z} \setminus \{-1, 1\}$ is a closed set since it is a finite union of closed sets, as pointed out above. Consequently, $\{-1, 1\}$ is an open set, which is a contradiction since all open sets in this topology are infinite.

2.5 Prime Reciprocal Harmonic Series

The sixth and last proof was originally proved by Paul Erdös in the 20th century [10] and can be viewed as inspired by the proof found in Section 2.3. The main idea is to consider another series of reciprocal numbers, but instead of using the positive integers, the prime numbers are used, i.e., $\sum_{i=1}^{n} \frac{1}{p_i}$. As a finite summation of numbers converges, if this series diverges, the set of primes must be infinite.

In this proof, the set of primes is divided into two types: the *Small* primes, which are smaller or equal to a prime p_k, and *Big* primes, the remaining ones. From this classification, other sets are defined: $N(n)$, the set of positive numbers less than or equal to n; $N_s(n, k)$, the numbers from $N(n)$ with only *Small* prime divisors; $N_b(n, k)$ the numbers from $N(n)$ with at least one *Big* prime divisor. It can be shown that $N(n) = N_s(n, k) \cup N_b(n, k)$.

1. Consider a prime enumeration p_i and suppose that the series $\sum_{i=1}^{N} \frac{1}{p_i}$ converges. Therefore exists a κ such that $\sum_{i=\kappa+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$.
2. Define $N_{div}(d, n)$ the subset of $N(n)$ whose elements are multiples of $d \in \mathbb{N}, d \geq 1$. It can be proven that $|N_{div}(d, n)| = \lfloor \frac{|N(n)|}{d} \rfloor = \lfloor \frac{n}{d} \rfloor$. Noticing that $N_b(n, k)$ is the union of all $N_{div}(p_i, n)$, where $i > k$, one can estimate the size of $N_b(n, \kappa)$ by:
$$|N_b(n, \kappa)| \leq \sum_{i=\kappa+1}^{\infty} \left\lfloor \frac{n}{p_i} \right\rfloor \leq \sum_{i=\kappa+1}^{\infty} \frac{n}{p_i} < \frac{n}{2}$$
3. An element $m \in N_s(n, k)$ can be written as $m = a \cdot b$, where $a, b \in N_s(n, k)$, a is a square-free part of m, and b is a perfect square of an element of $N_s(n, k)$. From this observation, two other sets are defined: $S_{free}(n, k)$, composed of all elements a, and $S_{div}(n, k)$, composed of all elements b. With these considerations, the size of $N_s(n, k)$ is estimated:
$$|N_s(n, k)| \leq |S_{free}(n, k) \times S_{div}(n, k)| = |S_{free}(n, k)| \cdot |S_{div}(n, k)|$$
4. Since $m = a \cdot b$ for all $m \in N_s(n, k)$, the number of elements of $S_{div}(n, k)$ can be estimated by setting $a = 1$ and using the definition of b, i.e. $b = r^2$ for $r \in N_s(n, k)$. Finding the size of $S_{div}(n, k)$ turns into a problem of counting the numbers of valid $m = r^2$. Noticing that $N_s(n, k) \subseteq N(n)$, one can establish: $|S_{div}(n, k)| \leq \sqrt{|N_s(n, k)|} \leq \sqrt{|N(n)|} = \sqrt{n}$

5. An element of $S_{free}(n,k)$ is of the form $m = p_1^{\epsilon_1} \cdot p_2^{\epsilon_2} \cdots p_k^{\epsilon_k}$, where $\epsilon_i \in \{0,1\}$. Consequently, $|S_{free}(n,k)| \leq 2^k$.
6. Since $N(n) = N_s(n,k) \cup N_b(n,k)$, for every k, one concludes that:

$$|N(n)| \leq |N_s(n,\kappa)| + |N_b(n,\kappa)| < 2^\kappa \sqrt{n} + \frac{n}{2}$$

7. In particular, if $n = 2^{2\kappa+2}$ then $|N(n)| < 2^{2\kappa+2} = n$, which is a contradiction, since $|N(n)| = n$. Therefore, the original consideration of the convergence of a series of prime reciprocals must be false. That's only possible if there are infinitely many primes.

3 Description of the Formalization

Only the formalization of the proofs based on Mersenne Numbers and on the Euler Product Formula are detailed since they required much more effort than what was expected given the traditional proofs. The formalization based on the Harmonic Prime Reciprocal Series presented the most significant divergences from the informal proof. On the contrary, it was possible to develop a formalization fairly close to the manual proofs for the ones based on Fermat Numbers and on Fürstenberg's topological arguments .

Before diving into the details, it is worth noticing the main building blocks on which this effort is founded. In addition to the PVS prelude and basic NASALib libraries such as `set` and `structures`, the presented formalization leverages specialized results from the NASALib libraries `algebra`, `topology`, `series`, and `analysis`. Notably, the concepts of topological spaces and relations between open and closed sets were taken from the library `topology`. Some properties about limits and integrals were imported from the `analysis` library. The `series` library provided properties about convergence of (infinite) series. Finally, from the `algebra` library, results related to (finite) groups and cosets were used. As an original contribution to these libraries, several results were added, such as a reformulation of the Fundamental Theorem of Arithmetic and a version of the Cauchy Product Theorem, among others.

