



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

PVS Formalization of Proofs of the Infinitude of Primes

**(Formalização em PVS de Demonstrações da
Infinitude dos Primos)**

Bruno Berto de Oliveira Ribeiro

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Orientador

Prof. Dr. Mauricio Ayala-Rincón

Coorientadora

Prof.a Dr.a Thaynara Arielly de Lima

Brasília
2025



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

PVS Formalization of Proofs of the Infinitude of Primes

**(Formalização em PVS de Demonstrações da
Infinitude dos Primos)**

Bruno Berto de Oliveira Ribeiro

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Prof. Dr. Mauricio Ayala-Rincón (Orientador)
CIC/Universidade de Brasília

Prof. Dr. Flavio Leonardo Cavalcanti Moura
CIC/Universidade de Brasília

Dr. Mariano Miguel Moscato
AMA/NASA LaRC Formal Methods

Prof.a Dr.a Thaynara Arielly de Lima
IME/Universidade Federal de Goiás

Prof. Dr. Marcelo Grandi Mandelli
Coordenador do Bacharelado em Ciência da Computação

Brasília, 21 de Fevereiro de 2025

Dedicatória

Dedico este trabalho aos meus pais, que me apoiaram nos momentos mais difíceis ao longo de toda a minha graduação. Também dedico à minha avó paterna, que, apesar de sua condição atual, sempre sonhou em ver o neto se formando. Não poderia deixar de dedicar aos meus amigos de longa data, que, mesmo de forma indireta, contribuíram para essa jornada.

I dedicate this work to my parents, who supported me during the most challenging moments throughout my entire undergraduate journey. I also dedicate it to my paternal grandmother, who, despite her current condition, always dreamed of seeing her grandson graduate. I cannot forget to dedicate it to my long-time friends, who, even indirectly, have contributed to this journey.

Agradecimentos

Primeiramente, gostaria de agradecer a Deus, por me conceder forças e sabedoria ao longo dessa jornada. Sua orientação foi essencial em cada etapa desse trabalho. Agradeço profundamente à minha família, especialmente aos meus pais, por todo o amor, paciência e apoio. Sem vocês, eu não teria chegado até aqui. Obrigado por acreditarem em mim e me incentivarem a seguir meus sonhos, mesmo nos momentos mais desafiadores. Aos meus amigos, que me acompanharam em todos os momentos, oferecendo apoio emocional, risadas e conforto, meu muito obrigado. Vocês fizeram toda a diferença na minha caminhada. Aos meus orientadores, Mauricio Ayala-Rincón e Thaynara Arielly de Lima, agradeço imensamente pela orientação dedicada, pelos ensinamentos valiosos e pela paciência ao longo do desenvolvimento deste trabalho.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

First, I would like to thank God for granting me strength and wisdom throughout this journey. His guidance was essential at every stage of this work. I deeply thank my family, especially my parents, for all the love, patience, and support. Without you, I wouldn't have made it this far. Thank you for believing in me and encouraging me to follow my dreams, even in the most challenging moments. To my friends, who accompanied me at all times, offering emotional support, laughter, and comfort, my heartfelt thanks. You made all the difference in my journey. To my advisors, Mauricio Ayala-Rincón and Thaynara Arielly de Lima, I am immensely grateful for the dedicated guidance, valuable teachings, and patience throughout the development of this work.

This work was carried out with the support of the Coordination for the Improvement of Higher Education Personnel – Brazil (CAPES), through access to the Periodicals Portal.

Resumo

Este trabalho apresenta a mecanização de cinco abordagens diferentes para provar a infinitude dos números primos usando o assistente de prova Prototype Verification System (PVS). As técnicas de prova analítica abrangem várias áreas da matemática, como álgebra, teoria dos números, topologia e análise, e são baseadas nas elegantes provas selecionadas por Martin Aigner e Günter Ziegler no seu famoso livro "Proofs from THE BOOK". Nesse livro, são apresentadas seis diferentes provas da infinitude dos números primos, sendo a primeira a prova clássica de Euclides, que já está formalizada na biblioteca *NASALib* da NASA. Como resultado, nosso trabalho concentra-se na especificação e formalização das cinco provas restantes.

A mecanização das provas faz uso de outras bibliotecas de PVS, como *NASALib* e *prelude*, que abstraem estruturas matemáticas como grupos, produtos Cartesianos, series e conjuntos, entre outras. No entanto, a importação de provas que assumem a infinitude dos números primos foram evitadas para prevenir circularidade. Além disso, o trabalho visa corrigir abusos notacionais e informalidades presentes nas provas do livro, se aproveitando do sistema de tipos do PVS, que é robusto o suficiente para revelar falhas nas formulações.

Palavras-chave: Infinitude dos Primos, Dedução Automática, Prova de Teoremas, Prototype Verification System, Métodos Formais, Formalização de Teoremas, Verificação de Algoritmos

Abstract

This work presents the mechanization of five different approaches to proving the infinitude of prime numbers using the Prototype Verification System (PVS) proof assistant. The analytical proof techniques span various areas of mathematics, such as algebra, number theory, topology, and analysis, and are based on the elegant proofs selected by Martin Aigner and Günter Ziegler in their famous book "Proofs from THE BOOK". They present six different proofs of the infinitude of prime numbers, the first being the classical proof by Euclid, which is already specified in the NASA library *NASALib*. As a result, our work focuses on specifying and formalizing the remaining five proofs from the book.

The mechanization of the proofs makes use of other libraries such as *NASALib* and *prelude*, which abstract mathematical structures like groups, Cartesian products, series, sets, and others. However, the importing of proofs that assume the infinitude of prime numbers were avoided to prevent circularity. Additionally, the work aims to correct notational abuses and informalities present in the proofs from the book, as the PVS type system is robust enough to reveal flaws in the formalisms.

Keywords: Infinitude of Primes, Automated Deduction, Proof of Theorems, Prototype Verification System, Formal Methods, Formalization of Theorems, Algorithm Verification.

Contents

1	Introduction	1
1.1	Related work	2
1.2	Main contributions	3
1.3	Organization of the document	4
2	Prototype Verification System (PVS)	5
2.1	Introduction	5
2.2	PVS Environment	7
3	Fermat numbers	11
3.1	Proof structure	11
3.2	Specification details	12
4	Mersenne numbers	16
4.1	Proof structure	16
4.2	Specification details	17
5	Euler product formula	21
5.1	Proof structure	22
5.2	Specification details	22
5.2.1	Prime enumeration	22
5.2.2	A few inequalities	25
6	Fürstenberg's topological proof	35
6.1	Proof structure	35
6.2	Specification details	36
7	Prime reciprocal series	40
7.1	Proof structure	40
7.2	Specification details	42
7.2.1	<i>Big</i> primes multiple set $N_b(n, k)$	44

7.2.2	<i>Small</i> primes multiple set $N_s(n, k)$	46
7.2.3	Proof by contradiction	49
8	Conclusion and Future Work	51
	Bibliography	53

List of Figures

2.1	PVS User Interface	5
2.2	Emacs Editor	6
2.3	Visual representation of a proof script.	6
2.4	VSCoDe-PVS	7
2.5	PVS System Overview	9

Chapter 1

Introduction

The Euclid's proof of the infinitude of primes [1] is a classic and highly illustrative result. As the concept of primality is typically introduced in basic Math courses, this proof offers an excellent example of how to approach problems involving the notion of infinity. Over the years, many mathematicians, such as Paul Erdős, have provided new proofs of this result, each drawing from different areas of mathematics. These proofs are not only valuable for showcasing the tools of these diverse fields, but they also serve as a reminder that mathematics is a deeply interconnected discipline, where concepts and techniques from various branches often come together to solve fundamental problems.

In the context of formalizing mathematical proofs, proof assistants offer invaluable tools to ensure rigor and correctness. Various proof assistants, including PVS, Coq, Isabelle/HOL, Lean, and others, have been developed to aid in the mechanization of proofs across diverse mathematical domains. Not only in the case of proving infinitude, proof assistants provide a structured and reliable approach to formalizing and verifying such classical results, ensuring that the proof is free of errors and ambiguities.

This work aims to extend beyond Euclid's original proof by specifying and formalizing five alternative proofs of the infinitude of primes using the Prototype Verification System (PVS) [2]. These formalizations explore different proof techniques derived from various areas of mathematics, such as algebra, number theory, topology, and analysis. Each proof will be 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 [3], which offers six different proofs. The first, Euclid's classical proof, is omitted here as it is already included in *NASALib*. [↗](#)

The mechanization will be based on established libraries like *prelude* and NASA's PVS library, the *NASALib*, which provide useful abstractions for mathematical structures such as sets, groups, and Cartesian products. Importantly, the formalization does not assume the infinitude of primes beforehand, as we are trying to avoid circular reasoning.

Circularity can arise in theorem proving, when trying to prove Theorem A by using the Theorem B, but Theorem A is a prerequisite for proving B, for example, trying to use Gödel Completeness Theorem [4] to prove the Compactness Theorem. In the book, notations such as p_1, p_2, p_3, \dots was used for prime enumeration, but notice that this type of notation assumes infinitude of primes beforehand.

For dealing with the prime enumeration informality, a new definition of a function that enumerates primes will be discussed, as well as a new form to model the Fundamental Theorem of Arithmetic [5] in PVS, using the new prime enumeration and avoiding problems with assuming the infinitude of primes. This approach to formalizing prime-related concepts is just one example of the broader objectives of this study, which also focuses on identifying and correcting notational errors and informalities in "Proofs from THE BOOK". PVS's robust type system plays a critical role in highlighting and addressing these flaws, ensuring that the formalisms remain both precise and rigorous. Furthermore, the work underscores the educational value of using PVS to formalize mathematical proofs.

By breaking down the proofs into step-by-step files, this study 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

Since we are utilizing the *NASALib* library, a significant number of the necessary theorems for fields such as algebra, number theory, analysis, and topology have already been established [6][7][8]. These theorems were imported when the code was initially set up, which greatly streamlines our work. This allows us to build on a solid foundation, avoiding the need to reprove or reimplement basic results, and instead focus 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" project [9], which aims to formalize 100 important mathematical theorems across different proof assistants. 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 [10] and PVS' *NASALib*. The other approach employs a factorial plus one method, which is used in the Isabelle/HOL and Coq proofs.

In addition to the classical Euclid's proof of the infinitude of primes, other proofs have been developed in different proof assistants, such as those found in Isabelle. Such proofs are Fürstenberg's topology proof [11] and the one involving the zeta function [12]. The topology-based proof is simpler to formalize, as it relies on fewer mathematical structures compared to other proofs in the book, 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 our collection, as it offers an opportunity to showcase topology theory in *NASALib*. On the other hand, the proof of the zeta function, which is also presented in "Proofs from 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 our primary focus is on the first topic of "Proofs from 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 [13] and Fermat's two-square theorem [14].

1.2 Main contributions

The main contributions of this work is listed below:

- Five additional proofs for the infinitude of primes for PVS, which can be used for new users as an example of usage of various *NASALib*'s theories, such as ints, algebra, analysis and topology.
- Discussion and formalization of omitted details in "Proofs from THE BOOK".
- New approach for the PVS standard prime factorization theorem and general structure specification.
- Improvements in algebra library such as the $\mathbb{Z}/p\mathbb{Z}$ coset manipulation and type checking related problems.
- Minor improvements in integer manipulation in PVS, specially related with *gcd* function

1.3 Organization of the document

In the next Chapter, we are going to tell about PVS for the newcomers. The following Chapters 3 to 7 correspond to the proofs in "Proofs from THE BOOK", with each Chapter focusing on a different proof. Each proof Chapter will include an overview of the proof's general context, a step by step breakdown of the proof's structure as presented in "Proofs from THE BOOK", and a "Specification Details" section, where we discuss the formal mathematical approach used and provide commentary on its specifications in PVS. And last but not least, a conclusion Chapter will be presented. To be more specific:

- Chapter 2 will have a brief explanation of what the proof assistant PVS is, its architecture and some of its terminology.
- Chapters 3 and 4 present proofs that use special numbers for asserting the infinitude of primes, that numbers being: Fermat numbers and Mersenne numbers, respectively. In particular, Chapter 3 uses the *NASALib* algebra library to handle group-theoretic proofs.
- Chapters 5 and 7 contain analysis-related proofs, with Chapter 5 addressing the divergence of the sum of reciprocals of positive integers (the Riemann zeta function at 1), and Chapter 7 dealing with the sum of reciprocals of the prime numbers.
- Chapter 6 uses topological notions, such as open and closed sets, to prove the infinitude of the set of primes.
- Chapter 8 contains future work and the conclusion of this document.

Chapter 2

Prototype Verification System (PVS)

2.1 Introduction

The Prototype Verification System [2] (Figure 2.1) is an open source integrated and interactive environment for formal specification and verification. The PVS was developed at the Software Research Institute (SRI) International in Menlo Park, CA, and is supported by the Formal Methods Team at NASA Langley Research Center[15], where it is widely used in formal verification projects. The PVS tutorials and documentation can be downloaded from the PVS web site[16].

