International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Proofs of the Infinitude of Prime Numbers Using the Euler Totient Function and the Mobius Function

Tabsum B

Assistant Professor, Department of Mathematics, Government College of Arts, Science and Commerce Quepem Goa, India

Abstract: ***What's particularly striking about this collection of proofs is how elegantly they extend Euclid's ancient logic using more modern number-theoretic tools like the Euler's totient and Möbius functions. Rather than simply reiterating the infinitude of primes, the author reshapes the argument with a fresh lens-employing parity-based reasoning and properties of coprimality to construct numbers that inevitably lead to contradiction if the list of primes were finite. This suggests that arithmetic functions-though defined based on known primes-can paradoxically reveal unknown ones. It is evident that this approach bridges classical and contemporary methods, offering a pedagogically rich and logically refined pathway to explore prime distribution. While some steps may benefit from tighter formalism, especially in transitions between cases, the underlying structure showcases a meaningful fusion of intuition and rigor. That said, the way parity, coprime constructs, and prime decomposition converge here opens up a thoughtful avenue for future inquiry-perhaps even toward generalizations using other multiplicative functions. One cannot help but wonder: could similar logic extend to primes in specific congruence classes or to more complex algebraic structures?***

Keywords: Euler's Totient Function, Mobius Function, Coprimality, Infinitude of Primes, Parity argument

Proof 1

Using the properties of Euler Totient function property
Property: $\varphi(n)$ is even $\forall\, n \geq 3$

Let there be finitely many primes
Say $p_1, p_2, p_3, \dots, p_k$ $(i.e. 2,3,5,7, \dots, p_k)$

Let $N = p_1 p_2 p_3 \dots p_k$
Consider the number $N+4$, clearly $N+4 > 3$ and is not a prime number as 2 is its factor.

Any prime number that divides $N+4$ will be among one of the above finite numbers of prime numbers, say p_i for some $1 \leq i \leq k$
i.e. $p_i | (N+4)$, also $p_i | N \Rightarrow p_i | (N+4-N) \Rightarrow p_i | 4 \Rightarrow p_i = 2$
for if $\exists\, p_j \neq 2$ for some $1 \leq j \leq k$ such that $p_j | (N+4)$, also $p_j | N \Rightarrow p_j | (N+4-N) \Rightarrow p_j | 4 \Rightarrow p_j = 2 \Rightarrow\Leftarrow$
$\therefore$ the only prime factor of $N+4$ is 2

$$\Rightarrow \varphi(N+4) = (N+4)\left(1-\frac{1}{2}\right) = (N+4)\left(\frac{1}{2}\right)$$
$$= p_2 p_3 \dots p_k + 2$$

considering $p_1 = 2$
$\Rightarrow \varphi(N+1)$ is odd $\because p_2 p_3 \dots p_k + 2$ is odd $\Rightarrow\Leftarrow$ (as $\varphi(n)$ is even $\forall\, n \geq 3$)

Proof 2

Let there be finitely many primes
Say $p_1, p_2, p_3, \dots, p_k$ $(i.e. 2,3,5,7, \dots, p_k)$
Let $N = p_1 p_2 p_3 \dots p_k$
Consider the number $N+1$, clearly $N+1 > 1$
If $N+1$ is a prime, then it is one among the listed primes say p_i $1 \leq i \leq k$
But p_i is also a factor of $N \Rightarrow (N, N+1) = p_i$ $\Rightarrow\Leftarrow$

Also if $N+1$ is composite, then any prime factor of $N+1$ will be among one of the above finite number of primes listed above, say p_j for some $1 \leq j \leq k$

$\Rightarrow (N, N+1) \neq 1 \Rightarrow\Leftarrow$

Proof 3

Let there be finitely many primes
Say $p_1, p_2, p_3, \dots, p_k$ $(i.e. 2,3,5,7, \dots, p_k)$
Let $N = p_1 p_2 p_3 \dots p_k$
Then $\varphi(N) = \varphi(p_1 p_2 p_3 \dots p_k) = (p_1-1)(p_2-1)(p_3-1)\dots(p_k-1)$ (even)
Consider the number $N+1$, clearly $N+1 > 1$
If $N+1$ is a prime, then it is one among the listed primes say p_i for some $1 \leq i \leq k$
Then $\varphi(N+1) = \varphi(p_i) = (p_i - 1)$ (even)