3.1 Mersenne Numbers

The first design decision addressed how to specify the multiplicative group $\mathbb{Z}_p \setminus \{\overline{0}\}$, where p is a prime number. Although there is a specification for the ring $\mathbb{Z}/n\mathbb{Z}$, there exists no direct implementation for the multiplicative group $\mathbb{Z}/n\mathbb{Z} \setminus \{n\mathbb{Z}\}$. The group-related theorems that were applied belong to theories that rely on the following assumption: the set of all elements of an abstract type `T` must satisfy a group predicate . In other words, the importation of these theories introduces a Type Correctness Condition (TCC) automatically generated by the system, which is a proof obligation for checking whether the type `T` consists of a complete set of elements forming a group. This is not a direct application of the lemma `Zp_prime_is_field` , already in NASALib, stating

that $\mathbb{Z}/p\mathbb{Z}$ is a field when p is a prime number and thus, that $\mathbb{Z}/p\mathbb{Z} \setminus \{p\mathbb{Z}\}$ forms a group under multiplication. Indeed, the specification of `field` in the theory `field_def` , from a division ring , gives the flexibility of considering the set of cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ as a parameter in the lemma `Zp_prime_is_field` , without excluding the identity for addition $n\mathbb{Z}$. To use the results in theory `finite_groups`, it was necessary to specify the type `nz_coset(n)` and then prove that it satisfies the group properties when n is a prime number . Roughly, it could be done by using the lemma `Zp_prime_is_field` combined with enough expansions of the definition of `group?[nz_coset(n)](Z(n))` in the lemma `nz_prime_is_group` .

Still, some TCCs appeared during the manipulation of elements of type nz_coset(p); for this reason, additional utility lemmas were proved and separated in the `ring_zn_extra.pvs` file, as they could be used in more general situations. The content of this file ranges from lemmas of equivalence of the operations in $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$ to some direct ring properties, such as product and summation closure, and the characteristic of the ring $\mathbb{Z}_p$ being p.

It is worth mentioning that some type-related proofs can be avoided; instead of using generic definitions such as the power function specified in the group file, it is possible to define a specialized function for handling this new `nz_coset` type. This could be done by forcing the type to be `nz_coset` instead of the PVS-deduced coset type. For example, the signature of the power function was restricted to $pow : \mathbb{Z}/p\mathbb{Z} \setminus \{p\mathbb{Z}\} \times \mathbb{Z}_{\geq 0} \to \mathbb{Z}/p\mathbb{Z} \setminus \{p\mathbb{Z}\}$ instead of using the more general version $pow : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}_{\geq 0} \to \mathbb{Z}/p\mathbb{Z}$.

After the explanation of these preliminaries, the actual proof of the infinitude of prime numbers can be finally discussed.

Lemma 1. *If d is a divisor of M_p where $p \in \mathbb{P}$, then d is odd*

Proof. Since p is a prime number, $p \geq 2$, implying that $M_p = 2 \cdot 2^{p-1} - 1$ is odd. Suppose that d is even. Since it is a divisor of M_p,

$$M_p = d \cdot k_1, k_1 \in \mathbb{Z}$$

By the evenness of d

$$M_p = 2 \cdot k_2 \cdot k_1, k_2 \in \mathbb{Z}$$

This is a contradiction since M_p is odd.

Lemma 2. *Let $q, p \in \mathbb{P}$, where q is a divisor of M_p, then*

$$(2 + q\mathbb{Z})^{q-1} = 1 + q\mathbb{Z}$$

Proof. By Lemma 1, q is an odd number since q is a prime $q \geq 3$; in particular, this means that $q \not| 2$. By Fermat's Little Theorem

$$2^{q-1} \equiv 1 (\text{mod } q)$$

$$\Rightarrow (2 + q\mathbb{Z})^{q-1} = 1 + q\mathbb{Z}$$

The last equation comes from the ring isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

In the PVS specification, the equivalence in the modular arithmetic formulation and quotient ring formulation was proved directly . It was also necessary to adapt Fermat's Little Theorem to the requirements in the proof: it was specified in the $a^p \equiv a \pmod{p}$ form, not in the $a^{p-1} \equiv 1 \pmod{p}$ form. The adaptations resulted in the file `Fermats_little_theorem_extra.pvs`.

Lemma 3. *Let $q, p \in \mathbb{P}$, where q is a divisor of M_p, then*

$$(2 + q\mathbb{Z})^p = 1 + q\mathbb{Z}$$

Proof. Since q divides M_p,

$$M_p \equiv 0 \pmod{q}$$
$$2^p - 1 \equiv 0 \pmod{q}$$
$$2^p \equiv 1 \pmod{q}$$

Using the isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

$$(2 + q\mathbb{Z})^p = 1 + q\mathbb{Z}$$

Theorem 1. *There are infinitely many primes*

Proof. Suppose there exists a finite amount of prime numbers, then there should exist a maximum prime p_{max}. Let $q \in \mathbb{P}$ be the divisor of $M_{p_{max}}$. Using Lemma 3,

$$(2 + q\mathbb{Z})^{p_{max}} = 1 + q\mathbb{Z}.$$

In particular, from the definition of order, it follows that $ord(2+q\mathbb{Z}) \mid p_{max}$, but that is only possible if $ord(2+q\mathbb{Z}) = 1$ or $ord(2+q\mathbb{Z}) = p_{max}$. If $ord(2+q\mathbb{Z}) = 1$, then $2 + q\mathbb{Z} = 1 + q\mathbb{Z}$, which is not possible since $q > 1$. Therefore, it must be the case that $ord(2 + q\mathbb{Z}) = p_{max}$.

Using Lemma 2,

$$(2 + q\mathbb{Z})^{q-1} = 1 + q\mathbb{Z}.$$

Again, by definition of order, $ord(2 + q\mathbb{Z}) \mid q - 1$ and $p_{max} \mid q - 1$. Since a divisor is smaller or equal to the number it divides, $p_{max} \leq q - 1$. More specifically, $p_{max} < q$. Therefore, q is a prime greater than the maximum prime, a contradiction.

