Wilson's Theorem:-

If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof:-

For $p=2$, $(p-1)! = 1! = 1 \equiv -1 \pmod{2}$

$p=3$, $(p-1)! = 2! = 2 \equiv -1 \pmod{3}$

Let $p > 3$.

Consider, $ax \equiv 1 \pmod{p}$.

This congruence has a unique solution, for all $a \in \{1, 2, \cdots, p-1\}$, as $p \nmid a$.

If x is solution, then $x = a^{-1} \pmod{p}$.

Let $a^{-1} = a$ for some a, $1 \le a \le p-1$.

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

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

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

$\Rightarrow a-1=0$ or $a+1=p$.

$\left(\because \begin{array}{l} a-1=p \Rightarrow a=p+1 \\ a+1=0 \Rightarrow a=-1 \end{array}\right)$

$\therefore a=1$ or $a=p-1$

$\therefore$ The congruence $ax \equiv 1 \pmod p$ has a unique solution for each a, $1 \le a \le p-1$ and $x=a$ only for $a=1$ and $a=p-1$.

$\Rightarrow$ Each of $2, 3, 4, \ldots, p-2$ has inverse $\pmod p$ which is distinct from itself.

$\therefore 2 \times 3 \times 4 \times \cdots (p-2) \equiv 1 \pmod p$

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

Multiplying by $(p-1)$, we get

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

i.e., $(p-1)! \equiv -1 \pmod{p}$.

Ex:- $p=17$, $2^{-1} \equiv 9 \pmod{17}$

$2 \times 9 \equiv 1 \pmod{17} \Rightarrow 9 \times 2 \equiv 1 \pmod{17}$

$3 \times 6 \equiv 1 \pmod{17} \Rightarrow 6 \times 3 \equiv 1 \pmod{17}$

$4 \times 13 \equiv 1 \pmod{17} \Rightarrow 13 \times 4 \equiv 1 \pmod{17}$

$5 \times 7 \equiv 1 \pmod{17} \Rightarrow 7 \times 5 \equiv 1 \pmod{17}$

$8 \times 15 \equiv 1 \pmod{17} \Rightarrow 15 \times 8 \equiv 1 \pmod{17}$

$10 \times 12 \equiv 1 \pmod{17} \Rightarrow 12 \times 10 \equiv 1 \pmod{17}$

$11 \times 14 \equiv 1 \pmod{17} \Rightarrow 14 \times 11 \equiv 1 \pmod{17}$

$1 \times 1 \equiv 1 \pmod{17}$ and

$16 \times 16 \equiv 1 \pmod{17}$

$\therefore 2 \times 3 \times 4 \times \cdots \times 15 \equiv 1 \pmod{17}$

$\Rightarrow 15! \equiv 1 \pmod{17}$

$\Rightarrow 16! \equiv -1 \pmod{17}$

Converse (of Wilson's theorem)

If $(n-1)! \equiv -1 \pmod{n}$, then n is a prime.

Proof :- If n is composite, then, n must have a divisor d, $1 < d < n$.

$\Rightarrow (n-1)! \equiv -1 \pmod{d}$, as $d \mid n$.

$\Rightarrow d \mid (n-1)! + 1$. , which is not possible, as $d \mid (n-1)!$

$(\because (n-1)! = 1 \times 2 \times \cdots \times d \times \cdots \times (n-1))$

Theorem :- The quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution if and only if the odd prime p is

such that $p \equiv 1 \pmod 4$.

Proof :- Let a be a solution of $x^2+1 \equiv 0 \pmod p$.

$\Rightarrow a^2 \equiv -1 \pmod p$.

By F.L.T., $a^{p-1} \equiv 1 \pmod p$.

$(\because p \nmid a)$

$\Rightarrow (a^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$

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

If $p \equiv 3 \pmod 4$, then $p = 4k+3$, for some k.

$\Rightarrow \frac{p-1}{2} = 2k+1$.

