International Journal of Engineering and Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 12 Issue 9 September 2023 || PP 33-37

An arithmetic function and some proofs of infinitude of primes

Samir Kumar Biswas
[1] *Assistant Professor, Department of Mathematics*
Surendranath College, 24/2 M.G. Road Kol-09
samir_biswas123@rediffmail.com

ABSTRACT : *In this paper we intend to prove three different methods to establish the infinitude of prime numbers.*
KEYWORDS : ***P****rime number, Arithmetic function*

Date of Submission: 06-09-2023 Date of Acceptance: 18-09-2023

I. INTRODUCTION

In this article we are going to discuss three distinct, ingenious proofs to establish infinitude of primes. One has been done by using a special arithmetic function. In basic number theory the most fascinating question is how to establish the infinitude of primes. This question had been raised first by Euclid, way back in 300 BC. He showed that the number of primes is actually infinite. In the last twenty three centuries many Mathematicians provided different fascinating proofs to establish the infinitude of primes. Mathematicians are till now overwhelmed in the study of prime numbers to find new avenues to prove that the number of primes is actually infinite. In this article, we intend to discuss three completely different methods to establish the infinitude of prime numbers.
There are several proofs. Some different approaches to prove were given by Euclid [4], Saidak [6] and Goldbach. Here we establish three different proofs.

We presume the following : $\mathbb{N}$= the set of natural numbers, P = the set of primes, gcd(a,b) = the greatest common divisor of the positive integers a and b, P_n= set of all primes dividing the natural number n, [x]= the greatest integer $\leq$ x for all real number x.

Some preliminary discussions regarding number theory are in order:
The greatest common divisor or gcd of two positive integers a and b is defined to be the positive integer d which divides a and b and for any common divisor c of a and b, c divides d.

A mapping $f: \mathbb{N} \to \mathbb{R}$ is said to be multiplicative if for any m,n $\in \mathbb{N}$ with gcd(m,n) = 1, $f(mn) = f(m)f(n)$. The mapping f is said to be completely multiplicative if for any m,n$\in \mathbb{N}$, $f(mn) = f(m)f(n)$.
The fundamental theorem of arithmetic states that every positive integer is either 1 or a prime or it can be expressed as a product of primes and the representation is unique up to the order of factors.

For any two integers a and b and for any positive integer d if d∣a and d∣b, then d∣ (ax+by) for any two integers x and y.

For any two natural numbers a,b and any prime p if p∣ab, then either p∣a or p∣b.

Any natural number n>1 has a prime factor.

For all n$\in \mathbb{N}$ a set S(n) is defined by
S(n) = {m$\in \mathbb{N}$: $P_m \subset P_n$ }, We say n generates the set S(n) or n generates the integers m, where $P_m \subset P_n$. **(1.1)**
Since $P_1 = \varphi$, S(1) = {1}.
We define a mapping $\xi: \mathbb{N} \to \mathbb{R}$ by

$$\xi(n) = \sum_{m \in S(n)} \frac{1}{m} \text{ , for all n} \in \mathbb{N} \qquad \textbf{(1.2)}$$

Obviously $\xi(1) = 1$. Let n>1and $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$, where $\{p_1, p_2, \ldots\ldots\ldots, p_k\}$ is a set of distinct primes and the integers $\alpha_i > 0$ for all i = 1,2,3,.....,k. So $P_n = \{p_1, p_2, \ldots\ldots\ldots, p_k\}$ and

$$\xi(n) = \sum_{P_m \subset P_n} \frac{1}{m} = \sum_{\beta_1 \geq 0, \beta_2 \geq 0, \ldots\ldots, \beta_k \geq 0} \frac{1}{p_1^{\beta_1} p_2^{\beta_2} \ldots\ldots p_k^{\beta_k}}$$

$$= \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \ldots\ldots\right)\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \ldots\ldots\right)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\left(1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \frac{1}{p_k^3} + \ldots\ldots\right)$$

$= \frac{p_1}{p_1 - 1}\frac{p_2}{p_2 - 1}\ldots\ldots\ldots\ldots\frac{p_k}{p_k - 1}$ which is a finite real number. Therefore the infinite series $\sum_{P_m \subset P_n} \frac{1}{m}$ is convergent for all n∈ ℕ. Thus the mapping $\xi: \mathbb{N} \to \mathbb{R}$ is well defined.

