Euler's totient function $\phi(n)$ is defined to be the number of positive integers that are less than n and relatively prime to n.

For a prime number p : $\phi(p) = p-1$

For $n = pq$ (p and q are two prime numbers)

$$\phi(n) = \phi(pq) = pq - [(q-1)+(p-1)+1] = pq - (p+q)+1 = (p-1)\times(q-1) = \phi(p)\times\phi(q)$$

Euler's Theorem

For every a and n that are relatively prime, then $a^{\phi(n)} \bmod n = 1 \bmod n$.

Proof: Let R be the set of all integers that are less than n and relatively prime to n,

$R = \{x_1, x_2, \cdots, x_{\phi(n)}\}$

Now multiply each element by a, and then modulo n,

we get $S = \{ax_1 \bmod n, ax_2 \bmod n, \cdots, ax_{\phi(n)} \bmod n\}$

Then $R = S$ for two reasons:

1. Since a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n, Thus all the members of S are integers $\boxed{\text{less than } n}$ and they are relatively prime to n.
2. All the members of S are distinct. If $ax_i \bmod n = ax_j \bmod n$, then $x_i = x_j$ (contradiction to that all the elements in R are distinct)

Since $R = S$,

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\Rightarrow a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i = \prod_{i=1}^{\phi(n)} x_i \quad (\text{less than } n)$$

$$\Rightarrow (a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i) \bmod n = (\prod_{i=1}^{\phi(n)} x_i) \bmod n$$

$$\Rightarrow a^{\phi(n)} \bmod n = 1 \bmod n_1 \ (\text{Lemma } 1)$$