$$\varphi\big(N(N+1)\big) = N(N+1)\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\dots\left(1-\frac{1}{p_k}\right)$$
$$= N(N+1)\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\left(\frac{p_3-1}{p_3}\right)\dots\left(\frac{p_K-1}{p_k}\right)$$
$$= N(N+1)\left(\frac{(p_1-1)(p_2-1)(p_3-1)\dots(p_k-1)}{N}\right)$$
$$= (N+1)(p_1-1)(p_2-1)(p_3-1)\dots(p_k-1)$$
$$= p_i(p_1-1)(p_2-1)(p_3-1)\dots(p_i-1)\cdots(p_k-1)\ \cdots(1)$$
$$\varphi(N)\varphi(N+1) = (p_1-1)(p_2-1)(p_3-1)\dots(p_i-1)\cdots(p_k-1)\,(p_i-1)$$
$$= (p_1-1)(p_2-1)(p_3-1)\dots(p_i-1)^2\cdots(p_k-1)\ \cdots(2)$$

Since N and $N+1$ are relatively prime, we have $\gcd(N, N+1) = 1$
$\Rightarrow\ \varphi\big(N(N+1)\big) = \varphi(N)\varphi(N+1)$
$\Rightarrow\ p_i(p_1-1)(p_2-1)(p_3-1)\dots(p_i-1)\cdots(p_k-1) = (p_1-1)(p_2-1)(p_3-1)\dots(p_i-1)^2\cdots(p_k-1)$
$\Rightarrow\ p_i = (p_i - 1)$
$\Rightarrow\ 1 = 0\ \Rightarrow\Leftarrow$
If $N+1$ is not a Prime number, and since $N+1 > 1 \Rightarrow N+1$ is a composite number

By fundamental Theorem of Arithmetic, $N+1$ has a prime factor say p_j for some $1 \leq j \leq k$

Clearly,

$$\varphi\big(N(N+1)\big) = N(N+1)\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\dots\left(1-\frac{1}{p_k}\right)$$
$$= N(N+1)\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\left(\frac{p_3-1}{p_3}\right)\dots\left(\frac{p_K-1}{p_k}\right)$$
$$= N(N+1)\left(\frac{(p_1-1)(p_2-1)(p_3-1)\dots(p_k-1)}{N}\right)$$
$$= (N+1)(p_1-1)(p_2-1)(p_3-1)\dots(p_k-1)$$
$$\varphi(N)\varphi(N+1) = (p_1-1)(p_2-1)(p_3-1)\dots(p_i-1)\cdots(p_k-1)\,\varphi(N+1)$$

Since N and $N+1$ are relatively prime, we have $\gcd(N, N+1) = 1$
$\Rightarrow \varphi\big(N(N+1)\big) = \varphi(N)\varphi(N+1)$
$\Rightarrow (N+1)(p_1-1)(p_2-1)(p_3-1)\dots(p_k-1) = (p_1-1)(p_2-1)(p_3-1)\dots(p_i-1)\cdots(p_k-1)\,\varphi(N+1)$
$\Rightarrow N+1 = \varphi(N+1)$
$\Rightarrow N+1 = 1 \Rightarrow N = 0 \Rightarrow\Leftarrow$