It turns out that Lagrange's Theorem was not necessary. In fact, if it had been used, it would have been necessary to proof additional lemmas on group orders, but these proofs can be quite tedious. Instead, the following classical theorem was used: if an element a from a group G satisfies $a^n = 1$ for some integer n, then $ord(a)$ divides n. This theorem was not in the NASALib Algebra library as such, so it was proved and added in its own separate file `finite_group_extra.pvs`.

Related to TCCs, since the definition of structures in the NASALib's algebra library, such as ring, is built upon the group definition, and these upon monoid (and so on), type dependencies become an exhaustive issue. The problem arises because they require a significant number of TCCs. If such structures are

imported naively, each new algebraic structure used in a proof could generate around five new TCCs. Consequently, there is room for improvement in the algebra library from various angles, such as through new utility theorems, new proof strategies (conservative extensions of the proof calculus provided by PVS), and possibly type judgments, which provide more information to the type checker. Nevertheless, the algebra library contains many powerful theorems, including classic results from group and ring theory like Lagrange's Theorem, Sylow's Theorems, and many others, some of which facilitated the presented work.

3.2 Formalization Based on Euler Product Formula and Cauchy Equality

The fourth proof in "THE BOOK" relies on analytic number theory [2]. As a side effect of the Euler's Formula [11], proved in the 18th century by Leonhard Euler, this proof has a deep connection to the Riemann zeta function [24]. The key idea is to show that the zeta function can be factored into a product over primes. With this connection, the estimation for the number of primes can be as large as desired, confirming that primes are indeed infinite.

The Riemann-zeta function is defined as:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{for } s \in \mathbb{C}, \quad \text{Re}(s) > 1$$

The Euler's product formula, on the other hand, relates the primes in the following way:

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} \quad \text{for } s \in \mathbb{C}, \quad \text{Re}(s) > 1$$

Notice that, from the definition of zeta function, s must have real part greater than one. It turns out that this Euler product also works for $s = 1$, but the zeta function at this value tends to infinity, something that should not happen if there are finite primes.

In particular, it is possible to estimate the prime-counting function by the product of the primes according to the Euler formula, which by itself can be bounded using the natural logarithm function in the following way:

$$\log(n) \leq \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^{-1} \leq \pi(n) + 1$$

where $\log(n)$ is the natural logarithm function and $\pi(n)$ is the function that counts the number of prime numbers less than or equal to a given number n.

As is typical in traditional number theory proofs, this proof heavily relies on concepts from analysis, such as limits and series, which are addressed in NASALib Analysis library [15].

3.2.1 Prime enumeration The notation $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ in [1] has the problem of assuming that the set of prime numbers $\mathbb{P}$ is infinite beforehand, and the sequence should be undefined otherwise. For simplicity, in the specification, the starting index is zero, and the undefined cases are set to the number zero, meaning that if the prime numbers have an end at the nth value, then $p_i = 0$ for $i \geq n$. Therefore, $p_0 = 2 \quad p_1 = 3 \quad p_2 = 5$. The proper definition of the prime sequence is given by a function $\rho : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$. It remains to prove that for a subset of the domain, $S \subseteq \mathbb{Z}_{\geq 0}$, this function is an enumeration. For this purpose, some necessary properties are inductively formalized, such as:

1. $\rho(i+1) > \rho(i) \vee \rho(i+1) = 0$
2. $\forall \rho(i), \rho(j) \in \mathbb{P}, \rho(i) = \rho(j) \Rightarrow i = j$
3. $\forall p \in \mathbb{P}, \exists i \in \mathbb{Z}_{\geq 0}, \rho(i) = p$
4. Let $i, n \in \mathbb{Z}_{\geq 0}$, $i < \pi(n) \Rightarrow \rho(i) \in \mathbb{P}$

The ρ function is indeed an enumeration for a subset of the domain. If there are infinitely many primes, all primes will appear in ascending order in the domain $\mathbb{Z}_{\geq 0}$. Otherwise, for the domain $S = \{n \in \mathbb{Z}_{\geq 0} : n < \pi(p_{max})\}$, all primes will also appear in ascending order, and in its complement, $\mathbb{Z}_{\geq 0} \setminus S$, the function will be zero.

In the following proofs, it will be necessary to use the Fundamental Theorem of Arithmetic [13]. This theorem is in NASALib , but specified in a generic manner: any natural greater than one can be written as a product of a prime sequence, for example, $360 = 2{\cdot}3{\cdot}2{\cdot}5{\cdot}2{\cdot}3$. For the current purposes, a specialized version of this theorem was formalized that states that each natural greater than one can be written as a product of a sequence of sorted powers of primes, for instance, $360 = 2 \cdot 3 \cdot 2 \cdot 5 \cdot 2 \cdot 3$. But for this formalization, it is convenient to use this theorem in the form of sorted powers of primes, for instance $360 = 2^3 \cdot 3^2 \cdot 5$.

Because a prime enumeration was already specified, it can be used to specify the prime powers in sorted form. Still, knowing beforehand that there are infinitely many primes, one should be tempted to describe the Fundamental Theorem as the existence of the infinite product, with large enough terms having exponent zero, such as $360 = \rho(0)^3 \cdot \rho(1)^2 \cdot \rho(2)^1 \cdot \rho(3)^0 \cdot \rho(4)^0 \ldots$. However, this would lead to the same mistake of assuming that there are infinitely many primes circularly. Therefore, a new version of the Fundamental Theorem was formalized.

