Euler's theorem.

Euler's function:— The Euler's function $\phi(n)$ represents number of elements in the set A_n where

$$A_n = \{ m \in N : 1 \le m < n \text{ s.t. } (m,n) = 1 \}.$$

$(m,n) = 1$ means m and n are relatively prime.

Example — $\phi(1) = 1$ where $A_1 = \{1\}$.

$\phi(2) = 1$ where $A_2 = \{1\}$.

$\phi(3) = 2$ as $A_3 = \{1, 2\}$.

$\phi(8) = 4$ as $A_8 = \{1, 3, 5, 7\}$.

Euler's theorem:—

Statement:— If a and m are positive integers relatively prime, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Where $\phi(m)$ represents Euler's function and $m > 1$.

Proof:— Ist We shall make use of the following results

(i) If G is a finite group and $a \in G$ then $a^{O(G)} = e$.

(ii) The set G of prime residue classes modulo m is a group of order $\phi(m)$ relative to the operation of multiplication of residue classes.

A residue class $[a]$ is called a prime residue class if a and m are relatively prime.

Now the proof of the actual theorem starts.

Let $Y = \{[a] : a \text{ is integer prime to } m\}$.

Then Y is group of order $\phi(m)$ w.r.t. the multiplication of residue classes modulo m.

Let a and m be relatively prime so that $[a] \in Y$ and its order is $\phi(m)$.

hence $[a^{\phi(m)}] = [1]$, by result (i).

This $\Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$. Proved