PVS has been used in many fields in academia and industry, including, but not limited to, the design of flight control software and real-time systems[17].

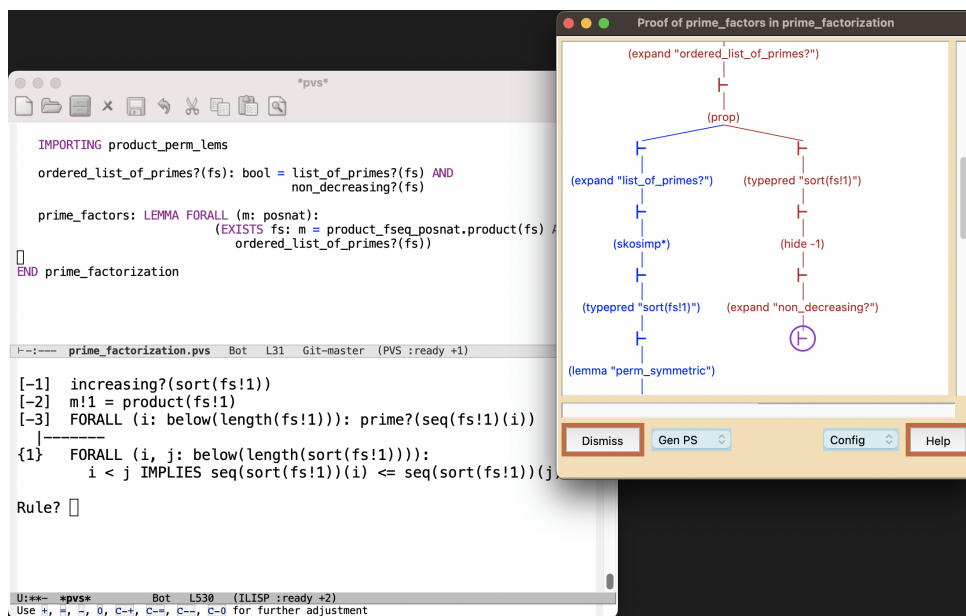


Figure 2.1: PVS User Interface

The PVS core system is implemented in Common LISP[18] with a front-end based on the Emacs¹[19] editor (Figure 2.2) plus Tcl/Tk² based GUI extensions that display proof trees, theory hierarchies and proof commands (Figure 2.3), as well as browsing tools, and L^AT_EX, HTML, and XML output capabilities.

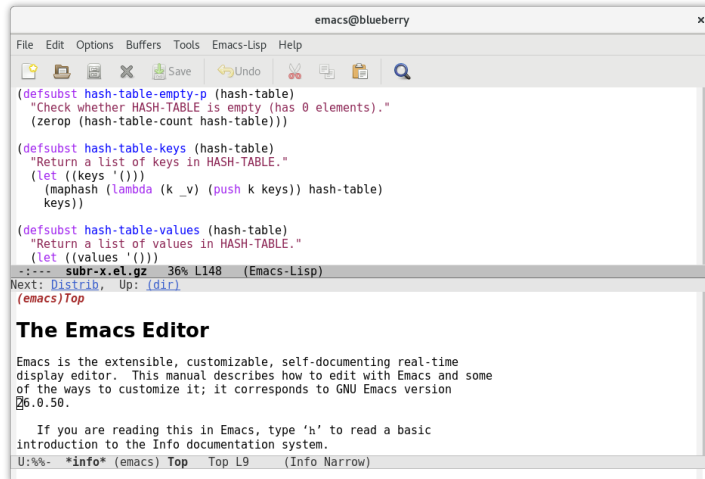


Figure 2.2: Emacs Editor

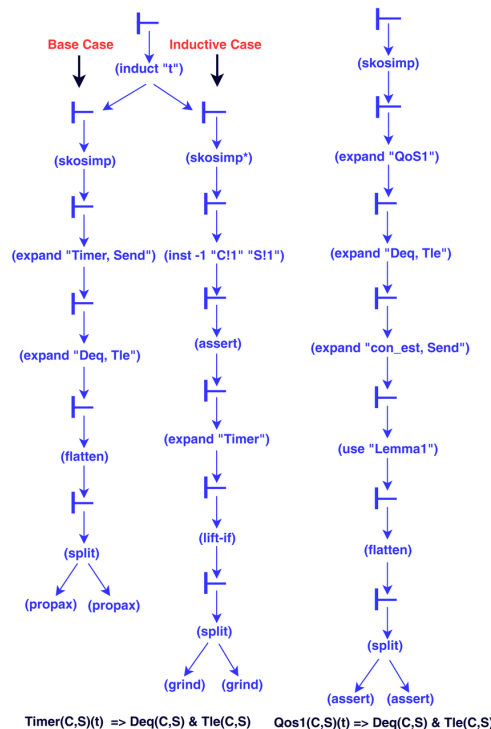


Figure 2.3: Visual representation of a proof script.

¹<https://www.gnu.org/software/emacs/>

²<https://www.tcl-lang.org/>

There is also the VSCode-PVS [20][21], which is more user friendly PVS interface based on Microsoft Visual Studio Code³. As described by Masci and Muñoz [20],

"It provides functionalities that developers expect to find in modern verification tools, but are not available in the standard Emacs frontend of PVS, such as auto-completion, point-and-click navigation of definitions, live diagnostics for errors, and literate programming."

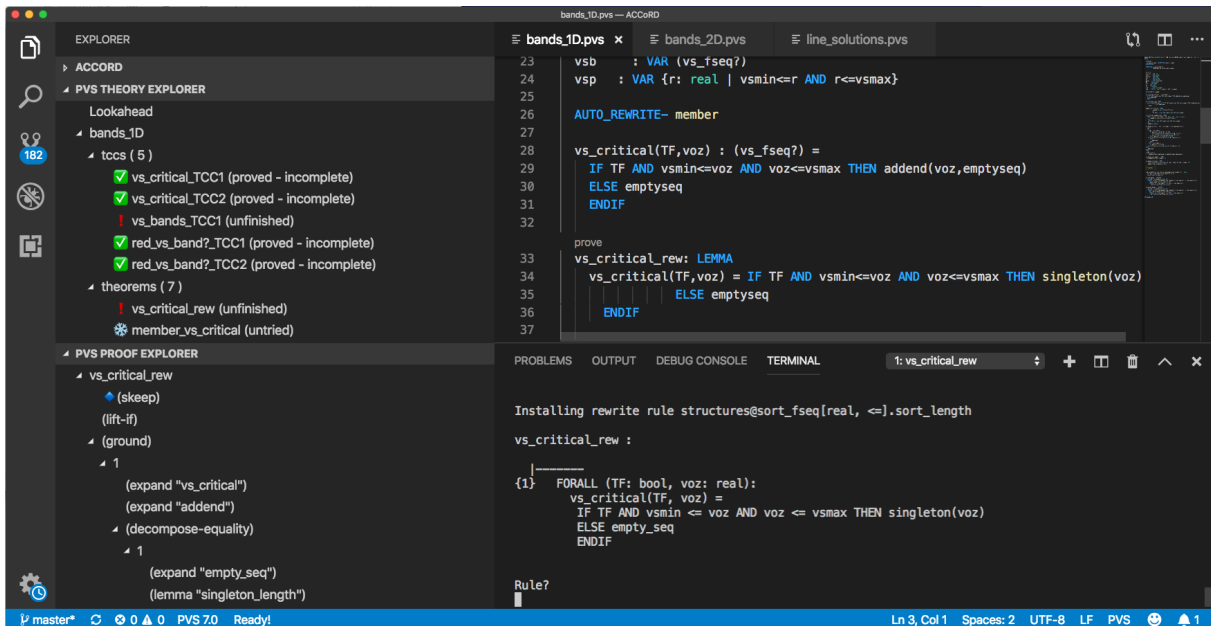


Figure 2.4: VSCode-PVS

2.2 PVS Environment

The PVS Environment (Figure 2.5) consists primarily of:

- **Specification Language:** a strongly typed specification language based on classical higher-order logic⁴. It is used to specify libraries of *theories*[22];
- **Parser:** The parser checks theories for syntactic consistency and builds an internal representation that is used by other components of the system[23];
- **Type Checker:** analyzes theories for semantic consistency and adds semantic information to the internal representation built by the parser[23];

³<https://visualstudio.microsoft.com>

⁴Functions can take functions as arguments and return them as values, and quantification can be applied to function variables

- **Theorem Prover:** The proof engine is based on Gentzen's sequent calculus [24], and supports the use of proof strategies for automated analysis. It is composed by a collection of basic inference rules and high-level proof strategies. Applied interactively within a sequent calculus framework. The proof engine yield proof scripts for manipulating and replaying proofs[25];
- **Specification Libraries:** allows files and theories from one context to be used in another, thus allowing for general reuse, and making it easier to standardize theories that are frequently used. There are two ways that the library facility can be used: by explicitly importing a theory from a different PVS context within a specification, or by issuing a command that effectively extends the prelude[23];
- **Various browsing tools:** allows displaying and navigation of cross reference definition and uses[23];

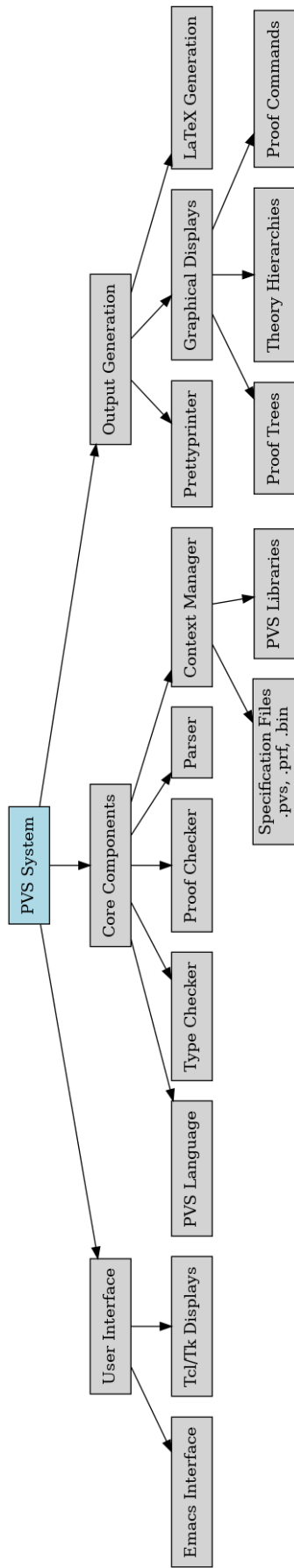


Figure 2.5: PVS System Overview

PVS is based on higher-order logic facilitates the specification of functions, predicates, and relations. For our case, this is specially useful, as the problem of infinitude of primes is a higher-order problem, as it is about a relation. PVS also supports the definition of recursive functions and inductive predicates. For a comprehensive and detailed explanation of PVS semantics, refer to the official documentation [26].

To ensure the correctness of recursive functions in PVS, it is crucial to prove their termination. A key aspect of this correctness is providing a termination proof for the function. This requires the user to define a measure over the function arguments that decreases with each recursive call, following a well-founded relation.

Once the measure is provided, PVS performs static analysis and generates proof obligations in the form of lemmas, which ensure the correctness of the argument types used in the function specification. These lemmas are known as Type Correctness Conditions (TCC).

While PVS attempts to discharge all lemmas automatically, any that remain unproved must be handled by the user.

Chapter 3

Fermat numbers

The second proof from the book (and our first proof) uses number theory [27]. More precisely it uses the infinitude of the Fermat numbers [28] to proof that the primes are infinite. The Fermat numbers are of the form:

$$F_n = 2^{2^n} + 1, \text{ where } n \in \mathbb{Z}_{\geq 0} \quad (3.1)$$

The main idea is to show that Fermat numbers are pairwise relatively prime. In other words, each Fermat number must have at least one distinct prime divisor. Since we can find infinitely many Fermat numbers, it follows that there must be infinitely many prime numbers.

Since the *NASALib* and the PVS' *prelude* libraries provide a strong set of theorems in number theory, this proof turned out to be one of the shortest.

3.1 Proof structure

The proof found in the book can be divided into the following steps.

1) Show that the product of Fermat numbers is of the form $F_n - 2$


$$\prod_{k=0}^{n-1} F_k = F_n - 2 \quad (3.2)$$

2) Use the product formula to prove that two non-equal Fermat numbers are relative primes

$$\gcd(F_i, F_j) = 1 \text{ where } i \neq j \quad (3.3)$$

3) Since the set of Fermat numbers is infinite, we can find an arbitrary number of distinct primes from the prime factorization of these Fermat numbers. Therefore, the set of primes is infinite.

