Thm (Wilson's thm) If p is a prime then $(p-1)! \equiv -1 \pmod{p}$

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

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

Suppose $p>3$

Consider the +ve integers

$1, 2, 3, \ldots, p-1$

and let 'a' take any one of these values. Clearly $(a,p)=1$

Hence the congruence $ax \equiv 1 \pmod{p}$ admits unique sol. for each 'a'. (say a') i.e. — (1)

$$aa' \equiv 1 \pmod{p} \quad [\text{Clearly } 1 \le a' \le p-1]$$

we have two cases

Case I $a = a' \Rightarrow a^2 \equiv 1 \pmod{p}$

$\Rightarrow a^2 - 1 \equiv 0 \pmod{p}$

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

$\Rightarrow a-1 \equiv 0 \pmod{p}$ or $a+1 \equiv 0 \pmod{p}$

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

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

Case II $a \neq a'$. Now we are left with the integers

$2, 3, 4, \ldots, p-2$

Note that from these integers we can have $(p-3)/2$ congruences of the form $aa' \equiv 1 \pmod{p}$ [$\because$ Both a & a' are selected from this list]

Multiplying all these congruences and re-arranging gives us

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

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

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

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

***Note** Converse of Wilson's theorem is also true.

"If $(n-1)! \equiv -1 \pmod{n}$ then n must be prime.

Pf. Suppose n is not prime then n has a divisor d with $1 < d < n$

Also $d \mid (n-1)!$ [$\because d \le n-1$] $\Rightarrow d \mid (n-1)! + 1$ [$\because d \mid n$]

$\Rightarrow d \mid 1 \Rightarrow$ Contradiction

Quadratic congruence

a congruence of the form $ax^2+bx+c \equiv 0 \pmod m$ $\quad a \not\equiv 0 \pmod m$

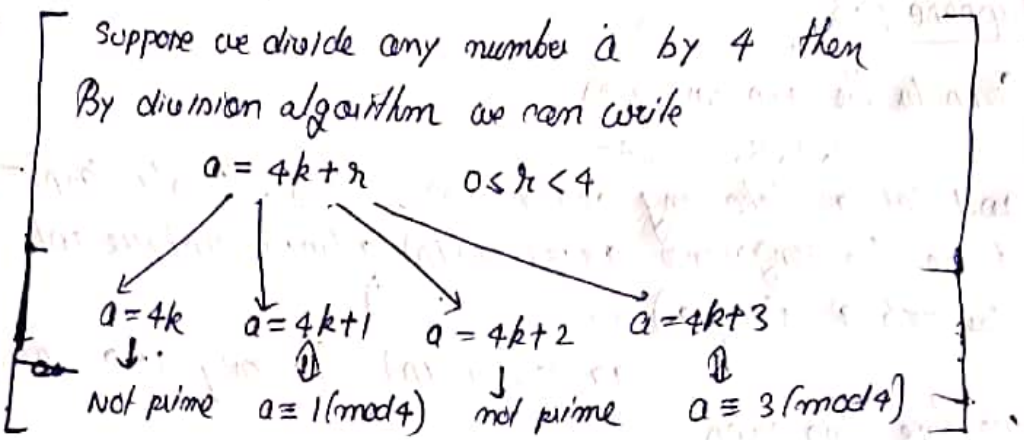
Thm 5.5 The quadratic congruence $x^2+1 \equiv 0 \pmod p$ where p is an odd prime has a sol- iff $p \equiv 1 \pmod 4$

Pf

Suppose we divide any number a by 4 then

By division algorithm we can write

$a = 4k+r \qquad 0 \le r < 4$



Suppose $x^2+1 \equiv 0 \pmod p$ has a sol- say a

Hence $a^2+1 \equiv 0 \pmod p$

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

$[\Rightarrow p \nmid a]$

$[\Rightarrow p \mid a^2+1$ $\quad p \mid a$ $\quad p \nmid a$

$p \mid a^2$

$\Rightarrow a^2 \equiv 0 \pmod p]$

Applying Fermat's theorem

$1 \equiv a^{p-1} \pmod p = (a^2)^{p-1/2} \pmod p \equiv (-1)^{p-1/2} \pmod p$

There are two possibilities for p

$p = 4k+3$; $\quad p = 4k+1$

If $p = 4k+3$ then

$(-1)^{p-1/2} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1$

Hence $1 \equiv -1 \pmod p \Rightarrow p \mid 2$

The only prime dividing 2 is 2 itself which is even

$\therefore$ $p = 4k+3$ is not possible

$\therefore$ p must be of the form $4k+1$

$\therefore$ $p = 4k+1 \Rightarrow p-1 = 4k$

$\Rightarrow 4 \mid p-1$

$\Rightarrow p \equiv -1 \pmod 4$

Conversely suppose $p \equiv 1 \pmod 4$

Consider the factorial product

$$(p-1)! = 1 \cdot 2 \cdots \underbrace{\frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1)}_{\text{Even no. of integers since } p-1 \text{ is even}}$$

Note that $\because p$ is odd $\therefore p-1, p+1$ are even and hence $\frac{p-1}{2}, \frac{p+1}{2}$ are integers. ~~Also~~

Note that

$$\left.\begin{aligned} p-1 &\equiv -1 \pmod p \\ p-2 &\equiv -2 \pmod p \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod p \end{aligned}\right\} \frac{p-1}{2} \text{ congruence}$$

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

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

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

~~$\Rightarrow$~~ Wilson's theorem gives

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

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

$\because p = 4k+1 \quad \therefore (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1$

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

Hence $\left(\frac{p-1}{2}\right)!$ is the required integer that satisfies the congruence

$$x^2 + 1 \equiv 0 \pmod p$$

Example Suppose $p = 13 = 4 \times 3 + 1$

$$\frac{p-1}{2} = 6$$

We calculate $(6!)^2 + 1 \pmod{13}$

Note that $6! = 720 \equiv 5 \pmod{13}$

$\therefore (6!)^2 + 1 = 5^2 + 1 = 26 \equiv 0 \pmod{13}$

$\therefore (6!)^2$ is a sol^n of the congruence

$$x^2 + 1 \equiv 0 \pmod{13}$$