Theorem (1.1) : For any p∈ P and any n∈ ℕ, $\xi(p^n) = \xi(p) = \frac{p}{p-1}$.

Proof: Clearly for any prime p and for any natural number n, $S(p^n) = S(p)$. So $\xi(p^n) = \xi(p)$. Now $S(p) = \{1, p, p^2, p^3, \ldots\ldots\ldots\}$ and hence $\xi(p) = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots\ldots\ldots\ldots\ldots = \frac{p}{p-1}$

Therefore $\xi(p^n) = \xi(p) = \frac{p}{p-1}$

Theorem (1.2) : For all m,n∈ ℕ, $P_m \subset P_n \Rightarrow \xi(m) \leq \xi(n)$ and $P_m = P_n \Rightarrow \xi(m) = \xi(n)$.

Proof: Obvious

Theorem (1.3) : ξ is multiplicative and for all m,n∈ ℕ, $\xi(mn) = \frac{\xi(m)\xi(n)}{\xi(d)}$, where d = gcd(m,n) which implies that ξ is not completely multiplicative.

Proof:) Let m,n∈ ℕ with gcd(m,n) = 1. Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ and $n = q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots\ldots q_l^{\beta_l}$,

$P_m = \{p_1, p_2, \ldots\ldots\ldots, p_k\}$ is a set of distinct primes and the integers α_i >0 for all i = 1,2,3,.....,k. Also $P_n = \{q_1, q_2, \ldots\ldots\ldots, q_l\}$ is a set of distinct primes and the integers β_j >0 for all j = 1,2,3,.....,l. Since gcd(m,n) = 1, $\{p_1, p_2, \ldots\ldots\ldots, p_k\} \bigcap \{q_1, q_2, \ldots\ldots\ldots, q_l\} = \varphi$.

Therefore $\xi(m) = \frac{p_1}{p_1 - 1}\frac{p_2}{p_2 - 1}\ldots\ldots\ldots\frac{p_k}{p_k - 1}$ and

$$\xi(n) = \frac{q_1}{q_1 - 1}\frac{q_2}{q_2 - 1}\ldots\ldots\ldots\frac{q_l}{q_l - 1}.$$

$$P_{mn} = P_m \bigcup P_n = \{p_1, p_2, \ldots\ldots\ldots, p_k, q_1, q_2, \ldots\ldots\ldots, q_l\}$$

$$\xi(mn) = \frac{p_1}{p_1 - 1}\frac{p_2}{p_2 - 1}\ldots\ldots\ldots\frac{p_k}{p_k - 1}\frac{q_1}{q_1 - 1}\frac{q_2}{q_2 - 1}\ldots\ldots\ldots\frac{q_l}{q_l - 1} = \xi(m)\xi(n)$$

Hence the function ξ is multiplicative.

Let gcd(m,n) = d and $d = q_1^{\beta_1} q_2^{\beta_2} .....q_l^{\beta_l}$. Also let $m = p_1^{\alpha_1} p_2^{\alpha_2} .....p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} .....q_l^{\beta_l}$ and $n = r_1^{\gamma_1} r_2^{\gamma_2} .....r_s^{\gamma_s} q_1^{\beta_1} q_2^{\beta_2} .....q_l^{\beta_l}$, p_i, q_j, r_t are distinct primes and $\alpha_i \geq 1, \beta_j \geq 1, \gamma_t \geq 1$ for all $1 \leq i \leq k, 1 \leq j \leq l, 1 \leq t \leq s$.

