Number Theory 12

11 February 2024 17:05

Q> Let p be a prime. Show that the remainder when $(p-1)!$ is divided by $p(p-1)$ is $p-1$.

Ans:- $(p-1)! = -1 \pmod p$

$(p-1)! = pq_1 - 1$

$r = 1$

$(p-2)! = pq_2 + r$

$(p-1)! = p(p-1)q_2 + pr - r$

$= p((p-1)q_2 + r) - r$

$\Rightarrow (p-1)! = p(p-1)q_2 + (p-1)$

$S = \{1, 2, \ldots, p-1\}$ $\quad \gcd(a,p) = 1$ $\quad p$ is a prime

$aS = \{a, 2a, \ldots, (p-1)a\}$

$aS \equiv S \pmod p$

<u>Theorem</u>:- (General Equal Sets) Let n be any integer and S be the set of integers less than n and relatively prime to n. Let a be any integer coprime to n. Then,

$$aS \equiv S \pmod n$$

<u>Proof</u>:- $S = \{n_1, n_2, \ldots, n_m\} \rightarrow n_i$'s distinct

$aS = \{an_1, an_2, \ldots, an_m\}$

$an_i - an_j \equiv a(n_i - n_j) \pmod n$

$\not\equiv 0 \pmod n$

$\Rightarrow$ All an_i's are distinct

an_i's $\pmod n \equiv K < n$

$\gcd(an_i, n) = 1$

$aS \equiv S \pmod{n}$

Unsigned

$x = (b_{n-1} b_{n-2} \cdots b_2 b_1 b_0)_2$

$x = 2^{n-1} b_{n-1} + 2^{n-2} b_{n-2} + \cdots + 2b_1 + b_0$

Signed

$-2^{n-1} < x < 2^{n-1}$ i.e., x is of n bits

$(1\, b_{n-2} \cdots b_1 b_0)_2 = -(2^{n-2} b_{n-2} + \cdots + 2b_1 + b_0)$

$(0\, b_{n-2} \cdots b_1 b_0)_2 = (2^{n-2} b_{n-2} + \cdots + 2b_1 + b_0)$

Two's Complement :-

x is of n bits.

$0 \le x < 2^{n-1}$ $\Rightarrow$ use x unsigned form

$-2^{n-1} \le x < 0$ $\Rightarrow$ use $2^n - |x|$ unsigned form

Two's complement of $x \equiv x \pmod{2^n}$

x is of n bits

Euler's Theorem :-

Let $|S|$ be the number of elements in S. S is a set of all relatively prime integers to n and less than n. Let $\gcd(a,n) = 1$.

Then,

$$a^{|S|} \prod_{\substack{1 \le i < n \\ \gcd(i,n)=1}} (i) \equiv \prod_{\substack{1 \le i < n \\ \gcd(i,n)=1}} (i) \pmod{n}$$

Product of all numbers in S

$\Rightarrow a^{|S|} \equiv 1 \pmod{n}$

Here $|S|$ is the Euler's totient function.

$\varphi(n) = |S|$ = no. of integers less than n and coprime to n.

$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Theorem:- Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Then,

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)$$

$$\varphi(n) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_m^{\alpha_m-1} (p_1-1)(p_2-1)\cdots(p_m-1)$$

Lemma:- φ is multiplicative, i.e., for any two coprime integers m, n we have,

$$\varphi(mn) = \varphi(m)\varphi(n)$$

$\varphi(4) = 2$

$\varphi(2) = 1$

$\Rightarrow \varphi(4) \neq \varphi(2)\varphi(2)$ as 2, 2 are not coprime.

Theorem:- Let $n \geq 2$ be any integer and a be any coprime integer to n. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$

Q> Show that $n \mid (2^{n!}-1)$ $\forall\, n \equiv 1 \pmod{2}$