25/09/22

Euler's Theorem (Generalization of Fermat's Theorem)

$p \to$ prime
$\downarrow$
$n \to$ arbitrary (+ve) integer

$$\boxed{\text{If } \gcd(a,n)=1 \ (n \geq 1) \text{ then } a^{\phi(n)} \equiv 1 \bmod n}$$

Example:- putting $n=30$, $a=11$

$\gcd(11,30)=1$

$\therefore \boxed{11^{\phi(30)} \equiv 1 \bmod 30}$

i.e $11^{8} \equiv 1 \bmod 30$

$\phi(n) = \phi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})$
$= n\left[1-\frac{1}{p_1}\right]\left[1-\frac{1}{p_2}\right] \cdots \left[1-\frac{1}{p_k}\right]$

$30 = 2\times3\times5$

$\phi(30) = \phi(2)\phi(3)\phi(5)$
$= 1\times2\times4 = 8$

verification: $11^{8} \equiv (11^2)^4 \bmod 30$
$\equiv (121)^4 \bmod 30$
$\equiv (1)^4 \bmod 30$
$\equiv 1 \bmod 30$ verified

$\therefore$

Lemma:- ① Let $n>1$ and $\gcd(a,n)=1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Proof:

Lemma ② $n>1$, if $\gcd(a_i, n)=1 \ \forall i=1,\ldots k$
then $\gcd(a_1 a_2 \cdots a_k, n)=1$

Proof: Euler's theorem:- If $n \geq 1$ and $\gcd(a,n)=1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. It is helpful in reducing large powers modulo n.

Proof:- If $n=1$, $\gcd(a,1)=1$ then

$a^{\phi(1)} \equiv 1 \bmod 1$ $\quad a \equiv 1 \bmod 1$

$\forall a$-1 trivial

take $n>1$; Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n that are relatively prime to n.

Because $\gcd(a,n)=1$, $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent to one of $a_1, a_2, \ldots, a_{\phi(n)}$.

Then

$$aa_1 \equiv a_1' \bmod n$$
$$aa_2 \equiv a_2' \bmod n$$
$$\vdots \qquad \vdots$$
$$aa_{\phi(n)} \equiv a'_{\phi(n)} \bmod n$$

where $a_1', a_2', \ldots, a'_{\phi(n)}$ are the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

on taking the product of these $\phi(n)$ congruences,

$$(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv a_1' a_2' \cdots a'_{\phi(n)} \bmod n$$

$$(*) \text{ — } a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \bmod n$$

$\because \gcd(a_i, n)=1$ for each i, the lemma

then $\gcd(a_1, a_2 \cdots a_{\phi(n)}, n)=1$

$\Rightarrow (*)$ becomes

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

$ab \equiv ac \bmod n$

$\Rightarrow b \equiv c \bmod n$

iff $\gcd(a,n)=1$

$n/a(b-c)$

$n/b-c$

Corollary; (Fermat) if $p \nmid a$, p prime

$a^{\phi(p)} \equiv 1 \bmod p$ or $\boxed{a^{p-1} \equiv 1 \bmod p}$

Application:-
find last two digits in the decimal representation of 3^{256}.

$$\boxed{3^{256} \equiv \underline{?} \mod 100}$$

$n=100$, $\phi(n) = \phi(100) = 40$, $a=3$ $\quad gcd(3,40)=1$

$\therefore 3^{\phi(100)} \equiv 1 \mod 100 \Rightarrow \boxed{3^{40} \equiv 1 \mod 100}$

now take $3^{256} \equiv 3^{40\times 6+16} \mod 100$

$\equiv (3^{40})^6 . 3^{16} \mod 100$

$\equiv 3^{16} \mod 100$

$\equiv 21 \mod 100$

$3^2 \equiv 9 \mod 100$

$3^4 \equiv 81 \mod 100$

$3^8 \equiv 81\times 81 \mod 100$

$\equiv 19\times 19 \mod 100$

$\equiv 361 \mod 100$

$\equiv 61 \mod 100$

$3^{16} \equiv 61\times 61 \mod 100$

$\equiv 21 \mod 100$