$$\xi(mn) = \xi\left(p_1 p_2 ....p_k q_1 q_2 ....q_l r_1 r_2 ....r_s\right) = \frac{p_1}{p_1 - 1}\frac{p_2}{p_2 - 1}.....\frac{p_k}{p_k - 1}$$

$$\frac{q_1}{q_1 - 1}\frac{q_2}{q_2 - 1}.....\frac{q_l}{q_l - 1}\frac{r_1}{r_1 - 1}\frac{r_2}{r_2 - 1}.....\frac{r_s}{r_s - 1}$$

$$= \left(\frac{p_1}{p_1 - 1}\frac{p_2}{p_2 - 1}.....\frac{p_k}{p_k - 1}\frac{q_1}{q_1 - 1}\frac{q_2}{q_2 - 1}.....\frac{q_l}{q_l - 1}\right)$$

$$\left(\frac{q_1}{q_1 - 1}\frac{q_2}{q_2 - 1}.....\frac{q_l}{q_l - 1}\frac{r_1}{r_1 - 1}\frac{r_2}{r_2 - 1}.....\frac{r_s}{r_s - 1}\right)$$

$$/\left(\frac{q_1}{q_1 - 1}\frac{q_2}{q_2 - 1}.....\frac{q_l}{q_l - 1}\right) = \frac{\xi(m)\xi(n)}{\xi(d)}$$

Thus the function ξ is not completely multiplicative.

Theorem (1.4) : $\xi(n) = \dfrac{n}{\varphi(n)}$ for all n∈ ℕ, where φ is Euler's totient.

Proof: Let $n = p_1^{\alpha_1} p_2^{\alpha_2} .....p_k^{\alpha_k}$; $p_1, p_2, ..., p_k$, are distinct primes and $\alpha_i \geq 1$ for all i = 1,2,3,.....,k.

$$\xi(n) = \frac{p_1}{p_1 - 1}\frac{p_2}{p_2 - 1}.....\frac{p_k}{p_k - 1} = \frac{1}{\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)} = \frac{n}{n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)} = \frac{n}{\varphi(n)}$$

Lemma (1.1): If 2,3,5,7,.....,p is the complete list of primes less than n(>3), then 2.3.5.7…….p>n.
Proof: We shall prove the lemma by induction on n>3. For n = 4: 2, 3 are only primes less than 4 and 2.3 = 6 > 4. So the result is true for n = 4. Let the result be true for n = m where m>3. Let 2,3,5,....., p be the complete list of primes less than m and 2.3.5……..p >m.
We shall show that the result is true for n = m+1.
Case1. Let m be a prime.
Then 2,3,5,.....,p,m is the complete list of primes less than m+1.
2.3.5……p>m. So 2.3.5……..p.m > m.m > m.3 = m+2m>m+1.

Case2. Let m be a composite number. So m has a prime factor q in {2,3,5,.....,p} and 2,3,5,.....,p is the complete list of primes less than m+1 since 2,3,5,.....,p is the complete list of primes less than m. Now
2.3.5……p>m
2.3.5…….p ≥ m+1
If 2.3.5……..p = m+1, then q∣(2.3.5……p) and q∣m imply q∣{(2.3.5…….p) - m}. Thus q∣1 or, q = 1 which is a contradiction since q is a prime. Hence 2.3.5…….p > m+1.
So in any case the result is true for n = m+1. Hence by induction the result is true for all n>3.

Theorem 1.5: For any n>1 there exists at least one prime between n and 2^n.

Proof: For all $n \in N$ with n>1, $\xi(n)$ = sum of reciprocals of all the natural numbers generated by n = sum of reciprocals of all natural numbers having prime factors in n.

For any natural number n>1, $\xi(n!) = \sum_{m \in S(n!)} \frac{1}{m} > 1 + \frac{1}{2} + \frac{1}{3} + \ldots\ldots\ldots\ldots + \frac{1}{n}$

Let n be >7.

$\xi(n!) = \xi(2)\xi(3)\xi(5)\xi(7)\xi(11)\xi(13)\ldots\ldots\xi(p)$, where p is the largest prime dividing n!.