3.2 Specification details

Lemma 3.2.1.  Let $n \in \mathbb{Z}_{>0}$, the product from 0 to $n - 1$ of the Fermat numbers has a closed form:

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

Proof. This formula can be proven via induction.

Case $n = 1$, we have

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3 \\ F_1 - 2 &= 2^{2^1} + 1 - 2 = 3 \\ \Rightarrow F_0 &= F_1 - 2 \end{aligned}$$


Case $n > 1$, by inductive hypothesis, we have

$$\begin{aligned} \prod_{k=0}^{n-1} F_k &= F_n - 2 \\ \Rightarrow \prod_{k=0}^n F_k &= \cdot F_n \cdot (F_n - 2) \\ &= (2^{2^n} + 1)(2^{2^n} + 1 - 2) = (2^{2^n})^2 - 1 \\ &= 2^{2^{n+1}} - 1 = 2^{2^{n+1}} + 1 - 2 \\ &= F_{n+1} - 2 \end{aligned}$$

□

As for the PVS specification, the PVS *ints* library already includes a recursive function for manipulating integer products. By importing this function, it generates trivial TCCs that PVS can solve automatically. Regarding algebraic manipulation, it's worth noting that it can be solved almost instantly using the "grind" command, which performs various tasks, such as attempting to rewrite arithmetic identities until it no longer finds a valid match.

The next Lemma can be proven trivially by analytical means, but still was needed for our PVS proof.

Lemma 3.2.2.  The n th Fermat number divides the Fermat numbers' product from 0 to k , where $k \geq n$.

$$F_n \mid \prod_{i=0}^k F_i$$

Proof. Notice that $k \geq n$ is equivalent of supposing there is exist $x \in \mathbb{Z}_{\geq 0}$, such that $k = n + x$, this new variable x will be chosen for the induction.

Case $x = 0$, we have

$$\prod_{i=0}^{n+0} F_i = F_n \cdot \prod_{i=0}^{n-1} F_i$$


which trivially satisfies our assumption

Case $x > 0$, we have by inductive hypothesis

$$\begin{aligned} F_n & \mid \prod_{i=0}^{n+x} F_i \\ \Rightarrow F_n & \mid \prod_{i=0}^{n+x} F_i \cdot F_{n+x+1} \\ \Rightarrow F_n & \mid \prod_{i=0}^{n+x+1} F_i \end{aligned}$$

□

With these Lemmas in hand, we can prove that Fermat numbers are indeed relative primes.

Lemma 3.2.3.  *Two different Fermat numbers are relative primes:*

$$\gcd(F_i, F_j) = 1 \text{ where } i \neq j$$

Proof. Since the \gcd operation is symmetric, the problem of proving for $i \neq j$ can be rephrased as proving for arbitrary i, j with $i < j$. Using the Euclid's algorithm:

$$\gcd(F_i, F_j) = \gcd(F_i, \text{mod}(F_j, F_i))$$

By the Lemma 3.2.2, F_i divides the product of Fermat numbers from 0 to $j - 1$, therefore

$$\prod_{k=0}^{j-1} F_k \equiv 0 \pmod{F_i}$$

Using the Lemma 3.2.1 this means

$$\prod_{k=0}^{j-1} F_k = F_j - 2 \equiv 0 \pmod{F_i}$$

$$F_j \equiv 2 \pmod{F_i}$$

Since a Fermat number is an odd number greater than one.

$$\text{mod}(F_j, F_i) = 2$$

$$\Rightarrow \text{gcd}(F_i, F_j) = \text{gcd}(F_i, 2) = 1$$

□

During the tool assisted proof, the particular property of a Fermat number being an odd number greater than one appeared in different TCCs and proofs, as a result, it was advantageous to add an explicit specification of this property [↗](#). It's also necessary for this proof to use the property of Euclid's algorithm, fortunately, this was in the same file as for the definition of gcd [↗](#).

To conclude the proof, we must prove that the set of primes is infinite. First, it's important to note that Fermat numbers are infinite by definition, as they are defined by a function that takes values from the infinite set of non negative integers. We can then use the infinitude of Fermat numbers to show that the set of primes is also infinite.

The link between Fermat numbers and prime numbers arises from the fact that every natural number greater than one has at least one prime divisor. This observation led to the definition of another function and set.

Definition 1 [↗](#) Let $n \in \mathbb{Z}_{\geq 0}$ and \mathbb{P} the set of prime numbers

$$f_{\text{prime}}(n) = \min(\{p \in \mathbb{P} : p \mid F_n\})$$

$$\mathbb{F}_{\text{prime}} = \{p \in \mathbb{P} : \exists n \in \mathbb{Z}_{\geq 0}, p = f_{\text{prime}}(n)\}$$

In the remaining of the document, the notation \mathbb{P} will be used for denoting the set of prime numbers.

By the well-ordering principle, the function f_{prime} is indeed well defined. The proof of infinitude can be finished by establishing an injection from the set $\mathbb{F}_{\text{prime}}$ to the set of prime numbers \mathbb{P} .

Theorem 3.2.4. [↗](#) *There are infinite primes*

Proof. By definition of $\mathbb{F}_{\text{prime}}$, this is the image of the function f_{prime} . Using Lemma 3.2.3, for any two $n, k \in \mathbb{Z}_{\geq 0}, n \neq k$, there is no common prime factor of F_n and F_k . In other words, $f_{\text{prime}}(n) \neq f_{\text{prime}}(k)$. Therefore, the function f_{prime} is an injection, mapping $\mathbb{Z}_{\geq 0} \rightarrow \mathbb{F}_{\text{prime}} \subseteq \mathbb{P}$, since the set $\mathbb{Z}_{\geq 0}$ is infinite, \mathbb{P} is also infinite.

□

For completion, the set theoretic properties, such as the transition of infinitude via injective mapping, can be found in [sets_aux](#) from *NASALib*. By importing this library, we have to specify the types of the set, PVS can transform a set into a type, which means that the sets \mathbb{F}_{prime} and \mathbb{P} were used as types for this particular proof. No further TCC has appeared because of the import of *sets_aux*, as these sets were defined on the well-behaved integer type.

Chapter 4

Mersenne numbers

The third proof uses another family of numbers from number theory, the Mersenne numbers[28]. These numbers are defined as

$$M_n = 2^n - 1 \tag{4.1}$$

and its function domain may vary depending on the author. Some authors use $n \in \mathbb{Z}_{\geq 0}$; others use $n \in \mathbb{P}$, which is the case of "Proofs from THE BOOK" and our case.

Nevertheless, the main idea of the proof is to consider the case where n equals a prime p , it turns out that there exists a prime divisor q of M_p , such that q is greater than p . If we assume that there are finite primes, there must exist a maximum prime p_{max} , as we can find a greater prime from the set of divisors of $M_{p_{max}}$, we have a contradiction.

For this proof, "Proofs from THE BOOK" uses a modern algebra approach, such as using Lagrange's Theorem [29] and the fact that $\mathbb{Z}_q \setminus \{0\}$ forms a group under multiplication. Because of that, we decided to import [NASALib's algebra library](#) [6], being more specific the theory [ring_zn.pvs](#), which includes a specification of a ring isomorphic to \mathbb{Z}_n .

4.1 Proof structure

The proof can be structured as follows:

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 as $2^p - 1$ is odd.

$$q \mid 2^p - 1, q \in \mathbb{P} \setminus \{2\} \tag{4.2}$$

2) Because q is odd, it must be relative prime to 2. By Fermat's Little Theorem:

$$2^{q-1} \equiv 1 \pmod{q} \tag{4.3}$$

3) Since q divides $2^p - 1$, this implies that $2^p \equiv 1 \pmod{q}$, since p is a prime number, it must be the order of the element 2 in $\mathbb{Z}_q \setminus \{0\}$.

$$\text{ord}(2) = p \tag{4.4}$$


4) Since an element $a \in \mathbb{Z}_q \setminus \{0\}$ of order n generates a subgroup $\langle a \rangle = \{a^i : i \in \mathbb{Z}_{\geq 0}\}$ with $|\langle a \rangle| = n$. In particular, by applying Lagrange's Theorem, $|\langle 2 \rangle| = p$ divides $|\mathbb{Z}_q \setminus \{0\}| = q - 1$, then:

$$p \mid q - 1 \tag{4.5}$$

5) Assume there exists a maximum prime p_{max} , then there exists $q \in \mathbb{P}$ such that $p_{max} \mid q - 1$, as a divisor is smaller than or equal the number it divides, $p_{max} \leq q - 1$, or $p_{max} < q$, a contradiction. Therefore, there exist infinite primes.

4.2 Specification details

To apply group-related theorems, we decided to use the algebra library from *NASALib*. First, we must decide how to define the multiplicative group $\mathbb{Z}_p \setminus \{0\}$.

While there is an implementation for the ring $\mathbb{Z}/n\mathbb{Z}$, there exist no direct implementation for the multiplicative group $\mathbb{Z}/n\mathbb{Z} \setminus \{n\mathbb{Z}\}$. Unfortunately, for the group-related theorems we need to use, the theories we must import rely on a postponed assumption. Specifically, the type we apply the theory to must satisfy a finite group predicate. In other words, when we import these theories, they introduce a TCC that checks whether the type consists of a complete set of elements forming a finite group. Essentially, we need to demonstrate that the set of all elements of a given type forms a group. This means that we cannot simply use the fact that $\mathbb{Z}/n\mathbb{Z}$ is a field, and thus, that $\mathbb{Z}/p\mathbb{Z} \setminus \{p\mathbb{Z}\}$ forms a group under multiplication. Instead, we must define the type for this multiplicative group first and then prove that it satisfies the group properties, which leads to the definition of a specific type for $\mathbb{Z}/p\mathbb{Z} \setminus \{p\mathbb{Z}\}$, named `nz_coset(p)` .

After its specification, it was necessary to prove that `nz_coset(p)`, for a given $p \in \mathbb{P}$, is really a finite group. Fortunately, it could be done by expanding the definition enough times and using the field property of $\mathbb{Z}/p\mathbb{Z}$, which was already in PVS. 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's 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, we can 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 power function was specialized and instead of using $pow : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}/p\mathbb{Z}$ for its function signature, it was used $pow : \mathbb{Z}/p\mathbb{Z} \setminus \{p\mathbb{Z}\} \times \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}/p\mathbb{Z} \setminus \{p\mathbb{Z}\}$ [↗](#).

With these preliminaries explained, we can discuss the proof of the infinitude of prime numbers.

Lemma 4.2.1. [↗](#) *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 , we have

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

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 4.2.2. [↗](#) *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 4.2.1, q is an odd number since q is a prime $q \geq 3$; in particular, this means that $q \nmid 2$. By Fermat's Little Theorem

$$2^{q-1} \equiv 1 \pmod{q}$$

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

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

During 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 our 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 4.2.3.  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 , we have

$$M_p \equiv 0 \pmod{q}$$

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

$$2^p \equiv 1 \pmod{q}$$

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

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

□

Theorem 4.2.4.  There are infinite primes

Proof. Suppose there exist finite primes, then there exists a maximum prime p_{max} . Let $q \in \mathbb{P}$ be the divisor of $M_{p_{max}}$, using Lemma 4.2.3, we have

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

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 $2 + q\mathbb{Z} = 1 + q\mathbb{Z}$, impossible, since $q > 1$. Therefore $ord(2 + q\mathbb{Z}) = p_{max}$.

Using Lemma 4.2.2

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

Again by definition of order

$$ord(2 + q\mathbb{Z}) \mid q - 1$$

$$p_{max} \mid q - 1$$

Since a divisor is smaller or equal to the number it divides, we have $p_{max} \leq q - 1$, 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, we used the classical theorem that states if an element a from a group G satisfies $a^n = 1$ for some integer n , then the order of a , denoted $ord(a)$, divides n . This theorem was not in the *NASALib*'s algebra library, as such, 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, PVS strategies (essentially LISP code for automating proofs), and possibly PVS 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 made our proof easier.

Chapter 5

Euler product formula

The fourth proof in the book relies on analytic number theory[30]. As a side effect of the Euler's Formula[31], proved in the 18th century by Leonhard Euler, this proof has a deep connection to the Riemann zeta function [32]. The key idea is to demonstrate that the zeta function can be factored into a product over primes. With this connection, we can estimate the number of primes as large as we wish, 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:

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

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, we can estimate the prime-counting function by the product of the primes according to the Euler formula, which by itself can be estimated by the natural logarithm function in the following way:

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

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 analytical number theory proofs, this chapter proof heavily relies on concepts from analysis, such as limits and series; for that reason, we decided to import the [NASALib's analysis library](#) [7].

5.1 Proof structure

The structure of the proof given by the book can be divided into the following parts.

1) Let $\pi(x)$ be the prime-counting function, suppose we have an enumeration of prime numbers in increasing order in \mathbb{P} .

