Chapter 1

GROUPS AND RINGS

Binary Operation :-

Let S be a non-empty set. A Binary Operation * on S is a function $* : S * S \to S$. The image of any ordered pair (a,b) of elements of S under * is denoted by $a*b$.

The Number sets are

N = the set of positive integers = $\{1, 2, 3, \}$

Z = the set of integers = $\{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$

Q = the set of rational numbers

$= \{\frac{p}{q} \mid p, q, \in Z, q \neq 0\}$

R = the set of real numbers

C = the set of complex numbers

$= \{a + ib \mid a, b \in R\}$.

Thus $(N, +)$, $(Z, +)$, $(Q, +)$, $(R, +)$ and $(C, +)$ are algebraic Systems.

Let $S = \{0, 1, 2\}$. A Binary Operation * on S is defined by $0*0 = 0$, $0*1 = 1*0 = 1$, $0*2 = 2*0 = 0$.

$1*1 = 2$, $1*2 = 2*1 = 1$, $2*2 = 1$.

The result of the operation can be displayed as a two way table.

The table is

*	0	1	2
0	0	1	0
1	1	2	0
2	0	1	1

This table is called the multiplication table or Operation table or cayley table.

Properties of Binary Operations.

(1) Associative property:

A Binary operation * on S is said to be associative if $a*(b*c) = (a*b)*c \quad \forall a,b,c \in S$.

(2) Commutative property:

A Binary operation * on S is said to be Commutative if $a*b = b*a \quad \forall a,b \in S$

(3) Existence of Identity.

A Binary operation * on S is said to have an identity element $e \in S$ if $e*a = a*e = a \quad \forall a \in S$.

(4) Existence of inverse.

Let * be a binary operation on S with an identity element e in S. An element $a \in S$ is said to have an inverse $a' \in S$ if $a*a' = a'*a = e$.

(5) Closure property.

Let * be a binary operation On S and A be a subset of S. A is said to be closed under * if $a*b \in A$ $\forall a,b \in A$

(6) Group:

A non-empty set G with a binary Operation * defined on it is called a group if the following axioms are satisfied. Let * be a binary Operation on S and A be a subset of S. A is said to be closed under * if $a*b \in A \quad \forall a,b \in A$.

1. Associativity:

For all $a,b,c \in G$, we have $a*(b*c) = (a*b)*c$.

2. Identity:

There exists an element $e \in G$ such that $a * e = e * a = a \ \forall a \in G$.

3. Inverse :

For each $a \in G$, there exists an element a' such that $a * a' = a' * a = e$.

The group is denoted by $(G, *)$ the set and the binary operation.

Order of a Group.

Let G be a group under the operation $*$. The number of elements in G is called the order of Group G and is denoted by $o(G)$.

If G has n elements, then $o(G) = n$.

If the $o(G)$ is finite, then G is called a finite group, otherwise it is an infinite group.

Abelian group:

A group $(G, *)$ is said to be abelian or commutative if $a * b = b * a \ \forall a, b \in G$.

THEOREM 1: Let $(G, *)$ be a group, then (i) identity element is unique (ii) For each $a \in G$, inverse is unique.

Proof :- Given $(G, *)$ is a group.

(i) Let e and e' be two identity elements of G. Then by identity axiom (2) of a group we get.

$e * e' = e$ [Treating e' as identity]

and $e * e' = e'$ [Treating e as "]

$e = e'$

Hence identity element is unique.

(ii) Let e be the identity element of G. Let $a \in G$ be any element. Suppose a' and a'' are two inverses of a, then by inverse axiom,

$$a * a' = a' * a = e$$

and $$a * a'' = a'' * a = e$$

Now, $a' = a' * e$ [$\because e$ is identity]

$= a' * (a * a'')$ [$\because a * a'' = e$]

$= (a' * a) * a''$ [by associative axiom]

$= e * a''$ [$\because a' * a = e$]

$= a''$.

THEOREM 2

In a group $(G, *)$ the cancellation laws hold.

For all $a, b, c \in G$.

(i) $a * b = a * c \Rightarrow b = c$ [Left cancellation law]

(ii) $b * a = c * a \Rightarrow b = c$ [Right cancellation law].

Proof: Given $(G, *)$ is a group. Let e be the identity element of G.

(i) Given $a * b = a * c$

Let a^{-1} be the inverse of a.

premultiplying by a^{-1}, we get

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$ [by associative]

$\Rightarrow e * b = e * c$ [by inverse]

$\Rightarrow b = c$ [by identity]

(ii) Given $b * a = c * a$

$\Rightarrow (b * a) * a^{-1} = (c * a) * a^{-1}$ [post multiplying by a^{-1}.

⇒ $b*(a*a^{-1}) = c*(a*a^{-1})$ [by associative]

⇒ $b*e = c*e$ [by inverse]

⇒ $b=c$ [by identity]

THEOREM 3 In a group $(G,*)$ the equation $a*x=b$ and $y*a=b$ have unique solutions for the unknowns x and y as $x=a^{-1}*b$, $y=b*a^{-1}$, where $a,b \in G$.

Proof: Given $(G,*)$ is a group and let e be the identity element of G and a^{-1} be the inverse of a.

Given $a*x=b$

⇒ $a^{-1}*(a*x) = a^{-1}*b$. [premultiplying by a^{-1}]

⇒ $(a^{-1}*a)*x = a^{-1}*b$ [by associative

⇒ $e*x = a^{-1}*b$ [by inverse

⇒ $x = a^{-1}*b$ [by identity

Thus $x = a^{-1}*b \in G$ is a solution.

We shall now prove the uniqueness.

Suppose, $x_1, x_2 \in G$ be two solutions of $a*x=b$ then

$a*x_1=b$ and $a*x_2=b$

$a*x_1 = a*x_2$

⇒ $x_1=x_2$ [by left cancellation laws.

Hence the solution is unique and the unique solution is $x=a^{-1}*b$.

Similarly we can prove that $y*a=b$ has unique solution $y=b*a^{-1}$.

Now $y*a=b$.

⇒ $(y*a)*a^{-1} = b*a^{-1}$ [post-multiplying by a^{-1}]

⇒ $(y*(a*a^{-1})) = b*a^{-1}$ [by associative.

$y * e = b * a^{-1}$

$y = b * a^{-1}$

$y = b * a^{-1} \in G$ is a solution.

We shall now prove the uniqueness.

Let y_1, y_2 be two Solutions of $y * a = b$.

$y_1 * a = b$ and $y_2 * a = b$.

$\Rightarrow y_1 * a = y_2 * a$

$\Rightarrow y_1 = y_2$ [by right cancellation law]

Hence the solution is unique and the unique solution is $y = b * a^{-1}$.

THEOREM 4 Let $(G, *)$ be a group, then

(i) for each $a \in G$, $(a^{-1})^{-1} = a$.

(ii) for all $a, b \in G$, $(a*b)^{-1} = b^{-1} * a^{-1}$.

Proof: (i) Let $a \in G$, then a^{-1} is the inverse of a and $(a^{-1})^{-1}$ is the inverse of a^{-1}.

$\therefore a * a^{-1} = a^{-1} * a = e$ [by inverse]

and $a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * (a^{-1}) = e$ [by inverse]

$\therefore a^{-1} * a = a^{-1} * (a^{-1})^{-1}$

$\Rightarrow a = (a^{-1})^{-1}$ [by left-cancellation law

(ii) We have to prove that the inverse of $a*b = b^{-1} * a^{-1}$

consider $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1}$ (by associative law.

$= a * e * a^{-1}$ [$\because b*b^{-1} = e$]

$= a * a^{-1} = e$ [$\because a*a^{-1} = e$]

Now consider, $(b^{-1} * a^{-1}) * (a*b) = b^{-1} * (a^{-1} * a) * b$

$$= b^{-1} * e * b$$

$$= b^{-1} * b = e$$

Thus $(a*b) * (b^{-1} * a^{-1}) = (b^{-1} * e^{-1}) * (a*b) = e$

Hence $b^{-1} * a^{-1}$ is the inverse of $a*b$

$\therefore \ (a*b)^{-1} = b^{-1} * a^{-1}$.

Worked Examples.

(1) Let $G = \{1, -1\}$. prove that G is a group under usual multiplication.

Soln: Given $G = \{1, -1\}$ and the binary operation is usual multiplication. Since G is a finite set, we form cayley table and verify the axioms of the group.

cayley table is

$\cdot$	1	-1
1	1	-1
-1	-1	1

Closure:

The body of the table contains only elements of G. So G is closed under multiplication.

Associativity: Since multiplication is associative in any number set, it is true here also. Hence it is satisfied.

Identity: 1 is the identity element.

Inverse: Inverse of 1 is 1 and inverse of -1 is -1

so $(G, \cdot)$ is a group.

Further it is abelian group, since $\cdot$ is commutative.

Eg.② Let $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$, show that G is a group under the operation of matrix multiplication.

Soln:- Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$

$B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

$\therefore G = \{I, A, B, C\}$. since it is finite set we shall form cayley table and verify the axioms of a group.

I is the identity element.

$A \cdot I = I \cdot A = A$, $BI = IB = B$, $C \cdot I = I \cdot C = C$

$\Rightarrow$ $A^2 = A \cdot A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$A \cdot B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = C$

$A \cdot C = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = B$

$\Rightarrow$ $B^2 = B \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$\Rightarrow$ $C^2 = C \cdot C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$

$B \cdot C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = A$

$CA = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = B.$

Similarly $BA = C$, $CB = A$.

$\therefore$ Cayley table is

$\cdot$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Closure :

The body of the table contains only all the elements of G. so G is closed under matrix multiplication.

Associative: since matrix multiplication is associative it is true for G also, so associative axiom is satisfied.

Identity: I is the identity element.

Inverse: Inverse of A is A, B is B, C is C.

so $(G, \cdot)$ is a group under matric multiplication.

Further elements equidistant from the main diagonal are same and hence the operation is commutative. Therefore $(G, \cdot)$ is abelian.

Note : This is an example of a famous group called klein's four group $A^2 = B^2 = C^2 = I$.

$AB = BA = C$; $BC = CB = A$ and $AC = CA = B$.

(3) Show that the set of all non-zero real numbers is an abelian group under the operation $*$ defined by $a*b = \frac{ab}{2}$.

soln:- Let G be the set of all non-zero real numbers.

$\therefore G = R - \{0\}$, where R is the set of real numbers.

The operation $*$ on G is defined by $a*b = \frac{ab}{2}$ $\forall a, b \in G$

Closure: $a*b = \frac{ab}{2}$, where a and b are non-zero real numbers and so $\frac{ab}{2}$ is non-zero.

$\therefore \frac{ab}{2} \in G \Rightarrow a*b \in G \quad \forall \ a,b \in G$

Hence G is closed under *.

Associativity: For any $a,b,c \in G$

$$a*(b*c) = a * \frac{bc}{2} = \frac{a\left(\frac{bc}{2}\right)}{2} = \frac{a(bc)}{4}.$$

and $$(a*b)*c = \left(\frac{ab}{2}\right)*c = \frac{\left(\frac{ab}{2}\right)c}{2} = \frac{a(bc)}{4}.$$

$\therefore$ usual multiplication is associative.

$\therefore \ a*(b*c) = (a*b)*c \quad \forall \ a,b,c \in G.$

So associative axiom is satisfied.

Identity:- Suppose $e \in G$ be the identity, then $a*e = a \ \forall \ a \in G$

$\Rightarrow \frac{ae}{2} = a \Rightarrow \frac{e}{2} = 1 \Rightarrow e = 1 \quad [\because a \neq 0]$

So, identity is 2.

Inverse: Let a be any element of G. suppose a' is its inverse then,

$$a*a^{*} = 2 \Rightarrow \frac{aa'}{2} = 2 \Rightarrow a' = \frac{4}{a} \quad [\because a \neq 0]$$

So, for every element $a \in G$ inverse is $\frac{4}{a}$.

Thus inverse axiom is satisfied.

Commutative: Let a, b be any two elements of G, then

$$a*b = \frac{ab}{2} = \frac{ba}{2} \quad \text{[usual multiplication is commutative]}$$
$$= b*a$$

Hence $(G,*)$ is an abelian group.

④ If S is the set of all ordered pairs (a,b) of real numbers with the binary operation ⊕ defined by $(a,b)\oplus(c,d) = (a+c, b+d)$, where a,b,c,d are real numbers, prove that $(S,\oplus)$ is a commutative group.

Soln:

Given $S = \{(a,b) \mid a,b \in R\}$

(b)

closure : Let $x, y \in S$, then $x = (a,b)$; $y = (c,d)$ where $a, b, c, d \in R$

now $x \oplus y = (a,b) \oplus (c,d) = (a+c, b+d)$

Since a, b, c, d are real numbers, $a+c$, $b+d$ are real numbers.

Hence $(a+c, b+d) \in S \Rightarrow x \oplus y \in S$

so, S is closed under $\oplus$

Associativity : Let x, y, z be any three elements in S.

Then $x = (a,b)$, $y = (c,d)$ $z = (p,q)$.

where a, b, c, d, p, q are some real numbers.

$$\text{Now } x \oplus (y \oplus z) = (a,b) \oplus ((c,d) \oplus (p,q))$$
$$= (a,b) \oplus (c+p, d+q)$$
$$= (a + (c+p), b + (d+q))$$
$$= ((a+c) + p, (b+d) + q) \rightarrow (1)$$

[$\because$ usual addition is associative)

$$\text{and } (x \oplus y) \oplus z = ((a,b) \oplus (c,d)) \oplus (p,q)$$
$$= (a+c, b+d) \oplus (p,q)$$
$$= ((a+c) + p, (b+d) + q) \rightarrow (2)$$

From (1) and (2)

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad \forall x, y, z \in S.$$

So associative axiom is satisfied.

Identity :- Let $x = (a,b)$ be any element in S.

Suppose $e = (c,d)$ be the identity element in S,

then $x \oplus e = x$

$\Rightarrow (a,b) \oplus (c,d) = (a,b)$

$\Rightarrow (a+c, b+d) = (a,b)$

$\Rightarrow a + c = a$, $b + d = b$

$\Rightarrow c = 0$, $d = 0$. $\therefore e = (0,0)$ is identity element of S.

Inverse: Let $x = (a,b)$ be any element of S.

Suppose $x' = (c,d)$ be the inverse,

then $x \oplus x' = e$

$\Rightarrow (a,b) \oplus (c,d) = (0,0)$

$\Rightarrow (a+c, b+d) = (0,0)$

$\Rightarrow a+c = 0, b+d = 0$

$\Rightarrow c = -a, d = -b$

$\therefore x' = (-a,-b)$ is the inverse of x.

So, inverse axiom is satisfied.

Commutativity: Let $x = (a,b)$ and $y = (c,d)$ be any two elements on S.

Now $x \oplus y = (a,b) \oplus (c,d)$

$= (a+c, b+d)$

$= (c+a, d+b)$ [Usual addition is commutative

$= (c,d) \oplus (a,b)$ [by definition of $\oplus$]

$= y \oplus x$

$\therefore x \oplus y = y \oplus x \quad \forall x,y \in S$

Hence $(S, \oplus)$ is a commutative group.

(ie), $(S, \oplus)$ is an abelian group.

PERMUTATION

Let S be a non-empty set. A bijective function $f: S \to S$ is called a permutation. If S has n elements, then the permutation is said to be of degree n.

Usually we take $S = \{1,2,3,\dots,n\}$

The set of all permutations on a set of n symbols is denoted by S_n.

(17) If $S=\{1,2,3\}$, then prove that $(S_3, \cdot)$ is a non-abelian group, where $\cdot$ is composition of function.

Soln: Given $S=\{1,2,3\}$. The total number permutation on S is $3! = 6$. The permutations are

$$P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \quad P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \quad P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

Then $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ and the binary operations on S_3 is the composition of functions.

The operation is performed on the left as below.

For example $(1)\cdot(P_2 \cdot P_3) = ((1)\cdot P_2) P_3$ i.e $1 \xrightarrow{P_2} 1 \xrightarrow{P_3} 2$

$= (1) P_3 = 2$. $(1) P_2 \cdot P_3 = 2$

Similarly for other elements.

since $(1) P_1 = 1$, $(2) P_1 = 2$, $(3) P_1 = 3$,

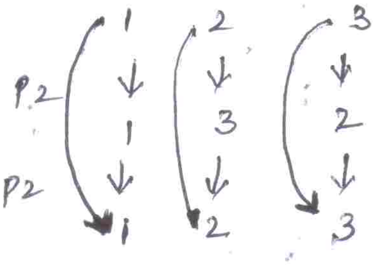
P_1 is the identity element on S.

$P_1 \cdot P_1 = P_1$; $P_1 \cdot P_2 = P_2 \cdot P_1 = P_2$;

$P_1 \cdot P_3 = P_3 \cdot P_1 = P_3$; $P_1 \cdot P_4 = P_4 \cdot P_1 = P_4$;

$P_1 \cdot P_5 = P_5 \cdot P_1 = P_5$; $P_1 \cdot P_6 = P_6 \cdot P_1 = P_6$.

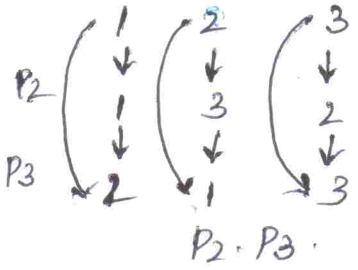
$$P_2 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$



$P_2 \cdot P_2$

$$P_2 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$

$$P_2 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$



$$\therefore P_2 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$

$$P_2 \cdot P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = P_3.$$

$$P_2 \cdot P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = P_6$$

$$P_2 \cdot P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5.$$

$$P_3 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = P_6$$

$$P_3 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5$$

$$P_3 \; P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = P_2.$$

$$P_3 \cdot P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$

$$P_3 \cdot P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$

$$P_4 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5.$$

$$P_4 \cdot P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_6$$

$$P_4 \cdot P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1 .$$

$$P_4 \cdot P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2 .$$

$$P_4 \cdot P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_3 .$$

$$P_5 \cdot P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_4 .$$

$$P_5 \cdot P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1 .$$

$$P_5 \cdot P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_6$$

$$P_5 \cdot P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_3 .$$

$$P_5 \cdot P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$$

$$P_6 \cdot P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_3$$

$$P_6 \cdot P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$$

$$P_6 \cdot P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_5$$

$$P_6 \cdot P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_4 .$$

$$P_6 \cdot P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1 .$$

The cayley table is,

$\cdot$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_1	P_4	P_3	P_6	P_5
P_3	P_3	P_6	P_5	P_2	P_1	P_4
P_4	P_4	P_5	P_6	P_1	P_2	P_3
P_5	P_5	P_4	P_1	P_6	P_3	P_2
P_6	P_6	P_3	P_2	P_5	P_4	P_1.

Closure: since the body of the table contains only the elements of S_3, S_3 is closed with respect to $\cdot$.

Associativity: we know composition of functions is associative and so it is true in S_3 also. So associative axiom is verified.

Identity: $P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ is the identity element of S_3.

Inverse: To find the inverse of an element P_i, find P_1 in the row through P_i, the column head of P_1 is the inverse of P_i ie P_i^{-1}.

$\therefore$ from the table we see that

$P_1^{-1} = P_1$, $P_2^{-1} = P_2$, $P_3^{-1} = P_5$, $P_4^{-1} = P_4$

$P_5^{-1} = P_3$, $P_6^{-1} = P_6$.

Thus inverse exists for every element. Hence inverse axiom is verified. So $(S_3, \cdot)$ is a group.

From the table we find that,

$P_3 \cdot P_4 = P_2$ and $P_4 \cdot P_3 = P_6$.

$\therefore P_3 \cdot P_4 \neq P_4 \cdot P_3$.

Hence the group is not commutative.

GROUP OF RESIDUE CLASSES Mod n

congruence mod n

Let n be a fixed positive integer. Let a and b be integers, we define $a \equiv b \pmod n$, if $a-b$ is divisible by n.

For example, $2 \equiv -1 \pmod 3$, since $2-(-1) = 3$ is divisible by 3.

$25 \equiv 5 \pmod 2$, since $25-5 = 20$ is divisible by 2.

$-1 \equiv 3 \pmod 2$, since $-1-3 = -4$ is divisible by 2.

The equivalence class of a is $[a] = \{x \mid x \equiv a \pmod n\}$

For eg, the congruence classes mod 4 are

$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$

$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$

$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\}$

$[3] = \{\dots, -5, -1, 3, 7, 11, \dots\}$

$[4] = \{\dots, -8, -4, 0, 4, 8, \dots\} = [0]$

similarly $[5] = [1]$, $[6] = 2$ etc..

$\therefore$ The distinct congruence classes mod 4 are $[0], [1], [2], [3]$.

The set of congruence classes mod 4 is denoted by,

$Z_4 = \{[0], [1], [2], [3]\}$ and is called the set of residue classes mod 4 or residual classes mod 4.

more generally, the set of residue classes mod n is $Z_n = \{[0], [1], [2], \dots [n-1]\}$.

(9) Let $Z_5^* = \{[1], [2], [3], [4]\}$ be the non-zero elements of Z_5 prove that $(Z_5^*, \cdot_5)$ is an abelian group.

Soln: $Z_5^* : \{[1], [2], [3], [4]\}$

we form the cayley table to verify axioms of a group.

$[2] \cdot_5 [2] = [4]$.

$[2] \cdot_5 [3] = [6] = [1]$ $[\because 6 \equiv 1 \pmod 5]$

ie the remainder when 6 is $\div$ by 5 is 1,

$[2] \cdot_5 [4] = [8] = [3]$ $[\because 8 \equiv 3 \pmod 5]$

$[3] \cdot_5 [2] = [6] = [1]$ $[\because 6 \equiv 1 \pmod 5]$

$[3] \cdot_5 [3] = [9] = [4]$ $[\because 9 \equiv 4 \pmod 5]$

$[3] \cdot_5 [4] = [12] = [2]$ $[\because 12 \equiv 2 \pmod 5]$

$[4] \cdot 5 [1] = [4]$.

$[4] \cdot_5 [2] = [8] = [3]$ $[\because 8 \equiv 3 \pmod 5]$

$[4] \cdot_5 [3] = [12] = [2]$ $[\because 12 \equiv 2 \pmod 5]$

$[4] \cdot 5 [4] = [16] = [1]$ $[\because 6 \equiv 1 \pmod 5]$

The cayley table is

$\cdot_5$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Closure : The body of table contains only elements of Z_5^*

$\therefore$ Z_5^* is closed w.r.to $\cdot_5$

Associativity : since usual multiplication is associative, it is true in Z^*_5 also.

Identity : [1] is the identity element, since $[1] \cdot_5 [a] = [a]$ $\forall\, a \in Z^*_5$

ie $[1]\cdot_5[1] = [1]$; $[1]\cdot_5[2] = 2$,

$[1]\cdot_5[3] = [3]$; $[1]\cdot_5[4] = 4$

Inverse : From the table we note that

inverse of [1] is [1]; inverse of [2] is [3]

inverse of [3] is [2] ; inverse of [4] is [4].

Further, the elements equidistant from the main diagonal are same and so $\cdot_5$ is commutative in Z_5^*. So $(Z_5^*\ \cdot_5)$ is an abelian group.

(10) Show that if every element in a group G is its own inverse, then the group G must be abelian.

(or)

In a group G, if $a^2 = e$ $\forall$ $a \in G$, then G is abelian.

Soln : Let $a, b \in G$ be any two elements, then $a * b \in G$. Given every element is its own inverse

$\therefore a^{-1} = a, \quad b^{-1} = b$ and $(a*b)^{-1} = a*b$

$\Rightarrow b^{-1} * a^{-1} = a*b$

$\Rightarrow b*a = a*b \quad \forall a,b \in G$

$\therefore$ G is abelian.

<u>note</u>: 1. consider the second part.

Given $a^2 = e \quad \forall a \in G$

$\therefore a^{-1} * a^2 = a^{-1} * e$

$\Rightarrow (a^{-1} * a) * a = a^{-1} * e.$ $\quad [\because a^{-1} * a = e]$

$\Rightarrow a = a^{-1} \quad \forall a \in G$

ie, every element is its own inverse. Now G is abelian by first part.

2. Is the converse true?

<u>ie</u>. If G is abelian, that every element is its own inverse

Ans: No. For example, $(z, +)$ is an abelian group. But inverse of 2 is -2 and not 2.

3. Let $(G, *)$ be a group. An element $a \in G$ is called an independent element if $a^2 = a$

Then $a^{-1} = a^2 = a^{-1} * a \Rightarrow a = e$. So, the only independent element in a group is the identity element.

(14) Let f and g be the permutations of the elements of $\{1,2,3,4,5\}$ given by $f=\begin{bmatrix}1&2&3&4&5\\2&3&1&4&5\end{bmatrix}$ and $g=\begin{bmatrix}1&2&3&4&5\\5&4&3&1&2\end{bmatrix}$ find gf^2g^{-1} and $g^{-1}fgf^{-1}$

[AU 2001]

Soln:

Given $f=\begin{bmatrix}1&2&3&4&5\\2&3&1&4&5\end{bmatrix}$, $g=\begin{bmatrix}1&2&3&4&5\\5&4&3&1&2\end{bmatrix}$

then $f^{-1}=\begin{bmatrix}2&3&1&4&5\\1&2&3&4&5\end{bmatrix}=\begin{bmatrix}1&2&3&4&5\\3&1&2&4&5\end{bmatrix}$

[Reversing of we get f^{-1}]

$g^{-1}=\begin{bmatrix}5&4&3&1&2\\1&2&3&4&5\end{bmatrix}=\begin{bmatrix}1&2&3&4&5\\4&5&3&2&1\end{bmatrix}$

$f^2=\begin{bmatrix}1&2&3&4&5\\2&3&1&4&5\end{bmatrix}\begin{bmatrix}1&2&3&4&5\\2&3&1&4&5\end{bmatrix}=\begin{bmatrix}1&2&3&4&5\\3&1&2&4&5\end{bmatrix}$

$fg=\begin{bmatrix}1&2&3&4&5\\2&3&1&4&5\end{bmatrix}\begin{bmatrix}1&2&3&4&5\\5&4&3&1&2\end{bmatrix}=\begin{bmatrix}1&2&3&4&5\\4&3&5&1&2\end{bmatrix}$

$\therefore gf^2g^{-1}=\begin{bmatrix}1&2&3&4&5\\5&4&3&1&2\end{bmatrix}\begin{bmatrix}1&2&3&4&5\\3&1&2&4&5\end{bmatrix}\begin{bmatrix}1&2&3&4&5\\4&5&3&2&1\end{bmatrix}$

$=\begin{bmatrix}1&2&3&4&5\\1&2&5&3&4\end{bmatrix}$

$g^{-1}fgf^{-1}=\begin{bmatrix}1&2&3&4&5\\4&5&3&2&1\end{bmatrix}\begin{bmatrix}1&2&3&4&5\\4&3&5&1&2\end{bmatrix}\begin{bmatrix}1&2&3&4&5\\3&1&2&4&5\end{bmatrix}$

$=\begin{bmatrix}1&2&3&4&5\\3&1&5&2&4\end{bmatrix}$

(15) If $f=\begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix}$ and $g=\begin{bmatrix}1&2&3&4\\3&1&4&2\end{bmatrix}$ find $f^{-1}gf$ and gfg^{-1}.

Soln:- Given $f=\begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix}$ and $g=\begin{bmatrix}1&2&3&4\\3&1&4&2\end{bmatrix}$ are permutations on four symbols

$\therefore f^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

$g^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

$\therefore f^{-1}gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

and $gfg^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$

---

(16) If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ are permutations, prove that $(g\cdot f)^{-1} = f^{-1}\cdot g^{-1}$. (AU 2006)

Soln

Given $f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$ and $g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$

$g\cdot f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$

$(g\cdot f)^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \longrightarrow ①$

Now $f^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$, $g^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$

$\therefore f^{-1}\cdot g^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$

$\longrightarrow ②$

from ① and ② we get,

$(g\cdot f)^{-1} = f^{-1}\cdot g^{-1}.$

(17) If $f=\begin{bmatrix}1&2&3&4&5\\2&4&5&1&3\end{bmatrix}$ and $h=\begin{bmatrix}1&2&3&4&5\\5&2&4&3&1\end{bmatrix}$ are permutations on the set $A=\{1,2,3,4,5\}$, find a permutation g on A such that $f\cdot g=h\cdot f$.

