Definition: n - positive integer.

$$\varphi(n) = \left| \{ 0 \le b < n \mid g.c.d.(b, n) = 1 \} \right|$$

= no. of non-negative integers less than n and relatively prime with n.

$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$ etc.

$\varphi(p) = p - 1$ (if p is a prime)

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha - 1}$$
$$= p^\alpha \left(1 - \frac{1}{p}\right)$$

Note:- The Euler phi function is multiplicative.

i.e., $\varphi(mn) = \varphi(m)\,\varphi(n)$, whenever $gcd(m, n) = 1$.

Let $S = \{ j \in \mathbb{Z},\ 0 \le j < mn \mid (j, mn) = 1 \}$

$S_1 = \{ j_1 \in \mathbb{Z},\ 0 \le j_1 < m \mid (j_1, m) = 1 \}$

$$S_2 = \{ j_2 \in \mathbb{Z},\ 0 \le j_2 < n \mid (j_2, n) = 1 \}$$

$$|S| = \varphi(mn)$$

$$|S_1| = \varphi(m) \quad \text{and} \quad |S_2| = \varphi(n)$$

For every pair of (j_1, j_2) Chinese Remainder theorem, there is a unique j such that

$$j \equiv j_1 \pmod m$$

$$j \equiv j_2 \pmod n$$

and $0 \le j_1 < m$, $0 \le j_2 < n$,

$$0 \le j < mn.$$

For any j, $0 \le j < mn$, we have $(j, mn) = 1$ if and only if

$(j, m) = 1$ and $(j, n) = 1$.

i.e., if and only if

$(j_1, m) = 1$ and $(j_2, n) = 1$.

Thus, by counting principle,

$$|S| = |S_1| \cdot |S_2|$$

i.e., $\underline{\varphi(mn) = \varphi(m)\,\varphi(n)}$

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = p_1^{\alpha_1}\left(1 - \tfrac{1}{p_1}\right) \cdots p_r^{\alpha_r}\left(1 - \tfrac{1}{p_r}\right)$$

$$= p_1^{\alpha_1} \cdots p_r^{\alpha_r}\left(1 - \tfrac{1}{p_1}\right) \cdots \left(1 - \tfrac{1}{p_r}\right)$$

$$= \underline{\underline{n \cdot \prod_{p \mid n}\left(1 - \tfrac{1}{p}\right)}}$$

Note:- Let n be a positive integer, which is product of two distinct prime numbers. Then knowledge of $\phi(n)$ is equivalent to knowledge of two primes p and q, where $n = pq$.

Proof:- If n is even $\Rightarrow$ trivial. In fact, let $p = 2$ and $q = \frac{n}{2}$.

$$\phi(n) = \phi(q) = \frac{n}{2} - 1$$

If n is odd, then both p and q are odd.

$$\phi(n) = (p-1)(q-1) = n+1-(p+q)$$

$\Rightarrow$ knowing p and q, we can find $\phi(n)$.

Conversely, suppose we know n and $\phi(n)$, but not p or q.

Now, $p+q = n+1-\phi(n)$.

$= \underline{\underline{2b}}$ (say) (even number)

$\Rightarrow$ p and q are roots of

$x^2 - (p+q)x + (pq) = 0$

$\Rightarrow x^2 - 2bx + n = 0$

$\Rightarrow \underline{\underline{x = b \pm \sqrt{b^2 - n}}}$

$\underline{\underline{Ex}}$:- $p = 89$ and $q = 101$.

$\Rightarrow n = pq = 8{,}989$

$\phi(n) = 88 \times 100 = 8{,}800$.

$p+q = n+1-\phi(n)$

$= 8{,}990 - 8{,}800$

$= 190$

$\therefore \underline{\underline{b = 95}}$

$x = 95 \pm \sqrt{95^2 - 8989}$

$\underline{\underline{= 89, 101}}$