2) The harmonic numbers can be estimated with natural logarithm.

$$\log(n) \leq H_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} \quad (5.1)$$

3) The product of geometric series of inverse prime numbers less than or equal to n is equal to another series which contains every $\frac{1}{k}$ from $H_n = 1 + \frac{1}{2} + \dots + \frac{1}{n}$.

$$H_n \leq \prod_{i=1}^{\pi(n)} \sum_{k=0}^{\infty} \frac{1}{p_i^k} = \sum_{\substack{k \in \mathbb{Z}_{>0}, \\ k=1 \vee \exists p \in \mathbb{P}, \\ (p \leq n \wedge p|k)}} \frac{1}{k} \quad (5.2)$$

4) Since the geometric series has closed form and as $p_i \geq i + 1$ (which implies that $\frac{p_i}{p_i-1} \leq \frac{i+1}{i}$), we can estimate the product of series through the following inequality:

$$\prod_{i=1}^{\pi(n)} \sum_{k=0}^{\infty} \frac{1}{p_i^k} = \prod_{i=1}^{\pi(n)} \frac{p_i}{p_i-1} \leq \prod_{i=1}^{\pi(n)} \frac{i+1}{i} = \pi(n) + 1 \quad (5.3)$$

5) By arranging inequalities, we find that the prime-counting function is greater than or equal to the natural logarithm; the latter being a strictly increasing function means that the π function is unbound, in other words, the prime-counting is infinite.

$$\log(n) \leq \pi(n) + 1 \quad (5.4)$$

5.2 Specification details

5.2.1 Prime enumeration

The definition given by the book has the problem of assuming when using the notation " $\mathbb{P} = \{p_1, p_2, p_3, \dots\}$ ", that the prime numbers \mathbb{P} are infinite beforehand, and the sequence

should be undefined otherwise. For simplicity, during the PVS specification, we decided to set the undefined cases to the number zero, meaning that if the prime numbers have an end at the n th value, then $p_i = 0$ for $i > n$. Another thing to consider is that as the natural numbers in PVS start from zero, the specification has a starting index of zero, meaning that the first three values are:


$$p_0 = 2 \quad p_1 = 3 \quad p_2 = 5$$

The proper definition of prime sequence is given by the following function ρ .


Definition 2  Let $\rho : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$

$$\rho(i) = \begin{cases} 2 & \text{if } i = 0 \\ \min(\{p \in \mathbb{P} : p > \rho(i-1)\}) & \text{if } i > 0 \wedge \exists p \in \mathbb{P}, p > \rho(i-1) \\ 0 & \text{if } i > 0 \wedge \nexists p \in \mathbb{P}, p > \rho(i-1) \\ 0 & \text{if } \rho(i-1) = 0 \end{cases}$$


Given this definition, it remains to prove that, indeed, for a subset of the domain $S \subseteq \mathbb{Z}_{\geq 0}$, this function is an enumeration. For this purpose, we will need to demonstrate some properties of ρ first.

Corollary 5.2.0.1.  $\rho(i+1) > \rho(i) \vee \rho(i+1) = 0$

Proof. From the definition of the function ρ , it only returns a prime or 0. Case $\rho(i) = 0$, by the last case of the definition $\rho(i+1) = 0$. Case $\rho(i) \in \mathbb{P}$, if $\rho(i+1) = 0$ then is trivially true, otherwise, by the second case of the definition $\rho(i+1) > \rho(i)$. □

Lemma 5.2.1.  $\forall \rho(i), \rho(j) \in \mathbb{P}, \rho(i) = \rho(j) \Rightarrow i = j$

Proof. When $i = j$, this is trivial. Since the proposition is symmetric, without loss of generality, we can choose $i < j$. Notice that if there existed a number k , such that $i \leq k \leq j, \rho(k) = 0$, by the fourth case of the ρ definition, we could prove via recursion that $\rho(j) = 0$, this can not be the case, because $\rho(j) \in \mathbb{P}$. Using the Corollary 5.2.0.1, as there is no intermediary value $\rho(k) = 0$, in this domain, this function is strictly increasing. Therefore, $\rho(i) < \rho(j)$. □

Lemma 5.2.2.  $\forall p \in \mathbb{P}, \exists i \in \mathbb{Z}_{\geq 0}, \rho(i) = p$

Proof. Proving this statement is equivalent of showing that for every $n \in \mathbb{Z}_{\geq 0}$, every element q of the set $\mathbb{P}_n = \{p \in \mathbb{P} : p \leq n\}$ can be written as $\rho(i) = q$, for some $i \in \mathbb{Z}_{\geq 0}$. This can be done by recursion on the variable n .


For the case $n \leq 1$, $P_n = \emptyset$.

For the case $n = 2$, we have $P_2 = \{2\}$, its only element can be written as $\rho(0) = 2$.

If all elements of P_n can be written as $\rho(i)$, considering $\rho(j) = \max(P_n)$.

Case $n + 1$ is prime, then it is the minimum prime greater than $\rho(j)$; otherwise, there would exist a prime $r < n + 1$ such that $\max(P_n) < r$, an absurd. In other words, $\rho(j + 1) = n + 1$.

Case $n + 1$ is not a prime, then $P_{n+1} = P_n$, trivially satisfying the recursion. □

Lemma 5.2.3.  Let $i, n \in \mathbb{Z}_{\geq 0}$, $i < \pi(n) \Rightarrow \rho(i) \in \mathbb{P}$

Proof. As proved during the Lemma 5.2.2, all values \mathbb{P}_n can be written by some $\rho(i)$, and using Lemma 5.2.0.1, this enumeration is strictly increasing while $\rho(i)$ is a prime, which is the case as all elements of \mathbb{P}_n are primes. In particular, that means that $\rho(0), \rho(1), \dots, \rho(\pi(n) - 1)$ is an enumeration in ascending order of prime numbers. □

With those properties proved, the ρ function is indeed an enumeration for a subset of the domain. In particular, if there are infinite 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 set $\mathbb{Z}_{\geq 0} \setminus S$ the function will be identically zero, as we expected.

In the following proofs, it will be necessary to use the Fundamental Theorem of Arithmetic [5]. This theorem is in *NASALib*, but it was specified in a more generic sense, which made a new specification necessary.

The *NASALib*'s original specification of Fundamental Theorem of Arithmetic describes that any positive natural number greater than one can be written as a product of a prime sequence, for example,

$$360 = 2 \cdot 3 \cdot 2 \cdot 5 \cdot 2 \cdot 3$$


But for our purpose, it is convenient to use this Theorem in the form of sorted powers of primes, i.e.

$$360 = 2^3 \cdot 3^2 \cdot 5$$



Because we already define a prime enumeration, we can use it to specify the prime powers in sorted form, but if you pay attention, by knowing beforehand that there are infinite 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

$$360 = \rho(0)^3 \cdot \rho(1)^2 \cdot \rho(2)^1 \cdot \rho(3)^0 \cdot \rho(4)^0 \dots$$

But we would be making the same mistake of assuming that there are infinite primes in a circular way. Because of that, we chose to change the description of the Fundamental Theorem.

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

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

The Fundamental Theorem can be rewritten as the existence of a unique element $(\rho(0)^{\epsilon_0}, \rho(1)^{\epsilon_1}, \dots, \rho(\pi(n)-1)^{\epsilon_{\pi(n)-1}}) \in D_n$, such that 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's worth mentioning that the definition of prime enumeration and prime factorization is going to be reused for the last proof of infinitude of primes, because of that, these proofs, alongside other general purpose ρ function manipulation, were separated to a new file called [prime_extra.pvs](#).

Using this new framework for the proof of the Fundamental Theorem of Arithmetic, the application of lemmas related to integer numbers was useful. Among these lemmas, some properties related to the *gcd* function were not available in the *NASALib*. For that reason another file was created [number_util.pvs](#)

5.2.2 A few inequalities

For the completion of our proof we must demonstrate a few inequalities, starting from a classic one.

Lemma 5.2.4.  $\forall n \in \mathbb{Z}_{\geq 0}, \log(n) \leq H_n$

Proof. This can be done by considering the inequality

$$\frac{1}{x} \leq \frac{1}{k} \quad \text{for } x \in [k, k + 1]$$

Considering the inequalities of integral, for a finite summation

$$\begin{aligned} \log(n + 1) &= \int_1^{n+1} \frac{1}{x} dx = \sum_{k=1}^n \int_k^{k+1} \frac{1}{x} dx \leq \sum_{k=1}^n \int_k^{k+1} \frac{1}{k} dx \\ &\Rightarrow \log(n + 1) \leq \sum_{k=1}^n \frac{1}{k} = H_n \end{aligned}$$

Since the log function is an increasing function.

$$\log(n) \leq \log(n + 1) \leq H_n$$

□

This inequality, despite being well known, was not explicitly enunciated in the *NASALib*, but all its prerequisites were already proven in the *NASALib*'s analysis theory. This makes 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 we sum over slices of the bigger integral, it was necessary to guarantee that everything is indeed integrable. But lemmas for these steps were also in the files defining the logarithmic function and integral operations.

For the next inequality, we need to define two functions.

Definition 3  Let $n \in \mathbb{Z}_{\geq 0}, n \geq 2$

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

One thing to notice is that in the ξ definition, we are dividing by $\rho(i)$, which can have zero value if we try to use a nonexistent prime number, but as we are taking the product from $i = 0$ to $i = \pi(n) - 1$, using Lemma 5.2.3 all $\rho(i)$ values are primes, i.e., non zero numbers.

It is not completely obvious from the definition, but these two functions are the same. For proving this statement some non-trivial lemmas must be proven first.

Given the Cauchy product [33], we can express the product of two convergent series a and b as another series.


$$\left(\sum_{n=0}^{\infty} a_n \right) \cdot \left(\sum_{n=0}^{\infty} b_n \right) = \sum_{n=0}^{\infty} \sum_{k=0}^n a_{n-k} b_k \quad (5.5)$$

That formula has the restriction of one of the series being absolutely convergent, but in our case, the series is defined over positive numbers, making this restriction trivially valid. The last series in the formula can be flattened in such a way it maintains its convergence, but to prove this, first, we need to define another function.

Definition 4  Let $n \in \mathbb{Z}_{\geq 0}$

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

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

Corollary 5.2.4.1.  Let $n, k \in \mathbb{Z}_{\geq 0}, 0 \leq k \leq n$, then $\theta\left(\frac{n(n+1)}{2} + k\right) = n$ and $\tau\left(\frac{n(n+1)}{2} + k\right)$

Proof. Since $0 \leq k$, we have

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


Since $k \leq n$, we have

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

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

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

□

Lemma 5.2.5.  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 Corollary 5.2.4.1, we have that $\theta(\frac{n(n+1)}{2} + k) = n$ and $\tau(\frac{n(n+1)}{2} + k) = k$, therefore, by change of basis.

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

□

Lemma 5.2.6.  Let $N \in \mathbb{Z}_{\geq 0}$

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

Proof. This can be proven through induction on the variable N .

Case $N = 0$, by Corollary 5.2.4.1, we have $\theta(0) = 0$ and $\tau(0) = 0$, therefore

$$a_0 b_0 = a_{(\theta(0)-\tau(0))} \cdot b_{\tau(0)}$$

Case $N > 0$, by inductive hypothesis

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


By Lemma 5.2.5

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

The last equality comes from the fact that $\frac{(N+1)(N+2)}{2} = \left(\frac{N(N+1)}{2} + N + 1\right)$

□

For the next Theorem, we need to prove one more Lemma.

Lemma 5.2.7.  For every $n \in \mathbb{Z}_{\geq 0}$, there exists $m, r \in \mathbb{Z}_{\geq 0}$, where $0 \leq r \leq m$, such that $n = \frac{m \cdot (m+1)}{2} + r$

Proof. This can be done with induction on variable n .

Case $n = 0$, $m = r = 0$ satisfy our hypothesis.

Case $n > 0$, by inductive hypothesis.

$$n = \frac{m \cdot (m+1)}{2} + r$$

If $r = m$, this implies

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

If $r < m$, this implies

$$n+1 = \frac{m \cdot (m+1)}{2} + (r+1)$$

Since $r < m$ and both r, m are integers $r+1 \leq m$.

□

Now we can prove that the flattened version of the series is indeed equal to the original series in our case.