$\Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$

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

$\Rightarrow p \mid 2$, not possible as $p \neq 2$.

$\therefore p \equiv 1 \pmod{4}$

Conversely, let $p \equiv 1 \pmod{4}$

$\Rightarrow p = 4k+1$, for some k.

Now, $(p-1)! = 1 \cdot 2 \cdot \cdots \cdots (p-1)$

$= 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \cdots (p-1)$

We have,

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

$p-2 \equiv -2 \pmod{p}$

$\vdots$

$\frac{p+1}{2} \equiv -\left(\frac{p-1}{2}\right) \pmod{p}$

$$\therefore (p-1)! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \cdots \left(\frac{p-1}{2}\right) \cdot \left(-\frac{p-1}{2}\right) \pmod{p}$$

$$\equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot \cdots \left(\frac{p-1}{2}\right)\right)^2 \pmod{p}$$

$$\equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

$$\Rightarrow -1 \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

(∵ $(p-1)! \equiv -1 \pmod{p}$, Wilson's theorem)

But, as $p = 4k+1 \Rightarrow \frac{p-1}{2} = 2k$.

$\therefore (-1)^{\frac{p-1}{2}} = 1.$

$\therefore$ we have

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}$$

$$\therefore \left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0 \pmod{p}$$

Taking $x = \left(\frac{p-1}{2}\right)!$, we get a solution for $x^2 + 1 \equiv 0 \pmod{p}$

Ex:- S.T. $18! \equiv -1 \pmod{437}$

$18! \equiv -1 \pmod{19}$ (by Wilson's Thm)

$437 = 19 \times 23.$

To show $18! \equiv -1 \pmod{23}$

But $22! \equiv -1 \pmod{23}$

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

$\Rightarrow 21! \equiv 1 \pmod{23}$

$\Rightarrow 21! \equiv 24 \pmod{23}$

$\Rightarrow 21 \times 20! \equiv 8 \times 3 \pmod{23}$

$\Rightarrow 7 \times 20! \equiv 8 \pmod{23}$

$\Rightarrow 7 \times 20 \times 19! \equiv 8 \pmod{23}$

$\Rightarrow 7 \times 5 \times 19! \equiv 2 \pmod{23}$

$\Rightarrow 7 \times 5 \times 19 \times 18! \equiv 2 \pmod{23}$

$\Rightarrow 7 \times 5 \times 19 \times 18! \equiv 25 \pmod{23}$

$\Rightarrow 7 \times 19 \times 18! \equiv 5 \pmod{23}$

$\Rightarrow 7 \times 19 \times 18! \equiv 28 \pmod{23}$

$\Rightarrow 19 \times 18! \equiv 4 \pmod{23}$

$\Rightarrow 18! \equiv -1 \pmod{23}$

$\Rightarrow 23 \mid 18! + 1$, as required

$\therefore 19 \times 23 = 437 \mid 18! + 1$

Note :- $(n-1)! \equiv 0 \pmod{n}$ if n is composite, except $n = 4$.

For $n = 4$, $3! = 6 \equiv 2 \pmod{4}$

Let $n > 4$,

n is composite $\Rightarrow n = a \cdot b$.

g.c.d $(n, n-1) = 1$

$\therefore 1 < a < n-1$.

$\Rightarrow a$ is a factor in $(n-1)!$

Similarly, $1 < s < n-1$.

If $r \neq s$, Then r and s are distinct factors of $(n-1)!$

$\therefore n = r \cdot s \mid (n-1)!$

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

Let $r = s$. $\Rightarrow n = r^2$

Now $r < \frac{n}{2}$.

(∵ if $r \geq \frac{n}{2}$, then

$n = r^2 \geq n^2/4$ or $4n \geq n^2$

$\Rightarrow 4 \geq n$,

but $n > 4$).