Soln: Given $f=\begin{bmatrix}1&2&3&4&5\\2&4&5&1&3\end{bmatrix}$, $h=\begin{bmatrix}1&2&3&4&5\\5&2&4&3&1\end{bmatrix}$ are permutations on five symbols $A=\{1,2,3,4,5\}$.

so, they are bijective function on A and $f^{-1}=\begin{bmatrix}1&2&3&4&5\\4&1&5&2&3\end{bmatrix}$

we have to find g such that $f\cdot g=h\cdot f$.

Now, $f\cdot g=h\cdot f\Rightarrow f^{-1}\cdot(f\cdot g)=f^{-1}\cdot(h\cdot f)$.

$\Rightarrow(f^{-1}\cdot f)\cdot g=f^{-1}\cdot(h\cdot f)$ [composition of functions is associative]

$\Rightarrow I_A\cdot g=f^{-1}\cdot(h\cdot f)$

$\Rightarrow g=f^{-1}\cdot(h\cdot f)$

$$g=\begin{bmatrix}1&2&3&4&5\\4&1&5&2&3\end{bmatrix}\begin{bmatrix}1&2&3&4&5\\5&2&4&3&1\end{bmatrix}\begin{bmatrix}1&2&3&4&5\\2&4&5&1&3\end{bmatrix}$$

$$=\begin{bmatrix}1&2&3&4&5\\5&3&2&4&1\end{bmatrix}.$$

(18) Prove that the set of all matrices $\begin{bmatrix}a&b\\-b&a\end{bmatrix}$ forms an abelian group with respect to matrix multiplication, where a and b are real numbers, not both 0.

Soln: Let $G=\left\{\begin{bmatrix}a&b\\-b&a\end{bmatrix}\,\middle|\,a,b\in R,\ a\neq 0\text{ or }b\neq 0\right\}$

we veify the group axioms. * is matrix multiplication.

1. Closure : Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ be any two elements of G. Not both a,b zero and not c,d zero (i.e) $a^2+b^2 \neq 0$ and $c^2+d^2 \neq 0$.

$$A*B = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix}$$

$= \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$, where $x = ac-bd$, $y = ad+bc$ are real numbers.

and $x^2+y^2 = (ac-bd)^2 + (ad+bc)^2$

$= a^2c^2 + b^2d^2 \, 2abcd + a^2d^2 + b^2c^2 + 2abcd.$

$= a^2c^2+b^2d^2 + a^2d^2 + b^2c^2$

$= a^2(c^2+d^2) + b^2(c^2+d^2)$

$= (a^2+b^2)(c^2+d^2) \neq 0$

$\therefore \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in G \Rightarrow A*B \in G$

$\therefore$ G is closed under $*$.

2. Associativity : We know matrix multiplication is associative. Hence it is true in G also

3. Identity : Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in G be the Identity element,

since $A*I = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = A.$

and $I*A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = A.$

4. Inverse : Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ be an element in G.

where $a^2+b^2 \neq 0$. Suppose $A' = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$.

be the inverse A then $A*A' = I$.

$$\Rightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} * \begin{bmatrix} x & y \\ -y & x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

$$\Rightarrow \begin{bmatrix} ax-by & ay+bx \\ -bx-ay & -by+ax \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\therefore ax-by=1 \rightarrow (1)$ and $ay+bx=0 \rightarrow (2)$

$(1) \times a \Rightarrow a^2x-aby=a$

$(2) \times b \Rightarrow b^2x+aby=0.$

Adding, $(a^2+b^2)x = a \Rightarrow x = \frac{a}{a^2+b^2}$ $[\because a^2+b^2 \neq 0]$

$(2) \Rightarrow ay=-bx \Rightarrow y = \frac{-b}{a} \cdot \frac{a}{a^2+b^2} = \frac{-b}{a^2+b^2}.$

$$\therefore A' = \begin{bmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix}$$

Now $x^2+y^2 = \frac{a^2}{(a^2+b^2)^2} + \frac{b^2}{(a^2+b^2)^2} = \frac{a^2+b^2}{(a^2+b^2)^2} = \frac{1}{a^2+b^2} \neq 0.$

$A' \in G.$

Hence inverse exists.

5. Commutative: Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ be any elements in G, then $A*B = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} * \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$

$$= \begin{bmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{bmatrix}.$$

and $B*A = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} * \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{bmatrix}$

$\therefore A*B = B*A \quad \forall A, B \in G.$

Hence $(G, *)$ is an abelian group.

MODULAR SYSTEM :-

In this set, we define the addition modulo n by

$a +_n b = r$, $0 \leq r < n$

(i.e) r is the remainder when a+b is divided by n.

Multiplication mod n is $a \cdot_n b = r$, $0 \leq r < n$,

(i.e) r is the remainder when ab is divided by n.

For eg, if n=6, the set is {0,1,2,3,4,5}

$2 +_6 5 = 1$, since when $2+5 = 7$ is divided by 6, the remainder is 1 and $3 \cdot_6 4 = 0$, since when $3 \times 4 = 12$ is divided by 6, the remainder is 0.

---

(19) Show that the set G = {0,1,2,3,4,5} is group under addition modulo 6.

Soln : Given G = {0,1,2,3,4,5} is the modulo set we have t prove that $(G, +_6)$ is a group.

We form the cayley table and verify the group axioms

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Closure :- The body of the table containe only elements of G once in each row and column. So, G is closed under $+6$.

Associativity : Since usual addition is associative, $+6$ is associative.

Inverse : Inverse of 0 is 0, Inverse of 1 is 5
" " 2 is 4, " " 3 is 3
" " 4 is 2, " " 5 is 1.

Further $a +_6 b = b +_6 a$ ∀ $a, b \in G$, since the elements equidistant from the main diagonal are the same.

∴ $(G, +_6)$ is an abelian group.

IIIly, $G = \{0, 1, 2, 3, \ldots, n-1\}$ is a group under $+_n$.

Note :

But G is not a group under $\cdot_6$.

The cayley table is given below.

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	3	0	4	3
5	0	5	4	3	2	1

In the body of the table, the elements are repeated in some of the rows and columns.

For a group, there should not be repetition in any row or column. So $(G, \cdot_6)$ is not a group.

If $n = p$ is a prime, then the non-zero modular set $\{1, 2, 3, \ldots, p-1\}$ is a group under multiplication mod p.

SUBGROUP.

Let $(G, *)$ be a group. A non-empty subset H of G is said to be a subgroup of G is H itself is a group under the same operation * of G.

It is obvious $(\{e\}, *)$ and $(G, *)$ are subgroups of $(G, *)$. These two subgroups are called trivial subgroups of $(G, *)$. All other subgroups of $(G, *)$ are called non-trivial subgroups.

The non-trivial subgroups are also known as proper subgroups.

THEOREM 7 :- A Non-empty subset H of a group $(G, *)$ is a subgroup of G if and only if $a * b^{-1} \in H$ $\forall a, b \in H$ [AU 2008, 2012]

Proof! Let H be a subgroup of G.

Then H itself is a group under $*$.

$\therefore a, b \in H \Rightarrow a, b^{-1} \in H$

Hence $a * b^{-1} \in H$, by closure.

Conversely, let H be a non-empty subset of G such that $a * b^{-1} \in H$, $\forall a, b \in H$.

We have to prove H is a subgroup of G. So, we have to verify the axioms.

Since H is non-empty, there exists an element $a \in H$.

Then by the given condition $a * a^{-1} \in H \Rightarrow e \in H$.

So, identity exists in H.

If $x \in H$ is any element, then

$$x, e \in H \Rightarrow e * x^{-1} \in H$$
$$\Rightarrow x^{-1} \in H$$

$\therefore$ inverse exists in H for every element in H.

Further, $a, b \in H \Rightarrow a, b^{-1} \in H$ [$\because$ inverse exists in H.

$\Rightarrow a*(b^{-1})^{-1} \in H \Rightarrow a*b \in H$

So, H is closed under * and hence closure axiom is Satisfied.

Since $H \subset G$, associative axiom is inheited in H so associative axiom is satisfied.

$\therefore (H, *)$ is a group and hence a subgroup of $(G, *)$.

NOTE: If the Binary operation of a group G is denoted by +, then the inverse of a denoted by $-a$ instead of a^{-1}. So the condition $a*b^{-1} \in H$ is written as $a-b \in H$.

Next we shall prove that a finite subset is a subgroup if closure is satisfied.

(23) If H_1 and H_2 are subgroups of a group $(G, *)$ prove that $H_1 \cap H_2$ is a subgroup of $(G, *)$.

Soln: Given H_1, H_2 are subgroups of $(G, *)$

Let $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H$ and $a, b \in H_2$.

Since H_1 and H_2 are subgroups by criterion for subgroup (theorem 7).

$a, b \in H_1 \Rightarrow a*b^{-1} \in H_1$.

and $a, b \in H_2 \Rightarrow a*b^{-1} \in H_2$.

$\therefore a*b^{-1} \in H_1 \cap H_2$

Thus $a, b \in H_1 \cap H_2 \Rightarrow a*b^{-1} \in H_1 \cap H_2$.

Hence $H_1 \cap H_2$ is a subgroup of G.

NOTE: It can be extended to more than two subgroups.

If $H_1, H_2, \dots H_n$ are subgroups of G, then $H_1 \cap H_2 \cap, \dots, \cap H_n$ is a subgroup of G.

(24) Let S be a non-empty set and $p(S)$ denote the power set of S. Verify whether $(p(S), \cap)$ is a group. [AU 2008]

Soln: We know that the power set $p(S)$ is the set of all subsets of S. The binary operation on $p(S)$ is $\cap$.

Let $G = p(S)$. We shall verify the axioms of a group.

Closure: Let A, B be any two subsets of S.

$\therefore A \cap B$ is a subset of S.

Thus $A, B \in p(S) \Rightarrow A \cap B \in p(S)$

So $p(S)$ is closed under $\cap$.

Associativity: Since $\cap$ is associative in any collection of sets, it is true in $p(S)$.

So associative axiom is satisfied.

Identity:- Let $A \in p(S)$ be any element. (i.e) A is any subset of S. Then $A \cap S = S \cap A = A$

$\therefore S$ is the identity element in $p(S)$ for $\cap$.

Inverse: Let A be any subset of S.

Since S is the identity, it is obvious there is no subset B of S such that $A \cap B = S$.

So inverse axiom is not satisfied.

Hence $(p(S), \cap)$ is not a group.

NOTE: $(p(S), \cap)$ is only a semi-group with identity or monoid.

(26) Find all the non-trivial subgroups of $(Z_6, +_6)$ [AU 2006]

Soln: $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$

$H_1 = \{[0], [3]\}$, $H_2 = \{[0], [2], [4]\}$ are all the non-trivial subgroups of $(Z_6, +_6)$.

$+_6$	[0]	[3]
[0]	[0]	[3]
[3]	[3]	[0]

$+_6$	[0]	[2]	[4]
[0]	[0]	[2]	[4]
[2]	[2]	[4]	[0]
[4]	[4]	[0]	[2]

Since H_1, H_2 are finite subsets of G_1, H_1 and H_2 are closed under $+_6$, $(H_1, +_6)$, $(H_2, +_6)$ are subgroups of $(z_6, +_6)$.

(27) Determine $H = \{0,5,10\}$ and $K = \{0,4,8,12\}$ are subgroups of the group $(Z_{15}, +_{15})$ [AU 2007]

Soln: The modular set $Z_{15} = \{0,1,2,3 \cdots 14\}$

Given $H = \{0,5,10\}$, $K = \{0,4,8,12\}$ are finite subsets of Z_{15}. To verify they are subgroups, it is enough to verify the closure axiom.

$+_{15}$	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

H.

$+_5$	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

K

H is closed under $+_{15}$ and so H is a subgroup. But K is not closed under $+_{15}$, because the body of the composition table contains elements not in K. Hence K is not a subgroup of Z_{15}.

CYCLIC SUBGROUP

Let $(G, *)$ be a group and $a \in G$. Then $H = \{a^n \mid n \in Z\}$ is a subgroup of G. H is called the cyclic subgroup of G generated by a and it is denoted by (a) or $\langle a \rangle$.

In the group $(Z_{12}, +_{12})$, $\{[0], [3], [6], [9]\}$ is the cyclic subgroup generated by $[3]$, since $2[3]=6$, $3[3]=9$, $4[3]=12]$ $=[0]$.

CYCLIC GROUP.

A Group $(G, *)$ is said to be a cyclic group if there exists an element $a \in G$ such that every element $x \in G$ is of the form a^n for some integer n. The element a is called a generator of G and is written as $G=(a)$ or $\langle a \rangle$. It is read as G is cyclic group generated by a.

For eg,

The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic group generated by i, since $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.

It can be seen easily that $-i$ is another generator

1. **Theorem 9:** Any cyclic group is abelian.

Proof: Let G be a cyclic group generated by 'a'.

Then $G = \{a^n \mid n \in Z\}$

Let $x, y \in G$ be any 2 elements then $x = a^m$, $y = a^n$ for some integers m and n

Now $x * y = a^m * a^n = a^{m+n}$

$y * x = a^n * a^m = a^{n+m}$

$x * y = y * x \quad \forall x, y \in G$

Hence G is abelian.

Note: The converse is not true (i,e) abelian group is not acyclic. Eg: $(Q, +)$ is abelian but not cyclic

2. **Theorem 10:** Every subgroup of cyclic group is cyclic

Proof: Let $(G, *)$ be cyclic group generated by a

Then $G = \{a^n \mid n \in Z\} = \langle a \rangle$

Let H be a subgroup of G

Since H is subset of G, every element of H is of the form a^r for some $r \in Z$

Since H is a group if $a^r \in H$, then its inverse $(a)^{r-1} = a^{-r} \in H$. So either r or $-r$ is +ve integer. Hence H contains positive integer powers of a.

Let m be a least +ve integer such that $a^m \in H$. We shall prove a^m is generator of H. Let $x \in H$ be any element, then $x = a^n$ for some $n \in Z$.

For integers 'n', 'm' by Eucledian division ~~distance~~ algorithm, we can find integers 'q' and 'r' Such that $n = mq + r$, $0 \le r < m$.

Then, $x = a^n = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r$

$$\Rightarrow (a^m)^{-q} * x = (a^m)^{-q} * (a^m)^q * a^r$$

$$= e * a^r$$

$$= a^r$$

$$\therefore a^r = (a^m)^{-q} * x = a^{-mq} * x.$$

Now $a^m \in H \Rightarrow (a^m)^q \in H$, by closure

$\Rightarrow a^{mq} \in H$

$\Rightarrow a^{-mq} \in H$, Since H is group

$\therefore a^{-mn} \in H$, by closure

$\Rightarrow a^r \in H$, where $r < m$

If $r \neq 0$, then $a^r \in H$ is a contradiction to the fact that 'm' is the least positive integer such that $a^m \in H$

Hence $r = 0$

$$n = mq \Rightarrow x = (a^m)^q$$

Thus any element of H is integral power of a^m.

So H is acyclic group generated by a^m

(i,e) $H = \langle a^m \rangle$

Theorem 11 : If $(G, *)$ is cyclic group generate by 'a', then prove a^{-1} is also generator.

Proof: ~~G~~ ~~Given G = <a>~~ Given $G = \langle a \rangle$

So any element $x \in G$ is $x = a^n$ for some integer n.

Now $x = a^n = (a^{-1})^{-n}$

Thus 'x' is integral ~~part~~ power of a^{-1} and

So a^{-1} is also a generator.

Order of element:

Definition: Let $(G, *)$ be a group and let $a \in G$. The order of 'a' is least positive integer 'm' such that $a^m = e$.

The order of 'a' is denoted by $O(a)$ and we write $O(a) = m$

If no such integer exist, then we say that 'a' is of infinite order.

Example: In group $G = \{1, -1, i, -i\}$ under usual multiplication, $O(i) = 4$, $O(-i) = 4$ and $O(-1) = 2$

Ans: Since $i^2 = -1$

$i^4 = (-1)^2 = 1$ and $(-1)^2 = 1$

Theorem 12: Let $(G, *)$ be finite cyclic group generated by an element $a \in G$. If $O(G) = n$, then $a^n = e$ and so $G = \{a, a^2, a^3, a^{n-1}, a^n = e\}$. Further $O(a) = n$

That is 'n' is least positive integer such that $a^n = e$

Proof: Given $(G, *)$ is finite cyclic group generated by 'a'.

First we shall prove that $a^m = e$ is not possible for $m < n$.

Assume it is possible (i,e) $a^m = e$, $m < n$

Since G is cyclic group generated by 'a' by any element $x \in G$ is integral power of 'a'. (i,e) $x = a^k$ for some integers k.

Now for integers m, k by Eucledian division, we can find integers q & r such that $k = mq + r$, $0 \le r < m$.

$$\therefore x = a^k = a^{mq+r} = a^{mq} * a^r = e * a^r = a^r$$

Thus any element of G is a^r for $r < m$. This means the no: of elements of G is atmost 'm'. (i,e) $O(G) = m < n$, which contradics the hypothesis $O(G) = m$.

Hence $a^m = e$ is not possible for $m < n$

$$\therefore a^n = e$$

Next we shall prove that elements $a, a^2, a^3 \dots a^n$ are all distinct.

Suppose it is not true, then there are repititions.

Let $a^s = a^r$, $0 < r < s \leq n$

$\Rightarrow a^s * a^{-r} = a^r * a^{-r}$

$\Rightarrow a^{s-r} = a^0 = e$, $0 < s-r < n$

This is again a contradiction by 1st part,

$\therefore$ all elements are distinct

$\therefore a, a^2 \ldots a^n = e$ are all distinct

Since $O(G) = n$, it follows $G = \{a, a^2 \ldots a^n = e\}$ and $a^n = e$. So $O(a) = n$.

Cycles and transpositions

Def: Let $S = \{a_1, a_2 \ldots a_n\}$ and σ be permutation on S. σ is called cycle of length r if there exist r elements $a_1, a_2 \ldots a_r$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3 \ldots \sigma(a_{r-1}) = a_r$ and $\sigma(a_r) = a_1$

This cycle is represented by symbol $(a_1, a_2 \ldots a_r)$ or $(a_1\, a_2 \ldots a_r)$

Def: Two cycles are said to be disjoint if they have no elements in common

eg: $(1\ 2\ 3)$, $(4\ 5)$ disjoint cycles.

Def: A cycle of length 2 is transposition

Def: If a permutation σ is a product of even number of transposition, then σ is even transposition.

If a permutation σ is pdt of odd no: of transposition, then σ is odd transposition

Example sum

1. Compute pdt. $(1\ 2)(2\ 4)(3\ 6)$ as permutation on $\{1, 2, 3, 4, 5, 6\}$. Find (i) even/odd (ii) order

ANSWER:

Let $\sigma = (1\ 2)(2\ 4)(3\ 6)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 4 & 5 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix}$$

We shall write σ as pdt. of disjoint cycles

$\sigma = (1\ 4\ 2)(3\ 6)$ $\quad 1 \to 4 \to 2 \to 1$ cycles

$3 \to 6 \to 3$

Order of cycle $(1\ 4\ 2)$ is 3 and the order of cycle $(3\ 6)$ is 2

$\therefore$ Order of $\sigma = \text{lcm}\{3,2\} = 6$

Now to decide σ is odd or even, we shall write σ as product of transposition

$$\sigma = (1\ 4)(1\ 2)(3\ 6)$$

σ is pdt of 3 transposition.

$\boxed{\therefore \sigma \text{ is odd permutation}}$

Examples 2:

Express $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$ in S_9 as a pdt of disjoint cycles. Decide its order and test it is odd or even.

ANSWER:

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$$

we see $1 \to 2 \to 3 \to 4 \to 5 \to 1$

So one cycle is $(1\ 2\ 3\ 4\ 5)$

6 and 7 are left fixed.

$8 \to 9 \to 8$. So another cycle $(8\ 9)$

$$\theta = (1\ 2\ 3\ 4\ 5)(8\ 9)$$

Order of $(1\ 2\ 3\ 4\ 5)$ is 5 and order of $(8\ 9)$ is 2.

$\therefore$ order of $\theta = \text{lcm}(5,2) = 10$.

Further $\theta = (1\ 2)(1\ 3)(1\ 4)(1\ 5)(8\ 9)$ is a pdt 5 transposition.

$\boxed{\therefore \theta \text{ is odd permutation}}$

Cosets & Legrange's theorem

Cosets: Let $(H, *)$ be a subgroup of $(G, *)$. Then set Let $a \in G$ be any element. $aH = \{a * h \mid h \in H\}$ is called left coset of H in G determined by 'a'.

Sometimes aH is written as $a * H$

The set $Ha = \{h * a \mid h \in H\}$ is called right coset of H in G determined by 'a'.

Theorem 13: Let $(H, *)$ be a subgroup of $(G, *)$ Then the set of all left cosets of H in G form partition of G. That is every element of G belongs to only one left coset of H in G.

Proof: Let aH and bH be any 2 left coset.

We shall prove either $aH = bH$ or $aH \cap bH = \phi$

Suppose $aH \cap bH \neq \phi$ then there exist an element $x \in aH \cap bH$

$\Rightarrow x \in aH$ and $x \in bH$

$\Rightarrow x = a*h_1$ and $x = b*h_2$, for some $h_1, h_2 \in H$

$\therefore a*h_1 = b*h_2$

$\Rightarrow (a*h_1)*h_1^{-1} = (b*h_2)*h_1^{-1}$

$\Rightarrow a*(h_1*h_1^{-1}) = b*(h_2*h_1^{-1})$

$\Rightarrow a*e = b*(h_2*h_1^{-1})$

$\Rightarrow a = b*(h_2*h_1^{-1})$

If 'x' is any element in aH, then

$x = a*h$

$x = b*(h_2*h_1^{-1})*h$

$= b*(h_2*h_1^{-1}*h) \in bH$

$x \in aH \Rightarrow x \in bH$

$\therefore aH \subseteq bH \rightarrow \textcircled{2}$

Similarly we can prove $bH \subseteq aH \rightarrow \textcircled{3}$

From (2) & (3), $\boxed{aH = bH}$

Thus any 2 cosets are either equal or disjoint

Further $\bigcup_{a \in G} aH \subseteq G$. since union of subset is subset.

If 'x' is any element in G, then

$x = x * e \in xH$

$\therefore$ x is in left coset and hence $x \in \bigcup_{a \in G} aH$

Hence

$x \in G \Rightarrow x \in \bigcup_{a \in G} aH$

$\Rightarrow G \subseteq \bigcup_{a \in G} aH$ $\boxed{\therefore G = \bigcup_{a \in G} aH}$

This is all left coset partition G.

Theorem 14: There is one to one correspondance between any 2 left cosets of H in G

Proof: Let (H,*) be subgroup of (G,*) Let aH be any left coset of H in G. we know H itself is left coset. So its enough to prove that there is 1 to 1 correspondence between H and aH

Let $f : H \to aH$ be defined by $f(h) = a * h$ $\forall h \in H$

The maping is 1 to 1.

For any $h_1, h_2 \in H$ if $f(h_1) = f(h_2)$

then $a * h_1 = a * h_2$

$\Rightarrow h_1 = h_2$ (left cancelation law)

Now we prove f is onto

Let $x \in aH$ be any element, then $x = a*h$ for some $h \in H$. For this h we have $f(h) = a*h = x$.

So, f is onto.

Hence 'f' is bijective function of H onto aH

$\therefore$ f set up a 1 to 1 corresponce between H and aH

<u>Note</u>: (1) If H is finite, H and aH have same no: of elements

$$\therefore O(H) = O(aH)$$

(2) 13 and 14 theorem are true for right coset also.

<u>Theorem 15</u>: Legrange Theorem.

The order of a subgroup H of finite group G divides the order of group. That is of Order H divides order of G.

Proof: Let $(G,*)$ be a group of order 'n' and $(H,*)$ be a subgroup of order m.

Since G is finite group, the no: of left coset of H in G is finite

Let 'r' be no: of cosets of H in G

Let 'r' cosets be $a_1H, a_2H \ldots\ldots a_rH$

we know that left coset of G form partition of G. [by theorem-13]

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

$$\therefore O(G) = O(a_1H \cup a_2H \ldots \cup a_rH)$$

$$= O(a_1H) + O(a_2H) \ldots\ldots + O(a_rH)$$

But $O(a_iH) = O(H)$ (theorem-14)

$\therefore O(G) = O(H) + O(H) + \cdots O(H)$, r times

$$\Rightarrow O(G) = r\, O(H)$$

$$\Rightarrow \frac{O(G)}{O(H)} = r$$

Thus $O(H)$ divides $O(G)$.

Index of H in G

Def: Let $(H,*)$ be subgroup of $(G,*)$. Then the no: of different left (right) cosets of H in G is called index of H in G and is denoted by $[G:H]$ or $i_G H$

Note: * In case of finite group $i_G(H) = \frac{O(G)}{O(H)}$

* It is quite possible in an infinite group there is a subgroup of finite index.

Corollary 1: The order of any element of finite group G divides $O(G)$

Proof: Let G be finite group of order 'n'.

Let $a \in G$ be element & $O(a) = m$.

Then cyclic group $\langle a \rangle$ is of order m.

By legrange theorem,

$$\boxed{O(\langle a \rangle) \mid O(G) \Rightarrow m \mid n}$$

$\therefore$ order of element divides $O(G)$

Corollary 2: Any group of prime order is ~~spe~~ cyclic

Proof: Let 'G' be a group of order P, where P is a prime number

Let $a \in G$, $a \neq e$. Let $H = \langle a \rangle$

Since $a \neq e$, $O(H) \neq 1$ $\therefore O(H) \geq 2$

By legrange theorem, $O(H) \mid O(G)$

$\Rightarrow O(H) \mid P \Rightarrow O(H) = P$ (Since P is prime ≥ 2)

$= O(G)$

Hence $G = H = \langle a \rangle$. G is cyclic.

$\therefore$ Any group of prime order is cyclic.

Note: * If $O(G) = P$, then every element other than identity e is generator of group.

* If G is cyclic group of order P, a prime then G has no proper subgroup

Normal Subgrps & Quotient groups:

Normal Subgroups: In general, $Ha \neq aH$. The subgroup H of G for which $Ha = aH$ $\forall a \in G$ is a special class of subgroups called normal subgroups.

Def: A subgroup $(H, *)$ of $(G, *)$ is called normal subgroup of G if $aH = Ha$ $\forall a \in G$

Examples 1: Every group of an abelian group is normal

Sol: Let $(G,*)$ be an abelian group and $(H,*)$ be a subgroup of G

Let $a \in G$ be any element

Then $aH = \{a*h \mid h \in H\}$

$= \{h*a \mid h \in H\}$ [$\because G$ is abelian]

$= Ha$

Since 'a' is arbitary, $aH = Ha \ \forall a \in G$

$\therefore H$ is normal subgroup of G

Note: Since $H_n = nZ$ is subset of Z and $(Z,+)$ is an abelian group, subgroup $(H_n,+)$ is a normal subgroup of Z

Examples: Prove that intersection of two normal subgroup of $(G,*)$ is a normal subgroup of $(G,*)$

Sol: Let $(N_1,*)$ and $(N_2,*)$ be 2 normal subgroup of $(G,*)$.

~~Since~~ To prove $(N_1 \cap N_2, *)$ is normal subgroup of $(G,*)$

Since N_1, N_2 are normal subgroup of G, they are basically subgroups. We know $N_1 \cap N_2$ is subgroup of G. Now we shall prove it is a normal subgroup of G.

Let $n \in N_1 \cap N_2$ be any element and $a \in G$ be any element.

Then $n \in N_1$ and $n \in N_2$.