Given a family of sets $E_p = \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}_{\geq 0}, n = p^k\}$, where $p \in \mathbb{P}$, the set D_n can be defined as the finite Cartesian product shown below .

$$D_n = \bigtimes_{i=0}^{\pi(n)-1} E_{\rho(i)}$$

Thus, the Fundamental Theorem can be rewritten as the existence of a unique element $(\rho(0)^{\epsilon_0}, \rho(1)^{\epsilon_1}, \ldots, \rho(\pi(n)-1)^{\epsilon_{\pi(n)-1}}) \in D_n$, such that the product of its entries equals n for every $n \in \mathbb{Z}, n > 1$; i.e.,

$$n = \prod_{i=0}^{\pi(n)-1} \rho(i)^{\epsilon_i}$$

Since the greatest prime divisor of a number is the number itself, the upper limit of the product, $\pi(n) - 1$, guarantees that all prime divisors will appear in the product.

It is worth mentioning that the definition of prime enumeration and prime factorization is reused for the formalization based on prime reciprocal series (Subsection 2.5); because of that, these proofs, alongside another general purpose ρ function manipulation, were separated to a new file called `prime_extra.pvs`. Additionally, using this new framework for the proof of the Fundamental Theorem of Arithmetic, the application of lemmas related to integers was useful. Among these lemmas, some properties related to the *gcd* function were not available in NASALib. For that reason, another file was created `number_util.pvs`.

3.2.2 A few inequalities For the completion of the proof, a few inequalities must be proven, starting from a classic one.

Lemma 4. $\forall n \in \mathbb{Z}_{\geq 0}, \log(n) \leq H_n$

Despite being well known, this inequality was not explicitly enunciated in NASALib, but all its prerequisites were already proven in the `analysis` library. This made its assisted proof relatively easy. The only small problem was a TCC related to the integrability of each integral expression required in the proof; as the summation is applied over slices of the bigger integral, it was necessary to guarantee that everything is indeed integrable. However, lemmas for these steps were also in the files defining the logarithmic function and integral operations.

For the next inequality, two definitions of functions are given. At first glance, the defined functions appear to be different, but they are actually equivalent . Let $n \in \mathbb{Z}_{\geq 0}, n \geq 2$

$$\xi(n) = \prod_{i=0}^{\pi(n)-1} \sum_{k=0}^{\infty} \frac{1}{\rho(i)^k} \qquad \mu(n) = \sum_{\substack{k \in \mathbb{Z}_{>0}, \\ k=1 \ \vee \ \exists p \in \mathbb{P}, \\ (p \leq n \ \wedge \ p \mid k)}} \frac{1}{k}$$

One thing to notice is that in ξ, there are divisions by $\rho(i)$, which can have zero value if one tries to use a nonexistent prime number, but as the product is taken from $i = 0$ to $i = \pi(n) - 1$, using property 4, all $\rho(i)$ values are primes. Even though not completely obvious, these two functions are indeed the same. Some non-trivial lemmas must be proven first to formalize this fact.

Given the Cauchy product [7], the product of two convergent series is another series.

$$\left(\sum_{n=0}^{\infty} a_i\right) \cdot \left(\sum_{n=0}^{\infty} b_i\right) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} a_{n-k} b_k \tag{1}$$

This formula has the restriction of one of the series being absolutely convergent, but the series in the formalization is defined over positive numbers, making this restriction trivially valid. The last series in the formula can be flattened in

such a way that it maintains its convergence, but to prove this, first, two other functions are defined. Let $n \in \mathbb{Z}_{\geq 0}$

$$\theta(n) = max\left(\left\{k \in \mathbb{Z}_{\geq 0} : \frac{k(k+1)}{2} \leq n\right\}\right) \qquad \tau(n) = n - \frac{\theta(n)(\theta(n)+1)}{2}$$

Corollary 1. *Let $n, k \in \mathbb{Z}_{\geq 0}, 0 \leq k \leq n$, then $\theta(\frac{n(n+1)}{2} + k) = n$ and $\tau(\frac{n(n+1)}{2} + k) = k$.*

Lemma 5. *Let $n, k \in \mathbb{Z}_{\geq 0}, 0 \leq k \leq n$, then*

$$\sum_{k=0}^{n} a_{n-k} b_k = \sum_{k=\frac{n(n+1)}{2}}^{\frac{n(n+1)}{2}+n} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)}.$$

Lemma 6. *Let $N \in \mathbb{Z}_{\geq 0}$, then*

$$\sum_{n=0}^{N} \sum_{k=0}^{n} a_{n-k} b_k = \sum_{n=0}^{\frac{N(N+1)}{2}+N} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)}.$$

The next theorem requires formalizing one more lemma.

Lemma 7. *Let $n \in \mathbb{Z}_{\geq 0}$, there exist $m, r \in \mathbb{Z}_{\geq 0}$, with $r \leq m$, and $n = \frac{m \cdot (m+1)}{2} + r$.*

Now, the flattened version of the series can be proved equal to the original series.

Theorem 2. *Let a_n and b_n be positive sequences and $\sum_{n=0}^{\infty} \sum_{k=0}^{n} a_{n-k} b_k$ convergent. Then $\sum_{n=0}^{\infty} \sum_{k=0}^{n} a_{n-k} b_k = \sum_{k=0}^{\infty} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)}$.*

Since there was no previous specification of the Cauchy product in PVS, its formalization was essential to obtain a complete theory.

The series flattening process was generalized for the product of more series.

