Q) Compute 3^8 modulo 13.

W.k.t. $3^2 \equiv 9 \pmod{13}$

sq

$3^4 \equiv 9^2 \equiv 81 \pmod{13}$

$\equiv 3 \pmod{13}$

sq

$3^8 \equiv 3^2 \equiv 9 \pmod{13}$

Ans: $\underline{\underline{9}}$

Q) Let $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$ then $a \equiv b \pmod{n}$ if & only if $a \equiv b \pmod{p_i^{n_i}}$ for every i. (primes p_i are assumed to be distinct)

T.P: $n \mid a$ iff $p_i^{n_i} \mid a$ $\forall i$.

<u>if</u>

if $p_i^{n_i} \mid a$, then $n \mid a$.

$\Rightarrow$ Assuming $n = p_1^{n_1} \cdots p_k^{n_k}$ & $p_i^{n_i} \mid a$ $\forall i$

Then, T.P: $n \mid a$.

Let $a = a_1 p_1^{n_1}$ & $p_2^{n_2} \mid a$ $(\because p_i^{n_i} \mid a)$

$a = a_2 p_2^{n_2}$

or, in general, $a = a_i p_i^{n_i}$ $\forall i$.

> Since $a = a_i p_i^{n_i}$ $\forall i$, while factorizing a, we prime factorize a_i such that a comes in the form of some $a_i \times p_i^{n_i}$

> Therefore if $a = \underbrace{p_1^{m_1} \cdots p_k^{m_k}}_{\text{some } m_i \text{ can be } 0} \underbrace{q_1^{l_1} \cdots q_k^{l_k}}_{\text{other prime factors}}$ is the prime factorization of 'a', we have that $m_i \geq n_i$ for each $i = 1, 2, \ldots, k$.

> As $m_i \geq n_i$ $p_i^{m_i} = k . p_i^{n_i}$

$\Rightarrow a = k . \underbrace{(p_1^{n_1} \cdots p_k^{n_k})}_{= n}$

$\Rightarrow n \mid a$

Hence, proved.

<u>only if</u>

$\Rightarrow$ $n \mid a$ only if $p_i^{n_i} \mid a$

$\Rightarrow$ whenever $n \mid a$, $p_i^{n_i} \mid a$.

True. Because, $p_i^{n_i} \mid n$ & $n \mid a$

$\Rightarrow p_i^{n_i} \mid a$

Hence, proved.