Since N_1, N_2 are normal, $a n a^{-1} \in N_1$ and $a n a^{-1} \in N_2$

$\therefore a n a^{-1} \in N_1 \cap N_2$.

Hence $N_1 \cap N_2$ is normal, from above example.

Quotient group or factor group:

If $(N, *)$ is a normal subgroup of $(G, *)$ then the group $((G/N, \oplus)$ is called quotient group or factor group of G by N or quotient group modulo N.

Direct product of 2 groups:

Theorem 17: Let $(G, *)$ and (H, Δ) be two groups. Let $G \times H$ be cartesian product of G and H.

If $\cdot$ is the binary operation $G \times H$ gn/. by $(g_1 h_1) \cdot (g_2 h_2) = (g_1 * g_2, h_1 \Delta h_2)$ for any $(g_1, h_1), (g_2 h_2) \in G \times H$ then $(G \times H, \cdot)$ is group.

Proof: Given $(G, *)$, (H, Δ) are groups, Let e_1, e_2 be identities of G and H.

$G \times H = \{(g, h) \mid g \in G, h \in H\}$

$\cdot$ is binary operation componentwise multiplication.

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \Delta h_2) \; \forall (g_1, h_1), (g_2, h_2) \in G \times H$

$g_1 * g_2 \in G$ and $h_1 \Delta h_2 \in H$

$(g_1 * g_2, h_1 \Delta h_2) \in G \times H$

$\Rightarrow (g_1, h_1) \cdot (g_2, h_2) \in G \times H$

So closure is satisfied.

Associativity: Let x, y, z be any 3 elements of $G \times H$.

$\therefore x = (g_1, h_1), y = (g_2, h_2), z = (g_3, h_3)$

for some $g_1, g_2, g_3 \in G$ and $h_1, h_2, h_3 \in H$.

$$\begin{aligned}
\text{Now } x \cdot (y \cdot z) &= (g_1 \cdot h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)) \\
&= (g_1, h_1) \cdot (g_2 * g_3, h_2 \Delta h_3) \\
&= (g_1 * (g_2 * g_3), h_1 \Delta (h_2 \Delta h_3)) \\
&= ((g_1 * g_2) * g_3, (h_1 \Delta h_2) \Delta h_3)
\end{aligned}$$

[$\because$ $*$ and Δ are associative]

$= \left((g_1, h_1) \cdot (g_2, h_2) \right) \cdot (g_3, h_3)$

$= (x \cdot y) \cdot z$

$\therefore$ associative axiom is satisfied

Identity: (e_1, e_2) is identity element of $G \times H$, where e_1 is the identity of G and e_2 is identity of H.

For if $(g, h) \in G \times H$ be any element then

$(g, h) \cdot (e_1, e_2) = (g * e_1, h \Delta e_2) = (g, h)$

and $(e_1, e_2) \cdot (g, h) = (e_1 * g, e_2 \Delta h) = (g, h)$

$\therefore$ (e_1, e_2) is identity of $G \times H$

Inverse: Let (g, h) be any element of $G \times H$.

Since $g \in G$, $h \in H$ and so $(g^{-1}, h^{-1}) \in G \times H$

Now $(g, h) \cdot (g^{-1}, h^{-1}) = (g * g^{-1}, h \Delta h^{-1}) = (e_1, e_2)$

$(g^{-1}, h^{-1}) \cdot (g, h) = (g^{-1} * g, h^{-1} \Delta h) = (e_1, e_2)$

$\therefore$ (g^{-1}, h^{-1}) is inverse of (g, h)

$\therefore$ Inverse axiom is satisfied.

Hence $(G \times H, \cdot)$ is group.

This group is called direct product of G and H

Group Homomorphism :

Let $(G, *)$ and $(G', \cdot)$ be 2 groups. A mapping $f : G \to G'$ is called group homomorphism if for all $a, b \in G$.

$$f(a * b) = f(a) \cdot f(b)$$

Elementary properties of homomorphism :

Theorem 18 : If f is a homomorphism from group $(G, *)$ into $(G', \cdot)$ then prove that

(i) $f(e) = e'$, where e, e' are identities of G and G' respectively.

(ii) $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$

Proof (i) Let $a \in G$ be any element.

Then $a * e = a$

$\Rightarrow f(a * e) = f(a)$

$\Rightarrow f(a) \cdot f(e) = f(a)$ [$\because f$ is homomorphism

$\Rightarrow f(a) \cdot f(e) = f(a) \cdot e'$

By left cancellation law in G', we get $f(e) = e'$

(ii) Let $a \in G$ be any element.

Then $a * a^{-1} = a^{-1} * a = e$

$\therefore f(a * a^{-1}) = f(e) = f(a) \cdot f(a^{-1}) = e'$ (by (i))

and $f(a^{-1} * a) = f(e) \Rightarrow f(a^{-1}) \cdot f(a) = e'$

$\therefore f(a^{-1})$ is inverse of $f(a)$ in G'.

$\Rightarrow [f(a)]^{-1} = f(a^{-1})$

This theorem says that under homomorphism identities correspond and inverse correspond

Types of homomorphism:

Def: Let $f: G \to G'$ be homomorphism of groups

(i) If f is one-one, the f is monomorphism

(ii) If f is onto, then f is epimorphism

(iii) In case G' is called homomorphic image of G

(iii) If f is one-one and onto, then f is isomorphism.

In case the two groups are said to be isomorphic and we write $G \approx G'$.

Def: Let $(G, *)$ be a group. A homomorphism $f : G \to G$ is called endomorphism.

If f is one-one and onto, then f is automorphism of G. (i,e) an isomorphism of G onto G is called automorphism

Def: Kernel of group homomorphism

Let $(G, *)$ and $(G', \cdot)$ be groups with e' as identity of G'. Let $f : G \to G'$ be ~~homo~~ homomorphism.

The kernel of f is set of all elements of G which are maped onto e' and denoted by ker f.

Thus $\ker f = \{ a \in G \mid f(a) = e' \}$

Theorem 19: Show that kernel of a group homomorphism is a normal subgroup of the group.

Proof: Let $(G, *)$ and $(G', \cdot)$ be the group and $f : G \to G'$ is a group homomorphism then we know $f(e) = e'$, where e, e' are identities of G and G'

$\therefore$ $e \in \ker f$ and hence $\ker f$ is non-empty subset of G.

First we shall prove $\ker f$ is a subgroup of G.

Let $x, y \in \ker f$, then $f(x) = e'$ & $f(y) = e'$

Now $f(x * y)^{-1} = f(x) \cdot f(y^{-1})$ [$\because f$ is homomorphism]

$$= f(x) \cdot [f(y)]^{-1}$$

$$= e' \cdot (e')^{-1} = e'$$

$\therefore$ $x * y^{-1} \in \ker f$.

~~Now~~ Hence $\ker f$ is subgroup of G

Next we shall prove that $\ker f$ is normal subgroup.

Let $n \in \ker f$ be any element and $a \in G$ be any element.

$\therefore$ $f(n) = e'$, $f(a) \in G'$

Now $f(a * n * a^{-1}) = f(a) \cdot f(n) \cdot f(a^{-1})$

$$= f(a) \cdot e' \cdot (f(a))^{-1}$$

$$= f(a) \cdot (f(a))^{-1} = e'$$

$\therefore$ $a * n * a^{-1} \in \ker f$

∴ Hence ker f is normal subgroup of G

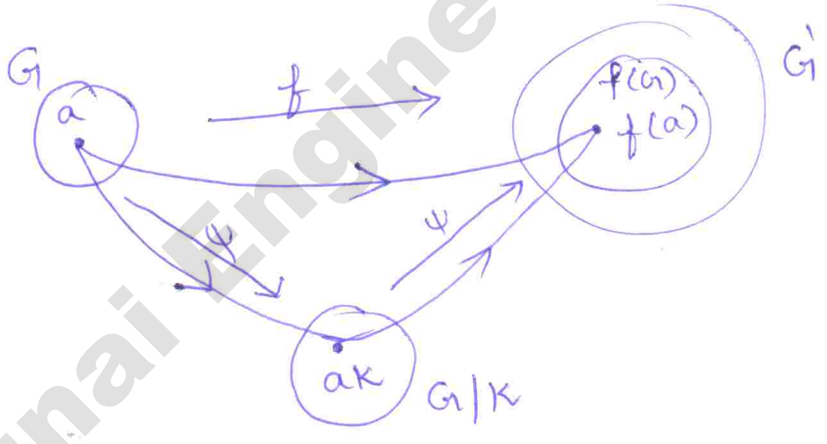
Theorem 21: Fundamental theorem of group homomorphism.

Let $(G, *)$ and $(G', \cdot)$ be two groups.

Let $f : G \to G'$ be a homomorphism of groups with kernal K. Then G/K is isomorphic to $f(G) \subseteq G'$.

Proof: we have to prove $G/K \cong f(G)$

Define the map $\psi : G/K \to f(G)$ by $\psi(aK) = f(a)$ $\forall$ $aK \in G/K$ and $a \in G$



First we shall prove ψ is well defined.

If $aK = bK$, then $a * x_1 = b * x_2$ for some $x_1, x_2 \in K$

$\Rightarrow a = b * x_2 * x_1^{-1} = b * x$, where $x = x_2 * x_1^{-1} \in K$

$\therefore f(a) = f(b * x) = f(b) \cdot f(x)$

[∵ f is homomorphism]

$= f(b) \cdot e' = f(b)$ $[\because x \in K \Rightarrow f(x) = e']$

$\Rightarrow \varphi(aK) = \varphi(bK)$

$\therefore \varphi$ is well defined.

Now we shall prove φ is homomorphism.

Let $aK, bK \in G/K$ be any 2 elements.

Then $\varphi(aK \oplus bK) = \varphi((a * b)K) = f(a * b)$

$= f(a) \cdot f(b)$

$= \varphi(aK) \cdot \varphi(bK)$

$\therefore \varphi$ is homomorphism of G/K into $f(G)$.

Next we shall prove φ is one-one and onto.

Suppose $\varphi(aK) = \varphi(bK)$

then $f(a) = f(b)$

$\Rightarrow [f(a)]^{-1} \cdot f(b) = e' \Rightarrow f(a^{-1} * b) = e'$

$\Rightarrow a^{-1} * b \in K \Rightarrow b = aK$

$\Rightarrow bK = aK$ $[\because KK = K]$

$\therefore \varphi$ is one-one

Finally, suppose $x \in f(G)$ then there exist an $a \in G$ such that

$x = f(a) = \varphi(aK)$

$\therefore \varphi$ is onto

Thus ψ is isomorphism of G/K onto $f(G)$

$$\boxed{\therefore\ G/K \approx f(G)}$$

Note Supose $f : G \to G'$ is onto, $G' = f(G)$

$\therefore$ the result will be $G/K \approx G'$

Theorem 24: Cayley's theorem.

Every finite group of order n is isomorphic to permutation group of degree n.

Proof: Let $a \in G$ be any element. Correspondi to 'a' we define a map

$f_a : G \to G$ by $f_a(x) = a * x \ \forall\ x \in G$

Then f is one-one, for $f_a(x) = f_a(y)$.

$\Rightarrow a * x = a * y$.

$\Rightarrow x = y$ (by left cancellation)

Now $y \in G$ (codomain), then $a^{-1} * y \in G$ such that $f_a(a^{-1} * y) = a * (a^{-1} * y) = (a * a^{-1}) * y$

$= e * y = y$

$\therefore f_a$ is onto

Thus f_a is one-one and onto function

from $G \to G$ and so it is permutation on G. Since G has 'n' elements f_a is a permutation on 'n' symbols or permutation of degree 'n'.

Let $G' = \{f_a \mid a \in G\}$. we shall prove G' is group

we verify axioms of the group.

Let $f_a, f_b \in G'$ be any 2 elements, (i,e) f_a, f_b are functions from $G \to G$.

$$\text{Then } (f_a \cdot f_b)(x) = f_a(f_b(x)) = f_a(b*x)$$
$$= a*(b*x)$$
$$= (a*b)*x$$
$$= f_{a+b}(x) \;\forall\, x \in G$$

$$\Rightarrow f_a \circ f_b = f_{a+b} \longrightarrow (1)$$

Since $a, b \in G$, $a*b \in G$ and so $f_{a*b} \in G'$

$\Rightarrow f_a \circ f_b \in G'$. Hence G' is closed under composition of func operation.

$f_e \in G'$ is identity element. $f_{a^{-1}}$ is inverse of $f_a \in G'$.

So, G' is group.

Finally, we prove $\boxed{G \cong G'}$

Let $\phi : G \to G'$ be defined by $\phi(a) = f_a \ \forall a \in G$

Now for any $a, b \in G$, $\phi(a * b) = f_{a*b}$

$$= f_a \cdot f_b$$

$$= \phi(a) \cdot \phi(b)$$

$\therefore \phi$ is homomorphism.

Suppose $\phi(a) = \phi(b)$, then $f_a = f_b$

$\Rightarrow f_a(x) = f_b(x) \ \forall x \in G$

$\Rightarrow a * x = b * x$

$\Rightarrow a = b$

$\therefore \phi$ is one-one

Now let $f_a \in G'$ be any element, with $a \in G$

Then $\phi(a) = f_a$ and so ϕ is onto

Thus ϕ is isomorphism of G onto G'

$\therefore G \cong G'$

Example sums:

38. Determine all cosets of subgroup $H = \{1, a^2\}$ of group $G = \{1, a, a^2, a^3\}$ under multiplication where $a^4 = 1$

ANSWER:

Given $G = \{1, a, a^2, a^3\}$, $a^4 = 1$ is group under

$H = \{1, a^2\}$. we shall find all left coset of H

Now $H = \{1 \cdot h \mid h \in H\} = \{1, a^2\} = H$

$aH = \{a \cdot h \mid h \in H\} = \{a \cdot 1, a \cdot a^2\} = \{a, a^3\}$

$a^2H = \{a^2 \cdot h \mid h \in H\} = \{a^2 \cdot 1, a^2 \cdot a^2\} = \{a^2, a4\}$

$a^3H = \{a^3 \cdot h \mid h \in H\} = \{a^3 \cdot 1, a^3 \cdot a^2\} = \{a^3, a$[illegible]$\}$

$[\because a^4 = 1]$

$\rightarrow a^2H = \{a^2, 1\} = H$

Thus there are 2 distinct left cosets of H in G namely

$H = \{1, a^2\}$ and $\{a, a^3\}$

Example sum

39) If H is a subgrp of G such that $x^2 \in H$ $\forall$ $x \in G$, prove H is normal subgrp of G

ANSWER:

Let G be a multiplicate group. ~~$x^2 \in H$~~

Gn, H is subgroup of G such that ~~$\forall x \in G$~~

$x^2 \in H \quad \forall x \in G \longrightarrow ①$

we have to prove H is normal Subgrp.

Let $h \in H$ be any element and $a \in G$ be any element.

Then $ah \in G$ $\therefore (ah)^2 \in H$ (from ①)

Since $a^{-1} \in G$, $(a^{-1})^2 \in H \Rightarrow a^{-2} \in H$ (from ①)

Since $h \in H$ and H is subgroup, we have $h^{-1} \in H$

$\therefore h^{-1} a^{-2} \in H$

Hence $(ah)^2 h^{-1} a^{-2} \in H$ [by closure]

$\Rightarrow ah(ah)h^{-1}a^{-2} \in H$

$\Rightarrow aha(hh^{-1})a^{-2} \in H$ [associative]

$\Rightarrow ahaea^{-2} \in H$ [e → identity]

$ahaa^{-2} \in H$

$aha^{-1} \in H$

Hence H is normal subgroup of G

Example sum:

40) Let G be group and $a \in G$. Show that the map $f: G \to G$ defined by $f(x) = axa^{-1}$ $\forall x \in G$ is an isomorphism

ANSWER

Let G be multiplicative group

Given $f: G \to G$ and $f(x) = axa^{-1}$ $\forall x \in G$ and $a \in G$ is fixed element.

First we shall prove it is homo-morphism

For any $x, y \in G$, $f(xy) = a(xy)a^{-1}$ [by definiti

$= axeya^{-1}$ [e identity of G)

$= ax(a^{-1}a)ya^{-1}$

$= (axa^{-1})(axa^{-1})$

$= f(x) f(y)$

∴ f is homomorphism

Now we shall prove f is one-one & onto.

Suppose $f(x) = f(y)$ then $axa^{-1} = aya^{-1}$

$\Rightarrow x = y$,

∴ f is one-one.

If $y \in G$ (co-domain) be any element

then $a^{-1}ya \in G$

Let $x = a^{-1}ya$

Now $f(x) = axa^{-1} = a(a^{-1}ya)a^{-1}$

$= $ ~~eye~~ eye

$= y$

Thus for any $y \in G$ we are able to find $x \in G$ whose image is y. Hence 'f' is onto

Hence f is isomorphism

Semi group & Monoids

Semigroups : Let S be non-empty set with binary operation $*$ defined on it. The algebraic system $(S, *)$ is called semi group if $*$ is associative.

(i,e) $a*(b*c) = (a*b)*c \;\; \forall a,b,c \in S$

Monoids : A semi group $(M,*)$ with identity element e is called monoid

Example Sum

48) For any commutative monoid $(M,*)$ prove that set of all idempotent element of M forms a submonoid

ANSWER : Given $(M,*)$ be commutative monoid.

Let e be its identiety element.

Let S be set of all idempotent elements of M. (i,e) $S = \{x \in M \mid x*x = x\}$

Since $e*e = e$, e is an idempotent element of M.

$\therefore e \in S$ and hence S is non-empty.

Let $a, b \in S$ be any 2 elements. They are idempotent elements.

$\therefore a * a = a$ and $b * b = b$

we have to porove $a * b$ is idempotent

Now $(a*b)*(a*b) = a*(b*a)*b$ [$\because$ * associative]

$= a*(a*b)*b$ [$\because$ * comutative]

$= (a*a)*(b*b)$ [$\because$ * associtivity]

$= a*b$.

Hence $a*b$ is idempotent and so S is closed under * and $e \in S$. so $(S,*)$ is submonoid of $(M,*)$

Q. If Z_6 is the set of equivalence classes generated by the equivalence relation "congruence modulo 6", prove that (Z_6, X_6) is a monoid where the operation X_6 on Z_6 is defined as $[j] X_6 [k] = [(j \times k) \bmod 6]$ for any $[j], [k] \in Z_6$

A. We know $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$

We shall form the composition table

X_6	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

The body of the table contains only all the elements of Z_6.

So Z_6 is closed under X_6

Since the $[a] X_6 ([b] X_6 [c])$

$= [a] X_6 [bc] = [a(bc) (\bmod 6)]$

X_6 depends on associativity of usual multiplication

$\therefore X_6$ is associative

From the table we find $[1] X_6 [a] = [a]$ for all $[a] \in Z_6$

$\therefore$ [1] is the identity element

Hence (Z_6, X_6) is a monoid

Q. let $S = N \times N$, the set of ordered pairs of positive through integers with the operation $*$ defined by $(a,b) * (c,d) = (ad + bc, bd)$ and if $f : (S, *) \longrightarrow (Q, +)$ is defined by $f(a,b) = \frac{a}{b}$, then show that f is a semi-group homomorphism.

A. We have the semigroups $(S, *)$ and $(Q, +)$

Given $f : (S,*) \longrightarrow (Q,+)$ is defined by $f(a,b) = \frac{a}{b}$

let $x, y \in S$ be any two elements, then $x = (a,b)$, $y = (c,$

for integers a, b, c, d.

Now $x * y = (a,b) * (c,d) = (ab + bc, bd)$

$$\therefore f(x * y) = f(ad + bc, bd) = \frac{ad+bc}{bd}$$

$$= \frac{a}{b} + \frac{c}{d} = f(a,b) + f(c,d)$$

$$f(x * y) = f(x) + f(y)$$

Q. If $*$ is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by & $(a,b) * (x,y) = (ax, ay + b)$. Show that $(S, *)$ is a semi group. Is it commutative? Also find the identity element of S.

A. Given $S = Q \times Q$, where Q is the set of all rational numbers

$$\therefore S = \{(x,y) \mid x, y \in Q\}$$

A binary operation $*$ on S is defined as $(a,b)*(x,y) = (ax, ay+b)$

To prove $(S,*)$ is a semigroup, we have to prove $*$ is associat

let $A = (a,b)$, $B = (c,d)$, $C = (x,y)$ be any three elements in

Then $A*(B*C) = (a,b)*((c,d)*(x,y))$

$= (a,b)*(cx, cy+d)$

$= (a(cx), a(cy+d)+b)$

$= (acx, acy+ad+b)$

and $(A*B)*C = ((a,b)*(c,d))*(x,y)$

$= (ac, ad+b)*(x,y)$

$= ((ac)x, (ac)y + ad+b)$

$= (acx, acy+ad+b)$

from (1) and (2) we find $A*(B*C) = (A*B)*C$ for all $A, B, C \in S$.

So $*$ is associative. Hence $(S,*)$ is a semi group

Now we shall test $*$ is commutative

$A*B = (a,b)*(c,d)$ $\quad$ $B*A = (c,d)*(a,b)$

$= (ac, ad+b)$ $\quad$ $= (ca, cb+d)$

$= (ac, bc+d)$

$\therefore A*B \neq B*A$

Hence $*$ is not commutative and so $(S,*)$ is not commutative

We shall now find identity element of S.

Suppose identity element $I = (x, y)$ exists in S

then $I * A = A * I = A$ for any $A = (a, b) \in S$

Now $A * I = A \Rightarrow (a, b) * (x, y) = (a, b)$

$\Rightarrow (ax, ay + b) = (a, b)$

$\Rightarrow ax = a$ and $ay + b = b$

$\Rightarrow x = 1$ and $ay = 0 \Rightarrow y = 0$

$\therefore I = (1, 0)$ exists in S, since $0, 1 \in Q$

Definition 1 : Ring

A non empty set R with two binary operations denoted by $+$ and $\cdot$, called addition and multiplication is called a ring if the following axioms are satisfied

(i) $(R, +)$ is an abelian group, with 0 as identity

(ii) $(R, \cdot)$ is a semigroup

(iii) The operation $\cdot$ is distributive over $+$

ie. $a \cdot (b + c) = a \cdot b + a \cdot c$

and $(b + c) \cdot a = b \cdot a + c \cdot a \;\forall\; a, b, c \in R$

The additive identity 0 is called the zero element of the ring

Definition 2 : A ring $(R, +, \cdot)$ is said to be commutative if $a \cdot b = b \cdot a \;\forall\; a, b \in R$.

Note : (1) The multiplicative identity 1 is called the unit element or identity of R.

Definition : Integral domain

A commutative ring $(R,+,\cdot)$ with identity and without zero is called an interval domain.

Definition : Field

A commutative ring $(R,+,\cdot)$ with identity in which every non-zero element has multiplicative inverse is called as field.

Theorem 3 :

Every field is an integral domain

Proof :

left $(F,+,\cdot)$ be a field. Then it is a commutative ring with identity.

To prove F is an integal domain, it is enough to prove that it has no zero divisors.

Suppose $a,b \in F$ with $a.b=0$, $a \neq 0$

Since a is non-zero element, its multiplicati inverse a^{-1} exists.

$$\therefore a^{-1}.(a.b) = a^{-1}.0$$

$\Rightarrow (a^{-1}.a).b = 0$

$1 \cdot b = 0 \rightarrow b = 0$

Thus $ab = 0$, $a \neq 0 \Rightarrow b = 0$

$\therefore$ F has no zero divisors

Hence $(F, +, \cdot)$ is an integral domain

Theorem 4: Prove that any finite integral domain is a field

Proof: Let $(R, +, \cdot)$ be a finite integral domain.

$\therefore$ R is a commutative ring with identity and without zero divisors. Hence to prove R is a field.

it is enough to prove that every non-zero element in R has multiplicative inverse

Let $R = \{0, 1, a_1, a_2, \cdots a_n\}$

where 0 is zero of the ring

1 is identity of ring

Let $a \in R$ and $a \neq 0$

Multiplying the non-zero elements of R by a, we get the set $\{a.1, a.a_1, \cdots a.a_n\}$

Since R is without zero divisors, these elements are all non-zero and they are distinct.

Suppose $aa_r = aa_s$, $r \neq s$,

then $a(a_r - a_s) = 0$

$\Rightarrow a_r - a_s = 0$, since $a \neq 0$

$\Rightarrow a_r = a_s$ which is a contradiction to the fact that a_r and a_s are distinct elements in R

$\therefore aa_r \neq aa_s$

And all the aa_is are distinct from 'a' also

Since R is finite, these $(n+1)$ elements are as same as $(n+1)$ non-zero element of R in some order by pigeon hole principle.

$\therefore 1 = aai$ for some $a_i \in R$

Since R is commutative $aai = aia$

$\therefore aai = aia = 1 \Rightarrow ai = a^{-1}$

$\therefore$ every non-zero element in R has multiplicative inverse

Hence any finite integral domain is a field

Rings and Fields

Defn :- Ring

A non-empty set R with two binary operations denoted by '+' and '·' called addition and multiplication is called a ring if the following axioms are satisfied.

(i) $(R,+)$ is an abelian group, with '0' as identity

(ii) $(R,\cdot)$ is a semigroup

(iii) the operation · is distributive over +

ie $a\cdot(b+c) = a\cdot b + a\cdot c$

and $(b+c)\cdot a = b\cdot a + c\cdot a \quad \forall a,b,c \in R$

Examples: 1. $(Z,+,\cdot)$, $(Q,+,\cdot)$, $(R,+,\cdot)$ and $(C,+,\cdot)$ are all rings

2. If $(R,+,\cdot)$ is a ring, then the singleton set $\{0\} \subset R$ is itself a ring, called the null ring or zero ring.

Defn: A ring $(R,+,\cdot)$ is said to be commutative if $a\cdot b = b\cdot a \;\; \forall a,b \in R$

Defn: A ring $(R,+,\cdot)$ is said to be a ring with identity if there exists an elements $1 \in R$ such that $a\cdot 1 = 1\cdot a = a$ $\forall a \in R$

Note ① The multiplicative identity 1 is called the unit element or identity of R

②. In a ring $(R,+,\cdot)$ if the additive identity '0' and the multiplicative identity '1' are not equal, then R is not the zero ring. ie $R \neq \{0\}$. If $0=1$, then $R=\{0\}$.

Theorem : Let $(R,+,\cdot)$ be a ring then for $a,b \in R$

1. $a\cdot 0 = 0\cdot a = 0$
2. $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$
3. $(-a)(-b) = a\cdot b$
4. $a\cdot(b-c) = a\cdot b - a\cdot c$

In addition if R has unit element 1, then

5. $(-1)\cdot a = -a$
6. $(-1)\cdot(-1) = 1$

Proof:- 1. If $a\in R$, then $a\cdot 0 = a\cdot(0+0)$

$$= a\cdot 0 + a\cdot 0$$

$$\Rightarrow a\cdot 0 + 0 = a\cdot 0 + a\cdot 0$$

$$0 = a\cdot 0$$

Similarly, $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a \Rightarrow 0\cdot a = 0$

$\therefore a\cdot 0 = 0\cdot a$ this proves 1.

2. Since $a\cdot 0 = 0$ we have

$$a\cdot(b+(-b)) = 0 \text{ , for any } b\in R$$

$$\Rightarrow a\cdot b + a\cdot(-b) = 0$$

$$\therefore a\cdot(-b) = -(a\cdot b)$$

Similarly $0\cdot b = 0$

$$\Rightarrow (-a+a)\cdot b = 0$$

$$\Rightarrow (-a)\cdot b + a\cdot b = 0$$

$$\Rightarrow a\cdot(-b) = (-a)\cdot b = -(a\cdot b).$$

this proves 2

3. Since $a\cdot(-b) = (-a)\cdot b$ $\forall a,b\in R$

replacing a by $-a$ we get $(-a)\cdot(-b) = a\cdot b$

4. $a\cdot(b-c) = a\cdot(b+(-c)) = a\cdot b + a\cdot(-c) = a\cdot b - a\cdot c$

5. Let the ring R have identity 1.

Since $(-a)\cdot b = -(a\cdot b)$ $\forall a,b\in R$ replacing a by 1 we get $(-1).b = -b \quad \forall b \in R$

$\Rightarrow (-1).a = -a \quad \forall a \in R$

6. Replacing 'a' by -1 in the above relation we get

$$(-1)\cdot(-1) = -(-1) = 1$$

Some Special Rings

Defn:- If $(R,+,\cdot)$ is a commutative ring, then $a \neq 0 \in R$ is said to be a zero divisor if there exists a non zero $b \in R$ such that $ab = 0$.