Lemma 8. *Let $n \in \mathbb{Z}_{>0}$, then*

$$\prod_{i=0}^{n-1} \sum_{k=0}^{\infty} a_i(k) = \sum_{\substack{k, j_l \in \mathbb{Z}_{\geq 0} \\ j_0 + j_1 + \ldots + j_{n-1} = k}} \prod_{i=0}^{n-1} a_i(j_i).$$

The equality of functions ξ and μ, used in the informal proof, can be obtained using Lemma 8 and the Fundamental Theorem of Arithmetic. However, in PVS, as this property was only needed in the next lemma, it was faster to associate each term directly in the next proof instead of stating this equality as a separate PVS lemma.

Lemma 9. *Let $n \in \mathbb{Z}_{>0}$, $H_n \leq \mu(n)$*

Proof. From the definition of the μ function, and since it is an absolutely convergent series, if for every $\frac{1}{k}$, $1 < k \leq n$, there exists a prime $p \mid k$, $p \leq n$, the series can be ordered as

$$\mu(n) = \sum_{k=1}^{n} \frac{1}{k} + \sum_{\substack{k \in \mathbb{Z}_{\geq n}, \\ k=1 \ \vee \ \exists p \in \mathbb{P}, \\ (p \leq n \ \wedge \ p \mid k)}} \frac{1}{k}$$

Which trivially results in $H_n \leq \mu(n)$. To conclude, since $1 < k \leq n$ and a divisor is less than or equal to the number it divides, all prime divisors of k satisfy the inequality $p \leq k$. Therefore, the maximal prime divisor of k, say p, is such that $p \leq n$.

For the PVS formalization, such a series rearrange needed to be expressed in a more explicit form; for that reason, a theory called `sequence_extra.pvs` was included, in which a constructive specification of the function that orders by common summed values is given.

Lemma 10. *Let $n, i \in \mathbb{Z}_{\geq 0}$, for $i < \pi(n)$, $\frac{\rho(i)}{\rho(i)-1} \leq \frac{i+2}{i+1}$*

Proof. Notice that $\frac{\rho(i)}{\rho(i)-1} \leq \frac{i+2}{i+1} \iff 1+\frac{1}{\rho(i)-1} \leq 1+\frac{1}{i+1} \iff i+1 \leq \rho(i)-1 \iff i+2 \leq \rho(i)$.

This is proved by induction. For $i = 0$, $0+2 \leq 2$; for $i > 0$, by i.h., $i+1 \leq \rho(i-1) \Rightarrow i+2 \leq \rho(i-1)+1$. By the property 4, $\rho(i) \neq 0$, and using Lemma 1, it can be shown that $\rho(i-1) < \rho(i)$. Since $\rho(i-1)$ is an integer, $\rho(i-1)+1 \leq \rho(i)$; therefore, $i+2 \leq \rho(i)$.

Lemma 11. $\xi(n) \leq \pi(n) + 1$

Theorem 3. *There are infinitely many primes*

Proof. Composing the inequalities from Lemmas 4, 11 and 9, one obtains $\log(n) \leq \xi(n) = \mu(n) \leq \pi(n) + 1$. Since the logarithm is a strictly increasing function, there is no maximum $\pi(n)$ value.

4 Conclusion

The presented PVS library helps show mathematicians the potential of interactive theorem provers in formalizing complex mathematical concepts, showcasing that substantial and technically intricate proofs can be rigorously verified using computer software. The complete formalization of distinct proofs of the infinitude of primes from the renowned book "Proofs from THE BOOK" contributed significantly to developing a rich and mathematically diverse library to attract the interest of researchers from various branches of mathematics.

Table 1 shows a quantitative overview of the formalization effort.

Table 1: Quantitative data.

PVS theory	Formulas	TCCs	Specification Size (.pvs lines)	Proof Commands (.prf lines)	Main Dependencies					
					Prime enum	Cauchy Product	Series	Topology (NASALib)	Algebra (NASALib)	Num Theory Extra
Fermat	17	8	75	981						✔
Mersenne	28	17	112	2568					✔	✔
Euler	39	28	112	3408	✔	✔	✔			✔
Fürstenberg	19	2	115	1822				✔		✔
Erdös	71	35	273	8117	✔		✔			✔

Additional Theories Quantitative Data				
PVS theory	Formulas	TCCs	Specification Size	Proof Commands
Primes enumeration	65	37	212	4574
Cauchy product formula	21	10	111	2302
Series extra	23	8	109	1610
Others	89	51	419	5125

This work highlighted essential differences between the informal proofs and the formalizations. One key difference was the need to adjust the original proofs regarding prime enumeration. The original proofs assumed data structures in which the set of primes was infinite, a flaw given the level of rigor required in the formalization. To address such an imprecision, an enumeration function was defined in PVS that avoids assuming the infinitude of primes, ensuring a rigorous foundation for the required adaptation of the Fundamental Theorem of Arithmetic. This result can be found in the file `prime_extra.pvs`. Furthermore, the strong typing features of PVS played a crucial role in highlighting the importance of distinguishing between different types of structures, particularly, for the proof using Mersenne numbers, where the type system helped clarify the relationships between the different algebraic structures involved. Although Lagrange's theorem was not used, the formalization leveraged a result about group orders, proving that the order of any group element satisfying a particular condition divides a given integer. Another key difference between the proof in "THE BOOK" and its formalization is using the Cauchy product to prove the Euler product. In "THE BOOK", the Euler product's connection to the harmonic series was somewhat informal, which required more rigorous proof. As the Cauchy product was not formalized in NASALib, this allows for improving both the Analysis and the Series libraries.

Also, distinguished features from PVS were crucial to guide the formalizations, particularly in handling topology and number theory aspects. Fürstenberger's topological proof was straightforward due to the well-established PVS topology library. Similarly, the proof using Fermat numbers benefited from the comprehensive number theory library in the PVS prelude. All that, conjugated with the typing system and the ability to define custom functions, made it possible to address the nuances of the infinitude of primes and formalize the proofs in a rigorous and structured manner while addressing the impressions and omissions, as well as determining proof alternatives simpler than those in the traditional proofs.