Theorem 5.2.8. Let a_n and b_n be positive sequences and let $\sum_{n=0}^{\infty} \sum_{k=0}^n a_{n-k} b_k$ be convergent, then

$$\sum_{n=0}^{\infty} \sum_{k=0}^n a_{n-k} b_k = \sum_{n=0}^{\infty} a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)}$$

Proof. Letting $L = \sum_{n=0}^{\infty} \sum_{k=0}^n a_{n-k} b_k$, for every real $\epsilon > 0$, for larger enough $n \geq N$, we want

$$\left| L - \sum_{k=0}^n a_{(\theta(k)-\tau(k))} \cdot b_{\tau(k)} \right| < \epsilon$$

Using Lemma 5.2.7, rewrite n as $n = \frac{m \cdot (m+1)}{2} + r$, where $0 \leq r \leq m$, we can estimate our difference as

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

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

By Corollary 5.2.4.1

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

By Lemma 5.2.6

$$\leq \left| L - \sum_{n=0}^m \sum_{k=0}^n a_{n-k} b_k \right| + \left| \sum_{k=r+1}^m a_{m-k} b_k \right|$$

Since both a_n and b_n sequences are positive.

$$\begin{aligned}
&\leq \left| L - \sum_{n=0}^m \sum_{k=0}^n a_{n-k} b_k \right| + \sum_{k=r+1}^m a_{m-k} b_k \\
&\leq \left| L - \sum_{n=0}^m \sum_{k=0}^n a_{n-k} b_k \right| + \sum_{k=0}^m a_{m-k} b_k
\end{aligned}$$

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

$$\begin{aligned}
\left| L - \sum_{n=0}^m \sum_{k=0}^n a_{n-k} b_k \right| &< \frac{\epsilon}{2} \\
\sum_{k=0}^m a_{m-k} b_k &< \frac{\epsilon}{2}
\end{aligned}$$

Therefore, for $N = \max(N_1, N_2)$

$$\left| L - \sum_{k=0}^n a_{(\theta(k) - \tau(k))} \cdot b_{\tau(k)} \right| < \epsilon$$

□

With that in mind, during the PVS specification, there was no previous specification of the Cauchy product. Being a well-known theorem and due to its specification being very time-consuming, we chose to use the theorem as an axiom in PVS.

That series flattening process  can be generalized for the product of more series.

Lemma 5.2.9.  Let $n \in \mathbb{Z}_{>0}$, then

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

Proof. That can be done through induction on the variable n . For case $n = 1$, this trivially says that

$$\sum_{k=0}^{\infty} a_0(k) = \sum_{k=0}^{\infty} a_0(k)$$

For case $n > 1$, using the inductive hypothesis.

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

By Cauchy product (Formula 5.5).

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

Finally, using the flattening process of Theorem 5.2.8.

$$= \sum_{\substack{k, j_l \in \mathbb{Z}_{\geq 0} \\ j_0 + j_1 + \dots + j_n = k}} \prod_{i=0}^n a_i(j_i)$$

□

A more step-by-step proof of this theorem was given in the PVS specification. We can finally show that, indeed, the functions ξ and μ are equal.

Theorem 5.2.10. $\xi(n) = \mu(n)$

Proof. Using Lemma 5.2.9, we have

$$\prod_{i=0}^{\pi(n)-1} \sum_{k=0}^{\infty} \frac{1}{\rho(i)^k} = \sum_{\substack{k, j_i \in \mathbb{Z}_{\geq 0} \\ j_1 + j_2 + \dots + j_{(\pi(n)-1)} = k}} \prod_{i=0}^{\pi(n)-1} \frac{1}{\rho(i)^{j_i}}$$

Notice that every term of the right series is of the form

$$\frac{1}{\rho(0)^{\epsilon_1}} \cdot \frac{1}{\rho(1)^{\epsilon_2}} \cdots \frac{1}{\rho(m)^{\epsilon_m}}, \quad m = \pi(n) - 1$$

By the Fundamental Theorem of Arithmetic, this product results in a unique number $\frac{1}{n}$. In particular, $\frac{1}{1}$ appears in the right series ($\epsilon_i = 0$) and since we are summing over all possibilities of exponents, every $\frac{1}{n}$, for a n that's divisible by some $p \in \mathbb{P}, p \leq n$ is in the summation. As a result

$$\sum_{\substack{k, j_i \in \mathbb{Z}_{\geq 0} \\ j_1 + j_2 + \dots + j_{(\pi(n)-1)} = k}} \prod_{i=0}^{\pi(n)-1} \frac{1}{\rho(i)^{j_i}} = \sum_{\substack{k \in \mathbb{Z}_{>0}, \\ k=1 \vee \exists p \in \mathbb{P}, \\ (p \leq n \wedge p|k)}} \frac{1}{k}$$

□

In PVS, it was not necessary to prove directly this property, it was faster to use Lemma 5.2.9 and associate it each factor of the sum in the next proof. But for completion, we chose to write the analytic proof for this Theorem.

Lemma 5.2.11.  Let $n \in \mathbb{Z}_{>0}$, $H_n \leq \mu(n)$

Proof. Notice from the definition of μ function.

$$\mu(n) = \sum_{\substack{k \in \mathbb{Z}_{>0}, \\ k=1 \vee \exists p \in \mathbb{P}, \\ (p \leq n \wedge p|k)}} \frac{1}{k}$$

If for every $\frac{1}{k}$, $1 < k \leq n$, there exists a prime $p | k$, $p \leq n$, since $\mu(n)$ is an absolutely convergent series, we can order the series such that.

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

Which trivially results in $H_n \leq \mu(n)$.

Since $1 < k \leq n$ and since a divisor is less than or equal to the number it divides, all of k 's prime divisors have the inequality $p \leq k$, therefore, the max prime divisor k can get is $p \leq n$.

□

During the PVS specification, this series rearrange needed to be expressed in a more explicit form; for that reason, we created a file called [sequence_extra.pvs](#), in which we have a more formal description of the function which orders by common summed values.

Lemma 5.2.12.  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

$$\begin{aligned} & \frac{\rho(i)}{\rho(i) - 1} \leq \frac{i + 2}{i + 1} \\ \iff & 1 + \frac{1}{\rho(i) - 1} \leq 1 + \frac{1}{i + 1} \\ \iff & i + 1 \leq \rho(i) - 1 \\ \iff & i + 2 \leq \rho(i) \end{aligned}$$

This can be proven through induction. For case $i = 0$, we have

$$0 + 2 \leq 2$$

For case $i > 0$, by inductive hypothesis

$$\begin{aligned} & i + 1 \leq \rho(i - 1) \\ \Rightarrow & i + 2 \leq \rho(i - 1) + 1 \end{aligned}$$

Because of Lemma 5.2.3 $\rho(i) \neq 0$, using Lemma 5.2.0.1, we have $\rho(i - 1) < \rho(i)$, since $\rho(i - 1)$ is a integer, $\rho(i - 1) + 1 \leq \rho(i)$, therefore

$$i + 2 \leq \rho(i)$$

□


Lemma 5.2.13.  $\xi(n) \leq \pi(n) + 1$

Proof. Since the geometric series has a closed form, we can simplify $\xi(n)$

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

Using Lemma 5.2.12, we have the inequality

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

Notice that the product $\prod_{i=0}^{\pi(n)-1} \frac{i+2}{i+1}$ is a telescoping product , therefore we have

$$\prod_{i=0}^{\pi(n)-1} \frac{i + 2}{i + 1} = \frac{(\pi(n) - 1) + 2}{0 + 1} = \pi(n) + 1$$

□

Theorem 5.2.14.  *There are infinite primes*

Proof. Composing the inequalities from Lemmas 5.2.4, 5.2.10, 5.2.13 and 5.2.11, we have

$$\log(n) \leq \xi(n) = \mu(n) \leq \pi(n) + 1$$

Because the logarithm is a strictly increasing function, there can't be a maximum $\pi(n)$ value.

□

We are done with the proof, but if you look closely, this proof also gives an estimation of how large the prime-counting function increases. Still, that is not the best approximation, theorems such as Prime number theorem [34] estimate $\pi(x) \sim \frac{x}{\log(x)}$, which is an estimation that grows faster than $\log(x)$.

Chapter 6

Fürstenberg's topological proof

The Fürstenberg proof of the infinitude of primes is an elegant and non-traditional approach to proving that there are infinitely many prime numbers. Hillel Fürstenberg introduced this proof in 1955 [35], and it uses concepts from topology [36].

The main idea is to use a family of integer sets, $N_{a,b} = \{a + bn : n \in \mathbb{Z}\}$, where $b > 0$, to define a topology on \mathbb{Z} . From this family of sets, one should expect to reconstruct almost all of \mathbb{Z} set through a union of prime family, to be more precise. $\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}$. It turns out that by this topology properties, this construction forces the prime set to be infinite.

Since we are dealing with topological definitions, we chose to import the [NASALib's topology library](#) [8].

6.1 Proof structure

The structure of the proof given by the book can be divided into the following parts.

- 1) Given $a, b \in \mathbb{Z}$, where $b > 0$, define the set family $N_{a,b} = \{a + bn : n \in \mathbb{Z}, b > 0\}$.
- 2) An open set will a set $O \subseteq \mathbb{Z}$, if either $O = \emptyset$ or if for every element $a \in O$, there exists some $b \in \mathbb{Z}, b > 0$ with $N_{a,b} \subseteq O$. Also a closed set is defined as a complement of open set, as usual in topology.
- 3) Notice that by this definition of open set, the union of two open sets O_1, O_2 is another open set.
- 4) We can also prove that the intersection of two open sets is another open set. This can be verified by letting $a \in O_1 \cap O_2$, we have that $N_{a,b_1} \subseteq O_1$ and $N_{a,b_2} \subseteq O_2$ then

$a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Therefore, this definition of open set indeed forms a topology.

5) By the definition of an open set O , there exists $N_{a,b} \subseteq O$, where $N_{a,b}$ is an infinite set. Therefore, any non-empty open set is infinite.

6) The set $N_{a,b}$ can be rewritten as the complement of the finite union of others $N_{c,d}$ sets, in other words, it is a closed set.

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b} \quad (6.1)$$


7) Since every number $n \neq 1, -1$ has a prime divisor p , implies that n is contained in $N_{0,p}$. Meaning that we can recover the set $\mathbb{Z} \setminus \{-1, 1\}$ through union of $N_{0,p}$ sets.

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p} \quad (6.2)$$


8) From topology theory, a finite union of closed sets is also closed, as such, $\mathbb{Z} \setminus \{-1, 1\}$ is closed, which implies that the set $\{-1, 1\}$ is open, which is a contradiction since all open sets in this topology are infinite.

6.2 Specification details

This proofs give us a definition of open and close sets, we first need to check if the check if a finite union/intersection of open sets is also an open set.

Lemma 6.2.1.  *The union of two open sets is an open set*


Proof. Given open sets A, B , if any of them is an empty set, this is trivially true because the union equals the remaining set, otherwise, for every element $a \in A \cup B$, implies $a \in N_{a,b} \subseteq A$ or $a \in N_{a,c} \subseteq B$, for both cases, there exists $d > 0$, with $a \in N_{a,d} \subseteq A \cup B$. \square

Corollary 6.2.1.1.  *The union of finite open sets is an open set*

Proof. This can be proved by induction, for the base case we have an open set O_1 which is trivially an open set. By inductive hypothesis, the union of n open sets $\bigcup_{i=1}^n O_i$ is open, using Lemma 6.2.1, if O_{n+1} is an open set than

$$O_{n+1} \cup \bigcup_{i=1}^n O_i = \bigcup_{i=1}^{n+1} O_i$$

is also an open set. \square


Lemma 6.2.2.  *The intersection of two open sets is an open set*

Proof. If any of the open sets is an empty set, the intersection is also an empty set, which is open. Otherwise, for every element $a \in O_1 \cap O_2$, where O_1, O_2 are open sets, there exists N_{a,b_1} and N_{a,b_2} , such that $a \in N_{a,b_1} \subseteq O_1$ and $a \in N_{a,b_2} \subseteq O_2$.

For every element $c \in N_{a,b_1 \cdot b_2}$, we have for some $n \in \mathbb{Z}$

$$c = a + b_1 \cdot b_2 \cdot n$$


Therefore $c \in N_{a,b_1} \subseteq O_1$ and $c \in N_{a,b_2} \subseteq O_2$, in other words, $N_{a,b_1 \cdot b_2} \subseteq O_1 \cap O_2$. Also notice that $a = a + b_1 \cdot b_2 \cdot 0 \in N_{a,b_1 \cdot b_2}$. Therefore for every element $a \in O_1 \cap O_2$, there exists $a \in N_{a,b_1 \cdot b_2} \subseteq O_1 \cap O_2$, which means that $O_1 \cap O_2$ is open. □

Corollary 6.2.2.1.  *The intersection of finite open sets is an open set*


Proof. Once again, this can also be proved by induction, for the base case we have an open set O_1 which is trivially an open set. By inductive hypothesis, the intersection of n open sets $\bigcap_{i=1}^n O_i$ is open, using Lemma 6.2.1, if O_{n+1} is an open set then

$$O_{n+1} \cap \bigcap_{i=1}^n O_i = \bigcap_{i=1}^{n+1} O_i$$

is also an open set. □

With that Lemmas, we can properly use the *NASALib*'s topology theory, as the families of open sets O fulfil the criterion for being a topology .


