QUESTION

Let x be a primitive root modulo p where p is an odd prime and $1 \le x \le p-1$.

(i) Explain why the two sets of congruence classes mod (p),

$$\{[1],[x],[x^2],\ldots,[x^{p-2}]\} \text{ and } \{[1],[2],\ldots,[p-1]\}$$

are equal.

(ii) Using (i) or otherwise, show that if $p-1$ divides n then

$$1^n + 2^n + \ldots + (p-1)^n \equiv -1 \bmod (p).$$

(iii) Using (i) or otherwise, show that if $p-1$ does not divide n then

$$1^n + 2^n + \ldots + (p-1)^n \equiv \bmod (p).$$

(Hint: In this case $n = q(p-1)+r$ with $1 \le r \le p-2$.)

ANSWER

(i) It suffices to show that the $[x^i]=[x]^i$ are distinct for $1 \le i \le p-1$. If $x^i \equiv x^j \bmod (p)$ with $1 \le i < j \le p-1$ then $p|x^i(1-x^{j-i})$ and so $p|(1-x^{k-i})$, since $\mathrm{HCF}(p,x)=1$. Hence $x^{j-i} \equiv 1 \bmod (p)$. This implies that $p-1 = \mathrm{order}(x) \le j-i < p-1$, which is a contradiction.

(ii) By (i), the congruence class mod (p), $[1^n+2^n+\ldots+(p-1)^n]$, satisfies

$$\begin{aligned}[1^n+2^n+\ldots+(p-1)^n] &= [1]^n+[2]^n+\ldots+[(p-1)]^n \\ &= [1]^n+[x]^n+[x^2]^n+\ldots+[x^{p-2}]^n\end{aligned}$$

If $p-1$ divides n then $[x^i]^n = [x^{in}] = [1]$ since $x^{p-1} \equiv 1 \bmod (P)$ so that in this case

$$[1]^n+[x]^n+[x^2]^n+\ldots+[x^{p-1}]^n = (p-1)[1] = [p-1] = [-1]$$

as required.

(iii) When $p-1$ does not divide n we must have $n = q(p-1)+r$ for some q and some $1 \le r \le p-1$. Hence $[x^n] = [x^r]$ so that it will suffice to show that

$$[1]^r + [x]^r + [x^2]^r + \ldots + [x^{p-2}]^n = [1 + x^r + x^{2r} + \ldots + x^{(p-2)r}] = [0]$$

Since x^r is not congruent to 1 mod (p) we must have $\mathrm{HCF}(x^r - 1, p) = 1$. Therefore $[x^r - 1][y] = [0]$ if and only if $[y] = [0]$. However,

$$\begin{aligned}
& [x^r - 1][1 + x^r + x^{2r} + \ldots + x^{(p-1)r}] \\
= \ & [x^r + x^{2r} + \ldots + x^{(p-1)r} + x^{(p-1)r} - 1 - x^r - x^{2r} - \ldots - x^{(p-10r}] \\
= \ & [x^{(p-1)r} - 1] \\
= \ & [x^{p-1}]^r - [1] \\
= \ & [1] - [1] \\
= \ & [0]
\end{aligned}$$

as required.