European Journal of Mathematics and Statistics
Vol 6 | Issue 3 | May 2025
ISSN 2736-5484

RESEARCH ARTICLE

Exploring the Infinitude of Primes and Related Conjectures

Arya Mosahab*

ABSTRACT

This paper presents several classical and modern proofs demonstrating the infinitude of prime numbers. The discussion includes Euclid's original argument as well as alternative approaches including analytic, topological, and combinatorial proofs. In addition, this paper discusses two open problems in number theory: the infinitude of Mersenne primes and the Twin Prime Conjecture. The aim is to provide an overview of both established results and ongoing challenges in the study of prime numbers.

Keywords: Infinitude, prime numbers.

Submitted: April 10, 2025

Published: May 22, 2025

10.24018/ejmath.2025.6.3.399

University of Manchester, UK.

**Corresponding Author:*
e-mail:
arya.mosahab@student.manchester.ac.uk

1. Introduction

Prime numbers play a central role in number theory and mathematics as a whole. Their distribution and properties have been studied extensively, yet many fundamental questions remain open. One of the most well-known results in this area is the infinitude of primes, first proven by Euclid. Since then, numerous alternative proofs have been developed, each offering distinct mathematical insights.

This paper collects and presents a variety of such proofs, ranging from classical number-theoretic arguments to analytic, combinatorial, and topological methods. The objective is not only to illustrate the robustness of the result but also to highlight the diversity of tools used across different branches of mathematics. The final section addresses two unsolved problems concerning special classes of primes–Mersenne and twin primes–and summarises current progress and conjectures related to them.

2. Proofs of the Infinitude of Primes

2.1. Euclid's Proof

The oldest proof of the infinitude of prime numbers was provided by Euclid. This proof relies on the Fundamental Theorem of Arithmetic (FTA), which states that any integer greater than 1 can be written uniquely as a product of prime numbers up to the order. First, suppose there are n (finitely many) prime numbers $p_1, p_2, p_3, \ldots, p_n$. This means that all positive integers greater than 1 must be a multiple of at least one these prime numbers. However, we can consider a positive integer q such that

$$q = \left(\prod_{i=1}^{n} p_i\right) + 1 \equiv 1 \pmod{p_i}, \quad \forall\, i \in \{1, 2, \ldots, n\} \tag{1}$$

Note that q is a positive integer greater than 1 but not a multiple of any of the prime factors. This is a contradiction, and therefore there are infinitely many primes. □

2.2. Proof Using Fermat Numbers

Fermat numbers are defined by the following sequence

$$F_n = 2^{2^n} + 1, \; n \geq 0 \tag{2}$$

We first show that Fermat numbers are pairwise coprime. To do so, consider two distinct Fermat numbers F_a and F_b, WLOG set $a < b$.

$$F_a = 2^{2^a} + 1 \tag{3}$$

$$F_b = 2^{2^b} + 1 = (2^{2^a})^{2^{b-a}} + 1 \tag{4}$$

Now let $c|F_a$, where c is an integer greater than 1. We have that

$$\begin{aligned} & F_a && \equiv 0 \pmod{c} \\ \Rightarrow\ & 2^{2^a} && \equiv -1 \pmod{c} \\ \Rightarrow\ & F_b && = \left(2^{2^a}\right)^{2^{b-a}} + 1 \\ & && \equiv (-1)^{2^{b-a}} + 1 \\ & && \equiv 1 + 1 \\ & && \equiv 2 \pmod{c} \end{aligned} \tag{5}$$

Note that $F_b \equiv 0 \pmod{c}$ iff $c = 2$, which is impossible as $2 \nmid F_n$. Thus, we have shown that Fermat numbers are pairwise coprime. It follows that each Fermat number has at least one unique prime factor, but since there are infinitely many Fermat numbers, this means there are also infinitely many prime numbers. □

2.3. *Analytic Proof Using Euler Product*

In general, for any Dirichlet series with bounded and multiplicative $a(n)$, and $\mathrm{Re}(s) > 0$

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p \in \mathbb{P}} P(p, s) \tag{6}$$

However, prior to this, in the specific case that $s = 1$ and $a(n)$ is totally multiplicative, Euler proved the following (Euler's Product Formula), formally

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p \in \mathbb{P}} \left(\sum_{i=0}^{\infty} \frac{1}{p^i} \right) = \prod_{p \in \mathbb{P}} \frac{p}{p-1} \tag{7}$$

Assume, for contradiction, that there are finitely many primes. This implies that the product is also finite, and hence the harmonic series converges. This is clearly false, which leads to a contradiction. Therefore, there must be infinitely many primes. □

2.4. *Furstenberg's Topological Proof*

Furstenberg introduced a topological proof for the infinitude of primes [1]. We define a topology on the integers $\mathbb{Z}$, where a subset $S \subseteq \mathbb{Z}$ is open if:

- it is empty, or
- for every element $a \in S$, there is an arithmetic progression $A(a, b) = \{a + bn \mid n \in \mathbb{Z}\} \subseteq S$.

