PROPERTIES OF EULER TOTIENT FUNCTION $\phi(n)$

- $\phi(1) = 1$, SINCE 1 ITSELF IS THE ONLY NUMBER WHICH IS CO-PRIME TO IT

- $\phi(p) = p-1$ IF p IS PRIME

PROOF: THERE ARE $p-1$ NUMBERS LESS THAN p WHICH ARE CO-PRIME TO p

$$\Rightarrow \phi(p) = p-1$$

BY DEFINITION

THEOREM: If α is integer and p is PRIME

Consider $n = p^{\alpha} \Rightarrow \phi(n) = p^{\alpha}\left(\frac{p-1}{p}\right)$

Consider the number

$p, 2p, 3p, \ldots, p^{\alpha-1}p$

These are the only numbers $\leq n$ which have the factor p, which is prime.

$\Rightarrow$ There are $p^{\alpha-1}$ numbers less than n which are divisible by p

$\rightarrow$ The rest of the numbers are co-prime to n

$$\Rightarrow \phi(n) = n - p^{\alpha-1} = p^{\alpha} - p^{\alpha-1}$$

$$\Rightarrow \phi(n) = p^{\alpha}\left(1 - \frac{1}{p}\right)$$

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

FACTORIZATION THEOREM

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

α_1, α_k integers

$p_1, \cdots, p_k$ PRIME NUMBERS

$$\phi(n) = \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k})$$

$$= p_1^{\alpha_1}\left(\frac{p_1-1}{p_1}\right) \cdots p_k^{\alpha_k}\left(\frac{p_k-1}{p_k}\right)$$

$$\rightarrow \quad \phi(n) = \left[p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right]\left(\frac{p_1-1}{p_1}\right) \cdots \left(\frac{p_k-1}{p_k}\right)$$

$$\boxed{\phi(n) = n\left(\frac{p_1-1}{p_1}\right) \cdots \left(\frac{p_k-1}{p_k}\right)}$$

THEOREM 1: IN AN ARITHMETIC PROGRESSION WITH A DIFFERENCE OF m, IF WE TAKE n TERMS AND FIND THEIR MODULO n, IF n and m are PRIME, WE WILL GET the numbers from 0 to $(n-1)$ in SOME ORDER

CONSIDER

$$\underbrace{a+0m,\ a+1.m,\ \ldots,\ a+(n-1)m}_{n \text{ terms}}$$

Example: $a=1,\ m=7,\ n=3$ (m, n co-prime)

$\rightarrow$ 3 terms are $(1, 8, 15)$

$\rightarrow$ modulus 3 of each $\rightarrow (1, 2, 0)$

PROOF: No remainder has the same value as another when performing modulo n operation on set above.

Why? Suppose there are 2 numbers with same remainder, $a+pm$ and $a+qm$ $\quad 0 \leq p, q \leq n-1$

$$\Rightarrow (a+qm)-(a+pm) \equiv 0 \mod n$$

$$m(q-p) \equiv 0 \mod n$$

m, n co-prime $\rightarrow q \equiv p \mod n$

contradiction!

THEOREM 2: IF $x > y$, x, y are co-prime, The remainder of x divided by y is co-prime to y

PROOF: $x = ky + r$

IF y, r are not coprime

$\forall d$ which divides y & r

$\rightarrow$ d divides $ky + r = a$

So d divides y, r, and x!

This is impossible because y and x are coprime.

If m, n are coprime, then

$$\phi(mn) = \phi(n)\,\phi(m)$$

$\phi(m \times n)$ GIVES THE NUMBERS COPRIME TO $m \times n$.

IF x IS CO-PRIME TO $m \times n$, THEN IT IS ALSO COPRIME TO m and n, separately.

We need to count the number of positive numbers less than or equal to $m \times n$ which are coprime to both m and n.

We build a Table with n rows and m columns

1	2	3	$\cdots$	m	n rows
$1+m$	$2+m$	$3+m$	$\cdots$	$2m$	
$1+2m$	$2+2m$	$3+2m$		$3m$	
$\vdots$	$\vdots$				
$1+(n-1)m$	$2+(n-1)m$	$3+(n-1)m$		nm	

each column is an arithmetic progression of n terms with a difference of m; m & n are co-prime (Theorem 1)

How many numbers in each column are coprime to n? $\rightarrow$ we modulo all entries in table with n $\rightarrow$ each column will then contain a permutation of numbers from 0 to $n-1$

Using Theorem 2, if the remainder of a number is coprime to n, then the number itself is coprime..

How many numbers between 0 to $n-1$ are coprime to n? 0 is the same as n in modulo n arithmetic $\rightarrow$ how many numbers between 1 to n are coprime to n, it is

$\phi(n)$ by definition.

What are the numbers coprime to BOTH n & m?

Take all elements in Table modulo m

Each row has remainder 0 to $m-1$ occuring once exactly. If we consider 0 to be m, the table $\rightarrow$ each row has values 1 to $m-1$ The table looks like

$$
n \left\{
\begin{array}{cccccc}
 & & & & & m \\
1 & 2 & - & - & - & m \\
1 & 2 & & & & \\
 & & & & & \\
 & & & & - & m \\
1 & 2 & - & - & &
\end{array}
\right.
$$

Each row has $\phi(m)$ elements coprime to m

So, we have $\phi(m)$ columns which are co-prime to m and each column has $\phi(n)$ values coprime to n.

Therefore there are
$\phi(m) \times \phi(n)$
elements which are coprime to BOTH m & n

$$\boxed{\phi(m \times n) = \phi(m) \times \phi(n)}$$

when m & n are coprime