Further expansions of the presented formalization can include additional proofs uncovered in "Proofs from THE BOOK," particularly those exploring other branches of mathematics or offering alternative perspectives on well-known approaches. One area of interest could be the formalization of a geometry-related proof of the infinitude of primes, such as the given in [6], which would broaden the scope of the library beyond number theory, analysis, topology, and algebra. Additionally, incorporating more advanced results in number theory, such as Dirichlet's Theorem on primes in arithmetic progressions, would be a valuable addition. In general, a key focus will also be improving the level of automation in PVS. For instance, leveraging algebraic manipulations for structures other than number fields (highly automated through the Manip package [25]), particularly in streamlining the process of formalizing proofs without obscuring essential mathematical reasoning steps.

References

1. Aigner, M., Ziegler, G.M.: Proofs from THE BOOK. Berlin. Germany **1**(2), 12 (1999). https://doi.org/10.1007/978-3-662-57265-8
2. Apostol, T.M.: Introduction to analytic number theory. Springer Science & Business Media (2013). https://doi.org/10.1007/978-1-4757-5579-4
3. Artmann, B.: Euclid—the creation of mathematics. Springer Science & Business Media (2012). https://doi.org/10.1007/978-1-4612-1412-0
4. Ayala-Rincón, M., de Lima, T.A., Avelar, A.B., Galdino, A.L.: Formalization of algebraic theorems in PVS (invited talk). In: Proceedings of 24th International Conference on Logic for Programming, Artificial Intelligence and Reasoning LPAR. EPiC Series in Computing, vol. 94, pp. 1–10. EasyChair (2023). https://doi.org/10.29007/7JBV
5. Bortin, M.: From THE BOOK: Two Squares via Involutions. Archive of Formal Proofs (August 2022), https://isa-afp.org/entries/Involutions2Squares.html
6. de Castro, D.: Infinitude of primes: Euclid's proof using angles between lattice vectors. Elemente der Mathematik **76**(1), 28–32 (2021). https://doi.org/10.4171/EM/425
7. Cauchy, A.L.: Cours d'analyse de L'Ecole Polytechnique. oeuvres completes **2**, t–3 (1821)
8. Eberl, M.: The Hurwitz and Riemann ζ Functions. Arch. Formal Proofs (2017), https://www.isa-afp.org/entries/Zeta_Function.html
9. Eberl, M.: Furstenberg's topology and his proof of the infinitude of primes. Archive of Formal Proofs (2020), https://isa-afp.org/entries/Furstenberg_Topology.html
10. Erdös, P.: Uber die Reihe $\Sigma\, 1/p$. Mathematica, Zutphen B **7**, 1–2 (1938)
11. Euler), L.E.L.: Introductio in analysin infinitorum, vol. tomus primus. Marcum-Michaelem Bousquet & Socies, Lausanne (1748)
12. Furstenberg, H.: On the infinitude of primes. Amer. Math. Monthly **62**(5), 353 (1955). https://doi.org/10.1080/00029890.1955.11988641, note in *Mathematical Notes*, pages 349-353
13. Gauss, C.F.: Disquisitiones arithmeticae. Springer-Verlag, English edn. (1986). https://doi.org/10.1007/978-1-4939-7560-0
14. Gödel, K.: Über Formal Unentscheidbare Sätze der Principia Mathematica Und Verwandter Systeme I. Monatshefte für Mathematik **38**(1), 173–198 (1931)
15. Gottliebsen, H., Hardy, R., Lightfoot, O., Martin, U.: Applications of real number theorem proving in PVS. Formal Aspects Comput. **25**(6), 993–1016 (2013). https://doi.org/10.1007/S00165-012-0232-9
16. Hua, L.K.: Introduction to number theory. Springer Science & Business Media (2012)
17. Koepke, P., Marcol, M., Schäfer, P.: Formalizing Sets and Numbers, and some of Wiedijk's "100 Theorems" in Naproche (2023), https://naproche.github.io/100_theorems.ftl.pdf, naproche repository document
18. de Lagrange, J.L.: Réflexions sur la résolution algébrique des équations. Prussian Academy (1770)
19. Lester, D.R.: Topology in PVS: continuous mathematics with applications. In: Proceedings of the second workshop on Automated formal methods AFM. pp. 11–20. ACM (2007). https://doi.org/https://doi.org/10.1145/1345169.1345171
20. Mendelson, B.: Introduction to topology. Dover Publications, third edn. (1990)

21. Owre, S., Rushby, J.M., Shankar, N.: PVS: A prototype verification system. In: Proceedings 11th International Conference on Automated Deduction CADE-11. Lecture Notes in Computer Science, vol. 607, pp. 748–752. Springer (1992). https://doi.org/10.1007/3-540-55602-8_217
22. Paulson, L.C.: Irrational numbers from THE BOOK. Archive of Formal Proofs (2022), https://isa-afp.org/entries/Irrationals_From_THEBOOK.html
23. Robinson, R.M.: Mersenne and Fermat numbers. Proceedings of the American Mathematical Society **5**(5), 842–846 (1954)
24. Titchmarsh, E.C.: The theory of the Riemann Zeta-function. The Clarendon Press Oxford University Press (1986)
25. Vito, B.L.D.: Manip User's Guide. NASA Langley Research Center (2012), https://pvs.csl.sri.com/doc/manip-guide.pdf
26. Wiedijk, F.: Formalizing 100 Theorems (Formal proof–getting started) (Web page, last visited February 2023), https://www.cs.ru.nl/~freek/100/

A Proofs for Section 3 (Description of the Formalization)

Lemma 4. $\forall n \in \mathbb{Z}_{\geq 0}, \log(n) \leq H_n$

Proof. This can be done by considering the inequality $\frac{1}{x} \leq \frac{1}{k}$ for $x \in [k, k+1]$, and the inequalities for finite summations of integrations:

$$\log(n+1) = \int_1^{n+1} \frac{1}{x} dx = \sum_{k=1}^{n} \int_k^{k+1} \frac{1}{x} dx \leq \sum_{k=1}^{n} \int_k^{k+1} \frac{1}{k} dx$$

Then, $\Rightarrow \log(n+1) \leq \sum_{k=1}^{n} \frac{1}{k} = H_n$, and since log is an increasing function, $\log(n) \leq H_n$.

