Worksheet - 7

Ques-1:- Step-1:- To show $ord_{p^2}(g+np) = (p-1)$ or $p(p-1)$

Let $ord_{p^2}(g+np) = h$

$\Rightarrow (g+np)^h \equiv 1 \mod (p^2).$

by Eular's thm-

$$(g+np)^{\phi(p^2)} \equiv 1 \pmod{p^2}$$

$$(g+np)^{p(p-1)} \equiv 1 \pmod{p^2}$$

One can easily prove that, "if the integer a have order K modulo n. then $a^h \equiv 1 \mod n \Leftrightarrow k \mid h$".

So from the above thm-

$$h \mid p(p-1) \qquad -(i)$$

Now, $(g+np)^h \equiv 1 \pmod{p^2}$

$\Rightarrow g^h + np \cdot g^{h-1} + n^2p^2 g^{h-2} + \cdots + n^h \cdot p^h \equiv 1 \pmod{p^2}$

$\Rightarrow g^h + np\, g^{h-1} \equiv 1 \pmod{p^2}$

$\Rightarrow p^2 \mid (g^h + npg^{h-1} - 1)$

$\Rightarrow p \mid (g^h + npg^{h-1} - 1)$

$\Rightarrow g^h + npg^{h-1} \equiv 1 \pmod{p}$

$\Rightarrow g^h \equiv 1 \pmod{p}$

Since, g is a primitive root of modulo p.

So, $ord_p(g) = \phi(p) = p-1$. So, by above stated thm-

$$(p-1) \mid h \qquad -(2)$$

from (i) - $h \mid p(p-1)$

$\Rightarrow p(p-1) = k_1 h$

from (2) - $(p-1) \mid h \Rightarrow h = k_2(p-1)$

$\Rightarrow p(p-1) = k_1 k_2 (p-1)$

$\Rightarrow$ $K_1 \cdot K_2 = p$

$\Rightarrow$ $K_1 = p$ and $K_2 = 1$ or $K_2 = p$ and $K_1 = 1$

$\Rightarrow$ $h = (p-1)$ or $h = p(p-1)$

$\Rightarrow$ $\mathrm{Ord}_{p^2}(g+np) = h = (p-1)$ or $p(p-1)$

Step-2:- To show, $\mathrm{ord}_{p^2}(g+np) = (p-1)$ only for one of the p possible values of n.

(A) $f(x) = x^{p-1} - 1$

Since g is the primitive root modulo p.

$\Rightarrow$ $g^{p-1} \equiv 1 \pmod p$

$\Rightarrow$ g is a root of congruence $f(x) \equiv 0 \pmod p$

Now, $f'(x) = (p-1) \cdot x^{p-2} \Rightarrow f'(g) = (p-1)\, g^{p-2}$

We know that $p \nmid (p-1)$

and if $p \mid g^{p-2}$

$\Rightarrow$ $g^{p-2} \equiv 0 \mod p$

$\Rightarrow$ $g \cdot g^{p-2} \equiv 0 \pmod p$

$\Rightarrow$ $g^{p-1} \equiv 0 \mod p$

but $g^{p-1} \equiv 0 \pmod p$ $\in$

So, $p \nmid g^{p-2}$

$\Rightarrow$ $p \nmid (p-1)\, g^{p-2} \Rightarrow p \nmid f'(g)$.

(B) Thm- Let p be prime, a is a sol^n of $f(x) \equiv 0 \mod p^K$

(i) $p \nmid f'(a)$, then there is precisely one sol^n b of $f(x) \equiv 0 \pmod{p^{K+1}}$ s.t. $b \equiv a \pmod{p^K}$

The sol^n is given by $b = a + p^K t$, where t is the unique sol^n of $f'(a)\, t \equiv -\frac{f(a)}{p^K} \pmod p$.

So, take $K=1$, $f(x) = x^{p-1} - 1$ and $a = g, t = n$ in above thm.

Since, g is a root of the congruence
$f(x) \equiv 0 \pmod p$ and $p \nmid f'(g)$

So, by above thm.

$$f(x) = x^{p-1} - 1 \equiv 0 \pmod{p^2}$$ has

precisely one soln. and the soln given by

$$b = g + pn.$$

So, for precisely one value of n,

$$b^{p-1} - 1 \equiv 0 \pmod{p^2}$$

$$(g+pn)^{p-1} \equiv 1 \pmod{p^2}$$

$\Rightarrow$ $\text{ord}_{p^2}(g+pn) = (p-1)$ only for one of the p possible values of n.

<u>Step-3:-</u> Combine step (i) & (2).

from <u>step (i)</u> –

$$\text{ord}_{p^2}(g+np) = (p-1) \text{ or } p(p-1)$$

and from <u>step 2</u>:- $\text{ord}_{p^2}(g+np) = (p-1)$ only for one of the p posible values of n.

$\Rightarrow$ for rest $(p-1)$ values of n, $\text{ord}_{p^2}(g+np) = p(p-1)$

$\Rightarrow$ $\text{ord}_{p^2}(g+np) = \phi(p^2)$, for $(p-1)$ value of n.

