# Wilson's Theorem

2307kishanshukla

January 2018

## 1 Theorem Statement

Wilson's Theorem states that a natural number n ( n > 1 ) is a prime number iff

$$( n - 1 )! \equiv -1 \pmod{n}$$

## 2 Proof (By contradiction)

Assuming n a composite number, we will show a contradiction.If n is composite then n must have a divisor d such that d <= ( n - 1 ) . But since ( n - 1 )! is product of integers from 1 to n-1 , the product must contain d ,thus divisible by d. So , we have

$$( n - 1 )! \equiv 0 \pmod{d}$$

Also,

$$( n - 1 )! \equiv 0 \not\equiv -1 \pmod{d}$$

since d | n , contradicting the hypothesis . So, n can't be composite,hence prime.

HENCE PROVED..