Note ① zero divisor is also known as divisor of zero

②. All number rings are without zero divisors.

Defn:- In a commutative ring $(R,+,\cdot)$ if for any $a,b \in S$ such that $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$ then the ring is without zero divisors

Note① In a ring without zero divisors $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$.

Defn: Integral domain

A commutative ring $(R,+,\cdot)$ with identity and without zero divisors is called an integral domain.

Note ① The definition requires the ring has more than one element.

Example ① $Z_5 = \{[0],[1],[2],[3],[4]\}$, under $+_5$ and $\cdot_5$ is an integral domain

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\cdot_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

We can easily verify $(Z_5, +_5, \cdot_5)$ is a commutative ring with identity [1]

From the table for $\cdot_5$ we see product of non-zero elements is non-zero and so the ring is without zero divisors

Hence it is an integral domain.

Note ① $(Z_n, +_n, \cdot_n)$ is an integral domain if n is a prime number.

Defn: Field

A commutative ring $(R, +, \cdot)$ with identity in which every non-zero element has multiplicative inverse is called a field.

Example ① $(Q, +, \cdot)$ $(R, +, \cdot)$, $(C, +, \cdot)$ is a field but $(Z, +, \cdot)$ is an integral domain but not a field.

Theorem : A commutative ring R with identity is an integral domain if the cancellation laws holds in R.

Proof:- Let R be an integral domain

Let $a \cdot b = a \cdot c$ where $a \neq 0$

$\therefore a \cdot (b-c) = 0 \Rightarrow (b-c) = 0 \Rightarrow b = c$

So cancellation law holds

Conversly, Let R be a commutative ring with identity in which cancellation laws holds

To prove R is an integral domain, we prove that R has no zero divisors

Suppose $a \cdot b = 0$ and $a \neq 0$

then $a \cdot b = 0 \Rightarrow a \cdot b = a \cdot 0$

$\Rightarrow b = 0$

Hence R is without zero divisors

$\therefore$ R is an integral domain.

Theorem: Every field is an integral domain.

Proof:- Let $(F, +, \cdot)$ be a field

then it is a commutative ring with identity

To prove F is an integral domain, it is enough to prove that it has no zero divisors.

Suppose $a, b \in F$ with $a \cdot b = 0, a \neq 0$

Since 'a' is non-zero element its multiplicative inverse a^{-1} exists

$\therefore a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$

$\Rightarrow (a^{-1} \cdot a) \cdot b = 0 \Rightarrow 1 \cdot b = 0 \Rightarrow b = 0$

thus $ab = 0, a \neq 0 \Rightarrow b = 0$

$\therefore$ F has no zero divisors

Hence $(F, +, \cdot)$ is an integral domain.

Theorem : Any finite integral domain is a field.

Proof : Let $(R,+,\cdot)$ be a finite integral domain

$\therefore$ R is a commutative ring with identity and without zero divisors.

Hence to prove R is a field it is enough to prove that every non-zero element in R has multiplicative inverse

Let $R=\{0,1,a,a_2 \ldots a_n\}$ where 0 is the zero of the ring and 1 is the identity of the ring.

Let $a \in R$ and $a \neq 0$

Multiplying the non-zero elements of R by a, we get the set $\{a\cdot 1, aa_1, aa_2 \ldots aa_n\}$.

Since R is without zero divisors, these elements are all non-zero and they are distinct.

Suppose $aa_r = aa_s$, $r \neq s$ then $a(a_r - a_s)=0$

$$\Rightarrow a_r - a_s = 0 \quad \text{since } a \neq 0$$

$$\Rightarrow a_r = a_s$$

which is a contradiction to the fact that a_r and a_s are distinct elements in R

$$aa_r \neq a\cdot a_s$$

and all the aa_i are distinct from a also.

Since R is finite, these $(n+1)$ elements are same as the $(n+1)$ non-zero elements of R in some order by pigeon hole principle.

$$1 = aa_j \quad \text{for some } a_j \in R$$

Since R is commutative $aa_j = a_j a$

$$aa_j = a_j a = 1 \Rightarrow a_j = a^{-1}$$

$\therefore$ every non-zero element in R has multiplicative inverse. Hence any finite integral domain is a field.

Theorem : Z_n is a field if and only if 'n' is a prime

Proof :- We have $Z_n = \{[0] [1], [2], \dots [n-1]\}$

We know $(Z_n, +, \cdot)$ is a commutative ring with identity $[1]$

Let n be a prime

Suppose $0 < a < n$, then $\gcd(a, n) = 1$.

$\therefore$ there exists integers s, t, such that

$$sa + tn = 1 \Rightarrow sa - 1 = (-t)n$$

$\therefore$ $sa - 1$ is divisible by n

$$\Rightarrow sa \equiv 1 \pmod{n}$$

$$\Rightarrow [s][a] = [1]$$

$\therefore$ $[s]$ is the multiplicative inverse of $[a]$

$[a]$ is a unit in Z_n

Hence Z_n is a field.

Conversely, let Z_n be a field. So, Z_n is a commutative ring with identity and without zero divisors of zero

To prove 'n' is a prime

If n is not a prime then $n = n_1 n_2$ where $1 < n_1, n_2 < n$.

So, $[n_1] \neq 0$ and $[n_2] \neq 0$

But $[n_1][n_2] = [n_1 n_2] = [n] = [0]$

$\therefore$ $[n_1] \cdot [n_2]$ are divisors of zero which contradicts the fact Z_n is a field.

Hence 'n' is a prime.

Theorem : In Z_n $[a]$ is a unit if and only if 'a' and 'n' are relatively prime ie $g.c.d\ (a, n) = 1$.

Proof:- If $\gcd(a, n) = 1$, then there exist integers 's' and 't'

Such that $sa + tn = 1$

$\Rightarrow \quad sa - 1 = (t)n \quad \Rightarrow \quad sa \equiv 1 \pmod{n}$

$\therefore \quad [s][a] = [1] \quad \Rightarrow [a]^{-1} = [s]$

Hence $[a]$ is a unit of Z_n

Conversely, let $[a]$ be a unit of Z_n, say $[a]^{-1} = [s]$

$\Rightarrow \quad [a][s] = [1]$

$\Rightarrow \quad [as] = [1]$

$\Rightarrow \quad as = 1 \pmod{n} \quad \Rightarrow \quad as - 1 = tn$ for some $t \in Z$

$\Rightarrow \quad as + (-t)n = 1$

$\Rightarrow \quad \gcd(a, n) = 1.$

Defn: Boolean Ring

In a ring $(R, +, \cdot)$ if $a^2 = a \ \forall a \in R$, then the ring is called Boolean ring.

Problems

Prob. No ① Prove that a Boolean ring is always commutative.

Sol:- Given R is a Boolean ring

$\therefore \quad a^2 = a \quad \forall a \in R$

We prove the ring is commutative in three stages

(i) First we shall prove that $a + a = 0 \quad \forall a \in R$

Let $a \in R$ be any element, then $a + a \in R$

and $$\begin{aligned}(a+a) &= (a+a)^2 = (a+a)\cdot(a+a) \\ &= a\cdot(a+a) + a\cdot(a+a) \\ &= a\cdot a + a\cdot a + a\cdot a + a\cdot a \\ &= (a^2 + a^2) + (a^2 + a^2) \\ &= (a+a) + (a+a)\end{aligned}$$

$(a+a) + 0 = (a+a) + (a+a)$

$\Rightarrow \quad a + a = 0 \quad$ ($\because$ by left cancellation law)

(ii) Next we shall prove that $a+b=0 \Rightarrow a=b$

Let $a+b=0$

By first part we have $a+a=0$

$$a+b = a+a \Rightarrow b=a \quad (\because \text{by left cancellation in } (R,+))$$

$$\Rightarrow a=b$$

(iii) Finally we shall prove $a \cdot b = b \cdot a$ for any $a,b \in R$

Let $a,b \in R$. Then $a+b \in R$

$$\Rightarrow a+b = (a+b)^2$$
$$= (a+b).(a+b)$$
$$= a.(a+b)+b.(a+b)$$
$$= a \cdot a + a \cdot b + b \cdot a + b \cdot b$$
$$= a^2 + a \cdot b + b \cdot a + b^2$$
$$\therefore \; a+b = a + a \cdot b + b \cdot a + b$$

By left and right cancellation laws in the group $(R,+)$ we get

$$0 = a \cdot b + b \cdot a \Rightarrow a \cdot b = b \cdot a$$

$\therefore R$ is commutative.

Prob. No ②. Let $R = \{a,b,c,d\}$. Define $+$ and $\bullet$ on R by the tables here

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

$\longrightarrow$ ①

•	a	b	c	d
a	a	a	a	a
b	a	a	b	a
c	a	b	c	d
d	a	a	d	a

$\longrightarrow$ ②

Show that $(R,+,\cdot)$ is a ring. Is it commutative? Does it have an identity? what is the zero of the ring?

Sol:- Given $R=\{a,b,c,d\}$ and + and $\cdot$ are defined by the given tables, we shall now verify the axioms of a ring.

1. We have to prove that $(R,+)$ is an abelian group.

Since the body of the table ① contain only all the elements of R, R is closed under +

Since elements of each row and each column are different and for $\forall\, x\in R$

we have $x+a=a+x=x$, a is the zero element.

$(R,+)$ is a group with 'a' as additive identity. The additive inverse of 'a' is a and the inverse of 'b' is b the additive inverse of 'c' is 'd' and the inverse of 'd' is c,

Since $a+a=a$, $b+b=a$ $c+d=d+c=a$ from the given table.

Further, the elements equidistant from the main diagonal are same and + is commutative.

$\therefore$ $(R,+)$ is an abelian group.

2. Now we shall prove that $(R,\cdot)$ is a semi-group

the body of the table ② contains only the elements of R and hence R is closed under $\cdot$

Associativity: For $b,c,d\in R$ we have

$$b\cdot(c\cdot d)=b\cdot d=a \quad (\text{from table ②})$$

$$\text{and } (b\cdot c)\cdot d=b\cdot d=a \quad (\text{from table ②})$$

$$\therefore\ b\cdot(c\cdot d)=(b\cdot c)\cdot d$$

Similarly, we can prove for other elements in R

$\therefore$ Associative axiom is satisfied.

Hence $(R,\cdot)$ is a semigroup.

3. From tables ① and ②

$$a\cdot(b+c) = a\cdot d = a$$

and $a\cdot b + a\cdot c = a + a = a$

$$\therefore\ a\cdot(b+c) = a\cdot b = a\cdot c$$

Similarly, we can verify for each triplets

$\therefore$ $(R, +, \cdot)$ is a ring

In table ②, the elements equidistant from the main diagonal are same and so $\cdot$ is commutative. Hence R is commutative ring.

Since $a\cdot a = a$, $a\cdot b = b\cdot a = a$, $a\cdot c = c\cdot a = a$, $a\cdot d = d\cdot a = a$ etc. there is no identity element

4. The additive Identity 'a' is the zero of the ring.

Prob. No ③. Show that $(Z, +, X)$ is an integral domain where Z is the set of all integers.

Sol:- We know a commutative ring with identity and without zero divisors is called an integral domain.

If Z is the set of integers, then

(i) $(Z, +)$ is an abelian group

(ii) (Z, X) is a semi ring

(iii) $a \times b = b \times a \quad \forall\, a, b \in Z$

(iv) $a \times (b+c) = a \times b + a \times c \quad \forall\, a, b, c \in Z$

Hence $(Z, +, \times)$ is a commutative ring with identity

If $a \neq 0$ $b \neq 0$ in Z then we know $ab \neq 0$. So Z is without zero divisors

Hence $(Z, +, \times)$ is an integral domain.

Prob. No ④ Show that the set of integers Z with the binary operations $\oplus$ and $\odot$ defined by $a \oplus b = a+b-1$ and $a \odot b = a+b-ab \ \forall\ a,b \in Z$ is a commutative ring with identity.

Sol:- Given $a \oplus b = a+b-1$ and $a \odot b = a+b-ab \ \forall\ a,b \in Z$

To Prove $(Z, \oplus, \odot)$ is a ring we verify the axioms

1. We shall prove that $(Z, \oplus)$ is an abelian group

Closure: Since a,b are integers $a+b-1$ is an integer

So, Z is closed under $\oplus$

Associativity: $a \oplus (b \oplus c) = a \oplus (b+c-1)$

$$= a+b+c-1-1 = a+b+c-2$$

and $(a \oplus b) \oplus c = (a+b-1) \oplus c$

$$= a+b-1+c-1 = a+b+c-2$$

$\therefore\ a \oplus (b \oplus c) = (a \oplus b) \oplus c \ \forall\ a,b,c \in Z$

So $\oplus$ is associative

Identity: Let $a \in Z$ and let $e \in Z$ be the identity for $\oplus$

$\therefore\ a \oplus e = a \Rightarrow a+e-1 = a \Rightarrow e = 1$

$\therefore\ 1$ is the identity for $\oplus$

Inverse: Let $a \in Z$ and $a' \in Z$ be the inverse, then

$a \oplus a' = 1 \Rightarrow a+a'-1 = 1$

$a' = 2-a$

So additive inverse exists for every element

Commutativity: $a \oplus b = a+b-1$

$$= b+a-1 = b \oplus a \ \forall\ a,b \in Z$$

$\therefore\ (Z, \oplus)$ is an abelian group.

2. Now we shall prove $(Z, \odot)$ is a semigroup with identity

Closure: Let $a,b \in Z$ then $a+b-ab$ is an integer.

$\therefore\ a \odot b \in Z$ so, Z is closed under $\odot$

Associativity : For any $a,b,c \in Z$

$$a\odot(b\odot c) = a\odot(b+c-bc)$$
$$= a+b+c-bc-a(b+c-bc)$$
$$= a+b+c-bc-ab-ac+abc$$

and $(a\odot b)\odot c = (a+b-ab)\odot c$
$$= a+b-ab+c-(a+b-ab)c$$
$$= a+b+c-ab-ac-bc+abc$$

$\therefore$ $a\odot(b\odot c) = (a\odot b)\odot c \;\; \forall a,b,c \in Z.$

$\therefore$ $\odot$ is associative

Identity : Let $a \in Z$ be any element
We have the integer $0 \in Z$ such that $a\odot 0 = a+0-a\cdot 0 = a$

$\therefore$ 0 is the identity for $\odot$

$\therefore$ $(R,\odot)$ is a semigroup with identity.

3. we now verify the distributive axioms
For any $a,b,c \in Z$

$$a\odot(b\oplus c) = a\odot(b+c-1)$$
$$= a+b+c-1-a(b+c-1)$$
$$= a+b+c-1-ab-ac+a$$
$$= 2a+b+c-ab-ac-1$$

Now $(a\odot b)\oplus(a\odot c) = (a+b-ab)\oplus(a+c-ac)$
$$= a+b-ab+a+c-ac-1$$
$$= 2a+b+c-ab-ac-1$$

Hence $a\odot(b\oplus c) = (a\odot b)\oplus(a\odot c) \;\; \forall a,b,c \in Z.$

Similarly, we can prove $(b\oplus c)\odot a = (b\odot a)\oplus(c\odot a)$

Finally, $a\odot b = a+b-ab = b+a-ba = b\odot a$

$\therefore$ $(Z,\oplus,\odot)$ is a commutative ring with identity.

Prob. No ⑤ Prove that the set $Z_4 = \{0, 1, 2, 3\}$ is a commutative ring with respect to the binary operation $+_4, \times_4$.

Sol:- We know $Z_4 = \{0, 1, 2, 3\}$. Here $0, 1, 2, 3$ is used instead of class $[0]\ [1]\ [2]\ [3]$

We shall verify the axiom of a ring forming Cayley operation table.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

→ ①

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	1	2
3	0	3	2	1

→ ②

①. Closure : the body of the table ① contains only elements of Z_4 and hence Z_4 is closed under $+_4$

②. Associative : Associative axiom is inherited

③. Identity : 0 is the identity element

④. Inverse : Inverse of $0, 1, 2, 3$ are respectively $0, 3, 2, 1$

So, inverse axiom is satisfied

Since the element equidistant from the main diagonal are the same

$$a +_4 b = b +_4 a \quad \forall\, a, b \in Z_4.$$

$\therefore (Z_4, +_4)$ is an abelian group.

The body of the table ② contains only elements of Z_4

$\therefore Z_4$ is closed under $\cdot_4$

Further $\cdot_4$ is associative as it is inherited

$$a \cdot_4 b = b \cdot_4 a \quad \forall\, a, b$$

Since elements equivalent from main diagonal of ② are the same

Further $x \cdot_4 (y +_4 z) = (x \cdot_4 y) +_4 (x \cdot_4 z)$ $\forall x, y, z \in Z_4$ because the property is inherited from number system

By Commutativity of $\cdot_4$ $(y +_4 z) \cdot_4 x = (y \cdot_4 x) +_4 (z \cdot_4 x)$

$\forall x, y, z \in Z_4$

Hence $(Z_4, +_4, \cdot_4)$ is a commutative ring

Prob. No ⑥. Prove that the set $Z_4 = \{[0], [1], [2], [3]\}$ is a commutative ring with respect to the binary operation addition modulo and multiplication modulo $+_4$, X_4.

Sol: Given $Z_4 = \{[0], [1], [2], [3]\}$, the set of congruence classes mod 4.

We shall prove by forming cayley's operation tables for $+_4$ and X_4.

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\longrightarrow$ ①

X_4	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

$\longrightarrow$ ②

(i) Table ① contains only elements of Z_4

So, closure axiom is satisfied

(ii) $+_4$ is associative, because $[a] +_4 ([b] +_4 [c])$

$= [a] +_4 ([b] + [c])$

$$= [a+(b+c)]$$
$$= [(a+b)+c]$$
$$= [a+b] +_4 [c]$$
$$= ([a] +_4 [b]) +_4 [c] \text{ for all } [a],[b],[c] \in Z_4$$

(iii) $[0]$ is the identity for $+_4$

(iv) Inverse of $[0]$ is $[0]$, inverse of $[1]$ is $[3]$

Inverse of $[2]$ is $[2]$, inverse of $[3]$ is $[1]$

$\therefore$ Inverse exists for every element.

(v) $+_4$ is commutative, since

$$[a] +_4 [b] = [a+b] = [b+a] = [b] +_4 [a].$$

$\therefore$ $(Z_4, +_4)$ is an abelian group.

(vi) Z_4 is closed w.r.to X_4, because body of table ② contains only elements of Z_4

(vii) X_4 is associative, because it depends on X_4 of Z

(viii) Distributive axiom

$$[a]\, X_4\, ([b] +_4 [c]) = [a]\, X_4\, [b+c]$$
$$= [a(b+c)] = [ab+ac]$$
$$= [ab] +_4 [ac]$$
$$= [a]\, X_4\, [b] +_4 [a]\, X_4\, [c]$$

$\therefore$ Distributive axiom is satisfied for all $[a],[b]$, $[c] \in Z_4$

(viii) $[a]\, X_4\, [b] = [ab] = [ba] = [b]\, X_4\, [a]$ for all $[a],[b]$ in $[Z_4]$

So, all the axioms of a commutative ring are verified

So, $(Z_4, +_4, X_4)$ is a commutative ring.

Prob. No ⑦ Find (i) $[17]^{-1}$ in the ring Z_{1009} (ii) $[100]^{-1}$ in the ring Z_{1009} (iii) $[777]^{-1}$ in the ring Z_{1009}.

Sol:- (i) To find $[17]^{-1}$ in the ring Z_{1009}

Since 17 and 1009 are relatively prime, the gcd (17, 1009) = 1, the Euclidean algorithm leads to

$$1009 = 59(17)+6, \quad 0<6<17$$
$$\Rightarrow 17 = 2(6)+5, \quad 0<5<6$$
$$\Rightarrow 6 = 1(5)+1, \quad 0<1<5$$

As 1 is the last non-zero remainder, we have

$$1 = 6-1(5) = 6-1(17-2(6))$$
$$= 3(6)-17$$
$$= 3(1009-59(17)-17)$$
$$= 3(1009)-178(17)$$

Hence $1 \equiv (-178)(17) \bmod (1009)$ ($\because 1-(-178)(17)$ is divisible by 1009)

$\therefore [1] = [-178][17]$

$\Rightarrow [17]^{-1} = [-178]$

But $-178 \equiv 831 \pmod{1009}$

$\therefore [178] = [831]$

$\therefore [17]^{-1} = [831]$ in the ring Z_{1009}.

(ii) To find $[100]^{-1}$ in the ring Z_{1009}

Since 100 and 1009 are relatively prime, the gcd (100,1009) = 1, the Euclidean algorithm leads to

$$1009 = 10(100)+9, \quad 0<9<100$$
$$100 = 11(9)+1, \quad 0<1<9$$
$$1 = 100-11(9)$$
$$= 100-11(1009-10(100))$$
$$= 111(100)-11(1009)$$

$\Rightarrow \quad 1 - 111(100) = -11(1009)$

$\Rightarrow \quad 1 - 111(100)$ is divisible by 1009

$\Rightarrow \quad 1 \equiv 111(100) \pmod{1009}$

$\Rightarrow \quad [1] \equiv [111][100]$ in the ring Z_{1009}

$\therefore \quad [100]^{-1} = [111]$ in the ring Z_{1009}

(iii) To find $[777]^{-1}$ in the ring Z_{1009}.

Since 777 and 1009 are relatively prime to each other, the gcd $(777, 1009) = 1$, the Euclidean algorithm leads to

$$1009 = 1(777) + 232, \quad 0 < 232 < 777.$$
$$777 = 3(232) + 81, \quad 0 < 81 < 232$$
$$232 = 2(81) + 70, \quad 0 < 70 < 81$$
$$81 = 1(70) + 11, \quad 0 < 11 < 70$$
$$70 = 6(11) + 4, \quad 0 < 4 < 11$$
$$11 = 2(4) + 3, \quad 0 < 3 < 4$$
$$\therefore 4 = 1(3) + 1, \quad 0 < 1 < 3, \quad 1 = 4 - 1(3)$$
$$= 4 - (11 - 2(4))$$
$$= 3(4) - 11$$
$$= 3(70 - 6(11)) - 11$$
$$= 3(70) - 19(11)$$
$$= 3(70) - 19(81 - 1(70))$$
$$= 22(70) - 19(81)$$
$$= 22(232 - 2(81)) - 19(81)$$
$$= 22(232) - 63(81)$$
$$= 22(232) - 63(777 - 3(232))$$
$$= 211(232) - 63(777)$$
$$= 211(1009 - 1(777 - 63(777))$$

$$= 211\,(1009) - 274\,(777)$$

$$\Rightarrow 1 + 274\,(777) \equiv 211\,(1009)$$

$\Rightarrow 1 + 274\,(777)$ is divisible by 1009

$$1 \equiv (-274)(777) \pmod{1009}$$

$\therefore [1] = [-274][777]$ in the ring Z_{1009}

$$\therefore [777]^{-1} = [-274]$$

$\Rightarrow [777]^{-1} = [735]$ in the ring Z_{1009}

$(\because -274 \equiv 735 \pmod{1009})$

Subring

Defn:- Let $(R,+,\cdot)$ be a ring. A non-empty subset S of R is said to be a subring of R if S itself is a ring with respect to the same operations $+$ and $\cdot$ of R

Note ① In other words S is a subgroup of R if

(i) $(S,+)$ is a subgroup of $(R,+)$ and

(ii) S is closed under ie for $a,b \in S$, $a-b \in S$ and $a\cdot b \in S$

thus to verify a subset of a ring is subring it is enough to verify the above conditions.

Problem

Prob. No① Prove that in the ring of integers $(Z,+,\cdot)$ the subset of even integers $2Z$ is a subring.

Sol:- Let $a,b \in 2Z$, then $a = 2x$, $b = 2y$

$$a - b = 2x - 2y = 2(x-y) \in 2Z$$

and $$a\cdot b = 2x\cdot 2y = 2(2xy) \in 2Z$$

Hence $(2Z,+,\cdot)$ is a subring of Z.

Ring Homomorphism

Defn: Let $(R,+,\cdot)$ and $(S,\oplus,\odot)$ be rings. A mapping $f: R \to S$ is called a ring homomorphism if

(i) $f(a+b) = f(a) \oplus f(b)$

and (ii) $f(a \cdot b) = f(a) \odot f(b)$ $\forall a,b \in R$

Note that the ring homomorphism preserves both the operations

Defn: Isomorphism

Let $f: (R,+,\cdot) \to (S,\oplus,\odot)$ be a ring homomorphism. If f is one-to-one and onto, then f is called a ring isomorphism.

We then say that R and S are isomorphic rings.

Properties of Ring Homomorphism

If $f: (R,+,\cdot) \to (S,\oplus,\odot)$ is a ring homomorphism, then

(i) $f(0) = 0'$, where $0, 0'$ are the zero elements if R and S respectively.

(ii) $f(-a) = -f(a)$ $\forall a \in R$

(iii) $f(na) = nf(a)$ $\forall a \in R, n \in Z^+$

(iv) $f(a^n) = (f(a))^n$ $\forall a \in R, n \in Z^+$

(v) If A is a subring of R, then $f(A)$ is a subring of S.

Proof: (i) To Prove $f(0) = 0'$

where 0 and $0'$ are the identity elements of R and S respectively

we have $f(0) = f(0+0) = f(0) + f(0)$

$$\Rightarrow 0' \oplus f(0) = f(0) \oplus f(0) \Rightarrow 0' = f(0)$$

$\therefore f(0)=0'$

(ii) To prove $f(-a)=-f(a)\ \forall a\in R$

we have $f(0)=0'$

$\Rightarrow f(a+(-a))=0'$ for any $a\in R$

$\Rightarrow f(a)\oplus f(-a)=0'$

$\therefore f(-a)$ is the additive inverse of $f(a)$

$\Rightarrow f(-a)=-f(a)\ \forall a\in R$

(iii) To prove $f(na)=nf(a)$

Let $a\in R$ and $n\in Z^+$

we have $f(na)=f(a+a+a+\cdots+a)$, n times

$=f(a)\oplus f(a)\oplus+\cdots\oplus f(a)$ n times

$=nf(a)$

$\Rightarrow f(na)=nf(a)$

(iv) To prove $f(a^n)=(f(a))^n$

$f(a^n)=f(a.a.a\ldots a)$ (n times)

$=f(a)\odot f(a)\odot\ldots\odot f(a)$ (n times)

$=(f(a))^n$

$f(a^n)=(f(a))^n$

(v) To prove if A is subring of R, then f(A) is a subring of R

Given A is subring of R and so, $A\neq\phi$

$\therefore f(A)\neq\phi$.

If $x,y\in f(A)$, then $x=f(a)$, $y=f(b)$ for some $a,b\in A$

then $x\oplus y=f(a)\oplus f(b)=f(a+b)$

$\Rightarrow x\oplus y\in f(a)$ ($\because a+b\in A$ as A is a subring)

and $x\odot y=f(a)\odot f(b)=f(a.b)\in A$, since $a.b\in A$

So, $f(A)$ is closed under $\oplus$ and $\odot$

Also, if $x \in f(A)$, then $x = f(a)$ for some $a \in A$

So, $f(-a) = -f(a)$

Since $a \in A$, $-a \in A$

$f(-a) \in f(A) \Rightarrow -x \in f(A)$

Hence $f(A)$ is a subring of S.

