07/5/2020

Date:

Page:

Wilson's Thm:- If p is a prime then

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

Proof:- Let p be a prime and let a be an integer such that $1 \le a \le p-1$, and $(a, p) = 1$, Therefore, the congruence

$$ax \equiv 1 \pmod{p}$$

has a unique solution $\pmod{p}$ Let this solution be 'b'

Then $ab \equiv 1 \pmod{p}$,

if $b \equiv a \pmod{p}$ then

$$a^2 \equiv 1 \pmod{p}$$

$\Rightarrow p \mid (a^2-1)$

$\Rightarrow p \mid (a-1)$ or $p \mid (a+1)$

$\Rightarrow a \equiv 1 \pmod{p}$ or $a \equiv p-1 \pmod{p}$

Now there is an integer b' such that

$$bb' \equiv 1 \pmod{p}$$

$b \in \{2, 3, \ldots, p-2\}$.

Continuing we get

$$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p}$$

$$\Rightarrow (p-2)! \equiv 1 \pmod{p}$$

$$\Rightarrow (p-1)(p-2)! \equiv (p-1) \pmod{p}$$

$$\Rightarrow (p-1)! \equiv -1 \pmod{p}$$

Converse of Wilson's Thm:- If $(m-1)! + 1$ is divisible by m then m is a prime.

Proof:- Let $(m-1)! + 1$ be divisible by m. Then we have to show that m is a prime.

Suppose if possible m is a composite number and it has a divisor $d > 1$. Then

$1 \leq d \leq m-1 \Rightarrow d$ divides $(m-1)!$

but d does not divide $(m-1)! + 1$

$\Rightarrow m$ does not divide $(m-1)! + 1$

but this is a contradiction. Hence m must be a prime.

(ex)- Show that 17 is a prime by showing that $16! \equiv -1 \pmod{17}$

we have

$2.9 \equiv 1 \pmod{17}$

$3.6 \equiv 1 \pmod{17}$

$4.13 \equiv 1 \pmod{17}$

$5.7 \equiv 1 \pmod{17}$

$8.15 \equiv 1 \pmod{17}$

$10.12 \equiv 1 \pmod{17}$

$11.14 \equiv 1 \pmod{17}$

Multiply these relations we have

$$15! \equiv (2.9)(3.6)(4.13)(5.7)(8.15)(10.12)(11.14)$$
$$\equiv 1 \pmod{17}$$

$$\therefore 16! = 16.15!$$
$$\equiv 16 \pmod{17}$$
$$\equiv -1 \pmod{17}.$$

Thus $(p-1)! \equiv -1 \pmod{p}$ for $p = 17$.

Thus by Wilson the 17 is a prime