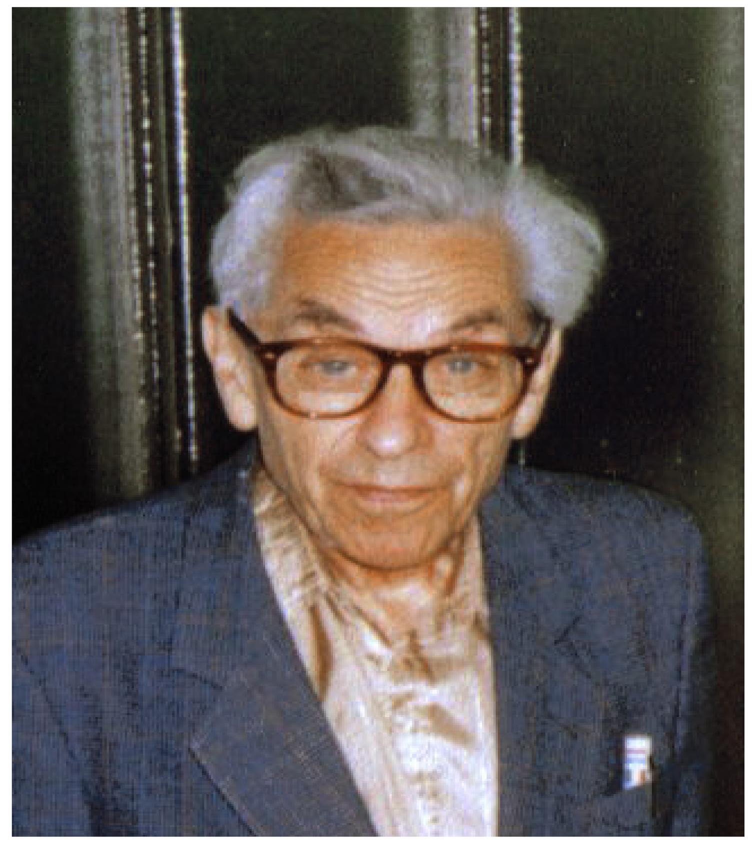
# Arithmetical and Analytical Proofs of the Infinitude of Primes

Claire Xu  Navya Chauhan  Advised by: Kabir Belgikar

The Ohio State University

DEPARTMENT OF MATHEMATICS

## Paul Erdős



**Paul Erdős (1913–1996)** was a Hungarian mathematician renowned for his contributions to number theory, combinatorics, and graph theory. With over 1,500 published papers, Erdős is considered one of the most influential mathematicians of the 20th century. Known for his nomadic lifestyle, he traveled the world, collaborating with hundreds of mathematicians and seeking out new mathematical problems.

## "The Book"

Paul Erdős' idiosyncratic idea, ***The Book***, was a hypothetical collection of elegant mathematical proofs written by God himself, which he aspired to discover.

## Proofs from THE BOOK

*Proofs from THE BOOK* by Günter M. Ziegler and Martin Aigner is a collection of elegant and beautiful mathematical proofs, inspired by the concept of ***The Book*** [1]. It serves as a tribute to mathematical beauty and Erdős' vision of perfect mathematical solutions. Each proof in the book is carefully selected for its clarity, making complex concepts accessible.

The first section of the book focuses on number theory and includes several proofs that demonstrate the infinitude of primes. Among the six proofs included in the first chapter we have selected two for presentation.

## An Arithmetical Proof of the Infinitude of Primes

For an integer $n \geq 0$, the $n^{\text{th}}$ Fermat number is defined to be $F_n = 2^{2^n} + 1$. The fact that there are infinitely many primes is an immediate consequence of the following:

**Theorem:** *Any two distinct numbers in the sequence $F_0, F_1, F_2, \ldots$ are coprime (i.e., they share no common prime factors).*

Indeed, letting $q_n$ be any prime divisor of $F_n$ for all $n \geq 0$ and assuming that the above Theorem holds, we see that $q_0, q_1, q_2, \ldots$ is an infinite sequence of distinct prime numbers.

## A Helpful Identity

We will first establish the formula

$$F_0 F_1 \cdots F_n = F_{n+1} - 2 \tag{1}$$

for all $n \geq 0$.

