* Euler ϕ and τ Function *

$\phi : \mathbb{N} \to \mathbb{N}$ $\qquad$ $\tau : \mathbb{N} \to \mathbb{N}$.

* $\phi(1) = 1$, $\phi(n)$ = no. of natural no. less than n and coprime to n.

* if $n = p^{n_1} \cdot q^{n_2} \cdot r^{n_3}$; p, q, r are primes

then $\phi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)$

* if n = prime (say p) then $\phi(p) = p-1$

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

* $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$; if $\gcd(m, n) = 1$.

* $\phi(10^n) = 4 \times 10^{n-1}$

* $\phi(n)$ is always even $\forall\, n > 2$.

* Euler ϕ function is neither one-one nor onto

$\because$ $\phi(n) = 1$ when $n = 1$ also when $n = 2$.

$\therefore$ ϕ is not one-one.

Now, $\phi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)$

$= \frac{n}{pqr}(p-1)(q-1)(r-1)$

$=$ even.

$\therefore$ $\phi(n)$ is not onto.

$\tau(n)$ = no. of positive divisors of n including 1 and n both.

* if $n = p^a \cdot q^b \cdot r^c$ then $\tau(n) = (a+1)(b+1)(c+1)$

* For any prime p, $\tau(p) = 2$.

e.g: $\tau(20) = 6$, $\tau(10) = 4$, $\tau(100) = 9$

* Euler τ function is neither one-one nor onto.

** $G_1 = \{1, 2, 4, 8, 16\}$; $a * b = HCF(a, b)$

$G_1 = \{2, 4, 6, 8, *\}$ where r is the remainder when $a * b$ divided by 10.

$G_1 = \{P(\mathbb{N}), *\}$; where $X * Y = X \Delta Y$

i.e. symmetric difference of X and $Y = X \cup Y - X \cap Y$

* Theorem :- The identity element in a group is unique.

proof :- Let e and e' be two identity element of a group G. Then we have

$e \cdot e' = e'$ if e is the identity element

and $e \cdot e' = e$ if e' is the identity element.

But ee_1 or ee' is an unique element of G

$\therefore ee' = e$ and $ee' = e' \Rightarrow e = e'$ #.

* Addition and multiplication modulo m $+_m, \times_m$

* Theorem :- Uniqueness of inverse :-
The inverse of every element of a group is unique.

proof :- Let a be any arbitrary element of a group G and let e be the identity element Let b and c are two inverse of a. Then

$a \cdot b = b \cdot a = e$ and $a \cdot c = c \cdot a = e$.

we have $b \cdot (ac) = b \cdot e = b$

Also $(ba) \cdot c = e \cdot c = c$.

But, $\because$ G is a group $\therefore$ $b \cdot (ac) = (ba) \cdot c$

$\therefore$ $b = c$ Hence inverse is unique.

* Que :- show that the set of matrices

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \text{ where } \alpha \in \mathbb{R},$$

forms a group under matrix multiplication.

solution :- $\sin(A \pm B) = \sin A \cdot \cos B \pm \cos A \cdot \sin B$.

$\cos(A \pm B) = \cos A \cdot \cos B \mp \sin A \cdot \sin B$.

Que:- Show that the set of cube roots of unity is an abelian group w.r.t to multiplication.

Soln:- Cube roots of unity is obtained by solving the following equation: $x^3-1=0$

$\Rightarrow (x-1)(x^2+x+1)=0$

$\Rightarrow x=1, \quad x=\frac{-1\pm\sqrt{1-4}}{2} \Rightarrow x=-\frac{1}{2}\pm\frac{\sqrt{3}i}{2}.$

$\therefore G=\left\{1, \frac{(-1)}{2}+i\frac{\sqrt{3}}{2}, \frac{(-1)}{2}-i\frac{\sqrt{3}}{2}\right\}$

if we put $\frac{(-1)}{2}+\frac{i\sqrt{3}}{2}=w$ then

$-\frac{1}{2}-\frac{i\sqrt{3}}{2}=w^2$ and $w^3=1$

Also $1+w+w^2=0.$

$\therefore G=\{1, w, w^2\}$

Now we form a composition table:

$\cdot$	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

Here $w\cdot w^2=w^3=1$

$w^2\cdot w^2=w^4=w^3\cdot w=1\cdot w=w$

1) closure: since all the entries $\in G$.
2) Associative:- multiplication of complex no. is asso.
3) Existance of identity and inverse.
4) Commutative:- multiplication of complex No. is commutative.

Que:- Prove that the set $G = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group of order 6 under the multiplication modulo 7.

Que:- $G = \{0, 1, 2, 3, 4, 5, 6, +_7\}$

Que:- $G = \{1, -1, i, -i\}$ with $\times$ to multiplication.

Que:- show that the set of all positive rational numbers forms an abelian group under composition defined by $a * b = \frac{ab}{2}$

Theo:- A non-empty subset H of a group G is a subgroup of G iff $a,b \in H \Rightarrow ab^{-1} \in H$.

proof:- Let H be a subgroup of a group G. Then

For any $a,b \in H \Rightarrow a, b^{-1} \in H$ ($\because H < G$)

$\Rightarrow a \cdot b^{-1} \in H$ (closure law)

Conversaly:- Let H be a subset of a group G such that $a,b \in H \Rightarrow ab^{-1} \in H$. we have to show that H is itself a group.

1) ~~closure law: we have $a,b \in H$~~

$\because H \neq \phi$, therefore there exist $a \in H$.

$\therefore aa^{-1} = e \in H$ i.e. H contains the identity.

Again let $a \in H$ and $e \in H$ $\therefore e,a \in H \Rightarrow ea^{-1} \in H$

$\Rightarrow a^{-1} \in H$

$\because$ a is arbitrary element $\therefore$ every element of H has an inverse in H.

Thus, for all $a,b \in H$, $a, b^{-1} \in H$ and so

$a \cdot (b^{-1})^{-1} = ab \in H$. (so H is closed)

Associative:- Let $a,b,c \in H$. since H is a subset of G we find that $a,b,c \in G$. Hence, by the associative property, we have $(ab)c = a(bc)$.

Hence H is a subgroup of G.