Wilson's Theorem

Bhavita

1st Feburary 2018

1 Theorem

Wilson's Theorem states that a natural number $p > 1$ is a prime number if and only if

$(p-1)! \equiv -1$ (mod p)

2 Proof

We use the fact that if a polynomial $f(X)$ has integer coefficients, degree d and there are more than d values of $a \in \{0, 1, 2.....p-1\}$ with $f(a) \equiv 0$(mod p) then all the coefficients of f are multiples of p.(It is essential that p be prime for this to be hold!).

We apply this observation to the polynomial

$$f(X) = X^{p-1} - 1 - (X-1)(X-2)....(X-(p-1)) = X^{p-1} - 1 - \prod_{p=1}^{k}(X-k)$$

If we substitute $X = a$ for $a \in \{1, 2, 3...., p-1\}$ in the product above,one of the factors become zero.Hence for $a \in \{1, 2...p-1\}$,

$$f(a) = a^{p-1} - 1 \equiv 1 - 1 = 0 \text{ (mod p)}$$

by Fermat's little theorem.The degree of f is less than p-1 as the coefficient of $X^{p-1}$is $1 - 1 = 0$.As there are p-1 solutions of $f(a) \equiv 0(modp)in\{1, 2, 3...p-1\}$,then all the coefficients of f are divisible by p. It follows that $f(0) \equiv 0$ (mod p) that is

$$0 \equiv -1 - \prod_{k=1}^{p-1}(-k) = -1 - (-1)^{p-1}\prod_{k=1}^{p-1}(k) = -1 - (p-1)! \text{ (mod p)}$$

On rearranging we get

$$(p-1)! \equiv -1 \text{ (mod p)}$$

Hence proved!!