Proof 4

Suppose there are finitely many Prime numbers
Say $p_1, p_2, p_3, \dots, p_k$ ($i.e.$ 2,3,5,7, … , p_k)
Let $N = p_1p_2p_3 \dots p_k$
$\Rightarrow$ for any $n > N$, the only possible prime factors of n are $p_1, p_2, p_3, \dots$ and p_k
$n > N$
$\Rightarrow n > p_1p_2p_3 \dots p_k$
Suppose n is a Prime number
$\Rightarrow n = p_j$ for some $1 \le j \le k$
$\Rightarrow p_j > p_1p_2p_3 \dots p_k$
$\Rightarrow p_j > p_1p_2p_3 \dots p_k$
$\Rightarrow 1 > p_1p_2p_3 \cdots p_{j-1}p_{j+1} \cdots p_k$
$\Rightarrow 1 < \dfrac{1}{p_1p_2p_3 \cdots p_{j-1}p_{j+1} \cdots p_k} \Rightarrow\Leftarrow$
Suppose n is not a prime number
Clearly $n > 1 \Rightarrow n$ is a composite number
$\Rightarrow n$ has a Prime factor say p_j for some $1 \le j \le k$
$\Rightarrow n = mp_j$
$\Rightarrow mp_j > N(\because n \ge N)$
$\Rightarrow mp_j > p_1p_2p_3 \cdots p_{j-1}p_j\,p_{j+1} \cdots p_k$
$\Rightarrow m > p_1p_2p_3 \cdots p_{j-1}p_{j+1} \cdots p_k$
If m is a Prime, by the previous argument, we get $1 < \frac{1}{Q}$ where Q is a product of prime numbers listed, a contradiction
If m is not a prime then, it is composite, as $m > 1$
By the same argument we get
$\Rightarrow m_1 > p_1p_2p_3 \cdots p_{j-1}p_{j+1} \cdots p_{l-1}p_{l+1} \cdots p_k$
Where $m = p_l m_1$, for some $1 \le l \le k$
Continuing with the same argument, we reach a stage where the smallest factor of m is prime and this prime number is one of the prime numbers listed on the right-hand side of the inequality
$\Rightarrow 1 >$ product of primes $\Rightarrow\Leftarrow$

Proof 5

Suppose there are finitely many Prime numbers
Say $p_1, p_2, p_3, \dots, p_k$ ($i.e.$ 2,3,5,7, … , p_k)
Let $N = p_1p_2p_3 \dots p_k$
$\mu(N) = (-1)^k$
Consider $N+1$
Clearly $N+1 > 1$
If $N+1$ is a prime, then it must be one of prime numbers listed above say p_j for some $1 \le j \le k$.
$\Rightarrow \mu(N+1) = \mu(p_j) = -1$
Also $\because$ both N and $N+1$ have prime factor p_j
$\Rightarrow N(N+1)$ has a factor ${p_j}^2$
$\Rightarrow \mu(N(N+1)) = 0$
Since N and $N+1$ are relatively prime, we have $\gcd(N, N+1) = 1$
$\Rightarrow \mu\big(N(N+1)\big) = \mu(N)\mu(N+1)$
$\Rightarrow 0 = (-1)^{k+1} \Rightarrow\Leftarrow$
If $N+1$ is not a prime, then it must be composite
Clearly it must have a prime factor which is one of prime numbers listed above say p_j for some $1 \le j \le k$.
Then there are three cases
$\mu(N+1) = 0$ or $\mu(N+1) = 1$ or $\mu(N+1) = -1$
Also $\because$ both N and $N+1$ have prime factor p_j
$\Rightarrow N(N+1)$ has a factor ${p_j}^2$
$\Rightarrow \mu(N(N+1)) = 0$
Since N and $N+1$ are relatively prime, we have $\gcd(N, N+1) = 1$
$\Rightarrow \mu\big(N(N+1)\big) = \mu(N)\mu(N+1)$
$\Rightarrow 0 = (-1)^{k+1}$ when $\mu(N+1) = -1 \Rightarrow\Leftarrow$
Or $0 = (-1)^k$ when $\mu(N+1) = 1 \Rightarrow\Leftarrow$
For the third case $\exists\, {p_i}^r, r > 1$ for some $1 \le i \le k$ such that ${p_i}^r | (N+1)$
$\Rightarrow p_i | (N+1)$
Also $p_i | N$ $p_i | (N+1-N) \Rightarrow p_i | 1 \Rightarrow p_i = 1 \Rightarrow\Leftarrow$

Results

The above proofs illustrate how the Euler totient function and Mobius function, though defined in terms of the prime factorization, can itself be used to produce a number coprime to, ensuring the discovery of a new prime. The use of the property even odd provides a simple parity argument enhancing Euclid's logic. The argument may inspire further exploration of other multiplicative functions (such as the sum-of-divisors function $\sigma(n)$) in relation to the distribution of primes.

References

[1] Euclid, Elements, Book IX, Proposition 20.
[2] H. Davenport, The Higher Arithmetic, Cambridge University Press, 2008.
[3] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 2008.
[4] W. Narkiewicz, The Development of Prime Number Theory: From Euclid to Hardy and Littlewood, Springer, 2000.
[5] T. Apostol, Introduction to Analytic Number Theory, Springer, 1976.