Vidyalankar Institute of Technology
Accredited A+ by NAAC

CSS

Prof. Amit K. Nerurkar
Assistant Professor
Department of Computer Engineering
Vidyalankar Institute of Technology, Wadala

Euclid's algorithm

Calculating the GCD

$GCD(x,y)$

if ($y == 0$)
  $GCD = x$
else
  $GCD(y, x \% y)$

eg 1 $(40, 20)$

$GCD(40,20) = GCD(20, 40 \bmod 20)$
$= GCD(20, 0)$

$$\boxed{GCD(40,20) = 20}$$

eg 2 $GCD(48,30)$

$GCD(48,30) = GCD(30, 48 \% 30)$
$= GCD(30, 18)$
$= GCD(18, 30 \% 18)$
$= GCD(18, 12)$
$= GCD(12, 18 \% 12)$
$= GCD(12, 6)$
$= GCD(6, 12 \% 6)$
$= GCD(6, 0)$

$$\therefore \boxed{GCD(48,30) = 6}$$

Euler's totient function

Represented as $\phi(n)$ & $n \geq 1$.

It is defined as No. of the integers less than n who are co-prime to n.

eg. $\boxed{N=5}$

$\phi(5) = \{1, 2, 3, 4\} = \boxed{4}$

eg $\boxed{N=6}$

$\phi(6) = \{1, 5\} = \boxed{2}$

Always remember if $\boxed{n \text{ is prime}}$

then $\boxed{\phi(n) = n - 1}$

i.e $\phi(5) = 4$

$\phi(11) = 10$

$\phi(13) = 12$

$\phi(23) = 22$

$\phi(29) = 28$

We can further evaluate as

$\phi(n) = \phi(a) * \phi(b)$

a & b are co-prime

eg $\phi(35) = \phi(5) * \phi(7)$

$= 4 * 6$

$\therefore \boxed{\phi(35) = 24}$

eg $\phi(165) = \phi(15) * \phi(11)$

$= \phi(3) * \phi(5) * \phi(11)$

$= 2 * 4 * 10$

$\therefore \boxed{\phi(165) = 80}$

Euler's theorm

It states that

$$\boxed{x^{\phi(n)} = 1 \bmod n}$$

ie when $x^{\phi(n)}$ is divided by n the remainder is 1

iff x & n are co-prime

ie $GCD(x, n) = 1$

eg $\boxed{x = 4 \quad n = 165}$

$GCD(4, 165) = 1$

$\therefore$ Apply Euler's theorm

$\therefore \boxed{x^{\phi(n)} = 1 \bmod n}$

$\therefore 4^{\phi(165)} = 1 \bmod 165$

$\therefore \phi(165) = 80$

$$\therefore \boxed{4^{80} = 1 \bmod 165}$$

ie when 4^{80} is divided by 165 the remainder is 1

(2) $x = 3 \quad n = 10$

$\because GCD(3, 10) = 1$

$\therefore x^{\phi(n)} = 1 \bmod n$

$\therefore 3^{\phi(10)} = 1 \bmod 10$

$\therefore \phi(10) = \phi(2) * \phi(5)$

$= 1 * 4$

$\phi(10) = 4$

$$\therefore \boxed{3^4 = 1 \bmod 10}$$

When 3^4 is divided by 10 the remainder is 1

Fermat's theorm:

A special case of Euler's theorm.

what is $(n-1)$?

Represented as

$$\boxed{x^{(n-1)} \equiv 1 \bmod n}$$

$\phi(n) \leftarrow$ Euler totient

$\downarrow$

$(n-1) \leftarrow n$ is prime

① n: Prime Number

② $(x \cdot 1 \cdot n) \neq 0$

eg $\boxed{x = 3}$ $\boxed{n = 7}$

I n is prime = TRUE

II $(x \cdot 1 \cdot n) \neq 0$ = TRUE

$$\boxed{x^{\phi(n)} \equiv 1 \bmod n}$$

$3^{\phi(7)} \equiv 1 \bmod n$

$\because$ 7 is prime

$\therefore \phi(7) = 6$.

$$\therefore \boxed{3^6 \equiv 1 \bmod 7}$$

729

When 3^6 is divided by 7 the Remainder is 1

② Solve using fermat's therom

① $\boxed{6^{10} \equiv 1 \bmod 11}$

find n, x, $\phi(n)$ & prove the fermat's therom.

Soln

$n = 11$
$x = 6$
$\phi(n) = 10$

Proof:

I n is Prime = TRUE

II $(x-1 \cdot n) \neq 0$ = TRUE

III $x^{\phi(n)} \equiv 1 \bmod n$

$\therefore 6^{\phi(11)} \equiv 1 \bmod 11$

$\therefore 6^{10} \equiv 1 \bmod 11$

when 6^{10} is divided by 11 the remainder will be 1

Q2

$\boxed{7^{(3)} \equiv 1 \bmod 4}$

Soln

I n is Prime = False

Hence cannot prove the F.T.

Thank You

Name: *Amit K. Nerurkar*

Designation: *Assistant Professor*

College: *Vidyalankar Institute of Technology*