$\Rightarrow$ $(g+np)$ is the primitive root modulo p^2 for exactly $(p-1)$ values of n.

<u>Ques-2:-</u> If g is primitive root modulo p^2, then to show g is a primitive root modulo p^K for all $K \geq 2$.

<u>Step-1:-</u> We will prove this by induction on $k \geq 2$.

~~Since, it~~ From the question g is primitive root modulo p^2, for it is ~~for~~ true for $K=2$.

Now, consider g is a primitive root modulo p^i $\forall i \leq K$

and we will prove that g is a primitive root modulo p^{K+1}.

(ii) we will show-

$$\text{Ord}_{p^{k+1}}\, g = p^{k-1}(p-1) \text{ or } p^k(p-1).$$

let $\text{Ord}_{p^{k+1}}\, g = h$

$\Rightarrow g^h \equiv 1 \pmod{p^{k+1}}$

by Euler's thm-

$g^{p^k(p-1)} \equiv 1 \pmod{p^{k+1}}$ [as $\phi(p^k) = p^k(p-1)$]

$\Rightarrow h \mid p^k(p-1)$ — (i)

by induction hypothesis -

g is primitive root of modulo p^k

$\Rightarrow g^{p^{k-1}(p-1)} \equiv 1 \bmod p^k$ [as $\phi(p^k) = p^{k-1}(p-1)$]

and since $g^h \equiv 1 \pmod{p^{k+1}}$

$\Rightarrow g^h \equiv 1 \pmod{p^k}$

$\Rightarrow p^{k-1}(p-1) \mid h$ — (2)

from (i) - $k_1 h = p^k(p-1)$

and (ii) $\Rightarrow h = k_2 p^{k-1}(p-1)$

$\Rightarrow k_1 \cdot k_2\, p^{k-1}(p-1) = p^k \cdot (p-1)$

$\Rightarrow p = k_1 \cdot k_2$

$\Rightarrow k_1 = p$ and $k_2 = 1$ or $k_1 = 1$ and $k_2 = p$

$\Rightarrow h = p^{k-1}\cdot(p-1)$ or $h = p^k \cdot (p-1)$

$\Rightarrow \text{Ord}_{p^{k+1}}\, g = p^{k-1}\cdot(p-1)$ or $p^k \cdot (p-1)$.

Step-2:- To show, $\text{ord}_{p^{k+1}}\, g = p^{k-1}(p-1)$ is not possible.

i.e. $g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$

Let $k \geq 3$, then by induction hypothesis.

Since g is a primitive root modulo p^{k-1}

So,

$$g^{p^{k-2}(p-1)} \equiv 1 \mod p^{k-1}$$

or we can write-

$$g^{p^{k-2}(p-1)} = 1 + ap^{k-1} \quad \text{and } p \nmid a$$

$$\Rightarrow \cancel{g^{p^{k}(p-1)}} = \cancel{\left(g^{p^{k-1}(p-1)}\right)^{p}} = \cancel{(1+ap^{k})^{p}} = \cancel{1 + a \cdot p \cdot p^{k+1}}$$

as g is primitive root modulo p^k also.

$$\Rightarrow g^{p^{k-1}(p-1)} \equiv 1 + ap^{k} \pmod{p^{k+1}} \text{ if } g^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{k+1}}$$

$$\Rightarrow p^{k+1} \mid a \cdot p^{k}$$

$$\Rightarrow p \mid a$$

Thus $g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$

$$\Rightarrow \operatorname{ord}_{p^{k+1}}(g) = p^{k-1}(p-1)$$

So, from step (i) & (2)

$$\operatorname{Ord}_{p^{k+1}}(g) = p^{k}(p-1) = \phi(p^{k+1})$$

$\Rightarrow$ g is also a primitive root modulo p^{k+1}.

Scanned with CamScanner

If $k = 3$, then-

$\text{Ord}_{p^3}\, g = p^2(p-1)$ or $p(p-1)$

Since g is a primitive root modulo p^2.

$\Rightarrow \quad g^{p-1} \not\equiv 1 \mod p^2$

by Fermat's thm -

$$g^{p-1} \equiv 1 \mod p$$

$\Rightarrow \quad g^{p-1} = 1 + bp \quad$ with $p \nmid b$

[if $p \mid b \Rightarrow p^2 \mid bp \Rightarrow$
$g^{p-1} \equiv 1 \pmod{p^2}$ - contradiction]

$$\Rightarrow \quad g^{p(p-1)} = (g^{p-1})^p$$

$$= (1+bp)^p$$

$$= 1 + \binom{p}{1} \cdot bp + \binom{p}{2} b^2p^2 + \cdots\cdots$$

$$\equiv 1 + bp^2 \pmod{p^3}$$

[$\because p > 2$
$\binom{p}{2} \equiv 0 \mod p$]

Since $p \nmid b \Rightarrow p^3 \nmid bp^2$

$$\Rightarrow \quad g^{p(p-1)} \not\equiv 1 \mod p^3$$

$\Rightarrow \quad \text{Ord}_{p^3}\, g = p^2(p-1).$