Theorem: If $f : (R, +, \cdot) \to (S, \oplus, \odot)$ is a ring homomor of R onto S, where $|S| > 1$, then

(i) If 1 is unity of R, then $f(1)$ is a unity of S

(ii) If a is a unit of R, $f(a)$ is a unit of S and $f(a^{-1}) = (f(a))^{-1}$

(iii) If R is commutative, then S is commutative.

Proof: (i) If 1 is the unity of R, then to prove $f(1)$ is the unity of S

Let $f(a)$ be any element of S. Then $a \in R$, since f is onto

Also $f(1) \in S$

$$\therefore f(1) \odot f(a) = f(1 \cdot a) = f(a)$$

$$\text{and } f(a) \odot f(1) = f(a \cdot 1) = f(a)$$

$\therefore$ $f(1)$ is the identity of S.

(ii) If a is a unity of R, then there is an element $a^{-1} \in R$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

$$\therefore f(a \cdot a^{-1}) = f(1) \Rightarrow f(a) \odot f(a^{-1}) = f(1)$$

$$\text{and } f(a^{-1} \cdot a) = f(1) \Rightarrow f(a^{-1}) \odot f(a) = f(1)$$

$$\therefore f(a) \odot f(a^{-1}) = f(a^{-1}) \odot f(a) = f(1)$$

$\therefore$ the multiplicative inverse of $f(a)$ is $f(a^{-1})$ and so $f(a)$ is a unit of S and $f(a^{-1}) = (f(a))^{-1}$

(iii) If R is commutative, then we have to prove S is commutative

Let $x, y \in S$, then we can find $a, b \in R$ such that $f(a) = x$, $f(b) = y$, since f is onto

$$\therefore x \odot y = f(a) \odot f(b) = f(a \cdot b) \quad (\because f \text{ is a Homomorphism})$$
$$= f(b \cdot a)$$
$$= f(b) \odot f(a)$$
$$\Rightarrow x \odot y = y \odot x$$

$\therefore$ S is commutative

Problems

Prob.No ① Prove that the only idempotent elements of an integral domain are '0' and 1.

Sol:- Let $(R, +, \cdot)$ be an integral domain. Let $a \in R$ be an idempotent element.

Then $a^2 = a \Rightarrow a^2 - a = 0 \Rightarrow a(a-1) = 0$

Since R has no zero divisors.

$$a(a-1) = 0 \Rightarrow a = 0 \text{ or } a - 1 = 0$$
$$\Rightarrow a = 0 \text{ and } a = 1$$

Hence 0 and 1 are the only idempotent elements of R.

Prob.No ②. Let F be a finite field with n elements. Prove that $a^n = a$ for all $a \in F$.

Sol:- Let $a \in F$, If $a = 0$ then $a^n - a = 0$

Let $a \neq 0$

Since F is a field, $F - \{0\}$ is a group under multiplication

$o(F-\{0\})=n-1$ and 1 is the identity element

Hence $a^{n-1}=1 \Rightarrow a^{n}=a$

Prob.No③. Let R be a ring with Identity. Prove that the set of all units of R is a group under multiplication.

Sol:- Let $(R,+,\cdot)$ is a ring with identity 1.

Let U be the set of all units of R.

Clearly $1\in U$ and so U is non-empty

Let $a,b\in U$, then a^{-1},b^{-1} exists in R

Now $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

$\Rightarrow (a\cdot b)(b^{-1}\cdot a^{-1}) = a\cdot 1\cdot a^{-1} = a\cdot a^{-1}=1$

and $(b^{-1}a^{-1})\cdot(a\cdot b) = b^{-1}(a^{-1}\cdot a).b = b^{-1}1.b = b^{-1}b=1$

$(a\cdot b)(b^{-1}\cdot a^{-1}) = (b^{-1}a^{-1})(a\cdot b)=1.$

$\therefore$ $a\cdot b$ has multiplicative inverse

$\therefore a\cdot b\in U$

If $a\in U$, a^{-1} exists in R and $(a^{-1})^{-1}=a\in U$

Hence $a\in U \Rightarrow a^{-1}\in U$

Thus $(U,\cdot)$ is a group.

Prob.No④. Test whether $f:(Z,+,\cdot)\rightarrow(2Z,+,\cdot)$ defined by $f(x)=2x$ $\forall x\in Z$ is a ring homomorphism.

Sol: Given $(Z,+,\cdot)$ and $(2Z,+,\cdot)$ are rings

Given the map $f: Z\rightarrow 2Z$ defined by

$$f(x)=2x \quad \forall x\in Z$$

Test whether 'f' is a ring homomorphism

Let $x,y\in Z$, $f(x+y)=2(x+y) = 2x+2y = f(x)+f(y)$

and $f(x\cdot y)=2(x\cdot y)= 2x\cdot 2y = 4xy$

$\therefore$ $f(x)\neq f(x)\cdot f(y)$

So, 'f' preserves addition but not multiplication. Hence f is not a ring homomorphism.

Prob. No (5). Give an example of a commutative ring with identity which is not a field.

Sol:- We know that $(Z,+,\cdot)$ is a commutative ring with identity 1

If $2 \in Z$, then $2^{-1} = 1/2 \notin Z$

$\therefore$ $(Z,+,\cdot)$ is not a field.

UNIT.2. FINITE FIELDS AND POLYNOMIALS

INTRODUCTION

A polynomial is an expression of the form $a_0+a_1x+a_2x^2+\cdots+a_nx^n$, where 'n' is a non-negative integer and $a_0, a_1, a_2 \ldots a_n$ are integers (rationals or real numbers)

we know how to add two polynomials, subtract one polynomial from another and multiply two polynomials

we shall now define polynomial with coefficients from a ring and this collection of all polynomials with respect to addition and multiplication is a ring.

Polynomials

Defn: Let $(R,+,\cdot)$ be a ring. An expression of the form $a_0+a_1x+a_2x^2+\cdots+a_nx^n$ where 'n' is a non-negative integer and $a_0, a_1, a_2 \ldots a_n \in R$, is called a polynomial over R in the indeterminate x and it is denoted by f(x). thus,

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_rx^r+\cdots+a_nx^n$$

where a_r is called the coefficient of x^r and a_rx^r is a term of the polynomial f(x).

Note ① If $a_n \neq 0$, where '0' is the zero element of R, then a_n is called the leading coefficient of f(x) and we say f(x) is of degree n.

②. we write $\deg f(x)=n$ and a_0 is called the constant term of f(x)

③. the set of all polynomials in x over R is denoted by R[x].

Defn: (i) Equal polynomials (ii) Zero polynomial (iii) Constant polynomial (iv) Monic Polynomial

(i) Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ be two polynomials in $R[x]$. then $f(x) = g(x)$ if $m = n$, $a_i = b_i \; \forall i = 0, 1, 2, \ldots n$

(ii) A polynomial in $R[x]$ with all coefficients zero is called the zero polynomial and is denoted by '0'. Zero polynomial has no degree. ie, degree is not defined for zero polynomial.

(iii) A polynomial of the form $f(x) = a_0$, where a_0 is a constant is called a constant polynomial. degree of non-zero constant polynomial is zero.

(iv) A polynomial in which the leading coefficient is 1 (identity of R) is called a monic polynomial For example: $a_0 + a_1x + a_2x^2 + x^3$ is a monic polynomial of degree 3.

Addition and multiplication of polynomials in $R[x]$

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and
$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ be two polynomials in $R[x]$. then

$f(x) + g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_sx^s$ where

$c_i = a_i + b_i \; \forall i$

And the product

$f(x) \cdot g(x) = (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)$

$= c_0 + c_1x + c_2x^2 + \cdots + c_rx^r + \cdots + c_kx^k$

where $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0$ $\cdots$ $c_r = a_0b_r + a_1b_{r-1} + \cdots + a_rb_0$.

For example: consider $f(x) = 2+3x+2x^2+x^3$ and $g(x) = 1+x+2x^2$ in $Z[x]$

then $f(x)+g(x) = (2+1)+(3+1)x+(2+2)x^2+(1+0)x^3$

$\therefore f(x)+g(x) = 3+4x+4x^2+x^3$ in $Z[x]$.

and $f(x).g(x) = (2+3x+2x^2+x^3).(1+x+2x^2)$

$= 2.1 + (3.1+2.1)x + (2.1+2.2+3.1)x^2$

$+ (1+2.1+3.2)x^3 + (1+2.2)x^4 + 1.2x^5.$

$= 2+5x+9x^2+9x^3+5x^4+2x^5$ in $Z[x]$

Theorem: Let R be a ring. then $(R[x],+,\cdot)$ is a ring.

Proof:- Given R is a ring.

Let $f(x)$ and $g(x) \in R[x]$

Let $f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$

and $g(x) = b_0+b_1x+b_2x^2+\cdots+b_mx^m$. where $a_i, b_i \in R$

By defn $f(x)+g(x) = c_0+c_1x+c_2x^2+\cdots+c_kx^k$

where $c_i = a_i+b_i$ since $a_i+b_i \in R \Rightarrow c_i \in R$

$\therefore f(x)+g(x) \in R[x]$

and $f(x).g(x) = c_0+c_1x+c_2x^2+\cdots+c_rx^r+\cdots+c_kx^k$

where $c_r = a_0b_r+a_1b_{r-1}+a_2b_{r-2}+\cdots+a_rb_0 \in R$

$\therefore f(x).g(x) \in R[x]$

Since addition $+$ and multiplication $\bullet$ are associative in R

addition and multiplication of polynomials are associative in $R[x]$

The zero polynomial 0 in $R[x]$ is the identity for $+$ in $R[x]$

Since $f(x)+0 = f(x) \ \forall f(x) \in R[x]$

If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ in $R[x]$

then $-f(x) = -a_0 - a_1x - a_2x^2 - \cdots - a_nx^n$ in $R[x]$

$\therefore f(x) + (-f(x)) = 0$

$\therefore -f(x)$ is the additive inverse of $f(x)$

Further $f(x)+g(x) = g(x)+f(x) \ \forall f(x), g(x) \in R[x]$

Since $a_i + b_i = b_i + a_i \ \forall a_i b_i \in R$

$\therefore (R[x], +)$ is an abelian group.

Let $f(x), g(x), h(x) \in R[x]$ and let

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$

$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$

$h(x) = c_0 + c_1x + c_2x^2 + \cdots + c_px^p$

Then the coefficient of x^i in the expansion of $(f(x)g(x))\,h(x)$ is the sum of the products of the form $(a_rb_s)c_t$, where r, s, t are non-negative integers such that $r+s+t=i$

Again the coefficient of x^i in the expansion of $f(x)\,(g(x)\,h(x))$ is sum of the products of the form $a_r(b_sc_t)$ where r, s, t are non-negative integers such that $r+s+t=i$

Since multiplication is associative in R

$a_r(b_sc_t) = (a_rb_s)c_t$

∴ Coefficient of x^i in $(f(x)/g(x))h(x)$ is equal to the coefficient of x^i in $f(x)(g(x)h(x))$

∴ Multiplication of polynomials is associative

ie $(f(x)g(x))h(x) = f(x)(g(x)h(x))$

Now $f(x)(g(x)+h(x)) = f(x)g(x) + f(x)h(x)$

Since the coefficient of x^i in the LHS is $a_r(b_s+c_t)$ and the coefficient of x^i in the RHS is $a_rb_s + a_rc_t$.

$$\therefore \quad a_r(b_s+c_t) = a_rb_s + a_rc_t.$$

Hence $(R[x], +, \cdot)$ is a ring under polynomial addition and multiplication.

Theorem! $R[x]$ is an integral domain iff R is an integral domain

Proof: Let R be an integral domain

then R is a commutative ring with identity and without zero divisor.

Hence $R[x]$ is commutative ring with identity 1

Since $f(x).1 = f(x)$.

we have to prove $R[x]$ is without zero divisors

ie to prove $f(x) \neq 0, g(x) \neq 0 \Rightarrow f(x)g(x) \neq 0$

let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $a_n \neq 0$

and $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$, $b_m \neq 0$

then $f(x).g(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n+m}x^{m+n}$

where $c_r = a_0b_r + a_1b_{r-} + \dots + a_rb_0$ and $c_{m+n} = a_n.b_m$

Since R is without zero divisors

$a_n \neq 0,\ b_m \neq 0 \Rightarrow a_n b_m \neq 0 \Rightarrow c_{n+m} \neq 0$

$f(x)g(x) \neq 0$

Hence $R[x]$ is an integral domain

Conversely, let $R[x]$ be an integral domain

we have to prove that R is an integral domain

we know that R is a subring of $R[x]$

$\therefore$ R is an integral domain.

Corollary: If F is a field, then $F[x]$ is an integral domain

Theorem: If R is an integral domain, then

$$\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x)$$

Proof: Let R be an integral domain

then R is a commutative ring with identity and without zero divisors ie $a\neq 0, b \neq 0 \Rightarrow ab \neq 0$

Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n,\ a_n \neq 0$

$\therefore \deg f(x) = n$

and $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m;\ b_m \neq 0$

$\therefore \deg g(x) = m.$

Since R is an integral domain, $a_n b_m \neq 0$

Now $f(x)g(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n+m}x^{n+m}$

where $c_{n+m} = a_n b_m \neq 0$

$\therefore \deg(f(x)g(x)) = n+m$

$\therefore \deg(f(x)g(x)) = \deg f(x) + \deg g(x).$

Defn: Root of a polynomial

Let R be a ring with identity 1 and let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$ with $\deg f(x) \geq 1$

An element $a \in R$ is called a root of $f(x)$ if $f(a) = a_0 + a_1a + a_2a^2 + \cdots + a_na^n = 0$

ie if $f(a) = 0$, then 'a' is root of $f(x)$.

Note ① If $R = (Z_6, +, \cdot)$ where $Z_6 = \{0, 1, 2, 3, 4, 5\}$ by writing $[a]$ as a

A polynomial over Z_6 can be written differently

$f(x) = 2x^3 + 5x^2 + 3x - 2$ over Z_6 is a polynomial.

Since $[4] = [-2]$, this polynomial $f(x)$ can also be written as $2x^3 + 5x^2 + 3x + 4$

what is its degree?

Since $[2] \neq [0]$ or $2 \not\equiv 0 \pmod 6$, the leading coefficient of $f(x)$ is non zero

$\therefore \deg f(x) = 3$.

Problems

Prob. No ① What is the degree of the polynomial $f(x) = 6x^3 + 5x^2 + 3x - 2$ over Z_6

Sol:- Given $f(x) = 6x^3 + 5x^2 + 3x - 2$

Since the coefficients are from $Z_6 = \{0, 1, 2, 4, 5, 6\}$

$\therefore 6 \equiv 0 \pmod 6$ is $[6] = [0]$, $[4] = [-2]$

$\therefore$ the polynomial is $0x^3 + 5x^2 + 3x + 4 = 5x^2 + 3x + 4$

So, the leading coefficient is $5 \neq 0$ in Z_6

Hence the $\deg f(x) = 2$.

Prob. No ②. Let $f(x) = 4x^2+3$ and $g(x) = 2x+5$ be two polynomials over Z_8. Find the deg $f(x).g(x)$

Sol:- Given $f(x) = 4x^2+3$, $g(x) = 2x+5$ are polynomial over Z_8

ie $f(x), g(x) \in Z_8[x]$.

The deg $f(x) = 2$ and deg $g(x) = 1$ Since $4 \neq 0, 2 \neq 0$ in Z_8

Now $f(x).g(x) = (4x^2+3)(2x+5)$

$$= 8x^3+20x^2+6x+15$$

Normally we expect degree of the product = sum of the degree

Since the coefficients belong to Z_8 we find $8 \equiv 0 \pmod 8$

ie $[8] = [0]$ and $20 \equiv 4 \pmod 8$ and $15 \equiv 7 \pmod 8$

$\therefore f(x)g(x) = 4x^2+6x+7$ over Z_8

$\therefore$ deg $f(x)g(x) = 2 < 3 =$ deg $f(x)+$ deg $g(x)$.

Prob. No ③ Find the roots of the polynomial x^2-2 over the real number R

Sol:- Given polynomial is x^2-2 over R

To find the roots of x^2-2, we solve

$$x^2-2=0 \Rightarrow x^2=2 \Rightarrow x = \pm\sqrt{2}$$

$\therefore$ the roots are $\sqrt{2}, -\sqrt{2}$ in R

If we consider the polynomial x^2-2 over Q, then the roots $\sqrt{2}, -\sqrt{2}$ do not belong to Q

So, the polynomial $x^2-2 \in Q[x]$ had no roots in Q

Prob. No (4). Find all the roots of $f(x) = x^2+4x$ in $Z_{12}[x]$.

Sol:- Given $f(x) = x^2+4x$ over Z_{12}

and $Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

We verify and find the roots

Now $f(0) = 0+0 = 0$ $\therefore$ 0 is a root of $f(x)$

$f(1) = 1+4 = 5 \neq 0$ $\therefore$ 1 is not a root

$f(2) = 2^2+4\cdot 2 = 4+8 = 12 \equiv 0 \pmod{12}$ $\therefore$ 2 is a root of $f(x)$

$f(3) = 3^2+4\cdot 3 = 9+12 = 21 \equiv 9 \pmod{12} \neq 0$

$\therefore$ 3 is not a root of $f(x)$

$f(4) = 4^2+4\cdot 4 = 16+16 = 32 \equiv 8 \pmod{12} \neq 0$

$\therefore$ 4 is not a root of $f(x)$

$f(5) = 5^2+4\cdot 5 = 25+20 = 45 \equiv 9 \pmod{12} \neq 0$

$\therefore$ 5 is not a root of $f(x)$

$f(6) = 6^2+4\cdot 6 = 36+24 = 60 \equiv 0 \pmod{12}$

$\therefore$ 6 is a root of $f(x)$

$f(7) = 7^2+4\cdot 7 = 49+28 = 77 \equiv 5 \pmod{12} \neq 0$.

$\therefore$ 7 is not a root of $f(x)$.

$f(8) = 8^2+4\cdot 8 = 64+32 = 96 \equiv 0 \pmod{12}$

$\therefore$ 8 is a root of $f(x)$.

$f(9) = 9^2+4\cdot 9 = 81+36 = 117 \equiv 9 \pmod{12} \neq 0$

$\therefore$ 9 is not a root of $f(x)$

$f(10) = 10^2+4\cdot 10 = 100+40 = 140 \equiv 8 \pmod{12} \neq 0$

$\therefore$ 10 is not a root of $f(x)$

$f(11) = 11^2 + 4 \cdot 11 = 121 + 44 = 165 \equiv 9 \pmod{12} \neq 0$

$\therefore$ 11 is not a root of $f(x)$.

$\therefore x = 0, 2, 6, 8$ are the roots of $f(x)$ over Z_{12}

Note ①: In your earlier classes you have seen that a polynomial of degree 2 had at most two roots, which is not true here for a polynomial over a ring.

Prob. No ⑤. Determine all the roots of $f(x) = x^3 + 5x^2 + 2x + 6$ in $Z_7[x]$.

Sol:- Given $f(x) = x^3 + 5x^2 + 2x + 6$ over Z_7

and $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

we verify and find the roots

Now $f(0) = 6 \equiv -1 \pmod 7 \neq 0$ $\therefore$ 0 is not a root

$f(1) = 1 + 5 + 2 + 6 = 14 \equiv 0 \pmod 7$

$\therefore$ 1 is root of $f(x)$

$f(2) = 8 + 20 + 4 + 6 = 38 \equiv 3 \pmod 7 \neq 0$

$\therefore$ 2 is not a root

$f(3) = 27 + 45 + 6 + 6 = 84 \equiv 0 \pmod 7$

$\therefore$ 3 is root of $f(x)$

$f(4) = 64 + 80 + 8 + 6 = 128 = 2 \pmod 7 \neq 0$

$\therefore$ 4 is not a root of $f(x)$

$f(5) = 125 + 125 + 10 + 6 = 266 \equiv 0 \pmod 7$

$\therefore$ 5 is root of $f(x)$

$f(6) = 216 + 180 + 12 + 6 = 434 \equiv 0 \pmod 7$

$\therefore$ 6 is root of $f(x)$ $\therefore$ the roots of $f(x)$ are 1, 3, 5, 6

Prob. No 6. Determine all the roots of $f(x) = x^2+3x+2 \in Z_6[x]$.

Sol:- Given $f(x) = x^2+3x+2$ in $Z_6[x]$

and $Z_6 = \{0,1,2,3,4,5\}$

We verify and find the roots

Now $f(0) = 2 \neq 0$ $\therefore$ 0 is not a root of $f(x)$

$f(1) = 1+3+2 = 6 \equiv 0 \pmod 6$ $\therefore$ 1 is root of $f(x)$

$f(2) = 4+6+2 = 12 \equiv 0 \pmod 6$ $\therefore$ 2 is root of $f(x)$

$f(3) = 9+9+2 = 20 \equiv 2 \pmod 6$ $\therefore$ 3 is not a root of $f(x)$

$f(4) = 16+12+2 = 30 \equiv 0 \pmod 6$ $\therefore$ 4 is root of $f(x)$

$f(5) = 25+15+2 = 42 \equiv 0 \pmod 6$ $\therefore$ 5 is root of $f(x)$.

$\therefore$ the roots of $f(x)$ are 1, 2, 4, 5.

Prob. No 7. Determine all the polynomials of degree 2 in $Z_2[x]$.

Sol:- We have to find all the polynomials of degree 2 over Z_2 and $Z_2 = \{0,1\}$.

Let the general polynomial of degree 2 is $f(x) = a_0 + a_1x + a_2x^2$, $a_2 \neq 0$

the possible coefficients are from Z_2, where $a_2 \neq 0$, so $a_2 = 1$

$f(x) = a_0 + a_1x + x^2$

$\therefore$ If $a_0 = 0$, $a_1 = 0$, then $f(x) = x^2$

If $a_0 = 0$, $a_1 = 1$, then $f(x) = x + x^2$

If $a_0 = 1$, $a_1 = 0$, then $f(x) = 1 + x^2$

If $a_0 = 1$, $a_1 = 1$, then $f(x) = 1 + x + x^2$

∴ there are four possible polynomials of degree 2

$x^2, x+x^2, 1+x^2, 1+x+x^2$ in $Z_2[x]$

Defn: Divisor of a Polynomial

Let F be a field and $f(x) \neq 0$ and $g(x)$ be a polynomials in $F[x]$. $f(x)$ is called a factor or a divisor of $g(x)$ if there exists $h(x) \in F[x]$ such that

$$g(x) = f(x) h(x)$$

Note ① We also say that $f(x)$ divides $g(x)$ or $g(x)$ is a multiple of $f(x)$. this leads to the division algorithm for polynomials

theorem (Division Algorithm)

Let $f(x) \neq 0$ and $g(x)$ be polynomials in $F[x]$. then there exists unique polynomials $q(x)$ and $r(x)$ belonging to $F[x]$ such that $g(x) = q(x) f(x) + r(x)$ where $r(x) = 0$ (or) $\deg r(x) < \deg f(x)$

Proof:- Given $f(x) \neq 0$ and $g(x) \in F[x]$

Consider the set $S = \{ g(x) - t(x) f(x) / t(x) \in F[x] \}$

If $0 \in S$, then for some $t(x) \in F[x]$

we have $g(x) - t(x) f(x) = 0$.

$$\Rightarrow g(x) = t(x) f(x).$$

then $q(x) = t(x)$ and $r(x) = 0$

∴ we have $g(x) = q(x) f(x) + r(x)$

If $0 \notin S$, then non-zero elements exist in S and among these elements in S,

We can find an element $r(x)$ in S with least degree (by well ordering principle). Since $r(x) \neq 0$, the result follows if $\deg r(x) < \deg f(x)$

If not, let $\deg r(x) \geq \deg f(x)$

Let $r(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, $a_n \neq 0$

and $f(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$, $b_m \neq 0$

$\therefore n \geq m$

Define $h(x) = r(x) - a_n b_m^{-1} x^{n-m} f(x)$

$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n - a_n b_m^{-1} x^{n-m} (b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m)$$

$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n - a_n b_m^{-1} b_0 x^{n-m} - a_n b_m^{-1} b_1 x^{n-m+1} - a_n b_m^{-1} b_2 x^{n-m+2} - \cdots - a_n b_m^{-1} b_{m-1} x^{n-m+m-1} - a_n b_m^{-1} b_m x^{n-m+m}$$

$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} - a_n b_m^{-1} b_0 x^{n-m} - a_n b_m^{-1} b_1 x^{n-m+1} - a_n b_m^{-1} b_2 x^{n-m+2} - \cdots - a_n b_m^{-1} b_{m-1} x^{n-1}$$

$\therefore \deg h(x) < n = \deg r(x)$

Since $r(x) \in S$, $r(x) = g(x) - q(x) f(x)$

$$h(x) = g(x) - q(x) f(x) - a_n b_m^{-1} x^{n-m} f(x)$$

$$= g(x) - [q(x) + a_n b_m^{-1} x^{n-m}] f(x)$$

$$= g(x) - p(x) f(x)$$

where $p(x) = q(x) + a_n b_m^{-1} x^{n-m} \in F[x]$

$\therefore h(x) \in S$ and $\deg h(x) < \deg r(x)$

which is contradiction to the fact that $\deg r(x)$ is minimum

$\therefore \deg r(x) < \deg f(x) = n$.

Thus, we have the existence part

$$g(x) = q(x) f(x) + r(x) \rightarrow (1)$$

where $r(x)=0$ or $\deg r(x) < \deg f(x)$

We now prove the uniqueness

Suppose we also have $g(x) = q_1(x) f(x) + r_1(x) \rightarrow ②$

where $r_1(x) = 0$ (or) $\deg r_1(x) < \deg f(x)$

then $q(x) f(x) + r(x) = q_1(x) f(x) + r_1(x)$

$$\Rightarrow (q(x) - q_1(x)) f(x) = r_1(x) - r(x) \rightarrow ③$$

If $q(x) - q_1(x) \neq 0$, then

$$\deg (q(x) - q_1(x)) f(x) \geq \deg f(x)$$

$$\Rightarrow \deg (r_1(x) - r(x)) \geq \deg f(x)$$

which is a contradiction

$$\therefore q(x) - q_1(x) = 0 \Rightarrow q(x) = q_1(x)$$

then $③ \Rightarrow r_1(x) - r(x) = 0 \Rightarrow r_1(x) = r(x)$

Hence in the eqn ① $q(x)$ and $r(x)$ are unique.

Note ①: the polynomials $q(x)$ and $r(x)$ in the division algorithm are called the quotient and remainder in the division of $g(x)$ by $f(x)$

Problems

Prob. No ①. Consider $f(x) = 3x^4 + x^3 + 2x^2 + 1$ and $g(x) = x^2 + 4x + 2$ in $Z_5[x]$. Find $q(x)$ and $r(x)$ when $f(x)$ is divided by $g(x)$.

Sol:- Given $f(x) = 3x^4 + x^3 + 2x^2 + 1$ and $g(x) = x^2 + 4x + 2$

Since Z_5 is a field, to find $q(x)$ and $r(x)$ when $f(x)$ is divided by $g(x)$.

We performs long division, keeping in mind the addition and multiplication are performed modulo 5.

$z_5 = \{0,1,2,3,4\}$ is a field.

the division is

$$\begin{array}{r l}
 & 3x^2+4x \\ \cline{2-2}
x^2+4x+2 & \big) \, 3x^4+x^3+2x^2+1 \\
 & 3x^4+2x^3+x^2 \\ \cline{2-2}
 & 4x^3+x^2+1 \\
 & 4x^3+x^2+3x \\ \cline{2-2}
 & 2x+1
\end{array}$$

$12 \equiv 2 \pmod 5$

$6 \equiv 1 \pmod 5$

$-1 \equiv 4 \pmod 5$

$16 \equiv 1 \pmod 5$

$8 \equiv 3 \pmod 5$

$-3 \equiv 2 \pmod 5$

$\therefore$ the quotient $q(x) = 3x^2+4x$ and the remainder $r(x) = 2x+1$

$\therefore 3x^4+x^3+2x^2+1 = (x^2+4x+2)(3x^2+4x)+2x+1.$

Prob. No ② If $f(x) = 2x^4+5x^2+2$, $g(x) = 6x^2+4$, then determine $q(x)$ and $r(x)$ in $z_7[x]$, when $f(x)$ is divided by $g(x)$.

