Number Theory 13

18 February 2024 16:54

Q) Find the value of $\gcd(n!+1, (n+1)!)$

Ans:– If $n+1$ is prime then $n! \equiv -1 \pmod{n+1} \Rightarrow n!+1 \equiv 0 \pmod{n+1}$

Let there be a prime p such that $p \mid (n!+1)$ and $p \mid (n+1)!$

Then $p \nmid n!$ but $p \mid (n+1)! \Longrightarrow p \mid (n+1)$

Then if $(n+1)$ is prime then $(n+1) \mid (n!+1) \Rightarrow \gcd(n!+1, (n+1)!) = n+1$

$p \nmid n! \Rightarrow p \geq n+1$ & $p \mid (n+1) \Rightarrow p = n+1 \Rightarrow \gcd(n!+1, (n+1)!) = n+1$ iff $n+1$ is prime

else $\gcd(n!+1, (n+1)!) = 1$

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

Ans:– $\gcd(n, 2) = 1$

$\Rightarrow 2^{\varphi(n)} \equiv 1 \pmod n$

$a^k \equiv g \pmod n \Rightarrow a^{kh} \equiv g^h \pmod n$

$\Downarrow$

$\varphi(n) < n \Rightarrow \varphi(n) \mid n! \Rightarrow 2^{\varphi(n)} \equiv 1 \pmod n$

$\Rightarrow 2^{n!} \equiv 1 \pmod n$

$\Rightarrow 2^{n!} - 1 \equiv 0 \pmod n$

$n \mid (2^{n!} - 1)$

General Inverses:–

Theorem:– Let $n \geqslant 2$ be any positive integer. Then every number a with $\gcd(a, n) = 1$ has an inverse, that is a number x such that $ax \equiv 1 \pmod n$. $x = a^{-1}$

- If $\gcd(a, n) \neq 1$ then it is not necessary to have an inverse

[illegible] $\equiv 1$ [illegible] $a = 2$

• If $\gcd(a,n) \neq 1$ then it is not necessary to have an inverse

Example, $n=6$, $a=2$

In (mod 6) $2\times1=2$, $2\times2=4$, $2\times3=6$, $2\times4=8$, $2\times5=10$

<u>Lemma</u>:- If n is a natural number and a is an integer, then a has an inverse if and only if $\gcd(a,n)=1$. In particular if $\gcd(a,n)>1$, then a does not have an inverse.

<u>Proof</u>:- $\gcd(a,n)=1 \Rightarrow$ a has an inverse is already shown.

$\gcd(a,n)>1 \Rightarrow d|a,\ d|n$ for $d=\gcd(a,n)$

for inverse to exist $ax=nk+1$ should be necessary

$\Rightarrow \quad ax-nk=1 \Rightarrow d|(ax-nk)$ and so $d|1$

$\Rightarrow d=1$

$\Rightarrow \Leftarrow$ Contradiction

<u>HomeWork</u>:- Do the other side of if and only if condition

Q> $\gcd(a,n)=1$. Find $\gcd(a^{-1},n)$.

Ans:— $ax \equiv 1 \pmod n$

$x \equiv a^{-1} \pmod n$

Using above lemma we get x has an inverse $\Rightarrow \gcd(x,n)=1$

$\Rightarrow \gcd(a^{-1},n)=1$

<u>HomeWork</u>:- Let a,m,n be integers and d satisfies,

$a^m \equiv 1 \pmod d$ and $a^n \equiv 1 \pmod d$.

Then show that, $a^{\gcd(m,n)} \equiv 1 \pmod d$

Let a and b be integers and p be a prime then prove that,

<u>HomeWork</u>:- Let a, b be integers and p be a prime then prove that,

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$