Group Theoretic Proof of Infinitude of Primes

Nazrul Haque

Abstract

There are numerous proofs on infinitude of primes using various tools. Starting from Euclid[1] to the analytical proofs given by Euler[2] and Paul Erdos[3]. The attractive proofs like **one line proof** by Northshield[4] and **topological proof** by Furstenberg[5] also fascinated the readers. We give here another proof of infinitude of primes using group theoretic argument.

Lemma. *If there are finitely many primes namely $p_1, p_2, p_3, ..., p_r$, and $n = p_1.p_2.p_3....p_{r-1}$, also $n-1 = p_1.p_2.p_3...p_{r-1} - 1$ then $\mid U(n) \mid = 2$, $\forall n > 2$ where, the group of units $U(n)$ is the set of numbers less than n and relatively prime to n under the operation multiplication modulo n and $n \in \mathbb{N}$.*

Proof. Assume that, $\mid U(n) \mid > 2$.

Then there exists at least one $k \in U(n)$ other than $n-1$ such that k is not a new prime.

Since, $gcd(k,n) = 1 \implies k \neq \prod_{i=1}^{r} {p_i}^{m_i}$, $(m_i \in \mathbb{Z}^+)$.

Otherwise, $gcd(k,n) \neq 1 \implies k \notin U(n)$

It's only possible if $k = n-1$ or k is a new prime. Both of these cases contradicts our assumption.

Since, k is arbitrary there is no such $k \in U(n) \implies \mid U(n) \mid = 2$. □

Theorem. *There are infinitely many primes.*

Proof. From the preceding section, it's clear that, $\mid U(n) \mid = 2$, if the number of primes are finite.

It's known that, there are infinitely many $U(n)$ groups where the number of non-identity elements in $U(n)$ that satisfy the equation,

$$x^4 = 1.$$

is a multiple of 4 i.e. $\mid U(n) \mid = 4s + t$, for infinitely many n where s and t are arbitrary constants.

But, here in this case, $\forall n, \mid U(n) \mid = 2$ i.e. there is only one non-identity element that satisfies the equation. (**contradiction**)

Hence, it is proved that, primes can not be finite. So, there are infinite number of primes.

□

Summary:

The upper proof looks quite similar in flavor with Euclid's proof. But, in that proof the basic idea was - greatest common divisor of two consecutive natural numbers is one. Thus, there exists at least one more distinct prime.

We have constructed our proof in such a way that, it does not required the G.C.D of two consecutive numbers. Also, we have used a little bit different approach to show that there must exist at least 3 different primes rather than $\{p_1, p_2, ..., p_r\}$ that satisfy $x^4 = 1$ in $U(n)$.

References

[1] Meštrović, Romeo. (2012). Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.–2012) and another new proof.

[2] W. Dunham, Euler: The Master of Us All, MAA, 1999

[3] Aigner, M. Ziegler, G.M. (1998), Proofs from The Book, Springer, Berlin

[4] Sam Northshield, A One-Line Proof of the Infinitude of Primes, The American Mathematical Monthly, 122(5), p. 466

[5] H. Fürstenberg, On the Infinitude of Primes, Amer. Math. Monthly 62 (1955), 353