Wilson's Theorem

Utkarsh Maken

February 2018

1 Statement:

Wilson's Theorem states that if integer p>1,then (p-1)! is divisible by p if and only if p is prime.

2 PROOF:

:

Let p be a prime.Consider the field of integers modulo by p.By Fermat's Little Theorem,every non zero element of this field is a root of the polynomial

$$P(x) = x^{p-1} - 1$$

Since this field has only p-1 non zero elements,it follows that

$$x^{p-1} - 1 = \prod_{r=1}^{p-1}(x - r)$$

Now either p=2 in which case $a \equiv -a(mod 2)$for any integer a,or (p-1) is even.In either case $(-1)^{p-1} \equiv 1(modp)$,so that

$$x^{p-1} - 1 = \prod_{r=1}^{p-1}(x - r) = \prod_{r-1}^{p-1}(-x + r)$$

If we set x=0,the theorem follows...