Sol:- Given $f(x) = 2x^4+5x^2+2$ and $g(x) = 6x^2+4$

Since $z_7 = \{0,1,2,3,4,5,6\}$ is field.

To find $q(x)$ and $r(x)$ in $z_7[x]$, when $f(x)$ is divided by $g(x)$

We use long division method keeping in mind addition and multiplication are done under modulo 7, the division is

$$\begin{array}{r l}
 & 5x^2+1 \\ \cline{2-2}
6x^2+4 & \big) \, 2x^4+5x^2+2 \\
 & 2x^4+6x^2 \\ \cline{2-2}
 & 6x^2+2 \\
 & 6x^2+4 \\ \cline{2-2}
 & 5
\end{array}$$

$30 \equiv 2 \pmod 7$

$20 \equiv 6 \pmod 7$

$-1 \equiv 6 \pmod 7$

$-2 \equiv 5 \pmod 7.$

$q(x) = 5x^2+1$ and $r(x) = 5$

$\therefore\ 2x^4+5x^2+2 = (5x^2+1)(6x^2+4)+5.$

Prob. No (3). If $f(x) = 3x^2+4x+2$ and $g(x) = 6x^4+4x^3+5x^2+3x+1$, are polynomials in $Z_7[x]$ find $q(x)$ and $r(x)$ when $g(x)$ is divided by $f(x)$

Sol:- Given $f(x) = 3x^2+4x+2$ and $g(x) = 6x^4+4x^3+5x^2+3x+1$

Since $Z_7 = \{0,1,2,3,4,5,6\}$ is a field, to find $q(x)$ and $r(x)$ in $Z_7[x]$

we perform long division method when $g(x)$ is divided by $f(x)$, keeping in mind addition and multiplication under modulo 7. The division is

$$\begin{array}{r|l}
 & 2x^2+x+6 \\
\hline
3x^2+4x+2 & 6x^4+4x^3+5x^2+3x+1 \\
 & 6x^4+x^3+4x^2 \\
\cline{2-2}
 & 3x^3+x^2+3x \\
 & 3x^3+4x^2+2x \\
\cline{2-2}
 & 4x^2+x+1 \\
 & 4x^2+3x+5 \\
\cline{2-2}
 & 5x+3
\end{array}$$

$8 \equiv 1 \pmod 7$

$-3 \equiv 4 \pmod 7$

$18 \equiv 4 \pmod 7$

$24 \equiv 3 \pmod 7$

$12 \equiv 5 \pmod 7$.

$-2 \equiv 5 \pmod 7$

$-4 \equiv 3 \pmod 7$.

$q(x) = 2x^2+x+6$ and $r(x) = 5x+3$

$6x^4+4x^3+5x^2+3x+1 = (2x^2+x+6)(3x^2+4x+2)+5x+3.$

Prob. No (4) If $f(x) = x^5+3x^4+x^3+x^2+2x+2 \in Z_5[x]$ is divided by $x-1$, find the quotient and remainder.

Sol:- Given $f(x) = x^5+3x^4+x^3+x^2+2x+2$ and

$g(x) = x-1$

Since $Z_5 = \{0,1,2,3,4\}$ is a field, to find $q(x)$ and $r(x)$ in $Z_5[x]$, we perform long division method, when $f(x)$ is divided by $g(x)$, keeping in mind addition and multiplication under modulo 5. The division is

$$\begin{array}{r|l} & x^4+4x^3+x+3 \\ \hline x-1 & x^5+3x^4+x^3+x^2+2x+2 \\ & x^5-x^4 \\ \hline & 4x^4+x^3 \\ & 4x^4-4x^3 \\ \hline & x^2+2x \\ & x^2-x \\ \hline & 3x+2 \\ & 3x-3 \\ \hline & 0 \\ \hline \end{array}$$

$5 \equiv 0 \pmod 5$

$\therefore$ $q(x) = x^4+4x^3+x+3$ and $r(x) = 0$

$\therefore$ $(x-1)$ is a factor of $f(x)$

$\therefore$ $f(x) = (x^4+4x^3+x+3)(x-1)$.

Prob. No (5). If $f(x) = x^3+5x^2+2x+6 \in Z_7[x]$, then write $f(x)$ as a product of first degree polynomials

Sol:- We know that $Z_7 = \{0,1,2,3,4,5,6\}$

Given $f(x) = x^3+5x^2+2x+6$

Now $f(0) = 6 \equiv -1 \pmod 7 \neq 0$

$f(1) = 1+5+2+6 = 14 \equiv 0 \pmod 7$

$\therefore$ 1 is a root of $f(x)$ and so, $(x-1)$ is a factor of $f(x)$

$f(2) = 8+20+4+6 = 38 \equiv 3 \pmod 7 \neq 0$

$f(3) = 27+45+6+6 = 84 \equiv 0 \pmod 7$

$\therefore$ 3 is a root of $f(x)$ and so, $(x-3)$ is a factor of $f(x)$

$f(4) = 64+80+8+6 = 128 \equiv 2 \pmod 7 \neq 0$

$f(5) = 125+125+10+6 = 266 \equiv 0 \pmod 7$

$\therefore$ 5 is a root of $f(x)$ and so $(x-5)$ is a factor of $f(x)$

$f(6) = 216+180+12+6 = 414 \equiv 1 \pmod 7$

$\therefore f(x) = (x-1)(x-3)(x-5)$ in $Z_7[x]$.

Prob. No 6. If $f(x) = (2x^3+1)(5x^3+5x+3)(4x-3) \in Z_7[x]$ then write $f(x)$ as a product of a unit and three monic polynomials

Sol: Given $f(x) = (2x^3+1)(5x^3+5x+3)(4x-3)$ in $Z_7[x]$

$Z_7 = \{0,1,2,3,4,5,6\}$

To write $f(x)$ as product of three monic polynomial, we have to take out 2 from first factor, 5 from second factor and 4 from third factor.

ie 2 from $2x^2+1$, 5 from $5x^3+5x+3$ and 4 from $4x-3$

Now $1 \equiv 8 \pmod 7$, $3 \equiv 10 \pmod 7$, $-3 \equiv 4 \pmod 7$

$f(x) = (2x^2+8)(5x^3+5x+10)(4x+4)$

$= 2(x^2+4)\,5(x^3+x+2)\,4(x+1)$

$= 40(x^2+4)(x^3+x+2)(x+1)$

$40 \equiv 5 \pmod 7$

$\therefore f(x) = 5(x^2+4)(x^3+x+2)(x+1)$

Corollary ① The remainder theorem

Let F be a field $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder when $f(x)$ is divided by $(x-a)$.

Proof: Given $f(x) \in F[x]$ and $a \in F$ and so, $(x-a) \in F[x]$

By division algorithm, $f(x) = q(x)(x-a) + r(x)$

where $r(x) = 0$ or $\deg r(x) < \deg(x-a) = 1$

$$\therefore \quad \deg(r(x)) = 0$$

$\Rightarrow r(x) = r$ (a constant), an element in F

$$\therefore \quad f(x) = q(x)(x-a) + r$$

Put $x = a$ $\quad f(a) = q(a) \cdot 0 + r = r \Rightarrow r = f(a)$

$$f(x) = q(x)(x-a) + f(a).$$

So, the remainder is $f(a)$.

Corollary ②: Factor theorem.

Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then 'a' is a root of $f(x)$ if and only if $(x-a)$ is a factor of $f(x)$.

Proof:- Given $f(x) \in F[x]$ and $a \in F \Rightarrow (x-a) \in F[x]$

If $(x-a)$ is a factor of $f(x)$, then $f(x) = (x-a)q(x)$ for some $q(x) \in F[x]$

$$f(a) = (a-a)q(a) = 0 \cdot q(a) = 0$$

Hence, a is a root of $f(x)$

Conversely, let $a \in F$ be a root of $f(x)$

$$f(a) = 0 \longrightarrow ①$$

$\therefore$ by remainder theorem. there exists $q(x) \in F[x]$ such that

$$f(x) = (x-a)q(x) + f(a)$$

$$f(x) = (x-a)q(x)$$ $\therefore (x-a)$ is a factor of $f(x)$

Problems

Prob. No ① what is the remainder when $f(x) = x^5 + 2x^3 + x^2 + 2x + 3 \in Z_5[x]$ is divided by $(x-1)$?

Sol:- Given $f(x) = x^5 + 2x^3 + x^2 + 2x + 3$

when $f(x)$ is divided by $(x-1)$, the remainder is $f(1)$

$$f(1) = 1 + 2 + 1 + 2 + 3 = 9 \equiv 4 \pmod 5$$

$\therefore$ the remainder is 4 in Z_5.

Prob. No ②. what is the remainder when $f(x) = 2x^3 + x^2 + 2x + 3 \in Z_5[x]$ is divided by $(x-2)$

Sol:- Given $f(x) = 2x^3 + x^2 + 2x + 3$

when $f(x)$ is divided by $(x-2)$, the remainder is $f(2)$

$$f(2) = 16 + 4 + 4 + 3 = 27 \equiv 2 \pmod 5$$

$\therefore$ the remainder is 2 in Z_5.

Prob. No ③ Find the remainder when $f(x) = x^{100} + x^{90} + x^{80} + x^{50} + 1$ is divided by $g(x) = (x-1)$ in $Z_2[x]$.

Sol:- Given $f(x) = x^{100} + x^{90} + x^{80} + x^{50} + 1$ and $g(x) = x - 1$

when $f(x)$ is divided by $(x-1)$, the remainder is

$f(1)$

$$f(1) = 1 + 1 + 1 + 1 + 1 = 5 \equiv 1 \pmod 2$$

$\therefore$ the remainder is 1 in Z_2

$\therefore$ $(x-1)$ is a factor of $f(x)$.

Theorem : If $f(x) \in F[x]$ is of degree $n \geq 1$, then $f(x)$ has atmost 'n' roots of F.

Proof:- Given $f(x) \in F[x]$ is of degree n where $n \geq 1$. We prove the theorem by induction on n.

If $n=1$, then $f(x) = ax+b$, $a,b \in F$ $a \neq 0$

clearly $-b/a$ or $-a^{-1}b \in F$ and $f(-a^{-1}b) = a(-a^{-1}b)+b$

$= -b+b = 0.$

$\therefore$ $f(x)$ has (at least) one root in F.

If c_1, c_2 in F are two roots of $f(x)$, then

$f(c_1)=0 \Rightarrow ac_1+b=0$ and $f(c_2)=0 \Rightarrow ac_2+b=0$

$ac_1+b = ac_2+b \Rightarrow ac_1 = ac_2$

Since F is a field, it is an integral domain and so cancellation laws hold

$\therefore$ $ac_1 = ac_2 \Rightarrow c_1 = c_2$

$\therefore$ there is exactly one root of F for

$f(x) = ax+b$, $a \neq 0$

Now assume that the theorem is true for all polynomials of degree $k (\geq 1)$ in $F[x]$

ie any polynomial of degree $k \geq 1$ has at most k roots in F.

Consider a polynomial $f(x)$ of degree $k+1$

If $f(x)$ has no roots in F, then the theorem is true

otherwise, let $r \in F$ be a root of $f(x)$

$\therefore$ $f(r)=0$.

$\therefore$ By factor theorem $f(x) = (x-r)g(x)$, where $g(x)$ is of degree k.

Hence by induction hypothesis, $g(x)$ has at the most k roots in F. And $r \in F$ is a root of $f(x)$

Hence $f(x)$ has at most $k+1$ roots

Hence by first Principle of induction, the theorem is true for all $n \geq 1$.

Irreducible Polynomials

Defn: Let F be a field and $f(x) \in F[x]$ is of degree ≥ 2. We call $f(x)$ is reducible over F if there exist $g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$

where $\deg g(x)$ and $\deg h(x)$ are greater than or equal to 1. ie $\deg g(x) \geq 1$ and $\deg h(x) \geq 1$.

If $f(x)$ is not reducible than we call it irreducible (or prime) over F. In other words, $f(x)$ is irreducible over F if one of $g(x)$ or $h(x)$ is of degree '0' (or a non zero constant)

Problems

Prob. No ①. Test whether the polynomial $f(x) = 2x^2+4$ is Irreducible over Z, Q, R and C

Sol:- Given $f(x) = 2x^2+4 = 2(x^2+2)$

Since 2 is constant polynomial in $Z[x]$. whose degree is 0 and $x^2+2 \in Z[x]$

Now $2x^2+4=0 \Rightarrow x^2+2=0 \Rightarrow x^2=-2 \Rightarrow x = \pm i\sqrt{2}$

$\therefore$ the roots do not belong to Z, Q and R

$\therefore$ $f(x) = 2x^2+4$ is Irreducible over Z, Q and R

But $i\sqrt{2}$ and $-i\sqrt{2}$ belong to C

$\therefore$ the roots belong to C

Hence $f(x) = 2x^2+4$ is reducible over C

Prob. No ②. Is $f(x) = x^2+1$ in $Z[x]$ is irreducible over Z

Sol:- Given $f(x) = x^2+1$ in $Z[x]$

Now $x^2+1=0 \Rightarrow x^2=-1 \Rightarrow x = \pm i$

$\therefore$ the roots $i, -i$ do not belong to Z

$\therefore$ $f(x) = x^2+1$ is irreducible over Z

Prob. No (3) Let $f(x) = x^3+x^2+x+1 \in Z.[x]$ is it reducible or Irreducible? If reducible find the other factor

Sol:- Given $f(x) = x^3+x^2+x+1 \in Z_2[x]$ and $Z_2 = \{0,1\}$

$f(0) = 1 \neq 0$ $\therefore$ 0 is a not in Z_2

$f(1) = 1+1+1+1 = 4 \equiv 0 \pmod{2}$. $\therefore$ 1 is a root in Z_2

Hence $(x-1)$ is a factor of $f(x)$ in $Z_2[x]$

$\therefore$ $f(x)$ is reducible.

$$\begin{array}{r|l} & x^2+1 \\ \hline x-1 & x^3+x^2+x+1 \\ & x^3-x^2 \\ \hline & x+1 \\ & x-1 \\ \hline & 0 \\ \hline \end{array}$$

$2 \equiv 0 \pmod{2}$.

$\therefore$ $f(x) = (x-1)(x^2+1)$.

Prob. No (4). Is $f(x) = x^3+x+1 \in Z_2[x]$ is irreducible.

Sol:- Given $f(x) = x^3+x+1 \in Z_2[x]$ and $Z_2 = \{0,1\}$

Now $f(0) = 1 \neq 0$

$f(1) = 1+1+1 = 3 \equiv 1 \pmod{2} \neq 0$

$\therefore$ 0 and 1 are not roots of $f(x)$

Hence $f(x)$ is irreducible over Z_2.

Prob. No (5). Test the polynomial x^2+x+4 in $Z_{11}[x]$ is irreducible over Z_{11}

Sol:- Let $f(x) = x^2+x+4$ in $Z_{11}[x]$ and $Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$ is a field, since 11 is a prime

$f(x) = x^2+x+4$ is a polynomial of degree 2 in $Z_{11}[x]$

We search for an element $a \in Z_{11}$ such that $f(a) = 0$

we have $f(0) = 4 \neq 0 \pmod{11}$

$f(1) = 1+1+4 = 6 \equiv -5 \pmod{11} \neq 0$

$f(2) = 4+2+4 = 10 \equiv -1 \pmod{11} \neq 0$

$f(3) = 9+3+4 = 16 \equiv 5 \pmod{11} \neq 0$

$f(4) = 16+4+4 = 24 \equiv 2 \pmod{11} \neq 0$

$f(5) = 25+5+4 = 34 \equiv 1 \pmod{11} \neq 0$

$f(6) = 36+6+4 = 46 \equiv 2 \pmod{11} \neq 0.$

$f(7) = 49+7+4 = 60 \equiv 5 \pmod{11} \neq 0$

$f(8) = 64+8+4 = 76 \equiv 10 \pmod{11} \neq 0.$

$f(9) = 81+9+4 = 94 \equiv 6 \pmod{11} \neq 0$

$f(10) = 100+10+4 = 114 \equiv 4 \pmod{11} \neq 0$

there is no root in Z_{11}

Hence $f(x)$ is irreducible over Z_{11}.

Prob. No 6 Find two non-zero polynomial $f(x)$ and $g(x)$ in $Z_{12}[x]$ such that $f(x)g(x) = 0$.

Sol:- We know $Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

Consider $f(x) = 3x^2 \in Z_{12}[x]$ $g(x) = 4x+8 \in Z_{12}[x]$

we known $f(x)$ and $g(x)$ are non-zero polynomials

But $f(x)\cdot g(x) = 3x^2(4x+8) = 12x^3 + 24x^2$

$= 0x^3 + 0x^2 = 0$ $\because 12 \equiv 0 \pmod{12}$

$24 \equiv 0 \pmod{12}$

$\therefore$ $f(x)\cdot g(x)$ is a zero polynomial in $Z_{12}[x]$

Prob. No 7 Find two non-zero polynomials $f(x), g(x)$ in $Z_7[x]$ such that $f(x)g(x) \neq 0$

Sol:- We know that $Z_7 = \{0,1,2,3,4,5,6\}$

Let $f(x) = 2x^2+4x+1$ and $g(x) = 6x^3$ be two non zero polynomials in $Z_7[x]$

$$\text{Now} \quad f(x)g(x) = (2x^2+4x+1)6x^3$$
$$= 12x^5+24x^4+6x^3 \qquad 12 \equiv 5 \pmod 7$$
$$= 5x^5+3x^4+6x^3 \qquad 24 \equiv 3 \pmod 7$$
$$\neq 0$$
$$\therefore f(x)g(x) \neq 0.$$

Theorem : Reducibility Test

Let F be a field and $f(x) \in F[x]$. Then (i) If $f(x)$ is of degree 1, then $f(x)$ is irreducible

(ii) If $f(x)$ is of degree 2 or 3, then $f(x)$ is reducible iff $f(x)$ has a root in F.

Proof:- (i) Let $f(x) = ax+b$, $a \neq 0$ in $F[x]$

Suppose $f(x)$ is reducible, then there exist $g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$

where $1 \leq \deg g(x) < \deg f(x)$ and $1 \leq \deg h(x) < \deg f(x)$

$$\therefore ax+b = g(x)h(x)$$
$$\therefore \deg(ax+b) = \deg g(x) + \deg h(x)$$
$$\Rightarrow 1 = \deg g(x) + \deg h(x)$$

This is impossible, since $\deg g(x) + \deg h(x) \geq 2$

$\therefore f(x)$ is irreducible over F.

(ii) Let $f(x) \in F[x]$ be of degree 2 or 3

Suppose $f(x)$ is reducible over F, then $f(x) = g(x)h(x)$ for some $g(x)\, h(x) \in F[x]$

where $1 \leq \deg g(x) < \deg f(x)$ and $1 \leq \deg h(x) < \deg f(x)$

Since $\deg f(x) = \deg g(x) + \deg h(x)$ and $\deg f(x) = 2$ or 3.

we have $\deg g(x) + \deg h(x) = 2$ or 3.

$\therefore$ at least one of $g(x)$ and $h(x)$ has degree 1.

Let $\deg g(x)=1 \Rightarrow g(x)=ax+b$, $a\neq 0$

Now $-a^{-1}b\in F$ and $g(-a^{-1}b)= a(-a^{-1}b)+b$

$$= -(a\cdot a^{-1})b+b = -b+b=0$$

$\therefore -a^{-1}b$ is a root of $g(x)$

Hence $-a^{-1}b$ is a root of $f(x)$ in $F[x]$. So, $f(x)$ has a root of $f(x)$ in F

Converseley, let $f(x)$ have a root $a\in F$. Then $(x-a)$ is a factor of $f(x)$

$$f(x)=(x-a)g(x) \quad , g(x)\in F[x]$$

Hence $f(x)$ is reducible over F.

Defn: Greatest common divisor (g.c.d)

Let F be a field and $f(x), g(x)\in F[x]$. A greatest common divisor (g.c.d) if $f(x)$ and $g(x)$ is a non-zero polynomial $d(x)$ such that (i) $d(x)$ divides $f(x)$ and $g(x)$ and (ii) if $c(x)$ is a divisor of $f(x)$ and $g(x)$, then $c(x)$ divides $d(x)$.

Theorem : Let F be a field and $f(x)$, $g(x)$ be polynomials in $F[x]$ with atleast one of them non-zero polynomial. Then their g.c.d $d(x)$ can be expressed as $d(x)= a(x)f(x)+b(x)g(x)$ for some $a(x), b(x)\in F[x]$

Proof:- Let $S=\{ s(x)f(x)+t(x)g(x) \,/\, s(x), t(x)\in F[x]\}$

$S\neq\phi$, since $f(x)\in S$

Let $d(x)$ be a polynomial of least degree in S

Then $d(x)= a(x)f(x)+b(x)g(x) \rightarrow ①$ for some $a(x), b(x)\in F[x]$

First we prove that $d(x)$ is a g.c.d of $f(x)$ and $g(x)$

Now consider $f(x), d(x)$

By division algorithm, there exist $q(x)$ and $r(x)$ such that

$$f(x) = q(x)d(x) + r(x) \rightarrow \textcircled{2}$$

where either $r(x) = 0$ or $\deg r(x) < \deg d(x)$

$$r(x) = f(x) - q(x)d(x)$$

$$= f(x) - q(x)\left(a(x)f(x) + b(x)g(x)\right)$$

$$= [1 - q(x)a(x)]f(x) - q(x)b(x)g(x)$$

$$= [1 - q(x)a(x)]f(x) + [[-q(x)b(x)]g(x)]$$

This is of the form $s(x)f(x) + t(x)g(x)$

$$\therefore r(x) \in S$$

If $r(x) \neq 0$, then $\deg r(x) < \deg d(x)$

which contradicts the choice of $d(x)$

$$r(x) = 0 \Rightarrow f(x) = q(x)d(x) \quad (\text{using } \textcircled{2})$$

$d(x)$ divides $f(x)$

Similarly, we can prove that $d(x)$ divides $g(x)$

Suppose $c(x)$ divides $f(x)$ and $g(x)$, then $c(x)$ divides $a(x)f(x)$ and $b(x)g(x)$

Hence $c(x)$ divides $a(x)f(x) + b(x)g(x)$

$\Rightarrow c(x)$ divides $d(x)$

$\therefore d(x)$ is the gcd of $f(x)$ and $g(x)$.

Defn: If the g.c.d of $f(x)$ and $g(x) \in F[x]$ is 1, then $f(x)$ and $g(x)$ are called relatively prime.

If $f(x)$ and $g(x)$ are relatively prime in $F[x]$, then there exist polynomials $a(x)$ and $b(x)$ in $F[x]$ such that

$a(x)f(x) + b(x)g(x) = 1$

Note① As in the case of integers, a practical way of finding g.c.d of two polynomials is by applying Euclidean algorithm.

Theorem : Euclidean Algorithm

Let F be a field and $f(x), g(x) \in F[x]$, where $g(x) \neq 0$ and $\deg g(x) \leq \deg f(x)$.

Applying the division algorithm, we write

$$
\begin{array}{ll}
f(x) = q_1(x) g(x) + r_1(x) & \deg r_1(x) < \deg g(x) \\
g(x) = q_2(x) r_1(x) + r_2(x) & \deg r_2(x) < \deg r_1(x) \\
r_1(x) = q_3(x) r_2(x) + r_3(x) & \deg r_3(x) < \deg r_2(x) \\
r_2(x) = q_4(x) r_3(x) + r_4(x) & \deg r_4(x) < \deg r_3(x) \\
\vdots & \\
r_{n-2}(x) = q_n(x) r_{n-1}(x) + r_n(x) & \deg r_n(x) < \deg r_{n-1}(x) \\
r_{n-1}(x) = q_{n+1}(x) r_n(x) + r_{n+1}(x) & r_{n+1}(x) = 0 .
\end{array}
$$

Then $r_n(x)$ is the last non-zero remainder

It can be seen that $r_n(x)$ is the g.c.d of $f(x)$ and $g(x)$.

Problems

Prob-No ① Find the g.c.d of $x^4 + x^3 + 2x^2 + x + 1$ and $x^3 - 1$ over Q

Sol:- Let $f(x) = x^4 + x^3 + 2x^2 + x + 1$, $g(x) = x^3 - 1$

and $\deg g(x) < \deg f(x)$, Divide $f(x)$ by $g(x)$ by division algorithm successively.

$$
\begin{array}{r|l}
 & x + 1 \\
\hline
x^3 - 1 & x^4 + x^3 + 2x^2 + x + 1 \\
 & x^4 - x \\
\hline
 & x^3 + 2x^2 + 2x + 1 \\
 & x^3 - 1 \\
\hline
 & 2x^2 + 2x - 2 \\
\hline
\end{array}
\qquad
\begin{array}{r|l}
 & \tfrac{1}{2}x - \tfrac{1}{2} \\
\hline
2x^2 + 2x + 2 & x^3 - 1 \\
 & x^3 + x^2 + x \\
\hline
 & -x^2 - x - 1 \\
 & -x^2 - x - 1 \\
\hline
 & 0 \\
\hline
\end{array}
$$

$f(x) = (x+1)(x^3-1) + 2(x^2+x+1)$, $\deg(2x^2+2x+2) < \deg(x^3-1)$

$x^3-1 = \left(\frac{x}{2}-\frac{1}{2}\right)(2x^2+2x+2) + 0 = (x-1)(x^2+x+1)$

∴ The last non zero remainder is x^2+x+1

$$f(x) = (x+1)(x-1)(x^2+x+1) + (x^2+x+1)$$
$$= (x^2+x+1)((x+1)(x-1)+1)$$

∴ the g.c.d is (x^2+x+1).

Characteristic of a Ring

Defn : Characteristic of a ring R is the least positive integer 'n' such that $na = 0 \ \forall a \in R$ and we write $\text{char}(R) = n$. If no such positive integer exists, then R is said to have characteristic 0.

For example ①. The ring $(Z_3, +, \cdot)$ has characteristic 3.

In $Z_3 = \{0, 1, 2\}$ $\quad 1+1+1 = 3(1) \equiv 0 \pmod 3$

∴ Characteristic is 3 $\quad 2+2+2 = 3(2) \equiv 0 \pmod 3$

$3(a) = 0 \ \forall a \in Z_3$

ie $\text{Char}(Z_3) = 3$.

More generally, characteristic of the ring $(Z_n, +, \cdot)$ is n.

2. $(Z, +, \cdot)$ and $(Q, +, \cdot)$ are rings

For any $a \in Z$ (or Q), there is no positive integer n such that $na = 0 \ \forall a \in Z$ (or Q)

∴ $\text{Char}(Z) = 0$ and $\text{Char}(Q) = 0$.

Theorem : The characteristic of a field $(F, +, \cdot)$ is either '0' or a prime number

Proof:- Let $(F, +, \cdot)$ be a field

If $\text{char}(F) = 0$, then there is nothing to prove

If char $(F) \neq 0$, then let char $(F) = n$.

To prove n is a prime

Suppose 'n' is not a prime, then $n = pq$, where $1 < p < n$, $1 < q < n$ ie p and q are proper factors of n.

Since char $(F) = n$, we have $na = 0 \;\forall a \in F$

Take $a = 1$, then $n \cdot 1 = 0$ (1 is identity of F)

$\Rightarrow (pq)\cdot 1 = 0 \Rightarrow (p\cdot 1)(q \cdot 1) = 0$.

$$(\because (pq)\cdot 1 = \underbrace{1+1+1+\cdots+1}_{pq \text{ terms}} = (\underbrace{1+1+1+\cdots+1}_{p \text{ terms}})(\underbrace{1+1+\cdots+1}_{q \text{ terms}}))$$

Since F is a field, F is an integral domain and so, it has no divisor of zero either $p\cdot 1 = 0$ or $q \cdot 1 = 0$

Since p and q are less than n, it contradicts the definition of characteristic of F

$\therefore n$ is a prime number.

