Euler's Totient Function and Euler's Theorem

“Euler Totient Function” is mainly related to the **“Cryptography”.**

What is Euler Totient Funciton for?

The main concept with which the Euler Totient function deals is with the **prime numbers**. The main aim of it is to provide the total count of the numbers which are coprime/relative prime/mutually prime to a given number.

NOTE:

What are coprime/relative prime/mutually Prime Numbers?

These are the numbers which are having their gcd(a, n) = 1, where “n” is the actual number, & at the place of “a” there can be multiple numbers. **For Example,** let n = 7. Now all those numbers which are having their gcd with n as 1, will be called as coprime/relative prime/mutually prime to m.

In the example, numbers which are coprime to n are: {1,2,3,4,5,6}.

Let us take n = 9, in this case coprime numbers are: {1, 2, 4, 5, 7, 8}.

Notation of Euler Totient Function!

It is denoted by the “phi” symbol.

For any number “n”, Euler Totient Function will be represented as phi(n). It represents the total count of numbers which are coprime to n. In the above examples, where n = 7, there phi(n) = 6, & when n = 9, there phi(n) = 6.

Euler's Totient Function and Euler's Theorem

The shortcut of calculating the phi(n) in case of Prime numbers!

When the number is prime, **then phi(n) = n -1 always**. It can be verified by taking any prime number, let us take the above given example where n = 7, then phi(n) = 6, take n = 5, then coprime numbers to 5 are {1, 2, 3, 4}, which means phi(n) = n -1 = 5 -1 =4.

Property of Euler Totient Function!

If the number whose phi(n) has to be calculated is very large, then there is a property to break that, & that property is given below.

$$\phi(n) = \phi(n1) * \phi(n2)$$

The above image represents the property which is used to break the number when n is large. For example, if n = 3127, then it can be broken into 2 multiples that are 53 & 59.

$$\phi(3127) = \phi(53) * \phi(59)$$

Now, it is well known that 53, as well as 59 both, are prime numbers, then the aforementioned shortcut can be applied easily here to calculate the values of phi(53) as well as phi(59).

The values for phi(53) & phi(59) are 52 & 58 respectively.

Euler's Totient Function and Euler's Theorem

Use-Cases of the Euler Totient Function!

It is heavily used in Cryptography various algorithms & Methods. It is even the base for the algorithms to work in Cryptography.

Some of the example algorithms where it is applied are:

- Euler/Euler-Fermat Theorem.
- Fermat's Theorem.
- RSA

NOTE:

The above mentioned are few examples of its use-case. Although it can be used in various situations in number system also, where count of coprime numbers are to be found for a number.

NOTE: relationships between n and $\varphi(n)$? **when *n* is a positive integer number** (e.g. 2, 3, 5, 7, 11, 13), $\boldsymbol{\varphi(n) = n\text{-}1}$.

Examples :

$\Phi(3) = 2$

gcd(1, 3) is 1 and gcd(2, 3) is 1

$\Phi(4) = 2$

gcd(1, 4) is 1 and gcd(3, 4) is 1

Euler's Theorem

In cryptography, there exists Euler Theorem which is based on Euler Totient Function .
It states that if there are 2 coprime numbers lets' say p & q, then:

$$p^{\phi(q)} \equiv 1 mod(q)$$

where phi(q) is the Euler Totient Function.

The simplified equation for the above equation is:

$$p^{\phi(q)} mod(q) = 1 mod(q)$$

Euler Theorem deals with the concept of prime numbers, modulus/remainder, & congruency.

It aims to provide a concept where coprime numbers can be correlated somehow to provide a value that can be used later as a hash value or for encryption key in cryptography.

Example based on Euler Theorem:
Let us take 2 numbers 15 & 7, as they are coprime to each other. Let p = 15 & q = 7.

$$15^{\phi(7)} mod(7) = 1 mod(7) = 1$$

Note: 1 mod(7) = 1 (RHS)

Now, lets verify the LHS, **phi(7) = 6 (apply euler totient function)** , which transforms the LHS of the above equation as shown below:

$$15^6 mod(7)$$

where 15 ^ 6 = 11390625 => (15 ^ 6) Mod (7)= (11390625) Mod(7) = 1

As it comes 1, & also 1 mod(7) is also 1, therefore, **LHS = RHS**, & hence the theorem is verified.

***Verify* Euler Theorem: p=3,q=10**