Note that A is open by definition. It is also closed as it can be written as the complement of a union of open sets

$$A(a, b) = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} A(a + i, b). \tag{8}$$

Now define:

$$B = \bigcup_{p \in \mathbb{P}} A(0, p) \tag{9}$$

We know B is both open and closed, but we also know $B = \mathbb{Z} \setminus \{-1, 1\}$. If there are finitely many prime numbers, B is closed and so $\{-1, 1\}$ is open, which is not possible as it is finite. Therefore, this is a contradiction and there must be infinitely many prime numbers. □

2.5. Proof Using Pigeonhole Principle

We start by assuming there are n (finitely many) primes $p_1,\ p_2,\ p_3,\ \dots,\ p_n$. This proof utilises the fact that

$$\forall n \in \mathbb{Z}^+,\ \exists \alpha \in \mathbb{Z}^+ \text{ such that } 2^\alpha > (\alpha+1)^n$$

Choose an α satisfying this and define the following mapping:

$$f : \{1,\ 2,\ 3, \dots, 2^\alpha\} \to \{0, \dots, \alpha\}^n$$

$$f(x) := (k_1, \dots, k_n)$$

where

$$x = \prod_{i=1}^{n} p_i^{k_i} \tag{10}$$

This function is well-defined due to the unique prime factorisation of integers. Due to our original choice of α, we have that:

$$|\{1, 2, 3, \dots, 2^\alpha\}| > \left|\{0, \dots, \alpha\}^n\right| \tag{11}$$

Hence, by the Pigeonhole Principle, we know

$$\exists\, x_1, x_2 \in \{1, 2, 3, \dots, 2^\alpha\},\ x_1 \neq x_2 \text{ such that } f(x_1) = f(x_2)$$

This contradicts the FTA as it implies that there are two distinct integers with the same prime factorisation, so there must be infinitely many prime numbers. □

2.6. Proofs Using van der Waerden's Theorem

Another result we can use is van der Waerden's Theorem, which is a theorem in Ramsey Theory. Formally, it states that for any r, $\exists N(l,\ m,\ r)$ so that for any function $C : [1,\ N(l,\ m,\ r)] \to [1, r]$, $\exists\ a,\ d_1,\ \dots,\ d_m \in \mathbb{Z}^+$ such that $C(a + \sum_{i=1}^{m} x_i d_i)$ is constant on each l-equivalence class of $[1, l]^m$ [2]. If we look at C as a form of colouring, this theorem tells us that there are arbitrarily many arithmetic progressions containing integers assigned the same colour.

A proof was suggested by Alpoge [3]. Suppose there are exactly n primes, $p_1,\ p_2,\ p_3,\ \dots,\ p_n$ in increasing order. We define a function $f : \mathbb{Z}^+ \to \{0,1\}^P \times \{0,1\}^P$ by

$$f(x) = \big(\delta_p(x),\ v_p(x) \mod 2\big)_{p \in \mathbb{P}} \tag{12}$$

where

$$\delta_p(x) = \begin{cases} 1 & \text{if } p \mid x, \\ 0 & \text{if } p \nmid x, \end{cases} \tag{13}$$

and $v_p(k)$ is the exponent of p in the prime factorisation of n.

There are a finite number of colours and we can apply van der Waerden's Theorem, so we can find a monochromatic arithmetic progression $a,\ a+d,\ \dots,\ a+kd$, where $k > p_n^2$. Note that $p \mid a \implies p \mid d$, and we can show that $v_p(a) < v_p(d)$ for all p using a parity argument. This implies that $v_p(a) = v_p(a+d)$ for all p, meaning that a and $a+d$ have the same prime factorisation, contradicting FTA. □

Alternatively, using a similar idea, we could have defined the function $g(x) = \prod_{p \in \mathbb{P}} p^{(v_p(x) \mod 2)}$. We assign the same colour to x and $g(x)$. We know $|\operatorname{Im}(g)| = 2^n$ and for some $R \in \operatorname{Im}(g)$ there exists a monochromatic arithmetic progression $a,\ a+d,\ \dots,\ a+kd$, with the same colour as R, with at least four terms. It follows that $\dfrac{a}{R},\ \dfrac{a+d}{R},\ \dfrac{a+2d}{R},\ \dfrac{a+3d}{R}$ is an arithmetic progression of four square numbers, which has been proven impossible to exist by Fermat. This is once again a contradiction. □

3. Unsolved Problems

3.1. Infinitude of Mersenne Primes

Mersenne primes are prime numbers of the form $2^p - 1$, where p is itself a prime. It is clear that if p is not prime, then $2^p - 1$ is composite. This is because if $p = mn$ with $m, n > 1$, then we can factor $2^{mn} - 1$:

$$2^{mn} - 1 = (2^m - 1)(2^{m(n-1)} + 2^{m(n-2)} + \cdots + 1),$$

showing that $2^p - 1$ will have non-trivial divisors. However, this condition is necessary but not sufficient, as a simple counter-example is $2^{11} - 1 = 2047 = 23 \times 89$.