Note ①: the characteristic of a ring need not be a prime. For example char $(Z_6) = 6$, which is not a prime

②. the characteristic of a finite field is a prime number p

③. the fields $(Q, +, \cdot)$ $(R, +, \cdot)$ are of characteristic zero.

Theorem: the number of elements of a finite field is p^n, where p is a prime number and 'n' is a positive integer.

Proof:- We know for a prime p, Z_p is a field having p elements and char $(Z_p) = p$, since $pa = 0 \;\forall a \in Z_p$

Consider the polynomial $f(x) = x^{p^n} - x$ in $Z_p[x]$.

Now the derivative $f'(x) = p^n x^{p^n - 1} - 1$

Since char $(Z_p) = p$, char $(Z_p[x]) = p$ and so $pg(x) = 0$ $\forall g(x) \in Z_p[x]$.

Hence $px^{p^n-1} = 0 \Rightarrow p^n . x^{p^n-1} = 0$

$\therefore f'(x) = -1$, a constant polynomial

Hence $f(x)$ and $f'(x)$ have no common root.

Hence $f(x)$ has no multiple roots ie the roots of $f(x)$ are all distinct.

If k is the smallest extension field containing all the roots of $f(x)$ ie k is the splitting field of $f(x)$.

then $f(x)$ has p^n distinct roots in k.

In k, let F be the set of all elements satisfying $f(x)$

$$F = \{a \in k \,/\, a^{p^n} = a\} < k$$

Hence F has only p^n elements

We now prove F is a field. Let $a, b \in F$. Then $a^{p^n} = a$ and $b^{p^n} = b$

$$(ab)^{p^n} = a^{p^n} . b^{p^n} = ab \Rightarrow a,b \in F \quad (\because a \cdot b = ba \,\forall a,b \in k$$

$$(a+b)^{p^n} = a^{p^n} + p^nC_1 a^{p^n-1} . b + p^nC_2 a^{p^n-2} . b^2 + \dots + p^nC_r a^{p^n-r} . b^r + \dots + b^{p^n} \text{ (using binomial expansion)}$$

Char $(k) = p$

$$pa^{p^n-r} . b^r = 0 \qquad r = 1, 2, 3 \dots$$

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a+b \Rightarrow a+b \in F$$

Similarly $(a-b)^{p^n} = a-b \Rightarrow a-b \in F$

$\therefore F$ is a subfield of k

Hence F is a field having p^n elements.

Exercise Problems (EX. 17.1 - Grimaldi)

Prob. No ① For each of the following pairs $f(x), g(x)$. Find $q(x), r(x)$ so that $g(x) = q(x)f(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg f(x)$

(i) $f(x), g(x) \in Q[x]$, $f(x) = x^4 - 5x^3 + 7x$, $g(x) = x^5 - 2x^2 + 5x - 3$

(ii) $f(x), g(x) \in Z_2[x]$, $f(x) = x^2+1$, $g(x) = x^4 + x^3 + x^2 + x + 1$

(iii) $f(x), g(x) \in Z_5[x]$, $f(x) = x^2 + 3x + 1$ $g(x) = x^4 + 2x^3 + x + 4$

Sol:- (i) Given $f(x), g(x) \in Q[x]$

$$\begin{array}{r|l} & x+5 \\ \cline{2-2} x^4-5x^3+7x & x^5-2x^2+5x-3 \\ & x^5-5x^4+7x^2 \\ \cline{2-2} & 5x^4-9x^2+5x \\ & 5x^4-25x^3+35x \\ \cline{2-2} & 25x^3-9x^2+30x-3 \\ \cline{2-2} \end{array}$$

Here $\deg r(x) < \deg f(x)$

(ii) Given $f(x), g(x) \in Z_2[x]$

$$\begin{array}{r|l} & x^2+x \\ \cline{2-2} x^2+1 & x^4+x^3+x^2+x+1 \\ & x^4+x^2 \\ \cline{2-2} & x^3+x \\ & x^3+x \\ \cline{2-2} & 1 \\ \cline{2-2} \end{array}$$

$$x^4 + x^3 + x^2 + x + 1 = (x^2+1)(x^2+x) + 1$$

(iii) Given $f(x), g(x) \in Z_5[x]$

$$\begin{array}{r|l} & x^2+4x+2 \\ \hline x^2+3x+1 & x^4+2x^3+x+4 \\ & x^4+3x^3+x^2 \\ \hline & 4x^3+4x^2+x \\ & 4x^3+2x^2+4x \\ \hline & 2x^2+2x+4 \\ & 2x^2+x+2 \\ \hline & x+2 \\ \hline \end{array}$$

$$x^4+2x^3+x+4 = (x^2+3x+1)(x^2+4x+2)+x+2$$

Prob. No ②. If $f(x) = x^4-16$, find its roots and factorization in $Q[x]$, $R[x]$, $C[x]$

Sol:- Given $f(x) = x^4-16$

$$x^4-16=0 \Rightarrow (x^2-4)(x^2+4)=0$$
$$\Rightarrow x^2=4 \text{ and } x^2=-4$$
$$\Rightarrow x=\pm 2 \text{ and } x=\pm 2i$$

Here $x=\pm 2 \in Q[x], R[x]$ and $x=\pm 2i \in C[x]$

Prob. No ③. Find all roots of $f(x) = x^2+4x$ in $Z_{12}[x]$

Sol:- Given $f(x) = x^2+4x$ and $Z_{12}[x] = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

$f(0)=0$	$f(3)=9$	$f(6)=0$	$f(9)=9$
$f(1)=5$	$f(4)=8$	$f(7)=5$	$f(10)=8$
$f(2)=0$	$f(5)=9$	$f(8)=0$	$f(11)=9$.

Exercise 17.2

Prob. No ①. Using Euclidean algorithm find g.c.d

(i) $f(x) = x^2+x-2$ $g(x) = x^5-x^4+x^3+x^2-x-1$ in $Q[x]$

(ii) $f(x)=x^4+x^3+1$, $g(x)=x^2+x+1$ in $Z_2[x]$.

Sol:- (i) Given $f(x)=x^2+x-2$ and $g(x)=x^5-x^4+x^3+x^2-x-1$ in $Q[x]$

$$x^3-2x^2+5x-8$$

$$x^2+x-2 \;\big)\; x^5-x^4+x^3+x^2-x-1$$

$$x^5+x^4-2x^3$$

$$-2x^4+3x^3+x^2$$

$$-2x^4-2x^3+4x^2$$

$$5x^3-3x^2-x$$

$$5x^3+5x^2-10x$$

$$-8x^2+9x-1$$

$$-8x^2-8x+16$$

$$17x-17$$

$\therefore g(x)=q_1(x)f(x)+r_1(x)$

$\therefore g(x)=(x^3-2x^2+5x-8)(x^2+x-2)+17x-17$

$$\tfrac{1}{17}x+\tfrac{2}{17}$$

$$17x-17 \;\big)\; x^2+x-2$$

$$x^2-x$$

$$2x-2$$

$$2x-2$$

$$0$$

$f(x)=q_2(x)r_1(x)+r_2(x)$

$\therefore$ GCD $\mu = 17x-17$ simply $(x-1)$

GCD can be written as GCD $= g(x)-q_1(x)f(x)$

$$x-1=\frac{1}{17}\left[(x^5-x^4+x^3+x^2-x-1)-(x^3-2x^2+5x-8)(x^2+x-2)\right]$$

(ii) Given $f(x)=x^4+x^3+1$ and $g(x)=x^2+x+1$ in $Z_2[x]$

$$\begin{array}{r|l} & x^2-1 \\ \hline x^2+x+1 & x^4+x^3+1 \\ & x^4+x^3+x^2 \\ \hline & -x^2+1 \\ & -x^2-x-1 \\ \hline & x \\ \hline \end{array}$$

$\therefore f(x)=q_1(x)g(x)+r_1(x)$

$$\begin{array}{r|l} & x+1 \\ \hline x & x^2+x+1 \\ & x^2 \\ \hline & x+1 \\ & x \\ \hline & 1 \\ \hline \end{array}$$

$\therefore g(x)=q_2(x)r_1(x)+r_2(x)$

$$\begin{array}{r|l} & x \\ \hline 1 & x \\ & x \\ \hline & 0 \\ \hline \end{array}$$

$r_1(x)=q_3(x).1+r_3(x)=0$

$\therefore$ GCD $r_2(x)=1$

$1=g(x)-q_2(x)r_1(x)$

$=(x^2+x+1)-(x+1)x$.

Prob. No (2). Construct a finite field of 25 elements

Sol:- Construct irreducible polynomial of degree 2 in $Z_2[x]$

$f(x)=x^2+2$ has to be reduced to degree 1 ?

ie Does it have a zero in Z_5

$f(0)=2$ $f(1)=3$ $f(2)=1$ $f(3)=1$ $f(4)=1$

no roots $\therefore$ It is not irreducible

$\therefore \dfrac{Z_5[x]}{x^2+2}$ is a field of $5^2=25$ elements

Prob. No(3) Construct a field Consisting of four elements.

Sol:- By using the irreducible binary polynomial x^2+x+1

consider $Z_2 = \{0,1\}$ and $f(x) = x^2+x+1 \in Z_2[x]$

$$f(0) = 1 \neq 0$$

$$f(1) = 1+1+1 = 3 \neq 1 \ (\mathrm{mod}\ 2) \neq 0$$

$\therefore$ $f(x)$ is irreducible over Z_2

$\therefore$ $\dfrac{Z_2[x]}{\langle f(x)\rangle} = \dfrac{Z_2[x]}{\langle x^2+x+1\rangle}$ is a field having $2^2=4$

elements

To find the four elements

this field consists of the different equivalence classes of mod (x^2+x+1) in $Z_2[x]$.

consider $f(x) \in Z_2[x]$ and $x^2+x+1 \in Z_2[x]$

By division algorithm

$$f(x) = q(x)(x^2+x+1) + r(x)$$

where either $r(x)=0$ or $\deg r(x) < \deg (x^2+x+2) = 2$

$\deg r(x) = 0$ or 1.

Hence $r(x) = ax+b$ where $a,b \in Z_2$

Since $f(x) - r(x) = q(x)(x^2+x+1)$

$$f(x) \equiv r(x) \bmod (x^2+x+1)$$

$\therefore$ $[f(x)] = [r(x)]$

So, to find the equivalence classes mod (x^2+x+1), it is enough to find the possible values of $r(x) = ax+b$.

If $a=0$, $b=0$ $r(x)=0$

If $a=0$, $b=1$ $r(x)=1$

If $a=1$, $b=0$ $r(x)=x$

If $a=1$, $b=1$ $r(x)=x+1$

∴ the equivalence classes are $[0], [1], [x], [x+1]$

∴ the 4 elements of the field $\frac{Z_2[x]}{\langle x^2+x+1\rangle}$ are $[0], [1]$, $[x]$, $[x+1]$

$$\therefore \frac{Z_2[x]}{\langle x^2+x+1\rangle} = \{[0], [1], [x], [x+1]\}.$$

Prob. No (4). In $Z_3[x]$, $s(x) = x^2+x+2$. Show that $s(x)$ is irreducible over Z_3 and construct the field $\frac{Z_3[x]}{\langle s(x)\rangle}$. What is the order of this field.

Sol:- Given $s(x) = x^2+x+2$ in $Z_3[x]$ and $Z_3 = \{0,1,2\}$

Now $s(0) = 2 \neq 0$

$s(1) = 1+1+2 = 4 \equiv 1 \pmod 3 \neq 0$

$s(2) = 4+2+2 = 8 \equiv 2 \pmod 3 \neq 0$

∴ $s(x)$ has no root in Z_3

Hence $s(x)$ is irreducible in $Z_3[x]$

∴ $\frac{Z_3[x]}{\langle s(x)\rangle}$ is a field.

Since $\deg s(x) = 2$, this field has $3^2 = 9$ elements

this field consists of '9' different equivalence classes (mod $s(x)$)

Let $f(x) \in Z_3[x]$

then $f(x) = q(x)(x^2+x+1) + r(x)$

where $r(x) = 0$ or $\deg r(x) < \deg(x^2+x+1) = 2$

∴ $\deg r(x)$ is '0' or '1'

$r(x) = ax+b$, $a, b \in Z_3$ and $[f(x)] = [r(x)]$

∴ the different equivalence classes mod (x^2+x+1) correspond to the different values of $r(x)$

Each of 'a' and 'b' can take 3 values from Z_3 and so there is $3 \cdot 3 = 9$ values for $r(x)$.

They are

1. If $a=0$, $b=0$, then $r(x)=0$

2. If $a=0$, $b=1$, then $r(x)=1$

3. If $a=0$, $b=2$, then $r(x)=2$

4. If $a=1$, $b=0$, then $r(x)=x$

5. If $a=1$, $b=1$, then $r(x)=x+1$

6. If $a=1$, $b=2$, then $r(x)=x+2$

7. If $a=2$, $b=0$, then $r(x)=2x$

8. If $a=2$, $b=1$, then $r(x)=2x+1$

9. If $a=2$, $b=2$, then $r(x)=2x+2$

$\therefore$ the nine equivalence classes are $[0]$, $[1]$, $[2]$, $[x]$, $[x+1]$, $[2x]$, $[2x+1]$, $[2x+2]$

$$\therefore \frac{Z_3[x]}{\langle x^2+x+2\rangle} = \{[0],[1],[2],[x],[x+1],[2x], [2x+1], [2x+2]\}$$

$\therefore$ the order of the field is 9

ie the number of elements is 9.

Prob. No (5) In the field $\frac{Z_3[x]}{\langle x^2+x+2\rangle}$ with 9 elements find (i) $[x+2][2x+2]+[x+1]$ and (ii) $[2x+1]^2[x+2]$ (iii) $[2x+1]^{-1}$

Sol:- Given $\frac{Z_3[x]}{\langle x^2+x+2\rangle}$ is a finite field with 9 elements (by using Prob. No. (4))

(i) To find $[x+2][2x+2]+[x+1]$

Now $[x+2][2x+2] = [2x^2+6x+4] = [2x^2+4] = [x]$

$$\begin{array}{r|l} & \quad 2 \\ \hline x^2+x+2 & 2x^2+4 \\ & 2x^2+2x+4 \\ \hline & \quad -2x = x \\ \hline \end{array} \qquad (\because -2 \equiv 1 \pmod 3).$$

$$\therefore [x+2][2x+2] + [x+1] = [x] + [x+1] = [2x+1]$$

(ii) To find $[2x+1]^2[x+2] = [4x^2+4x+1][x+2]$

$$= [x^2+x+1][x+2] \quad (\because 4 \equiv 1 \pmod 3)$$

$$\begin{array}{r|l} & \quad 1 \\ \hline x^2+x+2 & x^2+x+1 \\ & x^2+x+2 \\ \hline & -1 \equiv 2 \pmod 3 \\ \hline \end{array} \qquad \therefore [x^2+x+1] = [2]$$

$\therefore$ we get $[2x+1]^2[x+2] = 2[x+2] = [2x+4]$

$$= [2x+1]$$

(iii) Now consider $[2x+1][2x] = [4x^2+2x] = [x^2+x] = [-2]$

$$= [1]$$

Since $4 \equiv 1 \pmod 3$, $x^2+x \equiv -2 \pmod{(x^2+x+2)}$

and $-2 \equiv 1 \pmod 3$

$$[2x+1][2x] = [1] \Rightarrow [2x+1]^{-1} = [2x].$$

UNIT-3 DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS

Divisibility theory and division algorithm

Defn:- (Divisibility)

Let $a,b \in Z$. we say b divides a and write b/a if $a=bc$ for some integer c.

we also say that b is a factor of 'a' or 'b' is a divisor of 'a' or 'a' is a multiple of b.

If 'b' does not divide a, we write $b \nmid a$.

Theorem (1) If $a,b \in Z$ then (i) $a/a \ \forall \ a \neq 0 \in Z$ (reflexivity)

(ii) a/b and $b/c \Rightarrow a/c \ \forall \ a,b \neq 0, c \neq 0 \in Z$ (transitivity)

(iii) $a/b \Rightarrow a/bc \ \forall \ a \neq 0, b \in Z$

(iv) a/b and $a/c \Rightarrow a/xb+yc \ \forall x,y \in Z, a \neq 0 \in Z$ (linearity)

Proof:- (i) If $a \neq 0$, a/a ($\because a = a.1$)

(ii) $a/b \Rightarrow b = q_1 a$ and $b/c \Rightarrow c = q_2 b$ where $a \neq 0, b \neq 0$ in Z, q_1, q_2 are some integers

$\therefore c = q_2(q_1 a) = (q_2 q_1) a \Rightarrow a/c$

(iii) $a/b \Rightarrow b = q_1 a$

$\therefore bc = (q_1 a)c = q_1(ac) = q_1(ca) = (q_1 c)a$

$\Rightarrow a/bc \ \forall \ b \in Z$

(iv) $a/b \Rightarrow b = q_1 a$ and $a/c \Rightarrow c = q_2 a$ for some integers q_1 and $q_2 \in Z$

$$xb+yc = x(q_1 a) + y(q_2 a)$$
$$= (xq_1)a + (yq_2)a$$
$$= (xq_1 + yq_2)a \text{ ; } xq_1+yq_2 \text{ is an integer}$$

$$\Rightarrow \quad a/xb+yc$$

Note ①: $xb+yc$ is called a linear combination of 'b' and 'c' If $x=1, y=1, a/b+c$ and if $x=1, y=-1, a/b-c$.

Theorem ② (The Division Algorithm)

Let 'a' be any integer and 'b' a positive integer. Then there exist unique integers q and r such that

$$\underset{\text{dividend}}{a} = \underset{\text{quotient}}{q}\,\underset{\text{divisor}}{b} + \underset{\text{remainder}}{r} \quad \text{where } 0 \leq r < b.$$

Proof:- First we prove existence and then uniqueness

Existence is usually proved by suitable construction

Consider the set $S = \{a-nb \,/\, n \in Z, a-nb \geq 0\}$.

clearly $\underline{S \subset W}$

Given 'a' is any integer. Then $a<0$ or $a \geq 0$

If $a \geq 0$, then $a = a - 0.b \in S$ and so $a \in S$.

Hence S is non-empty

Now let $a<0$, since 'b' is a positive integer, $b \geq 1$.

multiplying by a, we get $ab \leq a$

$$-ab \geq -a$$

$$a - ab \geq 0$$

$$a-ab \in S \Rightarrow S \text{ is non empty.}$$

So, we find S is non-empty if $a \geq 0$ or $a<0$

Since S is set of non-negative integers (by its construction)

by well-ordering principle S contains a least integer r.

As $r \in S$, we can find an integer q such that

$$r = a - qb, \text{ where } r \geq 0$$

we shall now prove $r<b$. We prove by contradiction.

Suppose $r \geq b$, then $r-b \geq 0$ and hence $r-b \in S$

Since $r \geq 0$ and $b > 0$, $r - b < r$.

Now $r - b \in S$ and $r - b < r$, which contradicts the choice of r

$\therefore r < b$

Thus there exist integers q and r such that

$$a = qb + r \quad , 0 \leq r < b \rightarrow ①$$

We now prove the uniqueness

Suppose we also have $a = q_1 b + r_1 \quad , 0 \leq r_1 < b$

Then $qb + r = q_1 b + r_1$

$$(q - q_1) b = r_1 - r$$

$$b / r_1 - r$$

If $r_1 - r \neq 0$, then $b / r_1 - r$ which is contradiction

$$r_1 - r = 0 \Rightarrow r_1 = r$$

Hence $(q - q_1) b = 0 \Rightarrow q - q_1 = 0$

$$\Rightarrow q = q_1$$

$\therefore$ the expression $a = qb + r, 0 \leq r < b$ is unique which is the division algorithm.

Problems

Prob. No ①. Find the quotient and remainder when (i) -23 is divided by 5 (ii) 207 is divided by 15.

Sol:- (i)

$$\begin{array}{r|l} & -4 \\ 5 & -23 \\ & -20 \\ \hline & -3 \end{array}$$

but -3 cannot be a remainder as $0 \leq r < n$.

$$\begin{array}{r|l} & -5 \\ 5 & -23 \\ & -25 \\ \hline & 2 \end{array}$$

$\therefore q = -5$ and $r = 2$

(or) $-23 = -5(5) + 2 \quad 0 < 2 < 5$

Here $q = -5$, $r = 2$

(ii) $207 = 13(15) + 12$ where $0 < 12 < 15$

Here $q = 13$ and $r = 12$

$$\begin{array}{r|l} & 13 \\ 15 & 207 \\ & 15 \\ \hline & 57 \\ & 45 \\ \hline & 12 \end{array}$$

Prob. No 2 Let 'b' be an integer ≥ 2, suppose $b+1$ integers are randomly selected, Prove that the difference of two of them is divisible by 'b'.

Sol:- By division algorithm

If 'x' is divided by b,
$$\begin{array}{r} q \\ b\overline{)\,x\,} \\ \underline{r} \end{array}$$

$$x = bq + r \quad , 0 \leq r < b$$

ie there are b remainders $0, 1, 2, 3, \cdots, b-1$

Now take $b+1$ number $x_1, x_2, x_3 \cdots x_b, x_{b+1}$

Now consider the 'b' remainder as pigeon holes and remainder of the numbers $x_1, x_2, x_3 \ldots x_b, x_{b+1}$ when divided by b as Pigeons.

ie there are $(b+1)$ pigeons $r_1, r_2, \cdots r_b, r_{b+1}$

Now, By Pigeon hole Principle '2' numbers x_k, x_m occupies same pigeon hole ie $x_k = q_1 b + r_k$, $x_m = q_2 b + r_m$

as they occupy same pigeon hole $r_k = r_m$

$$\therefore x_k = q_1 b + r \quad , \quad x_m = q_2 b + r$$

$$x_k - x_m = (q_1 - q_2) b$$

Since 'b' divides RHS. $\Rightarrow$ 'b' divides $LHS = x_k - x_m$

Hence the proof.

Prob. No 3 Find the positive factors of the number (i) 12 (ii) 16 (iii) 15.

Sol:- (i) $12 = 2^2 \times 3$ $\therefore$ the positive factors are 1, 2, 3, 4, 6, 12

(ii) $16 = 2^4$, $\therefore$ the positive factors are 1, 2, 4, 8, 16

(iii) $15 = 3 \times 5$ $\therefore$ the positive factors are 1, 3, 5, 15.

Prob. No 4 (i) Evaluate $\sum_{d/12} d$ (sum of divisors of 12)

(ii) Evaluate $\sum_{d/12} 1$ (number of divisors of 12).

Sol:- (i) the number which divide 12 are 1, 2, 3, 4, 6, 12

$$= 1+2+3+4+6+12$$
$$= 28$$

(ii) the factors are 1, 2, 3, 4, 6, 12

$$\therefore \sum_{d/12} 1 = 6.$$

Prob. No 5. Prove that product of any two integers of the form $(3k+1)$ is also of the same form.

Sol:- Take two numbers of the form

$$(3m+1)(3n+1) = 9mn + 3m + 3n + 1$$
$$= 3(3mn + m + n) + 1$$
$$= 3l + 1$$ is also of the same form.

Prob. No 6. Prove 30 divides $n^5 - n$.

Sol:- $n^5 - n = n(n^4 - 1) = n(n^2-1)(n^2+1)$

$$= n(n-1)(n+1)(n^2+1).$$
$$= n(n-1)(n+1)(n^2-4+5)$$
$$= n(n-1)(n+1)(n^2-4) + 5n(n-1)(n+1)$$
$$= n(n-1)(n+1)(n-2)(n+2) + 5(n-1)n(n+1)$$
$$= (n-2)(n-1)n(n+1)(n+2) + 5(n-1)n(n+1)$$

Product of consecutive 5 integers, divisible by 5! = 120 in particular by 30

Product of consecutive 3 numbers divisible by 3! = 6 So altogether divisible by 30

$\therefore$ So entire number is divisible by 30.

Prob. No 7 Prove that difference of the squares of two positive integers cannot be 1.

Sol:- Suppose not, $m^2 - n^2 = 1$

then m^2 and n^2 are successive integers. For no two integers m, n; m^2, n^2 are successive.

Prob. No 8. using mathematical induction prove that $4^{2n} + 10^n - 1$ divisible by 25.

Sol:- $4^{2n} + 10^n - 1 = 25k$

$$4^{2(n+1)} + 10^{n+1} - 1 = 4^{2n} \cdot 4^2 + 10^n \cdot 10 - 1$$
$$= 16 \cdot 4^{2n} + 10^n \cdot 10 - 1$$
$$= 4^{2n} \cdot 16 + 10^n \cdot (16 - 6) - (16 - 15).$$
$$= (4^{2n} \cdot 16 + 10^n \cdot 16 - 16) - 10^n \cdot 6 + 15$$
$$= 16(4^{2n} + 10^n - 1) - 10^n \cdot 6 + 15$$
$$= 16\ 25k - 10^n \cdot 6 + 15.$$

Prob. No 9 Find the largest non-trivial factor of $2^{30} - 1$

Sol:- $(2^{30} - 1) = (2^{15} - 1)(2^{15} + 1)$

$2^{30} - 1 \cong 2^{30}$ has factors upto $\lfloor \sqrt{2^{30}} \rfloor = \lfloor 2^{15} \rfloor$

$\therefore$ largest factor is $(2^{15} + 1)$.

Prob. No 10. Prove by induction that $2n^3 + 3n^2 + n$ is divisible by 6 for all integers $n \geq 0$.

Sol:- Let $P(n)$ be the statement $2n^3 + 3n^2 + n$ is divisible by 6

To prove $P(n)$ is true $\forall n \geq 0$.

Basic Step : Here $n_0 = 0$

∴ $p(0) = 0$ is divisible by 6, which is true

So $p(0)$ is true

Inductive Step : Assume $p(k)$ is true, $k > 0$

$\Rightarrow 2k^3+3k^2+k$ is divisible by 6 is true

$\Rightarrow 2k^3+3k^2+k = 6x \rightarrow ①$ where 'x' is an integer

To prove $p(k+1)$ is true

ie to prove $2(k+1)^3 + 3(k+1)^2+(k+1)$ is divisible by 6.

Now

$$2(k+1)^3+3(k+1)^2+(k+1) = 2(k^3+3k^2+3k+1)+3(k^2+2k+1) + k+1$$

$$= (2k^3+3k^2+k) + 6k^2+6k+6k+3+1+2$$

$$= (2k^3+3k^2+k) + 6k^2+12k+6$$

$$= 6x + 6(k^2+2k+1)$$

$$= 6(x+k^2+2k+1)$$

where $x+k^2+2k+1$ is an integer

∴ $p(k+1)$ is true

thus $p(k+1)$ is true $\Rightarrow$ $p(k)$ is true

Hence by first principle of induction $p(n)$ is true $\forall n \geq 0$.

Prob. No ⑪ Prove by induction that $2^{4n}+3n-1$ is divisible by 9 $\forall n \geq 0$.

Sol:- Let $p(n)$ denote the statement

$2^{4n}+3n-1$ is divisible by 9

To prove $p(n)$ is true $\forall n \geq 0$

Basic Step: Here $n_0 = 0$

$p(0)$ is $2^0 + 3\cdot 0 - 1 = 0$ which is divisible by 9

∴ $p(0)$ is true.

Inductive step: Assume that $P(k)$ is true for $k \geq 0$

$\Rightarrow 2^{4k}+3k-1$ is divisible by 9 is true

$\Rightarrow 2^{4k}+3k-1 = 9x$ where x is an integer

To prove $p(k+1)$ is true

ie to prove $2^{4(k+1)}+3(k+1)-1$ is divisible by 9 is true.

Now $2^{4(k+1)}+3(k+1)-1 = 2^{4k}.2^{4}+3k+3-1$

$$= 16(9x-3k+1)+3k+2$$

$$= 144x-45k+18$$

$$= 9(16x-5k+2)$$

where $16x-5k+2$ is an integer

$\therefore 2^{4(k+1)}+3(k+1)-1$ is divisible by 9 is true

$\therefore p(k+1)$ is true

Thus $P(k)$ is true $\Rightarrow p(k+1)$ is true

Hence by first principle of induction $p(n)$ is true $\forall n \geq 0$.