We can also prove three more properties:

Lemma 6.2.3.  *Any non-empty open set is infinite*

Proof. Let O be the open set, for every element of $a \in O$, we have $N_{a,b} \subseteq O$, where $b > 0$. The elements of $N_{a,b}$ is a both sides linear progression $a + b \cdot n$, since $b > 0$, the function $f : \mathbb{Z} \rightarrow N_{a,b}$, such that

$$f(x) = a + b \cdot x$$

is an increasing function, as a result f is an injective function, since \mathbb{Z} is infinite, that implies that $N_{a,b}$ is also infinite and thus O is also infinite. □

Lemma 6.2.4.  *$N_{a,b}$ is a closed set and can be expressed as $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$*

Proof. Every element of $N_{a,b}$, is of the form $n = a + b \cdot k$, meaning that $n \equiv a \pmod{b}$ and vice-versa.

That means that every value n , such that $n \notin N_{a,b}$, must be in one of the $b-1$ remaining equivalent classes. In particular, let $0 \leq i < j < b$, suppose that $a + j \equiv a + i \pmod{b}$, this implies that

$$\begin{aligned} j - i &\equiv 0 \pmod{b} \\ \Rightarrow b \mid (j - i) &\Rightarrow b \leq j - i \end{aligned}$$

But the maximum difference is when

$$\begin{aligned} \max(j) - \min(i) &= (b - 1) - 0 = b - 1 \\ \Rightarrow b &> j - i \end{aligned}$$

thus we have a contradiction. Therefore, any two $N_{a+i,b}$, $N_{a+j,b}$, where $i \neq j$ is a different set.

That means the union

$$\bigcup_{i=1}^{b-1} N_{a+i,b}$$

contains every element $n \notin N_{a,b}$, as a result, $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$. By the definition of an open set, $N_{a+i,b}$ is an open set, since the union of open sets is open (Corollary 6.2.1.1), remember that a closed set is the complement of an open set, therefore $N_{a,b}$ is also a closed set.

□

With this last Lemma, we have that $N_{a,b}$ is a closed set. We need one more Lemma for building our main Theorem.

Lemma 6.2.5.  $\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}$

Proof. For every element m of $\mathbb{Z} \setminus \{-1, 1\}$, there exists a prime divisor q , therefore

$$m = q \cdot k, \quad k \in \mathbb{Z}$$

which is the form of an element of $N_{0,q}$, therefore $\mathbb{Z} \setminus \{-1, 1\} \subseteq N_{0,q} \subseteq \bigcup_{p \in \mathbb{P}} N_{0,p}$. For $n \in \bigcup_{p \in \mathbb{P}} N_{0,p}$, there exists a prime p such that


$$n = p \cdot k, \quad k \in \mathbb{Z}$$

Since n is an integer, we just need to ensure that $n \neq 1$ and $n \neq -1$. Notice that

$$|n| = |p| \cdot |k| = p \cdot |k|$$

Since p is a prime, $p > 1$. If $k = 0$ then $n = 0$, otherwise $|k| \geq 1$, which implies that $|n| > 1$. As a result, n is neither 1 nor -1. Therefore $\bigcup_{p \in \mathbb{P}} N_{0,p} \subseteq \mathbb{Z} \setminus \{-1, 1\}$.

□

Theorem 6.2.6.  *There are infinite primes*

Proof. By Lemmas 6.2.4 and 6.2.5, we have that $\mathbb{Z} \setminus \{-1, 1\}$ is a union of closed sets, since a finite union of closed sets is also a closed set, if the prime set is finite, $\mathbb{Z} \setminus \{-1, 1\}$ must be closed, which means that $\{-1, 1\}$ is an open set, a contradiction considering Lemma 6.2.3.

□

Chapter 7

Prime reciprocal series

The sixth and last proof was originally proved by Paul Erdős in the 20th century [37] and can be viewed as inspired by the fourth proof found in Chapter 5. 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., $\sum_{i=1}^{\infty} \frac{1}{p_i}$.

As a finite summation of numbers converges, if this series diverges, our set of primes must be infinite.

To show that this series diverges, we can divide the prime numbers into two types: the *Small* primes (primes which are smaller or equal to a prime p_k) and *Big* primes (the remaining primes). Using this classification, other sets can be 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* primes divisors; $N_b(n, k)$ the numbers from $N(n)$ with at least one *Big* prime divisor. It can be shown that $N(n) = N_s(n, k) \cup N_b(n, k)$.

The proof focuses on showing that if the series converges, we can find a k , such that we can estimate the size of $N_s(n, k)$, $N_b(n, k)$ such that $|N_s(n, k)| + |N_b(n, k)| < |N(n)|$, a contradiction.

7.1 Proof structure

1) Consider a prime enumeration p_i , suppose that the series of primes reciprocals converge.

$$\lim_{N \rightarrow \infty} \sum_{i=1}^N \frac{1}{p_i} < \infty \quad (7.1)$$

2) Therefore exists a κ such that the series starting from $\kappa + 1$ is less than one half.

$$\sum_{i=\kappa+1}^{\infty} \frac{1}{p_i} < \frac{1}{2} \quad (7.2)$$

3) Defining *Small* primes as all primes which are smaller than p_k and *Big* primes, the rest. Then define $N(n)$, $N_s(n, k)$ and $N_b(n, k)$ as previously mentioned.

4) By defining the subset $N_{div}(d, n)$ of all elements of $N(n)$ which is a multiple of a $d \in \mathbb{N}, d \geq 1$. 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 $i > k$, we can estimate the size of $N_b(n, \kappa)$ by:

$$|N_b(n, \kappa)| \leq \sum_{i=\kappa+1}^{\infty} \left\lfloor \frac{n}{p_i} \right\rfloor \leq \sum_{i=\kappa+1}^{\infty} \frac{n}{p_i} < \frac{n}{2} \quad (7.3)$$

5) Noticing that an element $m \in N_s(n, k)$ can be written as $m = a \cdot b$, where $a, b \in N_s(n, k)$ and a is a square-free part of m and b is a perfect square of an element of $N_s(n, k)$. We can define two more sets $S_{free}(n, k)$, composed of all elements a , and $S_{div}(n, k)$, composed of all elements b . With these considerations, we can estimate the size of $N_s(n, k)$:

$$|N_s(n, k)| \leq |S_{free}(n, k) \times S_{div}(n, k)| = |S_{free}(n, k)| \cdot |S_{div}(n, k)| \quad (7.4)$$

6) Since $m = a \cdot b$ for all $m \in N_s(n, k)$, we can estimate the number of elements of $S_{div}(n, k)$ 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 $N_s(n, k) \subseteq N(n)$, the estimation is:

$$|S_{div}(n, k)| \leq \sqrt{|N_s(n, k)|} \leq \sqrt{|N(n)|} = \sqrt{n} \quad (7.5)$$

7) The $S_{free}(n, k)$ is the set of all elements less than or equal n , with only *Small* primes divisors and square-free. In others words, an element of $S_{free}(n, k)$ is of the form $m = p_1^{\epsilon_1} \cdot p_2^{\epsilon_2} \cdot \dots \cdot p_k^{\epsilon_k}$, where $\epsilon_i \in \{0, 1\}$. This can be estimated with:

$$|S_{free}(n, k)| \leq 2^k \quad (7.6)$$

8) Since $N(n) = N_s(n, k) \cup N_b(n, k)$, for every k . Using the last item estimations, we must have:

$$|N(n)| \leq |N_s(n, \kappa)| + |N_b(n, \kappa)| < 2^\kappa \sqrt{n} + \frac{n}{2} \quad (7.7)$$

9) Choosing $n = 2^{2\kappa+2}$, our inequality simplifies to $|N(n)| < 2^{2\kappa+2} = n$, an absurd, since $|N(n)| = n$. Therefore, our original consideration of the convergence of a series of prime reciprocals must be false. That's only possible if there are infinite primes.

7.2 Specification details

The proof given by the book uses a prime enumeration p_i and considers its reciprocal series, but it doesn't explicitly consider the case where there are finite primes, as there shouldn't be a value greater than a certain i , this makes the sequence not well-defined. A mistake was also made in the proof of the Chapter 5. To avoid this circularity, we should redefine what sequence p_i means, and by consequence, what is the sequence $\frac{1}{p_i}$.

In Chapter 5, we defined a prime enumeration function ρ , as well as we proved some theorems with it, these theory was separated in its own file and will be reused here. By considering the series of reciprocal of prime numbers, we should account for the case where the prime set is finite. This can be done naturally from our definition of the prime enumerating function, as it returns zero if we try to enumerate a nonexistent prime. This natural definition is:

Definition 5  Let $\iota : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$

$$\iota(n) = \begin{cases} \frac{1}{\rho(n)} & \text{if } \rho(n) > 0 \\ 0 & \text{otherwise} \end{cases}$$

It follows from this definition that this sequence and its series are not only well-defined, this can be overcome if we turn the series into a finite sum in the case where there are finite primes, i.e.


$$\sum_{i=0}^{\infty} \iota(i) = \begin{cases} \sum_{i=0}^{k-1} \frac{1}{\rho(i)} & \text{if } |\mathbb{P}| = k \\ \sum_{i=0}^{\infty} \frac{1}{\rho(i)} & \text{otherwise} \end{cases}$$

Just as in Chapter 5, remember that our enumeration starts from zero, meaning our proofs from here on will have potentially shifted indices compared to the original proof. This was done with the intention of simplifying the proofs inside the PVS, as many proved lemmas, such as the ones involving sums and series, start with index zero.

For example:

$$\sum_{i=0}^{\infty} \iota(i) = \begin{cases} \sum_{i=1}^k \frac{1}{p_i} & \text{if } |\mathbb{P}| = k \\ \sum_{i=1}^{\infty} \frac{1}{p_i} & \text{otherwise} \end{cases}$$

With our ρ function defined, we can prove our first inequality.

Lemma 7.2.1.  Suppose that the series $\sum_{i=0}^{\infty} \iota(i)$ converges, then there exists an κ , such that $\sum_{i=\kappa}^{\infty} \iota(i) < \frac{1}{2}$

Proof. This lemma follows from the definition of convergence, that is, for every $\epsilon \in \mathbb{R}, \epsilon > 0$, there exists a $N \in \mathbb{Z}$, such that for every $n \in \mathbb{Z}, n \geq N$:

$$\left| \sum_{i=0}^{\infty} \iota(i) - \sum_{i=0}^n \iota(i) \right| < \epsilon$$

By letting $\epsilon = \frac{1}{2}$ and renaming $\kappa = n + 1$.

$$\left| \sum_{i=0}^{\infty} \iota(i) - \sum_{i=0}^n \iota(i) \right| < \frac{1}{2}$$

$$\left| \sum_{i=n+1}^{\infty} \iota(i) \right| = \left| \sum_{i=\kappa}^{\infty} \iota(i) \right| = \sum_{i=\kappa}^{\infty} \iota(i) < \frac{1}{2}$$

The last inequality comes from the fact that $\iota(i)$ is greater than or equal to zero. □



Now, given a positive integer k , it will be useful to divide the prime numbers into the categories of *Small* and *Big* primes. Based on the book's definition, we should call a value $\rho(i)$ a *Small* prime if $i < k$ and *Big* prime if $i \geq k$. Notice that this definition is close to what was given by the book, and it is still not formally defined when we have finite primes, for i larger enough, $\rho(i) = 0$, which is not a prime zero.

We can overcome this problem by formally defining *Small* and *Big* primes as sets of numbers in the following way.

Definition 6  Let $k \in \mathbb{Z}_{\geq 0}$

$$Small(k) = \{p \in \mathbb{P} : p < \rho(k) \vee \rho(k) = 0\}$$

$$Big(k) = \{p \in \mathbb{P} : p \geq \rho(k) \wedge \rho(k) \neq 0\}$$

As mentioned in Section 5.2.1, about prime enumeration, for all prime values this ρ function enumerates the primes in ascending order, meaning that for all $p \in \mathbb{P}$, there exists $i \in \mathbb{Z}_{\geq 0}$, such that $p = \rho(i)$, where it maintains the ordering of the prime numbers. In particular, if $\rho(i) < \rho(k)$, then $i < k$ , otherwise we have $\rho(i) \geq \rho(k)$, then $i \geq k$ . As such, this definition behaves analogous with the one given by the book.

With this new definition, instead of talking about an enumeration p_i, p_{i+1}, \dots , as mentioned in the book, we will be using the *Small* and *Big* prime sets. First, we can assert it really divides the primes into two different sets.

Corollary 7.2.1.1. *Small(k) and Big(k) are disjoint sets with $\mathbb{P} = \text{Small}(k) \cup \text{Big}(k)$*

Proof. It is noticeable that the restriction in the definition of the big primes set is the logical negation of the *Small* prime set restriction, and vice versa. In other words, each set is the complement of the other under the prime set, therefore their union is the whole \mathbb{P} . □

This can be proven in PVS by a simple "grind" command. But it will be helpful to have this last Corollary for later citation.