Note that for $n = 4$, repeated applications of the formula $(a-b)(a+b) = a^2 - b^2$ yield

$$\begin{aligned}
F_0F_1F_2F_3F_4 &= \left(2^{2^0}+1\right)\left(2^{2^1}+1\right)\left(2^{2^2}+1\right)\left(2^{2^3}+1\right)\left(2^{2^4}+1\right) \\
&= \underbrace{\left(2^{2^0}-1\right)}_{=1}\left(2^{2^0}+1\right)\left(2^{2^1}+1\right)\left(2^{2^2}+1\right)\left(2^{2^3}+1\right)\left(2^{2^4}+1\right) \\
&= \left(2^{2^1}-1\right)\left(2^{2^1}+1\right)\left(2^{2^2}+1\right)\left(2^{2^3}+1\right)\left(2^{2^4}+1\right) \\
&= \left(2^{2^2}-1\right)\left(2^{2^2}+1\right)\left(2^{2^3}+1\right)\left(2^{2^4}+1\right) \\
&= \left(2^{2^3}-1\right)\left(2^{2^3}+1\right)\left(2^{2^4}+1\right) \\
&= 2^{2^5}-1 \\
&= F_5 - 2.
\end{aligned}$$

The proof of formula (1) for the case of general $n \geq 0$ is similar.

## Proof of the Theorem

Let $F_n$ and $F_m$ be any distinct Fermat numbers with $0 \leq m < n$ and observe that

$$2 = F_n - F_0 F_1 \cdots F_m \cdots F_{n-1}$$

by formula (1).

It follows that if $k \geq 1$ is any common factor of both $F_n$ and $F_m$, then $k$ must be a factor of 2. In other words, $k = 1$ or $k = 2$. But since every Fermat number is odd, we can't have $k = 2$. Thus, $k = 1$ is the only factor common to both $F_m$ and $F_n$ as desired. □

## An Analytical Proof of the Infinitude of Primes

Let $p_1, p_2, p_3, \ldots$ be the list of primes in increasing order and $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ be the set of prime numbers. The prime counting function $\pi\colon \mathbb{R} \to \{0, 1, 2, \ldots\}$ counts the number of primes up to $x$: $\pi(x) = \#\{p \leq x : p \in \mathbb{P}\}$. Recall the natural logarithm, denoted by $\log$, is defined by

$$\log(x) = \int_1^x \frac{1}{t}\,dt.$$

We will establish the following:

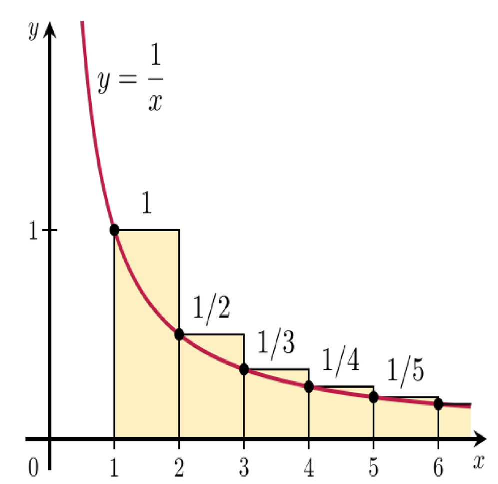
**Inequality:** *For all natural numbers $n$, we have*

$$\log(n) - 1 \leq \pi(n).$$

Since $\log(n) - 1$ grows without bound, the above inequality implies that the number of primes up to $n$ also grows without bound (which means there are infinitely many primes).

## Proof of Inequality

The integral test yields the following upper bound (see the picture):




$$\longrightarrow \quad \log(n) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}. \tag{2}$$

Since $p_1, p_2, \ldots, p_k$, where $k = \pi(n)$, are all the primes up to $n$, we have

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \sum \frac{1}{m}, \tag{3}$$

where the sum extends over all $m \in \mathbb{N}$ which have only prime divisors among $p_1, p_2, \ldots, p_k$. Since every number $m$ in our sum can be written as a unique product $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, we can rewrite our sum as

$$\sum \frac{1}{m} = \sum_{e_1, e_2, \ldots, e_k \in \mathbb{N}} \frac{1}{p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}} = \prod_{j=1}^{k} \sum_{e_i=0}^{\infty} \frac{1}{p_j^{e_i}} = \prod_{j=1}^{k} \frac{1}{1 - \frac{1}{p_j}} = \prod_{j=1}^{k} \left(1 + \frac{1}{p_j - 1}\right). \tag{4}$$

Since $p_j \geq j + 1$, it follows that

$$\prod_{j=1}^{k} \left(1 + \frac{1}{p_j - 1}\right) \leq \prod_{j=1}^{k} \left(1 + \frac{1}{j}\right) = \prod_{j=1}^{k} \frac{j+1}{j} = k + 1 = \pi(n) + 1. \tag{5}$$

Inequalities (2)-(5) together imply that $\log(n) \leq \pi(n) + 1$ as desired. □

## References

[1] Martin Aigner and Günter M. Ziegler. In *Proofs from THE BOOK*. Springer Berlin Heidelberg, Berlin, Heidelberg, 5 edition, 2014.