Corollary 1. *Let $n, k \in \mathbb{Z}_{\geq 0}, 0 \leq k \leq n$, then $\theta(\frac{n(n+1)}{2} + k) = n$ and $\tau(\frac{n(n+1)}{2} + k) = k$.*

Proof. Since $0 \leq k$, $\frac{n(n+1)}{2} \leq \frac{n(n+1)}{2} + k$. Also, since $k \leq n$,

$$\frac{n(n+1)}{2} + k \leq \frac{n(n+1)}{2} + n < \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$$

Therefore, by the definition of θ, one must have $\theta(\frac{n(n+1)}{2} + k) = n$, implying that

$$\tau\left(\frac{n(n+1)}{2} + k\right) = \frac{n(n+1)}{2} + k - \frac{\theta\left(\frac{n(n+1)}{2} + k\right)\left(\theta\left(\frac{n(n+1)}{2} + k\right) + 1\right)}{2}$$

$$= \frac{n(n+1)}{2} + k - \frac{n(n+1)}{2} = k$$

Lemma 5. *Let $n, k \in \mathbb{Z}_{\geq 0}, 0 \leq k \leq n$, then*
$\sum_{k=0}^{n} a_{n-k} b_k = \sum_{k=\frac{n(n+1)}{2}}^{\frac{n(n+1)}{2}+n} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)}$.

Proof. Using the Corollary 1, it holds that $\theta(\frac{n(n+1)}{2}+k) = n$ and $\tau(\frac{n(n+1)}{2}+k) = k$, therefore, by change of basis.

$$\sum_{k=\frac{n(n+1)}{2}}^{\frac{n(n+1)}{2}+n} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)}$$

$$= \sum_{k=0}^{n} a_{\left(\theta\left(\frac{n(n+1)}{2}+k\right)-\tau\left(\frac{n(n+1)}{2}+k\right)\right)} \cdot b_{\tau\left(\frac{n(n+1)}{2}+k\right)}$$

$$= \sum_{k=0}^{n} a_{n-k} b_k$$

Lemma 6. *Let $N \in \mathbb{Z}_{\geq 0}$, then*

$$\sum_{n=0}^{N}\sum_{k=0}^{n} a_{n-k}b_k = \sum_{n=0}^{\frac{N(N+1)}{2}+N} a_{(\theta(k)-\tau(k))}\cdot b_{\tau(k)}.$$

Proof. By induction on N.

Case $N = 0$, by Corollary 1, $\theta(0) = 0$ and $\tau(0) = 0$, therefore $a_0b_0 = a_{(\theta(0)-\tau(0))}\cdot b_{\tau(0)}$.

Case $N > 0$, by i.h.

$$\sum_{n=0}^{N+1}\sum_{k=0}^{n} a_{n-k}b_k$$

$$= \sum_{k=0}^{n+1} a_{n-k}b_k + \sum_{n=0}^{\frac{N(N+1)}{2}+N} a_{(\theta(k)-\tau(k))}\cdot b_{\tau(k)}.$$

Then, by Lemma 5, the last expression is equal to

$$\sum_{k=\frac{(N+1)(N+2)}{2}}^{\frac{(N+1)(N+2)}{2}+N+1} a_{(\theta(k)-\tau(k))}\cdot b_{\tau(k)} + \sum_{n=0}^{\frac{N(N+1)}{2}+N} a_{(\theta(k)-\tau(k))}\cdot b_{\tau(k)}$$

$$= \sum_{n=0}^{\frac{(N+1)(N+2)}{2}+N+1} a_{(\theta(k)-\tau(k))}\cdot b_{\tau(k)}.$$

Lemma 7. *Let $n \in \mathbb{Z}_{\geq 0}$, there exist $m, r \in \mathbb{Z}_{\geq 0}$, with $r \leq m$, and $n = \frac{m\cdot(m+1)}{2} + r$.*

Proof. By induction on n.

Case $n = 0$, $m = r = 0$ satisfy the equality.

Case $n > 0$. By i.h., if $r = m$,

$$n+1 = \frac{m\cdot(m+1)}{2} + m + 1 = \frac{(m+1)(m+2)}{2} = \frac{(m+1)[(m+1)+1]}{2} + 0.$$

Otherwise, if $r < m$, $n+1 = \frac{m\cdot(m+1)}{2} + (r+1)$, and $r+1 \leq m$.

Theorem 2. *Let a_n and b_n be positive sequences and $\sum_{n=0}^{\infty}\sum_{k=0}^{n} a_{n-k}b_k$ convergent. Then $\sum_{n=0}^{\infty}\sum_{k=0}^{n} a_{n-k}b_k = \sum_{k=0}^{\infty} a_{(\theta(k)-\tau(k))}\cdot b_{\tau(k)}$.*

Proof. It should be proved that $\left|L - \sum_{k=0}^{n} a_{(\theta(k)-\tau(k))}\cdot b_{\tau(k)}\right| < \epsilon$, for every real $\epsilon > 0$, for larger enough $n \geq N$, where $L = \sum_{n=0}^{\infty}\sum_{k=0}^{n} a_{n-k}b_k$.

