Wilson's Theorem

Pratyush Singh

February 2018

1 Introduction

Wilson's theorem helps to determine whether a positive integer is prime or not with the help of (number-1) factorial

2 Statement

Wilson's theorem states that a positive integer n is prime iff (n-1)! = nk-1 for some positive integer k

3 Proof

Here we will prove both way implication one by one in cases

3.1 case 1

given $(n-1)! = nk-1$ for some positive integer k we will prove that n is prime.

if possible let n be a composite number. this means $\exists$ a number $d < n-1$ such that n mod d is zero. hence $(n-1)! = md-1$ for some m ϵ N. hence (n-1)! mod d = -1. but since (n-1)! is divisible by d hence its mod with d is zero. therefore we arrive at a contradiction. hence n has to be prime.

3.2 case 2

given n is prime we have to prove $(n-1)! = nk-1$ for some k ϵ N

for n=2 it can be verified easily.

now consider $n > 2$ and n is odd.now by lagrange's identity for every $a < n$ a (a not equal to 1 or n-1) $\exists$ $a' < n$ such that aa' mod n = 1 . hence $(n-1)!$ = 1x$(n-1)$x(nm$_1$+1).....x(nm_i+1) $where i = (n-3)/2$.

rhs of above equation can be simplified to (n-1)x(zn+1) where z is a natural number,which can be further written as kn-1, where $k = zn + 1 - z$. hence proved.