With the *Small* primes and *Big* primes sets defined, other useful sets can be also defined.

Definition 7   Let $k \in \mathbb{Z}_{\geq 0}$ and $n \in \mathbb{Z}_{> 0}$

$$N(n) = \{m \in \mathbb{Z}_{> 0} : m \leq n\}$$

$$N_s(n, k) = \{m \in N(n) : \forall p \in \mathbb{P}, p \mid m \Rightarrow p \in \text{Small}(k)\}$$

$$N_b(n, k) = \{m \in N(n) : \exists p \in \text{Big}(k), p \mid m\}$$

Corollary 7.2.1.2.  *$N_s(n, k)$ and $N_b(n, k)$ are disjoint sets with $N(n) = N_s(n, k) \cup N_b(n, k)$*


Given an element $m \in N(n)$, if $m = 1$, it does not have a prime divisor, meaning $m \in N_s(n, k)$ and $m \notin N_b(n, k)$. If $m > 1$, if it has a *Big* prime divisor than $m \in N_b(n, k)$ by Corollary 7.2.1.1, the *Big* and *Small* primes are disjoint, therefore $m \notin N_s(n, k)$. The last case is $m > 1$, and it does not have a *Big* prime, again by Corollary 7.2.1.1, the prime divisor must be a *Small* prime, meaning $m \in N_s(n, k)$ and $m \notin N_b(n, k)$.

7.2.1 *Big* primes multiple set $N_b(n, k)$

For estimating the $N_b(n, k)$, we should define another set of numbers, the set of positive multiples of a number d , less or equal to n .

Definition 8  Let $d, n \in \mathbb{Z}_{>0}$

$$N_{div}(d, n) = \{m \in N(n) : d \mid m\}$$

Lemma 7.2.2.  For $d, n \in \mathbb{Z}_{>0}$, $|N_{div}(d, n)| = \left\lfloor \frac{n}{d} \right\rfloor$

Notice that the elements of $N_{div}(d, n)$ are of the form $m = d \cdot x, x \in \mathbb{Z}_{>0}$, therefore the minimum value is found with $x = 1$ and for the max value, it must be a value such $x \leq \frac{n}{d}, x \in \mathbb{Z}$, which is exactly the definition of $\left\lfloor \frac{n}{d} \right\rfloor$. Meaning all possible values are restricted to $d \cdot 1 \leq d \cdot x \leq d \cdot \left\lfloor \frac{n}{d} \right\rfloor$, on other words, $N_{div}(d, n) = \left\lfloor \frac{n}{d} \right\rfloor$.

With this lemma proved, we are ready to estimate $N_b(n, k)$:

Theorem 7.2.3.  $|N_b(n, k)| \leq n \cdot \sum_{i=k}^{\infty} \iota(i)$

Proof. From the definition of $N_b(n, k)$, its elements must be divisible by some *Big* prime, meaning that for all $m \in N_b(n, k)$, there exists a *Big* prime $\rho(i)$, such that $m \in N_{div}(\rho(i), n)$. As such, we can find an injection from $N_b(n, k)$ to $\bigcup_{i=k}^{\infty} N_{div}(\rho(i), n)$ by the identity function. It's worth mentioning that this infinite union is well defined for finite primes, as $N_{div}(\rho(i), n)$ will be equal to the empty set if $\rho(i) = 0$, as there are no positive integer which is divisible by zero. In conclusion, this injection leads to

$$|N_b(n, k)| \leq \left| \bigcup_{i=k}^{\infty} N_{div}(\rho(i), n) \right| \leq \sum_{i=k}^{\infty} |N_{div}(\rho(i), n)|$$

Now notice that if $N_{div}(\rho(i), n) = \emptyset$, this is only possible in the case $\rho(i) = 0$ or if $\rho(i) > n$.

If $\rho(i) = 0$, then by definition of ι function, $\iota(i) = 0$, meaning

$$|N_{div}(\rho(i), n)| = 0 = n \cdot \iota(i)$$

If $\rho(i) > n$, then $n > 0$ and $\iota(i) > 0$, meaning

$$|N_{div}(\rho(i), n)| = 0 \leq n \cdot \iota(i)$$

Now considering the case $N_{div}(\rho(i), n) \neq \emptyset$, by Lemma 7.2.2

$$|N_{div}(\rho(i), n)| = \left\lfloor \frac{n}{\rho(i)} \right\rfloor \leq \frac{n}{\rho(i)} = n \cdot \iota(i)$$

In other words, we have for all cases

$$|N_{div}(\rho(i), n)| \leq n \cdot \iota(i)$$

$$\Rightarrow |N_b(n, k)| \leq \sum_{i=k}^{\infty} |N_{div}(\rho(i), n)| \leq \sum_{i=k}^{\infty} n \cdot \iota(i) = n \cdot \sum_{i=k}^{\infty} \iota(i)$$

□


7.2.2 Small primes multiple set $N_s(n, k)$

With the estimation of the set $N_b(n, \kappa)$ size completed, it remains to estimate the size of $N_s(n, \kappa)$; for that, we must define two more sets.

Definition 9  Let $k \in \mathbb{Z}_{\geq 0}$ and $n \in \mathbb{Z}_{> 0}$

$$S_{div}(n, k) = \{m \in N_s(n, k) : \exists d \in \mathbb{Z}_{> 0}, m = d^2\}$$

$$S_{free}(n, k) = \{m \in N_s(n, k) : \nexists d \in \mathbb{Z}_{> 0}, d > 1, d^2 \mid m\}$$

Corollary 7.2.3.1.  For every $m \in N_s(n, k)$, there exists $a \in S_{free}(n, k)$ and $b \in S_{div}(n, k)$, such that $m = a \cdot b$.

Proof. There are finite possible divisors of the number n , take the maximum divisor b such that $b \in S_{div}(n, k)$, this value always exists as $x = 1$, if the number is square-free. By the definition of divisor $m = a \cdot b$, it remains to show that $a \in S_{free}(n, k)$. For that, suppose there exists a $d > 1$, such that $d^2 \mid a$, this implies that exists


$$a = y \cdot d^2$$

$$m = y \cdot d^2 \cdot x^2 = y \cdot (dx)^2$$

By the divisor inequality $(dx)^2 \leq m$, since $m \in N_s(n, k)$ we have $(dx)^2 \leq m \leq n$, therefore $(dx)^2 \in S_{div}(n, k)$ and $(dx)^2 > b$, an absurd since b is maximal. In conclusion a is square-free, by similar argument the condition $a \leq m \leq n$ is also true, meaning $a \in S_{free}(n, k)$.

□

This Corollary motivates us to divide the approximation into two steps, finding the estimation $|S_{div}(n, k)|$ and $|S_{free}(n, k)|$. This step is done loosely in the original book's proof, but during the specification, it was necessary to prove there exists an injection from $N_s(n, k)$ to $S_{div}(n, k) \times S_{free}(n, k)$, which is related to our next Lemma.

Lemma 7.2.4.  The decomposition of $m \in N_s(n, k)$, as $m = a \cdot b$ for $a \in S_{free}(n, k)$ and $b \in S_{div}(n, k)$, is unique.

Proof. This can be done via induction over the variable m ; the basis case is when $m = 1$, since $a \geq 1$ and $b \geq 1$, the only way $1 = a \cdot b$ is when $a = 1$ and $b = 1$. For m larger than one, $a > 1$ or $b > 1$. Suppose there exists another $c \in S_{free}(n, k)$ and $d \in S_{div}(n, k)$ with $m = c \cdot d$.

Case $a > 1$ there exists a prime p which divides a , in particular

$$\begin{aligned} p \mid a \quad \wedge \quad a \mid m \\ \Rightarrow p \mid m = c \cdot d \end{aligned}$$

Since p is prime, $p \mid c$ or $p \mid d$. Case $p \mid c$, we have

$$\begin{aligned} a = p \cdot x_1 \quad \wedge \quad c = p \cdot x_2 \\ \Rightarrow \begin{cases} m = p \cdot x_1 \cdot b \\ m = p \cdot x_2 \cdot d \end{cases} \Rightarrow \begin{cases} \frac{m}{p} = x_1 \cdot b \\ \frac{m}{p} = x_2 \cdot d \end{cases} \end{aligned}$$

But by inductive hypothesis $b = d$ and $x_1 = x_2$, therefore $a = c$.

Case $p \mid d$, we must have $p^2 \mid d$, since d is a perfect square, therefore $p^2 \mid m$, in other words, $d = p^2 \cdot x_3$ and $a = p \cdot x_1$, which means


$$\begin{aligned} p^2 \cdot x_3 &= p \cdot x_1 \cdot b \\ p \cdot x_3 &= x_1 \cdot b \\ p \mid x_1 \cdot b \end{aligned}$$

Notice that p does not divide x_1 , otherwise $a \in S_{free}(n, k)$ would have a square factor, meaning $p \mid b$, since b is a perfect square $p^2 \mid b$, as a result.

$$\begin{aligned} b = p^2 \cdot x_4 \quad \wedge \quad d = p^2 \cdot x_3 \\ \Rightarrow \begin{cases} m = p^2 \cdot x_4 \cdot a \\ m = p^2 \cdot x_3 \cdot c \end{cases} \Rightarrow \begin{cases} \frac{m}{p^2} = x_4 \\ \frac{m}{p^2} = x_3 \end{cases} \end{aligned}$$

But by inductive hypothesis $a = c$ and $x_3 = x_4$, therefore $b = d$. The last remaining case is when $b > 1$, which means there exists $p \mid b$; since b is a perfect square, we could use the same argumentation as case $p \mid d$ to prove the equality. \square

Now we can prove the following Theorem.

Theorem 7.2.5.  $|N_s(n, k)| \leq |S_{div}(n, k)| \cdot |S_{free}(n, k)|$

Proof. Using the Corollary 7.2.3.1 and Lemma 7.2.4, we can define a function.

$$f : N_s(n, k) \rightarrow S_{div}(n, k) \times S_{free}(n, k)$$

$$f(m) = (a, b)$$

Indeed this function is an injection by the uniqueness of Lemma 7.2.4, meaning that:

$$|N_s(n, k)| \leq |S_{free}(n, k) \times S_{div}(n, k)| = |S_{free}(n, k)| \cdot |S_{div}(n, k)|$$

□

It now remains to estimate these two sets. Let's start with the easy one.

Lemma 7.2.6.  $|S_{div}(n, k)| \leq \sqrt{n}$

Proof. Using the definition of the $S_{div}(n, k)$, every element of the set is of the form $m = d^2$, with the restriction $1 \leq m \leq n$, in particular, this implies that $1 \leq \sqrt{m} \leq \sqrt{n}$, in other words the square root function is a function that takes $S_{div}(n, k)$ to $N(\sqrt{n})$, since the square root function for real numbers is injective, $|S_{div}(n, k)| \leq \sqrt{n}$. □

The next inequality is easy to prove through analytical methods, but during the specification, some extra problems appeared.

Lemma 7.2.7.  $|S_{free}(n, k)| \leq 2^k$

Proof. Since ρ enumerates the primes, by the Fundamental Theorem of Arithmetic, all elements $m \in S_{free}(n, k)$ are of the form $m = \rho(0)^{\epsilon_1} \cdot \rho(1)^{\epsilon_2} \cdots \rho(l)^{\epsilon_k}$, for some $l \in \mathbb{Z}_{\geq 0}$. Notice that $\epsilon \leq 1$, otherwise m would not be a square-free number. To prove the inequality, we can consider an injection function $\gamma : S_{free}(n, k) \rightarrow \times_{i=0}^l \{1, \rho(i)\}$.

$$\gamma(m) = (\rho(0)^{\epsilon_1}, \rho(1)^{\epsilon_2}, \dots, \rho(l)^{\epsilon_l})$$

Since the Fundamental Theorem of Arithmetic guarantees that the factorization is unique under multiplication commutativity, this is indeed an injection, but we need to make sure two more things: first, we need to find l such that this factorization from 0 to l have all prime factors of m ; second, we need to guarantee that for i , where $0 \leq i \leq l$, this i value does not try to enumerate a non-existent prime, i.e. $\rho(i) = 0$.

This can be done considering the definition of $S_{free}(n, k)$, as all of its prime divisors p are $p < \rho(k)$, $l = k - 1$ satisfies the factors property. If there is infinite primes, by the definition of ρ , $\rho(i) \neq 0$, for any $i \in \mathbb{Z}_{\geq 0}$. For the case where there is finite prime, than $\pi(p_{max})$ corresponds for the maximum quantity of primes, by Lemma 5.2.3, the sequence

$\rho(0), \rho(1), \dots, \rho(\pi(p_{max}) - 1)$ contains all primes, then $l = \min(\pi(p_{max}) - 1, k - 1)$ serves our purpose. Therefore, we have

$$|S_{free}(n, k)| \leq \left| \prod_{i=0}^l \{1, \rho(i)\} \right| = 2^{l+1} \leq 2^k$$

□

This lemma relies heavily on the Fundamental Theorem of Arithmetic, as discussed in Chapter 5. The original *NASALib* approach was insufficient for our proof, which led to the decision to switch to the Cartesian product approach. In this specific case, this change made it significantly easier to estimate cardinality, as there is already a theorem in *NASALib* regarding the cardinality of the Cartesian product of finite sets [↗](#).