By rewriting n as $\frac{m\cdot(m+1)}{2} + r$, where $0 \leq r \leq m$ (Lemma 7), and using Lemma 6, the difference can be estimated as follows.

$$\left| L - \sum_{k=0}^{\frac{m\cdot(m+1)}{2}+r} a_{(\theta(k)-\tau(k))}\cdot b_{\tau(k)} \right|$$

$$= \left| L - \sum_{k=0}^{\frac{m\cdot(m+1)}{2}+m} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)} + \sum_{k=\frac{m\cdot(m+1)}{2}+r+1}^{\frac{m\cdot(m+1)}{2}+m} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)} \right|$$

$$\leq \left| L - \sum_{k=0}^{\frac{m\cdot(m+1)}{2}+m} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)} \right| + \left| \sum_{k=\frac{m\cdot(m+1)}{2}+r+1}^{\frac{m\cdot(m+1)}{2}+m} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)} \right|$$

$$\leq \left| L - \sum_{k=0}^{\frac{m\cdot(m+1)}{2}+m} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)} \right| + \left| \sum_{k=r+1}^{m} a_{m-k} \cdot b_k \right| \text{ (By Cor. 1)}$$

$$\leq \left| L - \sum_{n=0}^{m}\sum_{k=0}^{n} a_{n-k}b_k \right| + \left| \sum_{k=r+1}^{m} a_{m-k}b_k \right| \text{ (By Lemma 6)}$$

$$\leq \left| L - \sum_{n=0}^{m}\sum_{k=0}^{n} a_{n-k}b_k \right| + \sum_{k=0}^{m} a_{m-k}b_k \text{ (Since } a_n \text{ and } b_n \text{ are positive sequences).}$$

Since $\sum_{n=0}^{\infty}\sum_{k=0}^{n} a_{n-k}b_k$ is convergent, $\lim_{n\to\infty}\sum_{k=0}^{n} a_{n-k}b_k = 0$, implying that for every $\epsilon > 0$, there exist $N_1 \leq n, N_2 \leq n$, such that

$$\left| L - \sum_{n=0}^{m}\sum_{k=0}^{n} a_{n-k}b_k \right| < \frac{\epsilon}{2} \qquad \text{and} \qquad \sum_{k=0}^{m} a_{m-k}b_k < \frac{\epsilon}{2}.$$

Therefore, for $N = \max(N_1, N_2)$, $\left| L - \sum_{k=0}^{n} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)} \right| < \epsilon$.

Lemma 8. *Let $n \in \mathbb{Z}_{>0}$, then*

$$\prod_{i=0}^{n-1}\sum_{k=0}^{\infty} a_i(k) = \sum_{\substack{k, j_l \in \mathbb{Z}_{\geq 0} \\ j_0+j_1+\ldots+j_{n-1}=k}} \prod_{i=0}^{n-1} a_i(j_i).$$

Proof. By induction on n. For $n = 1$, this trivially says that $\sum_{k=0}^{\infty} a_0(k) = \sum_{k=0}^{\infty} a_0(k)$. For $n > 1$, by i.h.,

$$\prod_{i=0}^{n}\sum_{k=0}^{\infty} a_i(k) = \left(\sum_{k=0}^{\infty} a_n(k)\right) \cdot \left(\sum_{\substack{k, j_l \in \mathbb{Z}_{\geq 0} \\ j_0+j_1+\ldots+j_{n-1}=k}} \prod_{i=0}^{n-1} a_i(j_i) \right)$$

By Cauchy product (Formula 1),

$$= \sum_{m=0}^{\infty} \sum_{\substack{j_l \in \mathbb{Z}_{\geq 0} \\ j_0+j_2+\ldots+j_n=m}} a_n(m - (j_0 + j_1 + \ldots + j_{n-1})) \cdot \prod_{i=0}^{n-1} a_i(j_i)$$

$$= \sum_{m=0}^{\infty} \sum_{\substack{j_l \in \mathbb{Z}_{\geq 0} \\ j_0+j_2+\ldots+j_n=m}} a_n(j_n) \cdot \prod_{i=0}^{n-1} a_i(j_i) = \sum_{m=0}^{\infty} \sum_{\substack{j_l \in \mathbb{Z}_{\geq 0} \\ j_0+j_2+\ldots+j_n=m}} \prod_{i=0}^{n} a_i(j_i)$$

$$= \sum_{\substack{k, j_l \in \mathbb{Z}_{\geq 0} \\ j_1+j_2+\ldots+j_n=k}} \prod_{i=0}^{n} a_i(j_i).$$

The last equality uses the flattening process of Theorem 2.

Lemma 11. $\xi(n) \leq \pi(n) + 1$

Proof. Since the geometric series has a closed form, $\xi(n)$ can be simplified as shown below.

$$\prod_{i=0}^{\pi(n)-1} \sum_{k=0}^{\infty} \frac{1}{\rho(i)^k} = \prod_{i=0}^{\pi(n)-1} \frac{\rho(i)}{\rho(i)-1} \leq \prod_{i=0}^{\pi(n)-1} \frac{i+2}{i+1}$$

The last inequality is obtained using Lemma 10. Notice that the last expression is a telescoping product , therefore, $\prod_{i=0}^{\pi(n)-1} \frac{i+2}{i+1} = \frac{(\pi(n)-1)+2}{0+1} = \pi(n) + 1$.