Group Theoretic Proof of Infinitude of Primes

Lemma. *If there are finitely many primes namely $p_1, p_2, p_3, ..., p_n$, and $n = p_1.p_2.p_3....p_{n-1}$, and $n - 1 = p_1.p_2.p_3...p_{n-1} - 1$ then $| U(n) |= 2$, $\forall n > 2$ where $U(n)$ is a group under multiplication modulo n and $n \in \mathbb{N}$.*

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

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

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

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 $k \in U(n) \implies | U(n) |= 2$. □

Theorem. *There are infinitely many primes.*

Proof. From the preceding section, it's clear that, $| U(n) |= 2$, 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. $| U(n) |= 4q + r$, for infinitely many n where q and r are arbitrary constants.

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

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

□