

4.42 Theorem. (Converse of Wilson's Theorem) If n is a natural number greater than 1 such that $(n-1)! \equiv -1 \pmod{n}$, then n is prime.

Proof. Recalling Theorem 4.41, if n is prime, then we are done. Suppose n is not prime. This means there is a number that divides n ; let that number be an integer a where $1 < a < n$. By definition of the hypothesis, $n \mid (n-1)! + 1$. Since $a \mid n$, $a \mid (n-1)! + 1$. Since $a \mid (n-1)!$ and $a > 1$, TDA says that $(n-1)! + 1$ divided by a leaves a remainder of 1, a contradiction. Thus, for the theorem to be true, n must be prime. \square