Euler's theorem:

$\varphi(n) = \{1 \leq m \leq n \mid \gcd(m, n) = 1\}$

[if $n = p$ $\quad a^{p-1} \equiv 1 \bmod p$

for $n \in N$ $\quad$ & $a \in Z$ if $\gcd(a, n) = 1$

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

proof:

consider $\quad S = \{1 \leq x \leq n \mid \gcd(x, n) = 1\}$

$$= \{x_1, x_2, x_3 \ldots x_{\varphi(n)}\}$$

Take

$$a.S = \{ax_1, ax_2, \ldots ax_{\varphi(n)}\}$$

① claim $\gcd(ax_i, n) = 1$

otherwise we have a prime

$$p \mid ax_i \qquad p \mid n$$

$$\Rightarrow p \mid ax_i - n$$

$$\Rightarrow p \mid (a, n)$$

$$\Rightarrow p \mid 1$$

$\Rightarrow$ which is a contradiction

No 2 elements of aS are congruent on mod n

$$ax_i \equiv ax_j \pmod n$$

$$a(x_i - x_j) \equiv 0 \pmod n$$

$$n \mid a(x_i - x_j)$$

$$\Rightarrow n \mid x_i - x_j$$

$$\Rightarrow x_i - x_j = 0$$

$$\Rightarrow x_i = x_j$$

From ① & ②,

$aS \equiv S \pmod{n}$

$\Rightarrow a(x_1) \cdot a(x_2) \ldots a(x_{\varphi(n)}) \equiv x_1 x_2 x_3 \ldots x_{\varphi(n)} \bmod$

Let $x_1 x_2 \ldots x_n = X$

$\therefore a^{\varphi(n)} X \equiv X \bmod n$

multiplying X^{-1} on both sides,

$a^{\varphi(n)} \equiv 1 \bmod (n)$

Hence the proof