∴ $r < \frac{n}{2}$

$\square$

$\Rightarrow 2n < n$ or $2n \leq n-1$

$\Rightarrow n$ and $2n$ are two distinct factors of $(n-1)!$

$\therefore n \cdot (2n) \mid (n-1)!$

$\Rightarrow n^2 \mid (n-1)!$

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

Ex:- Let p be an odd prime number, then prove that

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

$(p-1)! \equiv -1 \equiv p-1 \pmod{p}$ (Wilson's thm)

$\Rightarrow p \mid (p-1)! - (p-1)$

$1+2+\cdots+(p-1) = \frac{p(p-1)}{2}$

$p-1$ is even $\Rightarrow \frac{p-1}{2}$ is integer.

Moreover, $\frac{p-1}{2} < p-1$

Also, $(p-1) \mid (p-1)! - (p-1)$

$\Rightarrow \frac{p-1}{2} \mid (p-1)! - (p-1)$

Now $\gcd\left(\frac{p-1}{2}, p\right) = 1$ ($\because$ p is a prime)

$$\left.\begin{array}{l} p \mid (p-1)! - (p-1) \\ \text{and} \\ \frac{p-1}{2} \mid (p-1)! - (p-1) \end{array}\right\} \Rightarrow$$

$\Rightarrow p\left(\frac{p-1}{2}\right) \mid (p-1)! - (p-1)$

i.e., $1+2+\cdots+(p-1) \mid (p-1)! - (p-1)$

$\Rightarrow (p-1)! \equiv (p-1) \left[\text{mod } 1+2+\cdots+(p-1)\right]$

Ex:- If p is a prime, prove that for any a,

$p \mid a^p + (p-1)!\, a$ and

$p \mid (p-1)!\, a^p + a$.

For any a, $a^p \equiv a \pmod{p}$

Wilson's theorem $\Rightarrow$

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

Multiplying above,

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

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

$\Rightarrow p \mid a^p + (p-1)!\, a$

Similarly, (multiplying cross-way)

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

$$\Rightarrow p \mid a^p (p-1)! + a$$

Ex:- If p and p+2 are twin primes, then

$$4\left((p-1)! + 1\right) + p \equiv 0 \pmod{p(p+2)}$$

Wilson's theorem $\Rightarrow$

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

$$\Rightarrow (p-1)! + 1 \equiv 0 \pmod{p}$$

$$\Rightarrow 4\left[(p-1)! + 1\right] \equiv 0 \pmod{p}$$

$$\Rightarrow 4\left[(p-1)! + 1\right] + p \equiv 0 \pmod{p} \quad (*)$$

Wilson's theorem $\Rightarrow$

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

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

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

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

$$\Rightarrow p! \equiv 1 \pmod{p+2}$$

$$(\because \gcd(p+1, p+2) = 1)$$

$$\Rightarrow 4p! \equiv 4 \pmod{p+2}$$

$$\Rightarrow 4p! \equiv 4 + 2p - 2p \pmod{p+2}$$

$$\Rightarrow 4p! \equiv 2(p+2) - 2p \pmod{p+2}$$

$$\Rightarrow 4p! \equiv -2p \pmod{p+2}$$

$$\Rightarrow 4p(p-1)! \equiv -2p \pmod{p+2}$$

$$\Rightarrow 4(p-1)! \equiv -2 \pmod{p+2}$$

$$(\because \gcd(p, p+2) = 1)$$

$$\Rightarrow 4(p-1)! + (p+2) \equiv -2 \pmod{p+2}$$

$$\Rightarrow 4(p-1)! + (p+4) \equiv 0 \pmod{p+2}$$

$$\Rightarrow 4[(p-1)! + 1] + p \equiv 0 \pmod{p+2} \rightarrow (*)$$

From $(*) \Rightarrow$

p and $p+2$ divide $4[(p-1)! + 1] + p$

$$\Rightarrow p(p+2) \mid [4(p-1)! + 1] + p.$$

$$\Rightarrow 4\left(\left[(p-1)! + 1\right]\right) + p \equiv 0 \pmod{p(p+2)}$$