7.2.3 Proof by contradiction

With all the estimations in hand, we can finally face the problem of the infinitude of primes directly.

Theorem 7.2.8. [↗](#) *The series $\sum_{i=0}^{\infty} \iota(i)$ diverges*

Proof. Let $k \in \mathbb{Z}_{\geq 0}$ and $n \in \mathbb{Z}_{> 0}$ be arbitrary. Using Lemma 7.2.1.2

$$|N(n)| \leq |N_s(n, k)| + |N_b(n, k)|$$

By Theorem 7.2.5 and Lemmas 7.2.7, 7.2.6, we have $|N_s(n, k)| \leq \sqrt{n} \cdot 2^k$. By the definition of $N(n)$, we have $|N(n)| = n$, therefore

$$n \leq \sqrt{n} \cdot 2^k + |N_b(n, k)|$$

Assuming the series converges, by Theorem 7.2.3 and Lemma 7.2.1, $|N_b(n, \kappa)| < \frac{n}{2}$, thus, by choosing $k = \kappa$.

$$n < \sqrt{n} \cdot 2^{\kappa} + \frac{n}{2}$$

Now considering an arbitrary $n = 2^{2\kappa+2}$

$$2^{2\kappa+2} < 2^{\kappa+1} \cdot 2^{\kappa} + 2^{2\kappa+1}$$

$$2^{2\kappa+2} < 2 \cdot 2^{2\kappa+1}$$

$$2^{2\kappa+2} < 2^{2\kappa+2}$$

A contradiction

□

Now for the infinitude of primes.

Corollary 7.2.8.1.  *There are infinite primes*

Proof. If there is only k finite primes by definition of the ι function, the series $\sum_{i=0}^{\infty} \iota(i)$ must be equal to $\sum_{i=0}^{k-1} \frac{1}{\rho(i)}$, which converges, by Theorem 7.2.8 this is a contradiction.

□

Chapter 8

Conclusion and Future Work

Proof assistants have not yet achieved widespread adoption in formal mathematics. This work serves multiple purposes, being a central one to demonstrate that technical proofs can be accomplished using computer software. To this end, proofs from various branches of mathematics were specified and mechanically proven, leading to the creation of a diverse PVS library focused on wonderful and brilliant proofs of the infinitude of primes.

We designed five new complete formalizations of the infinitude of prime numbers in the Prototype Verification System (PVS). The formalizations are based on the thoughtful selection of the famous book "Proofs from THE BOOK" [3]. In general, improvements were made to the manipulation theorems, especially those related to number theory and algebra, as a beneficial side effect of this formalization effort.

There remains a minor issue with the formalization of the Cauchy product formula, which is unavailable in PVS libraries (as far as we know). The Cauchy product formula is required in the fourth proof of the infinitude of prime numbers in Chapter 5, "Divergence of Zeta(1)". This issue is addressed assuming the Cauchy product formula, letting its formalization be a future work that will improve the PVS libraries on analysis.

During the formalization process, several omissions, informalities and notational inconsistencies we detected in the pen-and-paper proofs in [3] were identified and corrected. Such imprecisions arise because of the loose use of a sequence to enumerate the prime numbers (e.g., see the discussion in Subsection 5.2.1 and Section 7.2). In this respect, one significant outcome of this work is constructing a theory for prime enumeration that does not assume the infinitude of prime numbers, thereby avoiding circular reasoning.

Additionally, to facilitate further mathematical manipulations in the proofs in Chapter 5 "Divergence of Zeta(1)" and Chapter 7 "Divergence of primes reciprocal series", a new approach for the Fundamental Theorem of Arithmetic was formalized. The original form, available in PVS, had issues with how it was specified. In particular, it had a prob-

lem when trying to exhibit the existence of a specific prime power. Our new approach addresses this issue (see the discussion after Lemma 5.2.3).

PVS proved a valuable tool for proving theorems, as its type-checking system could identify inconsistencies. However, this also led to some challenges, such as the *type correctness conditions*, which sometimes required repetitive statements to complete a specific proof or theory in Chapter 4. While this could often be avoided by defining new lemmas, it occasionally became more time-consuming, especially when working with the algebra library, which relies heavily on the type hierarchy of algebraic structures (ring depends on groups, which depends on monoid, and so on). On the positive side, arithmetic and more complex symbolic manipulations were optimized through the usage of powerful commands of PVS, such as the "grind" command, which makes certain technical proofs that would be tedious by hand almost trivial, such as in the Lemma 3.2.1 in Chapter 3.

As the Chapter 4 suggest, there remains room for optimization in the *NASALib's algebra* library, such as reworking on the algebra library and trying to automate the type check related proof, such as the TCC that appears when importing algebra theories, this could be done by adding new PVS strategies and PVS judgements, or maybe refining abstractions and generalizing theorems. General reusable abstraction, such as used in the prime enumeration Section 5.2.1, may also appear in other parts of the *NASALib*. Investigation of this kind is something worth future work.

We also plan to formalize the Cauchy product to strengthen the *NASALib's analysis* library and to complete this proof collection. Another direction for future work is incorporating into the corpora of formalizations additional topics covered in "Proofs from THE BOOK" [3]. As mentioned in the Chapter 1, some particular proofs besides Chapter 1 from "Proofs from THE BOOK" were done, but not the entirety of it. For example, a possible work for the future is to formalize the geometry section, which would expand further the mathematical proofs available in PVS to another Math topic. Furthermore, exploring proofs of the infinitude of prime numbers from different fields of mathematics that may not be mentioned in this work would be a valuable addition to this collection, enhancing the diversity and depth of our mechanized proof repository.

Bibliography

- [1] Artmann, Benno: *Euclid—the creation of mathematics*. Springer Science & Business Media, 2012. 1
- [2] Owre, Sam, John M Rushby, and Natarajan Shankar: *PVS: A prototype verification system*. In *International Conference on Automated Deduction*, pages 748–752. Springer, 1992. 1, 5
- [3] Aigner, Martin and Günter M Ziegler: *Proofs from THE BOOK*. Berlin. Germany, 1(2):12, 1999. 1, 51, 52
- [4] Gödel, Kurt: *Über formal unentscheidbare sätze der principia mathematica und verwandter systeme i*. Monatshefte für mathematik und physik, 38:173–198, 1931. 2
- [5] Gauss, Carl Friedrich and William C Waterhouse: *Disquisitiones arithmeticae*. Springer, 2018. 2, 24
- [6] Ayala-Rincón, Mauricio, Thaynara Arielly de Lima, Andréia B Avelar, and André Luiz Galdino: *Formalization of Algebraic Theorems in PVS (Invited Talk)*. In *LPAR*, pages 1–10, 2023. 2, 16
- [7] Gottliebsen, Hanne: *Automated theorem proving for mathematics: real analysis in PVS*. University of St. Andrews (United Kingdom), 2002. 2, 22
- [8] Lester, David R: *Topology in PVS: continuous mathematics with applications*. In *Proceedings of the second workshop on Automated formal methods*, pages 11–20, 2007. 2, 35
- [9] Wiedijk, Freek: *Formal proof—getting started*. 2008. <https://www.cs.ru.nl/~freek/100/>, Formalizing 100 Theorems. 2
- [10] Koepke, Peter, Mateusz Marcol, and Patrick Schäfer: *Formalizing sets and numbers, and some of wiedijk’s” 100 theorems” in naproche*. 2023. 2
- [11] Eberl, Manuel: *Furstenberg’s topology and his proof of the infinitude of primes*. Archive of Formal Proofs, March 2020, ISSN 2150-914X. https://isa-afp.org/entries/Furstenberg_Topology.html, Formal proof development. 3
- [12] Eberl, Manuel: *The Hurwitz and Riemann ζ Functions*. Archive of Formal Proofs, October 2017, ISSN 2150-914X. https://isa-afp.org/entries/Zeta_Function.html, Formal proof development. 3

- [13] Paulson, Lawrence C.: *Irrational numbers from THE BOOK*. Archive of Formal Proofs, January 2022, ISSN 2150-914X. https://isa-afp.org/entries/Irrationals_From_THEBOOK.html, Formal proof development. 3
- [14] Bortin, Maksym: *From THE BOOK: Two Squares via Involutions*. Archive of Formal Proofs, August 2022, ISSN 2150-914X. <https://isa-afp.org/entries/Involutions2Squares.html>, Formal proof development. 3
- [15] *NASA PVS web site*. <https://shemesh.larc.nasa.gov/fm/pvs/>. Accessed: 2025-01-28. 5
- [16] *PVS web site*. <https://pvs.csl.sri.com/>. Accessed: 2025-01-28. 5
- [17] Muñoz, César and Ramiro Demasi: *Advanced theorem proving techniques in PVS and applications*. In Meyer, Bertrand and Martin Nordio (editors): *Tools for Practical Software Verification - LASER 2011, International Summer School*, volume 7682 of *Lecture Notes in Computer Science*, pages 97–133, 2012. 5
- [18] Steele, Guy: *Common LISP: the language*. Elsevier, 1990. 6
- [19] Lewis, Bil, Dan LaLiberte, and Richard Stallman: *GNU Emacs Lisp Reference Manual 1/2*. Samurai Media Limited, 2015. 6
- [20] Masci, Paolo and César A. Muñoz: *An Integrated Development Environment for the Prototype Verification System*. Electronic Proceedings in Theoretical Computer Science, 310:35–49, December 2019, ISSN 2075-2180. <http://dx.doi.org/10.4204/EPTCS.310.5>. 7
- [21] Masci, Paolo and Aaron Dutle: *Proof Mate: An interactive proof helper for PVS (tool paper)*. In Deshmukh, Jyotirmoy V., Klaus Havelund, and Ivan Perez (editors): *Proceedings of the 14th International Symposium NASA Formal Methods (NFM 2022)*, volume 13260, pages 809–815, Los Angeles, CA, USA, May 2022. Springer International Publishing. 7
- [22] Owre, Sam, Natarajan Shankar, John M Rushby, and David WJ Stringer-Calvert: *PVS language reference*. Computer Science Laboratory, SRI International, Menlo Park, CA, 1(2):21, 1999. 7
- [23] Owre, Sam, Natarajan Shankar, John M Rushby, and David WJ Stringer-Calvert: *PVS system guide*. Computer Science Laboratory, SRI International, Menlo Park, CA, 1(5):7, 1999. 7, 8
- [24] Ayala-Rincón, Mauricio and Flávio LC De Moura: *Applied logic for computer scientists: computational deduction and formal proofs*. Springer, 2017. 8
- [25] Shankar, N, S Owre, JM Rushby, and DWJ Stringer-Calvert: *PVS prover guide [computer software manual]*. Menlo Park, CA, 1999. 8
- [26] Owre, Sam and Natarajan Shankar: *The formal semantics of PVS*. Contract report 19990046202, Langley Research Center, 1999. 10

- [27] Hua, L K: *Introduction to number theory*. Springer Science & Business Media, 2012. [11](#)
- [28] Robinson, Raphael M: *Mersenne and Fermat numbers*. Proceedings of the American Mathematical Society, 5(5):842–846, 1954. [11](#), [16](#)
- [29] Lagrange, Joseph Louis de: *Réflexions sur la résolution algébrique des équations*. Prussian Academy, 1770. [16](#)
- [30] Apostol, Tom M: *Introduction to analytic number theory*. Springer Science & Business Media, 2013. [21](#)
- [31] Euler, Leonhard *et al.*: *Introductio in analysin infinitorum...; tomus primus*. 1748. [21](#)
- [32] Titchmarsh, Edward Charles: *The theory of the Riemann Zeta-function*. The Clarendon Press Oxford University Press, 1986. [21](#)
- [33] Cauchy, Augustin Louis: *Cours d'analyse de L'Ecole Polytechnique*. oeuvres complètes, 2:t–3, 1821. [27](#)
- [34] Jameson, Graham James Oscar: *The prime number theorem*. Number 53. Cambridge University Press, 2003. [34](#)
- [35] Furstenberg, Harry: *On the infinitude of primes*. Amer. Math. Monthly, 62(5):353, 1955. [35](#)
- [36] Mendelson, Bert: *Introduction to topology*. Courier Corporation, 1990. [35](#)
- [37] Erdős, Paul: *Über die Reihe $\sum 1/p$* . Mathematica, Zutphen B, 7:1–2, 1938. [40](#)