Summation 4

22 January 2024 17:31

Wilson's Theorem :-

For any prime p, $(p-1)! \equiv -1 \pmod p$

Proof:- For $p=2$, it is true

For $p \geq 3$ (odd primes) let us consider the polynomial

$g(x) = (x-1)(x-2) \cdots (x-(p-1))$

So $g(x)$ is of degree $p-1$.

$g(x) = x^{p-1} - (1+2+\cdots+p-1)\, x^{p-2} + \cdots + (p-1)!$

It's roots are $1, 2, \ldots, p-1$.

both has leading term x^{p-1}

Now let us consider, $h(x) = x^{p-1} - 1$

degree is $p-1$

Fermat's Little theorem says that, $h(x)$ also has $p-1$ roots modulo p, that are, $1, 2, \ldots, p-1$

Let, $f(x) = g(x) - h(x)$

degree at most $p-2$ as x^{p-1} is in both $g(x)$ and $h(x)$.

But $f(x)$ also has $p-1$ roots modulo p, but it cannot have more than $p-2$ roots unless its a zero function

$\Rightarrow f(x) = 0 \Rightarrow$ coefficient are all $0 \pmod p$

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

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

Q) Let $p > 3$ be a prime. Then show that,

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

Ans :- $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1} = \frac{1}{2}\sum_{k=1}^{p-1}\left(\frac{1}{k}+\frac{1}{p-k}\right)$

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

We just need to show $1+\frac{1}{2}+\cdots+\frac{1}{p-1} \equiv 0 \pmod{p^2}$

i.e, $p^2 \mid 2\left(1+\frac{1}{2}+\cdots\frac{1}{p-1}\right)$

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

So $\frac{2}{p}\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right) = \sum_{k=1}^{p-1}\frac{1}{k(p-k)}$

We just need to show $\sum_{k=1}^{p-1}\frac{1}{k(p-k)} \equiv 0 \pmod{p}$

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

$$\sum_{k=1}^{p-1}\frac{1}{k(-k)}$$

$$\Rightarrow -\sum_{k=1}^{p-1}\frac{1}{k^2} = -\sum_{k=1}^{p-1}k^{-2} \equiv 0 \pmod{p} \text{ as } p-1 \nmid -2$$

Harmonic Modulo p :-

Harmonic Modulo p :-

For any integer $k = 1, 2, \ldots, p-1$ we have

$$\frac{1}{k} \equiv (-1)^{k-1} \frac{1}{p} \binom{p}{k} \pmod{p}$$

Proof:- Check this.