The Euclid-Euler theorem states that there is a bijection between Mersenne primes and even perfect numbers (even numbers equal to the sum of their proper divisors). Firstly, Euclid proved injectivity by showing that there exists a corresponding even perfect number $2^{p-1}(2^p - 1)$ for every Mersenne prime $2^p - 1$. Afterwards, Euler proved surjectivity by showing that every even perfect number must be of this form, and hence must correspond to a Mersenne prime.

The Lucas-Lehmer test [4], [5] is used to find the prime numbers p such that $2^p - 1$ is also prime. The first few values of p satisfying this are:

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31, \ldots$$

Despite many discoveries of large Mersenne primes (the largest so far has been $2^{136279841} - 1$) [6], it remains an open problem whether there are infinitely many such primes.

There has been substantial research on the distribution of Mersenne primes. For instance, Gillies [7] conjectured that the number of Mersenne primes less than or equal to x, denoted $M(x)$, satisfies:

$$M(x) \sim c \log x \tag{14}$$

for some constant c. Later, Lenstra, Pomerance [8], and Wagstaff [9] conjectured that:

$$M(x) \sim e^{\gamma} \log_2(\log_2 x) \tag{15}$$

where γ is the Euler–Mascheroni constant.

3.2. *Twin Prime Conjecture*

A twin prime is a prime that differs from another prime by exactly 2. Twin primes are normally given in pairs $(p,\ p+2)$, where both p and $p+2$ are prime. The first few twin prime pairs are as follows:

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ \ldots$$

Just like Mersenne primes, it is conjectured that there are infinitely many twin primes, that is

$$\liminf_{n\to\infty}(p_{n+1} - p_n) = 2 \tag{16}$$

where p_n is the n-th prime, but this has yet to be proven.

Hardy and Littlewood [10] studied the distribution of primes, and a specific case of their first conjecture states that

$$\pi_2(n) \sim 2C_2 \int_2^n \frac{dt}{(\log t)^2} \tag{17}$$

where $\pi_2(n)$ denotes the number of twin primes less than n and

$$C_2 = \prod_{\substack{q\ \in\mathbb{P} \\ q\geq 3}} \left(1 - \frac{1}{(q-1)^2}\right) \approx 0.6601618\ldots \tag{18}$$

is the twin prime constant.

Goldston, Pintz, and Yildirim [11] found that

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\sqrt{\log p_n}\,(\log\log p_n)^2} < \infty \tag{19}$$

which was the best result until Zhang [12] showed that

$$\liminf_{n\to\infty}(p_{n+1} - p_n) < 7 \times 10^7 \tag{20}$$

Maynard [13] improved this bound even more to

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 600 \tag{21}$$

In fact, he also showed that if the Elliott-Halberstam conjecture [14] was proven true, the bound will reduce greatly to

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 12 \tag{22}$$

which could be a great step towards solving the conjecture.

4. Conclusion

The infinitude of primes is a foundational result with many beautiful and varied proofs. Understanding these proofs not only solidifies fundamental mathematical knowledge but also provides tools and inspiration for addressing deeper conjectures in prime number theory. By analysing and developing these methods, we may come closer to resolving open problems that have stood for centuries.

Conflict of Interest

Author declares no conflict of interest.

References

[1] Furstenberg H. On the infinitude of primes. *American Mathem Mont*. 1955;62(5):353.
[2] Graham RL, Rothschild BL. A short proof of van der Waerden's theorem on arithmetic progressions. *Proc American Mathem Soc*. 1974;42(2):385–6.
[3] Alpoge L. van der Waerden and the primes. *American Mathem Mont*. 2015;122(8):784–5.
[4] Lehmer DH. An extended theory of Lucas' functions. *Ann Mathemat*. 1930;31(3):419–48.
[5] Lucas E. Théorie des fonctions numériques simplement périodiques. *American J Mathem*. 1878;1(2):289–321.
[6] Great Internet Mersenne Prime Search (GIMPS). Mersenne prime number discovery-$2^{136279841}-1$ is Prime! [Internet]. 2024 [cited 2025 Mar 20]. Available from: https://www.mersenne.org/primes/?press=M136279841.
[7] Gillies DB. Three new Mersenne primes and a statistical theory. *Mathemat Computat*. 1964;18(85):93–7.
[8] Pomerance C. Recent developments in primality testing. *Mathemat Intellig*. 1981;3(3):97–105.
[9] Wagstaff SS. Divisors of Mersenne numbers. *Mathemat computat*. 1983;40(161):385–97.
[10] Hardy GH, Littlewood JE. Some problems of 'Partitio numerorum'; III: on the expression of a number as a sum of primes. *Acta Mathematica*. 1923;44(1):1–70.
[11] Goldston DA, Pintz J, Yildirim CY. Primes in tuples I. *Annf Mathemat*. 2009;170(2):819–62.
[12] Zhang Y. Bounded gaps between primes. *Ann Mathemat*. 2014;179(3):1121–74.
[13] Maynard J. Small gaps between primes. *Ann mathemat*. 2015;181(1):383–413.
[14] Elliott PD, Halberstam H. A conjecture in prime number theory. *Symposia mathematica*. 1968;4:59–72.