Number Theory 22

19 December 2024 18:41

Modular Arithmetics :-

$a, b \in \mathbb{Z}$

$$a \mid b \iff b \equiv 0 \pmod{a}$$

"$b \equiv b \pmod{a}$" what does it mean?

$0 \equiv 0 \pmod{a}$ → universally true statement

Remainder of b when divided a is the $\underline{\text{smallest } r}$ s.t. $r \geq 0$ and $b \equiv r \pmod{a}$

→ $b, a \in \mathbb{Z}^+$

$a \in \mathbb{Z}$, $0 \pmod{a}$, $1 \pmod{a}$, $2 \pmod{a}$, ..., $a-1 \pmod{a}$

are the residue classes

The k^{th} residue class will be $\{k + am\}_{m \in \mathbb{Z}}$

$b \equiv c \pmod{a}$, $d \equiv e \pmod{a}$

$\Rightarrow b + d \equiv c + e \pmod{a}$ and $bd \equiv ce \pmod{a}$

$\Rightarrow b^k \equiv c^k \pmod{a}$

$\Rightarrow kb \equiv kc \pmod{a}$

Q> Let p be a prime and a, b are coprime, then show that,

$$\gcd\left(\frac{a^p + b^p}{a+b}, a+b\right) \in \{1, p\}$$

Ans:-
$$\frac{a^p + b^p}{a+b} = \underline{a^{p-1}} \underline{- a^{p-2}b} + \underline{a^{p-3}b^2} - - - + b^{p-1}$$

$$\underline{a^{p-1} + a^{p-2}b - 2a^{p-2}b - 2a^{p-3}b^2 + 3a^{p-3}b^2 + \cdots - (\cdot) \boxed{-(p-1)b^{p-1}}} + b^{p-1}$$

extra term

$$= \Big[\underbrace{a^{p-2}(a+b)}_{1st} \underbrace{- 2a^{p-3}b^1(a+b)}_{2nd} \underbrace{+ 3a^{p-4}b^2(a+b)}_{3rd} \underbrace{+}_{4th} \cdots \underbrace{- (p-1)b^{p-2}(a+b)}_{(p-1)th}\Big] + b^{p-1}$$

$p-1$

$$= \underbrace{a(a+b)}_{1st} \; \underbrace{\quad}_{2nd} \; \underbrace{\quad}_{3rd} \; \underbrace{\quad}_{4th} \; \underbrace{\quad}_{(p-1)th}$$

$$\frac{a^p+b^p}{a+b} = (a+b)\left(a^{p-2} - 2a^{p-3}b + \cdots - (p-1)b^{p-2}\right) + b^{p-1} + (p-1)b^{p-1}$$
$$= (a+b)(\cdots) + pb^{p-1}$$

$$\gcd\left(\frac{a^p+b^p}{a+b}, a+b\right) = \gcd(pb^{p-1}, a+b) = \begin{cases} 1 & \text{if } p \nmid (a+b) \\ p & \text{if } p \mid (a+b) \end{cases}$$
$$= \gcd(p, a+b)$$

Q) Show that $ka \equiv kb \pmod{n} \Rightarrow a \equiv b \pmod{n}$ iff $\gcd(k,n)=1$

$\gcd(k,n)=1$ given, then,

Ans:- $ka - kb \equiv 0 \pmod{n}$

Let $d \in \mathbb{Z}$ such that $k(a-b) = nd \Rightarrow k \mid d \Rightarrow a-b = \frac{nd}{k}$

$\Rightarrow a-b = nc$

$\Rightarrow a-b \equiv 0 \pmod{n}$

Given, $ka \equiv kb \pmod{n} \Rightarrow a \equiv b \pmod{n}$

Then, $ka-kb = nd_1 \Rightarrow a \equiv b \pmod{n}$

$\Rightarrow (k(a-b) = nd_1 \Rightarrow a-b = nd_2)$

This must always be true.

Now if $\gcd(k,n) = d \neq 1 \Rightarrow k(a-b) = nd_1 \Rightarrow a-b = nd_2$

if $a-b = \frac{n}{d} \Rightarrow k'd\frac{n}{d} = nd_1$ but $\frac{n}{d} \neq nd_2$

$\Rightarrow\Leftarrow$

So the case eliminated is $\gcd(k,n) \neq 1$

For $\gcd(k,n)=1$ we get $k(a-b) = nd_1 \Rightarrow n \mid k(a-b)$

$\Rightarrow n \mid (a-b) \Rightarrow a \equiv b \pmod{n}$