

Theorem 1 (Divisibility by a Prime). *Any integer $n > 1$ is divisible by a prime number.*

Theorem 2. *For all integers n , if $n > 2$ then there is a prime number p such that $n < p < n!$*

Proof. Assume that n is an integer greater than 2 and that p is a prime number such that $p \mid (n! - 1)$ [by the prime divisibility theorem] and that $p \leq n$. Then, by definition of factorial, $p \mid n!$. So,

$$n! \equiv 0 \pmod{p} \quad (1)$$

However, by assumption since $p \mid (n! - 1)$ we can say,

$$n! - 1 \equiv 0 \pmod{p} \quad (2)$$

Manipulating the left hand side of (1) to match (2) gives,

$$\begin{aligned} n! &\equiv 0 \pmod{p} \\ n! - 1 &\equiv 0 - 1 \pmod{p} \\ n! - 1 &\equiv -1 \pmod{p} \\ \implies 0 &\equiv -1 \pmod{p} \end{aligned} \quad (3)$$

But, in order for equation 3 to be true p must be equal to 1 [for the sake of modular arithmetic assume our domain to be \mathbb{Z}^+]. Thus we have reached a contradiction since $p \leq n$ and $n > 2$ so $p \neq 1$. So, $p > n$ and $p \mid (n! - 1) \implies p \leq (n! - 1)$. Because $(n! - 1) < n!$, we know that $p \leq (n! - 1) < n!$ so, $n < p < n!$ [which was to be proved.] ■