Or, $\xi(n!) < \frac{2}{2-1}.\frac{3}{3-1}.\frac{5}{5-1}.\frac{7}{7-1}.\frac{8}{8-1}.\frac{9}{9-1}\ldots\ldots\ldots\frac{n}{n-1} = \frac{5n}{8}$

But $\xi(2^n!) > 1 + \frac{1}{2} + \frac{1}{3} + \ldots\ldots + \frac{1}{n} + \ldots\ldots\ldots + \frac{1}{2^n} = \log 2^n + \gamma_{2^n}$ where γ_{2^n} is Euler's constant and $0 < \gamma_{2^n} < 1$ for all $n \in N$.

Hence $\xi(2^n!) > n \log 2 > \frac{5n}{8}$.

Therefore,

$\xi(2^n!) > \xi(n!)$.

So there exists at least one prime between n and 2^n when n>7.

It is very obvious to check that the result is true for n = 2,3,4,5,6,7.

Therefore the theorem is true for all n>1.

Corollary (1.1): The number of primes is infinite.

Alternative proof of infinitude of primes (1):

Let n be any integer greater than 3. Let 2,3,5,7,.....,p be the list of all primes less than n. By lemma **(1.1)** we have 2.3.5……..p > n. Hence all the primes less than n cannot be the factors of n.

If n is a composite number, then each prime factor of n belongs to {2,3,5,.....,p}. Therefore $P_n \underset{\neq}{\subset} P_{n!}$ i.e

$P_n \subset P_{n!}$ and $P_n \neq P_{n!}$.

If n be a prime then obviously $P_n \underset{\neq}{\subset} P_{n!}$ as n is one of the prime factors of n! for n>3.

Thus

$P_n \underset{\neq}{\subset} P_{n!} \underset{\neq}{\subset} P_{(n!)!} \underset{\neq}{\subset} P_{((n!)!)!} \underset{\neq}{\subset} P_{(((n!)!)!)!} \underset{\neq}{\subset} \ldots\ldots\ldots\ldots$ is a strictly ascending infinite sequence of sets of primes.

Hence the number of primes is infinite.

Alternative proof of infinitude of primes (2):

Let the number of primes be finite and $p_1, p_2, \ldots\ldots, p_n$ be the complete list of primes where p_i, $(1 \le i \le n)$ be the i-th prime.

Let $\frac{1}{p_1} + \frac{1}{p_2} + \ldots\ldots\ldots + \frac{1}{p_{n-1}} + \frac{1}{p_n} = \frac{a}{b}$ where a,b are positive integers and gcd(a,b) = 1.

Case1. If $p_1, p_2, p_3, \ldots\ldots\ldots\ldots\ldots, p_n$ are all in the factorization of b, then none of $p_1, p_2, p_3, \ldots\ldots\ldots\ldots\ldots, p_n$ can be a factor of a since gcd(a,b) = 1. This implies that a =1 as $p_1, p_2, p_3, \ldots\ldots\ldots\ldots\ldots, p_n$ is the complete list of primes. So

$\frac{1}{p_1} + \frac{1}{p_2} + \ldots\ldots\ldots + \frac{1}{p_{n-1}} + \frac{1}{p_n} = \frac{1}{p_1 p_2 \ldots\ldots\ldots p_{n-1} p_n}$.

Obviously the above result is not true since

$\frac{1}{p_i} > \frac{1}{p_1 p_2 \ldots\ldots\ldots p_{n-1} p_n}$ for all i = 1,2,3,.....,n or , $\frac{1}{p_1} + \frac{1}{p_2} + \ldots\ldots\ldots + \frac{1}{p_{n-1}} + \frac{1}{p_n} > \frac{1}{p_1 p_2 \ldots\ldots\ldots p_{n-1} p_n}$

Case2. If at least one of $p_1, p_2, p_3, \ldots\ldots\ldots\ldots, p_n$ is not in the factorization of b, then let p_i $(1 \le i \le n)$ be not in the factorization of b.

Then $\frac{a}{b}\left(p_1 p_2 \ldots . p_{i-1} p_{i+1} \ldots\ldots p_n\right)$ is an integer.

