<u>Note</u>:- If $p \nmid a$, and $n \equiv m \pmod{p-1}$, then $a^n \equiv a^m \pmod{p}$.

Let $n > m \Rightarrow p-1 \mid n-m$

$$\Rightarrow n = m + c(p-1)$$

$$a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{c(p-1)} \equiv 1 \pmod{p}$$

$$\Rightarrow a^n = a^{m+c(p-1)}$$

$$\equiv a^m \pmod{p}$$

<u>Ex</u>:- $2^{1000000} \bmod 7$

$$10 \equiv 4 \pmod{6} \Rightarrow 10^2 \equiv 4^2 \equiv 16 \equiv 4 \pmod{6}$$

$$\Rightarrow 10^3 = 10^2 \cdot 10 \equiv 4 \pmod{6}$$

$$\Rightarrow 10^k \equiv 4 \pmod{6}$$

$$7 \nmid 2 \Rightarrow 2^{100000} \equiv 2^4 \pmod{7}$$

$$\equiv 16 \pmod{7}$$

$$\equiv 2 \pmod{7}$$

Note:- $(a, m) = 1$, and $n' \equiv n \pmod{\varphi(m)}$, then $a^n \equiv a^{n'} \pmod m$.

In the proof of $a^{\varphi(m)} \equiv 1 \pmod m$ whenever $(a, m) = 1$, we made use of $a^{\varphi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}}$ by repeated exponentiation of $\varphi(p_2^{\alpha_2}), \ldots, \varphi(p_r^{\alpha_r})$ to get $a^{\varphi(m)} \equiv 1 \pmod{p_1^{\alpha_1}}$

Instead we can take exponent of $\text{l.c.m}\{\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_r^{\alpha_r})\}$ to a so that

$$a^{\text{lcm}\{\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_r^{\alpha_r})\}} \equiv 1 \pmod{p_i^{\alpha_i}}$$

$$\Rightarrow a^{\text{lcm}\{\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_r^{\alpha_r})\}} \equiv 1 \pmod m$$

Ex:- $m = 105$. Let $(a, 105) = 1$.

$$a^{\varphi(105)} \equiv 1 \pmod{105}$$

i.e., $a^{48} \equiv 1 \pmod{105}$

$105 = 3 \times 5 \times 7$

$$\varphi(105) = \varphi(3) \times \varphi(5) \times \varphi(7)$$
$$= 2 \times 4 \times 6 = 48.$$

$$\text{l.c.m.}\{\varphi(3), \varphi(5), \varphi(7)\}$$
$$= \text{l.c.m.}\{2, 4, 6\} = 12$$

$$\therefore a^{12} \equiv 1 \pmod{105}$$

Compute:- $2^{1000000} \bmod 77$.

$$\varphi(77) = \varphi(7 \times 11) = 6 \times 10 = 60.$$

$$\text{lcm}(6, 10) = 30.$$

$\therefore \quad 2^{30} \equiv 1 \pmod{77}$

$1000000 = 30 \times 33333 + 10$

$2^{1000000} \equiv 2^{10} \equiv 23 \pmod{77}$

2nd method:

$$\left.\begin{aligned} 2^{1000000} &\equiv a \pmod{7} \\ 2^{1000000} &\equiv b \pmod{7} \end{aligned}\right\}$$

$2^3 \equiv 1 \pmod{7}$

$2^{1000000} = (2^3)^{33333} \cdot 2 = 2 \pmod{7}$

$$\left.\begin{aligned} 1000000 &\equiv 0 \pmod{10} \\ 2^{1000000} &\equiv 2^0 = 1 \pmod{11} \end{aligned}\right\}$$

$$\therefore \quad \left.\begin{aligned} 2^{1000000} &\equiv 2 \pmod{7} \\ 2^{1000000} &\equiv 1 \pmod{11} \end{aligned}\right\} \text{CRT}$$

$\Rightarrow \quad 2^{1000000} = 11 \times 2 \times 2 + 7 \times 8 \times 1$

$= 100 \equiv 23 \pmod{77}$

Ex:- Find the last two digits of 3^{400}.

$3^{400} \equiv ? \pmod{100}$

$\varphi(100) = \varphi(2^2 \times 5^2)$

$= 2 \times 20 = 40$

$\therefore 3^{40} \equiv 1 \pmod{100}$

$(\because \gcd(3, 100) = 1)$

$\therefore (3^{40})^{10} \equiv 1 \pmod{100}$

$\Rightarrow 3^{400} \equiv 1 \pmod{100}$

$\therefore$ '01' is the last pair of digits