

Proof the Seventh for CS250

Powered by L^AT_EX 2_ε

Molly Novash

February 24, 2017

This document will provide proof of the following statement:

For all natural numbers n where $n > 2$, there is a prime number p such that $n < p < n!$.

$$\forall n, n > 2 \in \mathbb{N} \exists p \in \mathbb{P}(n < p < n!) \quad (1)$$

Proof. We shall attempt to prove the preceding statement by cases.

We are trying to prove that for any natural number n which is greater than 2, there is a prime number between n and $n!$. As long as n is greater than 2, there are always a minimum of 2 natural numbers between n and $n!$ (as in the case of 3 and 3!, or 3 and 6, wherein the 2 natural numbers are 4 and 5; as n increases, so does the number of natural numbers between n and $n!$). Because of this, we know that $n < n! - 1 < n!$.

Therefore, by cases, we will consider whether or not there is a prime factor of $n! - 1$ which is greater than n . If there is in both cases, we will have proven that there are an infinite number of primes.

Case 1: $n! - 1$ is prime

This is the trivial case. We have already concluded that $n < n! - 1 < n!$, so if $n! - 1$ is prime, then it itself is our prime number between n and $n!$.

Case 2: $n! - 1$ is composite

If $n! - 1$ is composite, then by the definition of prime factorization, we know that it can be divided by at least one prime number.

If we can prove that the prime number it can be divided by is greater than n , and we know that $n! - 1$ is less than $n!$, then we will have proven that there is always a prime number between n and $n!$ when $n! - 1$ is composite.

Consider the definition of $n! \dots$

$$n! = 1 * 2 * 3 * 4 * \dots * n - 1 * n \quad (2)$$

By this definition, we know that $n!$ is divisible by every number less than and including n . However, if we take 1 away from $n!$, it can no longer be divisible by any of the natural numbers less than and including n and greater than 2 (which we defined in our original statement). For example, if you have a number divisible by 3, you need to add or subtract a multiple of 3 for that number to remain divisible by 3, and so on for all of the increasing natural numbers, as we have concluded in previous proofs. Here, we are only changing the value of $n!$ by one digit, so $n!$ will not be modified enough to remain divisible by numbers greater than 1.

This means that any factors of $n!$ where $n > 2$ are not factors of $n! - 1$. However, by the definition of prime factorization, we know that if $n! - 1$ is composite, it *must* have at least one prime factor in it. Therefore, we can conclude that the prime factor in the composite number $n! - 1$ *must* fall between n and $(n! - 1 - 1)$. Since $(n! - 1 - 1)$ is also greater than n and less than $n!$, we have proven that when $n! - 1$ is composite, it always contains a prime factor greater than n .

Thus, where $n! - 1$ is composite ...

$$n < p < n! - 1 < n! \tag{3}$$

By proving that there is always a prime factor of $n! - 1$, be it $n! - 1$ itself or a factor of $n! - 1$ that is greater than n , we have proven that there are infinitely many prime numbers. \square