Now

$$\frac{a}{b}-\left(\frac{1}{p_1}+\frac{1}{p_2}+\ldots\ldots+\frac{1}{p_{i-1}}+\frac{1}{p_{i+1}}+\ldots\ldots+\frac{1}{p_n}\right)=\frac{1}{p_i}$$

$$\frac{a}{b}\left(p_1 p_2 \ldots . p_{i-1} p_{i+1} \ldots\ldots p_n\right)-\left(p_1 p_2 \ldots . p_{i-1} p_{i+1} \ldots\ldots p_n\right)\left\{\frac{1}{p_1}+\frac{1}{p_2} \ldots .+\frac{1}{p_{i-1}}+\frac{1}{p_{i+1}}+\ldots .+\frac{1}{p_n}\right\} \quad \textbf{(1.3)}$$

$$=\frac{1}{p_i}\left(p_1 p_2 \ldots . p_{i-1} p_{i+1} \ldots\ldots p_n\right)$$

Now

$\frac{p_1 p_2 \ldots . p_{i-1} p_{i+1} \ldots\ldots p_n}{p_j}$ is an integer for all j = 1,2,3,...i-1,i+1,...n.

Since $p_1, p_2, p_3, \ldots\ldots\ldots\ldots, p_n$ is a list of distinct primes, $\frac{p_1 p_2 \ldots . p_{i-1} p_{i+1} \ldots\ldots p_n}{p_i}$ cannot be an integer.

Therefore the left hand side of **(1.3)** is an integer whereas the right hand side is a rational fraction. Thus we are at a contradiction. Hence the number of primes is infinite.

Corollary (1.2) : For any natural number n>2, there exists a prime between n and n!.

Proof: Although it is an immediate consequence of Theorem **(1.5)** but one can prove this nice proven result by applying ξ function.

Obviously the result is true for n = 3,4,5,6 and 7. For $n \ge 8$, $\xi(n!) < n-1$ and

$$\xi\left((n!)!\right) > 1+\frac{1}{2}+\frac{1}{3}+\ldots\ldots\ldots+\frac{1}{n!} > \log n!$$

Now by Stirling's formula $n! = \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n+\frac{\theta}{12n}}$, where $0 < \theta < 1$.

So $\log n! = \log\sqrt{2\pi} + \left(n+\frac{1}{2}\right)\log n - n + \frac{\theta}{12n} > \left(n+\frac{1}{2}\right)\log e^2 - n + \frac{\theta}{12n}$, since $n \ge 8 > e^2$.

Or, $\log n! > 2n+1-n+\frac{\theta}{12n} > n$.

Again $\xi(n!) < n-1$ and $\xi\left((n!)!\right) > n$ imply there exists at least one prime between n and n!.

It also proves that the number of primes is infinite.

II. CONCLUSION

There are many proofs of infinitude of primes. In most cases it is observed that the way of establishing the infinitude of primes is to show that there exists a prime greater than a given prime or greater than each of a given set of primes. Which imply that the number of primes is infinite. In the first proof it has also been done but a certain interval has been determined in which the next prime belongs. The basic fact that has been applied in the second proof is to show for any natural number n>3 the product of primes less than n is strictly greater than n which produces a simple infinite sequence of sets of primes.

REFERENCES

[1]. P. RIBENBOIM, THE BOOK OF PRIME NUMBER RECORDS, SPRINGER-VERLAG, NEW YORK, 1988.
[2]. P. Pollack and E. Trevi˜no, "The primes that Euclid forgot," Amer. Math. Monthly 121 (2014), 433–437.
[3]. Burton, David M. Elementary Number Theory. 6th ed. New York, NY: McGraw-Hill, 2007
[4]. Euclid, and Thomas Little Heath. The Thirteen Books of Euclid's Elements. New York: Dover Publications, 1956.
[5]. Koshy, Thomas. Elementary Number Theory with Applications. San Diego: Harcourt/Academic, 2002.
[6]. F. Saidak, A New Proof of Euclid's Theorem, The American Mathematical Monthly 113(10): 937–938, 2006.