Gourav Jhanwar
00301427 39

04/12/18

① Given: $aR(n) = R(n) \bmod n$

To prove: $\gcd(a, n) = 1$

Proof:-

① $aR(n) = R(n) \bmod n$ — ①

Take $r, s \in R(n)$ where $r \neq s$

$\Rightarrow ar \not\equiv as \bmod n$ (from ①)

$\Rightarrow n \nmid a(r-s)$

$\Rightarrow n \nmid a \Rightarrow \gcd(a, n) = 1$

② To prove:

$$\prod_i^{\phi(n)} aR_i = \prod_i^{\phi(n)} R_i \bmod n \quad \text{where } R_i \in R(n)$$

$$= a^{\phi(n)} \prod_i^{\phi(n)} R_i$$

Proof:-

We know that

$|aR(n)| = |R(n)|$ ∴

$aR(n)$, $R(n)$ are the same set of numbers in a different order

$$\Rightarrow \prod_i^{\phi(n)} a \cdot R_i = \prod_i^{\phi(n)} R_i$$

$$\Rightarrow n \mid \prod_i^{\phi(n)} aR_i - \prod_i^{\phi(n)} R_i$$

$$\Rightarrow \prod_i^{\phi(n)} aR_i = \prod R_i \bmod n$$

$$= a^{\phi(n)} \prod_i^{\phi(n)} R_i$$