Prob.No (12) If the sum of the cubes of three consecutive integers is a cube k^3 prove that $3/k$

Sol:- Let $n, n+1, n+2$ be the three consecutive integers

Given $n^3+(n+1)^3+(n+2)^3$ is a cube k^3

$$n^3+n^3+3n^2+3n+1+n^3+3n^2.2+3n.2^2+2^3=k^3$$

$$3n^3+9n^2+15n+9=k^3$$

$$3(n^3+3n^2+5n+3)=k^3$$

$3/k^3 \Rightarrow 3/k.k.k$ (∵ 3 is a prime $3/k$)

Prob. No $\textcircled{13}$. Show that $n^3+(n+1)^3+(n+2)^3=(n+3)^3$ has a unique solution.

Sol:- Given $n^3+(n+1)^3+(n+2)^3=(n+3)^3 \rightarrow \textcircled{1}$

Since LHS is the sum of cubes of three consecutive integers by prob. No $\textcircled{12}$, $3/n+3$

Since $3/n+3$ and $3/3$, we get $3/n+3-3 \Rightarrow 3/n$

$n=3m$, where m is an integer

$$\therefore \textcircled{1} \Rightarrow (3m)^3+(3m+1)^3+(3m+2)^3=(3m+3)^3$$

$$\Rightarrow 27m^3+(3m)^3+3(3m)^2.1+3(3m)+1+(3m)^3+3.(3m)^2.2$$
$$+3(3m).2^2+2^3=(3m)^3+3.(3m)^2.3+3.(3m)3^2+3^3$$

$$\Rightarrow 27m^3+27m^3+27m^2+9m+1+27m^3+54m^2+36m$$
$$+8 = 27m^3+81m^2+81m+27$$

Simplifying, we get $54m^3-36m-18=0$

$\Rightarrow 3m^3-2m-1=0$

$\Rightarrow (m-1)(3m^2+3m+1)=0$

$\Rightarrow m-1=0 \quad (\because 3m^2+3m+1\neq0)$

$\Rightarrow m=1$ (Because $3m^2+3m+1=0$ has no real roots).

$\Rightarrow n=3$

So, the solution of eqn $\textcircled{1}$ is unique.

The Principle of Mathematical Induction

1. First Principle of induction: Let $p(n)$ be a proposition corresponding to positive integers 'n' satisfying the following conditions

   (i) $p(n_0)$ is true for some integer n_0

   (ii) If $p(k)$ is true for an arbitrary integer $k > n_0$, then $p(k+1)$ is also true. then $p(n)$ is true for all integers $n \geq n_0$

2. Second Principle of induction (or) Strong principle of induction: Let $p(n)$ be a proposition corresponding to positive integers 'n' satisfying the following conditions

   (i) $p(n_0)$ is true for some integer n_0

   (ii) If the proposition is true for all integers upto k $(> n_0)$ ie if $p(n_0+1), p(n_0+2) \ldots p(k)$ are true, then $p(k+1)$ is true

   then $p(n)$ is true for all integers $n \geq n_0$.

The Pigeon hole Principle

The pigeon hole principle is also known as the Dirichlet box principle after the German mathematician Dirichlet who used it extensively in his work on number theory.

If m pigeons are assigned to n pigeon holes, when $m > n$, then at least two pigeons must occupy the same pigeon hole.

Theorem: (The Pigeonhole Principle) If 'm' pigeons are assigned to n pigeon holes, where $m > n$ then at least two pigeons must occupy the same pigeon hole

Proof:- By contradiction

Suppose the given conclusion is false. ie no two pigeons occupy the same pigeon hole. Then every pigeon must occupy a distinct pigeonhole, so $n \geq m$. which is a contradiction. Thus, two or more pigeons must occupy same pigeonhole.

Defn:- (Greatest integer function)

$[x]$ = the greatest integer $\leq x$

In computer science the greater integer function is called floor function and is denoted by $\lfloor x \rfloor$

Ex. $\lfloor 3.4 \rfloor$ = the greatest integer $\leq 3.4 = 3$.

$\lfloor -3.4 \rfloor$ = the greatest integer $\leq -3.4 = -4$

Defn:- (The ceiling function)

The ceiling function $\lceil x \rceil$ is the least integer $\geq x$

Ex. $\lceil 3.4 \rceil$ = the least integer $\geq 3.4 = 3$

$\lceil -3.4 \rceil$ = the least integer $\geq -3.4 = -3$

Theorem: Let 'a' and 'b' be any positive integers. Then the number of positive integers $\leq a$ and divisible by b is

$$\left\lfloor \frac{a}{b} \right\rfloor \text{ (or) } \left[\frac{a}{b} \right]$$

For Ex① the number of positive integers ≤ 2076 and divisible by 19 is

$$\left\lfloor \frac{2076}{19} \right\rfloor = \lfloor 109.26 \rfloor = 109.$$

Inclusion-Exclusion Principle

If S is a set, the number of elements in S is denoted by $|S|$

If A, B, C are finite sets, then

1. $|A \cup B| = |A| + |B| - |A \cap B|$

$= S_1 - S_2$

where S_1 = sum taken one at a time = $|A| + |B|$

$S_2 = |A \cap B|$.

2. $|A \cup B \cup C| = S_1 - S_2 + S_3$

where S_1 = sum taken one at a time

$= |A| + |B| + |C|$

S_2 = sum taken two at a time

$= |A \cap B| + |A \cap C| + |B \cap C|$

$S_3 = |A \cap B \cap C|$.

This can be extended for more number of sets.

Problems

Prob. No 1 Show that the number of leap year 'l' after 1600 and not exceeding a given year 'y' is given by

$$l = \left\lfloor \frac{y}{4} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor + \left\lfloor \frac{y}{400} \right\rfloor - 388$$

Sol:- consider a leap year 'l' such that $1600 < l \le y$

To be a leap year it shall be either

(i) a non-centuary year divisible by 4

(or) (ii) a centuary year divisible by 400.

So first find

A : no. of years divisible by 4 (in $1600 < l \le y$)

B : no. of centuries (in $1600 < l \le y$)

C : no. of centuries divisible by 400 (in $1600 < l \le y$)

By inclusion-exclusion

∴ our desired number = A − B + C

(since A includes all century years which are naturally divisible by 4).

$|A| : \left\lfloor \frac{1600}{4} \right\rfloor < \frac{l}{4} < \left\lfloor \frac{y}{4} \right\rfloor \Rightarrow |A| = \left\lfloor \frac{y}{4} \right\rfloor - 400.$

$|B| : \left\lfloor \frac{1600}{100} \right\rfloor < \left\lfloor \frac{l}{100} \right\rfloor \leq \left\lfloor \frac{y}{100} \right\rfloor \Rightarrow |B| = \left\lfloor \frac{y}{100} \right\rfloor - 16.$

$|C| : \left\lfloor \frac{1600}{400} \right\rfloor < \left\lfloor \frac{l}{400} \right\rfloor \leq \left\lfloor \frac{y}{400} \right\rfloor \Rightarrow |C| = \left\lfloor \frac{y}{400} \right\rfloor - 4.$

$\therefore \; l = |A| - |B| + |C|$

$= \left\lfloor \frac{y}{4} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor + \left\lfloor \frac{y}{400} \right\rfloor - 400 + 16 - 4$

$\therefore \; l = \left\lfloor \frac{y}{4} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor + \left\lfloor \frac{y}{400} \right\rfloor - 388$

Prob. No (2) Find the positive integers ≤ 3000 and divisible by 3, 5 or 7

Sol:- Let A, B, C be the set of numbers ≤ 3000 that are divisible by 3, 5, 7 respectively.

Required $|A \cup B \cup C|$

By inclusion and exclusion principle, we get

$|A \cup B \cup C| = S_1 - S_2 + S_3$

Now $|A| = \left[\frac{3000}{3}\right] = [1000] = 1000$, $|B| = \left[\frac{3000}{5}\right] = [600] = 600$

$|C| = \left[\frac{3000}{7}\right] = [428.57] = 428$

$S_1 = |A| + |B| + |C| = 1000 + 600 + 428 = 2028$

$|A \cap B| = \left[\frac{3000}{3 \times 5}\right] = [200] = 200$ $|A \cap C| = \left[\frac{3000}{3 \times 7}\right] = [142.85] = 142$

$|B \cap C| = \left[\frac{3000}{5 \times 7}\right] = [85.71] = 85.$

$S_2 = |A \cap B| + |A \cap C| + |B \cap C| = 200 + 142 + 85 = 427$

$S_3 = |A \cap B \cap C| = \left[\frac{3000}{3 \times 5 \times 7}\right] = [28.57] = 28$

$$|A\cup B\cup C| = S_1 - S_2 + S_3$$
$$= 2028 - 427 + 28$$
$$= 1629.$$

Prob. No ③ Find the number of positive integers ≤ 2076 and divisible by neither 4 nor 5.

Sol:- First we find the number of positive integers ≤ 2076 that are divisible by 4 or 5.

Let A, B be the set of integers ≤ 2076 that are divisible by 4 or 5 respectively

By inclusion - exclusion principle, we have

$$|A\cup B| = S_1 - S_2 = 934 - 103 = 831.$$

where $S_1 = |A| + |B|$, $S_2 = |A\cap B|$

Now $|A| = \left[\frac{2076}{4}\right] = [519] = 519$

$$|B| = \left[\frac{2076}{5}\right] = [415.2] = 415$$

$$\therefore S_1 = |A| + |B| = 519 + 415 = 934$$

$$S_2 = |A\cap B| = \left[\frac{2076}{4\times 5}\right] = [103.8] = 103.$$

$\therefore$ the set of integers divisible by neither 4 nor 5

is

$$A'\cap B' = (A\cup B)'$$

$|A'\cap B'| = |(A\cup B)'| =$ the total number of integer $- |A\cup B|$

$$= 2076 - 831$$

$$= 1245.$$

Prob. No ④. Find the number of positive integers in the range 1976 through 3776 that are not divisible by 17.

Sol:- First we shall find the number of integers that are divisible by 17.

The numbers of integers ≤ 1976 that are divisible by 17 is

$$= \left[\frac{1976}{17}\right] = [116.2] = 116.$$

The numbers of integers ≤ 3776 that are divisible by 17 is

$$= \left[\frac{3776}{17}\right] = [222.1] = 222.$$

$\therefore$ the number of integers from 1976 to 3776 that are divisible by 17 is $= 222 - 116 = 106$.

$\therefore$ the number of integers from 1976 to 3776 that are not divisible by 17 is

= total number of numbers $- 106$.

But the total number of integers from 1976 to 3776 is $= 3776 - 1976 + 1$

$= 1800 + 1$

$= 1801.$

$\therefore$ the number of numbers that are not divisible by 17 $= 1801 - 106 = 1695.$

Prob. No ⑤. Find the number of positive integers ≤ 3076 that are not divisible by 24.

Sol:- The number of integers ≤ 3076 that are divisible by 24 is $\left[\frac{3076}{24}\right] = [128.1] = 128$

the number of numbers not divisible by 24 is

= total number of numbers -128.

$= 3076 - 128$

$= 2498$

Base-b Representations

We are familiar with the use of decimal notation, base10, to express any integer or real number. We use it every day

For example: $352 = 3(10^2) + 5(10) + 2(10^0)$

This is called the decimal expansion of 352

and $35.23 = 3(10^1) + 5(10^0) + 2(10^{-1}) + 3(10^{-2})$

But computers usually use binary notation, base 2, when carrying out arithmetic operations. Very long binary numbers are often handled by using octal (base 8) or hexadecimal (base 16) notations similarly these bases are used for expressing characters such as letters or digits.

In fact, any integer ≥ 2 can be used as a valid base for representing integers.

We now state a fundamental result without proof.

Theorem: Let 'b' be an integer ≥ 2. If 'n' is a positive integer, then it can be uniquely expressed in the form $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$, where $a_0, a_1, \ldots a_k$ are non negative integers less than b and $a_k \neq 0$

Defn: (Base b)

If 'n' is a positive integer and $b \geq 2$ and

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \longrightarrow ①$$

where $a_0, a_1, a_2 \cdots a_k$ are non negative integers then the expression in ① is called the base b expansion of the integer n.

We the write $n = (a_k a_{k-1} \cdots a_1 a_0)_b$

for example, $(345)_{10} = 3(10^2)+4(10)+5(10^0)$

$$(345)_8 = 3(8^2)+4(8)+5 = 135.$$

Binary Expansions

When base is '2', then the expansion is called the binary expansion when $b=2$, each coefficient is '0' or '1'. The digits '0' and '1' are called binary digits or bits. So, the binary expansion of an integer is just a bit string. Binary expansion are used by computers to represent and do arithmetic with integers.

Note: ①. The number system with base 10 is called the decimal system because the latin word decem means 10.

The decimal system uses the 10 digits 0,1,2,3,...9.

②. If the base $b>10$, we use the letters A, B, C... to represents the digits 10, 11, 12,... respectively in decimal notation.

Hexadecimal Expansion

Another based used in computer science is 16. The base 16 expansion of an integer is called its hexadecimal expansion. Hexadecimal expansion uses the sixteen digits 0,1,2,3..9, A, B, C, D, E and F. where the letters A to F represents the digits 10 to 15 respectively (in decimal notation).

Problems

Prob. No ①. Express $(101011111)_2$ in base 10.

Sol:- $(101011111)_2 = 1(2^8)+0(2^7)+1(2^6)+0(2^5)+1(2^4)$
$+1(2^3)+1(2^2)+1(2)+1(2^0)$

$= 256+64+16+8+4+2+1$

$= 351.$

Prob. No ②. Express (i) $(3AB0E)_{16}$ in base 10

(ii) $(3ABC)_{16}$ in base 10.

Sol:- (i) we know that $A=10$, $B=11$, $E=14$

$(3AB0E)_{16} = 3(16^4)+A(16^3)+B(16^2)+0(16)+E(16^0)$

$= 3(16^4)+10(16^3)+11(16^2)+14.$

$= 196608+40960+2816+14$

$= 240398.$

(ii) we know that $A=10$, $B=11$, $C=12$.

$(3ABC)_{16} = 3(16^3)+A(16^2)+B(16)+C(16^0)$

$= 3(16^3)+10(16^2)+11(16)+12$

$= 12288+2560+176+12$

$= 15036$

Base conversion from Binary to octal.

To convert a binary system number to octal system, we group the binary digits into blocks of three bits from right to left and adding if necessary initial zero at the left most block and replace each group with the corresponding octal digit.

Problems

Prob. No ① convert the binary number into octal digit.

(i) $(11110011)_2$ (ii) $(111010)_{two}$ (iii) $(11100101)_2$

Sol:- (i) Given 11, 110, 011

we group the digits in blocks of three digits from right to left

Here the blocks are 011, 110, 011 (adding '0' to the left most block to get 3 digits).

$$\therefore 11,110,011 = 011, 110, 011$$

$$011 = 0(2^2)+1(2)+1 = 3$$
$$110 = 1(2^2)+1(2)+0 = 6$$
$$011 = 0(2^2)+1(2)+1 = 3.$$

$$\therefore (11110011)_2 = (363)_8$$

(ii) Given $(111010)_{two}$

we rewrite $111010 = 111, 010$

$$111 = 1(2^2)+1(2)+1 = 7$$
$$010 = 0(2^2)+1(2)+0 = 2$$

$$\therefore (111010)_2 = (72)_8$$

(iii) Given $(11100101)_2$

we rewrite $11100101 = 011, 100, 101$

$$011 = 0(2^2)+1(2)+1 = 3$$
$$100 = 1(2^2)+0(2)+0(2^0) = 4$$
$$101 = 1(2^2)+0(2)+1 = 5$$

$$\therefore (11100101)_2 = (345)_8$$

Base conversion from Binary to Hexadecimal

We group the binary digits into blocks of four bits from right to left, adding if necessary initial zero at the left most block to get a block of four bits. Replace each block by a hexadecimal number.

Problems

1. write the following as a hexadecimal digit.

(i) $(11\,1110\,1011\,1100)_2$ (ii) $(1110101)_2$ (iii) $(11110011)_2$

Sol:- (i) Given $(11\,1110\,1011\,1100)_2$

we rewrite $11\,1110\,1011\,1100 = 0011, 1110, 1011, 1100$

$$0011 = 0(2^3) + 0(2^2) + 1(2) + 1 = 3$$
$$1110 = 1(2^3) + 1(2^2) + 1(2) + 0 = 14 = E$$
$$1011 = 1(2^3) + 0(2^2) + 1(2) + 1 = 11 = B$$
$$1100 = 1(2^3) + 1(2^2) + 0(2) + 0 = 12 = C$$
$$\therefore (11\,1110\,1011\,1100)_2 = (3EBC)_{16}$$

(ii) Given $(1110101)_2$

we rewrite $1110101 = 0111, 0101$

$$0111 = 0(2^3) + 1(2^2) + 1(2) + 1 = 7$$
$$0101 = 0(2^3) + 1(2^2) + 0(2) + 1 = 5$$
$$\therefore (1110101)_2 = (75)_{16}$$

(iii) Given $(11110011)_2$

we rewrite $11110011 = 1111, 0011$

$$1111 = 1(2^3) + 1(2^2) + 1(2) + 1(2^0) = 15 = F$$
$$0011 = 0(2^3) + 0(2^2) + 1(2) + 1(2^0) = 3$$
$$\therefore (11110011)_2 = (F3)_{16}.$$

Prob.No ② . Rewrite the following as a binary digit.

(i) $(237)_{16}$ (ii) $(36)_{16}$ (iii) $(3AD)_{16}$ (iv) $(345)_8$ (V) $(237)_8$

Sol:- (i) Given $(237)_{16}$, so each digit we have to rewrite as blocks of four bits.

∴ we write $2 = 0(2^3) + 0(2^2) + 1(2) + 0(1) = 0010$

$3 = 0(2^3) + 0(2^2) + 1(2) + 1(1) = 0011$

$7 = 0(2^3) + 1(2^2) + 1(2) + 1(1) = 0111$

$\therefore (237)_{16} = (0010\ 0011\ 0111)_2$

$= (1000110111)_2$

(ii) Given $(36)_{16}$

we rewrite each digit as a block of four bits.

∴ we write $3 = 0(2^3) + 0(2^2) + 1(2) + 1(2^0) = 0011$

$6 = 0(2^3) + 1(2^2) + 1(2) + 0(2^0) = 0110$

$(36)_{16} = (00110110)_2$

$= (110110)_2$

(iii) Given $(3AD)_{16}$

we rewrite each digit as block of four digits.

∴ we write $3 = 0(2^3) + 0(2^2) + 1(2) + 1(2^0) = 0011$

$A = 10 = 1(2^3) + 0(2^2) + 1(2) + 0 = 1010$

$D = 13 = 1(2^3) + 1(2^2) + 0(2) + 1 = 1101$

$\therefore (3AD)_{16} = (001110101101)_2$

$= (111010\ 1101)_2$

(iv) Given $(345)_8$

we write each digits as block of three bits

∴ we write $3 = 0(2^2) + 1(2) + 1 = 011$

$4 = 1(2^2) + 0(2) + 0 = 100$

$5 = 1(2^2) + 0(2) + 1 = 101$

$$(345)_8 = (011100101)_2$$
$$= (11100101)_2$$

(V). Given $(237)_8$

we rewrite each digit as blocks of three bits.

we write $2 = 0(2^2)+1(2)+0 = 010$

$3 = 0(2^2)+1(2)+1 = 011$

$7 = 1(2^2)+1(2)+1 = 111$

$$(237)_8 = (010011111)_2$$
$$= (10011111)_2$$

Prob. No③. Arrange the binary numbers 1011, 110, 11011, 10110 and 101010 in increasing order of magnitude.

Sol:- Given 1011, 110, 11011, 10110, 101010.

we will convert these binary numbers into decimal numbers for comparison

∴ we write $1011 = 1(2^3)+0(2^2)+1(2)+1 = 11$

$110 = 1(2^2)+1(2)+0 = 6$

$11011 = 1(2^4)+1(2^3)+0(2^2)+1(2)+1 = 27$

$10110 = 1(2^4)+0(2^3)+1(2^2)+1(2)+0 = 22$

$101010 = 1(2^5)+0(2^4)+1(2^3)+0(2^2)$
$+1(2)+0 = 42.$

∴ the binary numbers in increasing order are

110, 1011, 10110, 11011, 101010.

Prob. No④. Find the number of ones in the binary representation of 2^4-1

Sol:- Given 2^4-1

Now we write $2^4-1 = 15 = 1(2^3)+1(2^2)+1(2)+1$

$= 1111$

So, the numbers of ones is 4.

Note: More generally, the number of ones is the binary form of $2^n - 1$ is n.

Prob. No ⑤ Find the value of the base b if $1001_b = 9$.

Sol:- Given $1001_b = 9$

Since the digits are binary, we expect $b = 2$

$$1001_b = 9$$
$$1(b^3) + 0(b^2) + 0(b) + 1 = 9$$
$$b^3 + 1 = 9 \Rightarrow b^3 = 8 = 2^3$$
$$\Rightarrow b = 2$$

Prob. No ⑥ If $144_b = 49$, find the base b.

Sol:- Given $(144)_b = 49$

$$1(b^2) + 4(b) + 4(b^0) = 49$$
$$b^2 + 4b - 45 = 0$$
$$(b+9)(b-5) = 0$$

Since base b is ≥ 2, $b + 9 \neq 0$

$$\Rightarrow b - 5 = 0 \Rightarrow b = 5$$

Base conversion algorithm - decimal to Base b

We shall now consider the converse problem of writing a decimal integer 'n' into base 'b' integer.

First divided 'n' by 'b' and obtain the quotient and remainder

ie $n = q_0(b) + r_0 \qquad 0 \leq r_0 < b$

Next we divided q_0 by b

$$q_0 = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

Next divided q_1 by P $\quad q_1 = q_2 b + r_2, \quad 0 \leq r_2 < b.$

Proceed in this way until we get zero quotient then the remainders in the reverse order gives the b representation of n.

Prob. No ① Express 1076 in the binary system

Sol:-

$1076 = 538(2) + 0$

$538 = 269(2) + 0$

$269 = 134(2) + 1$

$134 = 67(2) + 0$

$67 = 33(2) + 1$

$33 = 16(2) + 1$

$16 = 8(2) + 0$

$8 = 4(2) + 0$

$4 = 2(2) + 0$

$2 = 1(2) + 0$

$1 = 0(2) + 1$

```
     538          269          134
 2 ) 1076     2 ) 538      2 ) 269
     10           4            2
      7           13           6
      6           12           6
      16           18          9
      16           18          8
       0            0          1

     67           33           16
 2 ) 134      2 ) 67       2 ) 33
     12           6            2
      14          7            13
      14          6            12
       0          1             1
```

$\therefore 1076 = (10000110100)_2$

Prob. No ② Express the following in the octal system

(i) 12345 (ii) 1776 (iii) 3014.

Sol:- (i) $12345 = 1543(8) + 1$

$1543 = 192(8) + 7$

$192 = 24(8) + 0$

$24 = 3(8) + 0$

$3 = 0(8) + 3$

```
     1543            192
 8 ) 12345       8 ) 1543
     8               8
     43              74
     40              72
      34              23
      32              16
       25              7
       24
        1

     24              3
 8 ) 192         8 ) 24
     16              24
      32              0
      32
       0
```

$\therefore 12345 = (30071)_8$

(ii) $1776 = 222(8) + 0$

$222 = 27(8) + 6$

$27 = 3(8) + 3$

$3 = 0(8) + 3$

```
     222            27            3
 8 ) 1776       8 ) 222       8 ) 27
     16             16            24
      17             62            3
      16             56
       16             6
       16
        0
```

$\therefore 1776 = (3360)_8$

(iii) $3014 = 376(8) + 6$

$376 = 47(8) + 0$

$47 = 5(8) + 7$

$5 = 0(8) + 5$

$$\begin{array}{r} 376 \\ 8\,\overline{)\,3014} \\ \underline{24} \\ 61 \\ \underline{56} \\ 54 \\ \underline{48} \\ \underline{6} \end{array} \qquad \begin{array}{r} 47 \\ 8\,\overline{)\,376} \\ \underline{32} \\ 56 \\ \underline{56} \\ \underline{0} \end{array} \qquad \begin{array}{r} 5 \\ 8\,\overline{)\,47} \\ \underline{40} \\ \underline{7} \end{array}$$

$\therefore\ 3014 = (5706)_8$

Prob. No ③. Express the following in hexadecimal system

(i) 15036 (ii) 177130.

Sol:- (i) 15036

$15036 = 936(16) + 12 = C$

$936 = 58(16) + 11 = B$

$58 = 3(16) + 10 = A$

$3 = 0(16) + 3$

$$\begin{array}{r} 939 \\ 16\,\overline{)\,10536} \\ \underline{144} \\ 63 \\ \underline{48} \\ 156 \\ \underline{144} \\ \underline{12} \end{array} \qquad \begin{array}{r} 58 \\ 16\,\overline{)\,939} \\ \underline{80} \\ 139 \\ \underline{128} \\ \underline{11} \end{array} \qquad \begin{array}{r} 3 \\ 16\,\overline{)\,58} \\ \underline{48} \\ \underline{10} \end{array}$$

$\therefore\ 153036 = (3ABC)_{16}$

(ii) 177130

$177130 = 11070(16) + 10 = A$

$11070 = 691(16) + 14 = E$

$691 = 43(16) + 3$

$43 = 2(16) + 11 = B$

$2 = 0(16) + 2$

$$\begin{array}{r} 11070 \\ 16\,\overline{)\,177130} \\ \underline{16} \\ 17 \\ \underline{16} \\ 113 \\ \underline{112} \\ \underline{10} \end{array} \qquad \begin{array}{r} 691 \\ 16\,\overline{)\,11070} \\ \underline{96} \\ 147 \\ \underline{144} \\ 30 \\ \underline{16} \\ 14 \end{array}$$

$$\begin{array}{r} 43 \\ 16\,\overline{)\,691} \\ \underline{64} \\ 51 \\ \underline{48} \\ \underline{3} \end{array} \qquad \begin{array}{r} 2 \\ 16\,\overline{)\,43} \\ \underline{32} \\ \underline{11} \end{array}$$

$\therefore\ 177130 = (2B3EA)_{16}$

Number Patterns

Prob. No ① From the pattern

$$1.9+2=11$$
$$12.9+3=111$$
$$123.9+4=1111$$
$$1234.9+5=11111$$
$$\vdots$$

write down the n^{th} row and prove the validity of the number pattern.

Sol:- From the given pattern we find the n^{th} row is

$$1.2.3.4.5\ldots n.9+(n+1)=\underbrace{111\ldots1}_{(n+1)\text{ ones}}$$

$$LHS = 1.2.3.4.5\ldots n.9+(n+1)$$

$$=(n\times10^0+(n-1)\times10^1+\cdots+2\times10^{(n-2)}+1\times10^{(n-1)})(10-1)$$
$$+(n+1)$$

$$=(n.10+(n-1).10^2+\cdots+2\times10^{(n-1)}+1\times10^n)$$
$$-(n\times10^0+(n-1)10+\cdots+2\times10^{(n-2)}+1\times10^{(n-1)})$$
$$+n+1$$

$$=10^n+10^{n-1}+10^{n-2}+\cdots+10+1$$

$$=10000\ldots(n\text{ zeros})+10000\ldots((n-1)\text{ zeros})$$
$$+\cdots+10+1.$$

$$=111\ldots1_{(n+1)\text{ places}}$$

$$=R.H.S$$

Prob. No ②. Given the pattern

$$9.9+7=88$$
$$98.9+6=888$$
$$987.9+5=8888$$
$$\vdots$$

Find the formula for the n^{th} row and prove it.

Sol:- observing the pattern, we find the n^{th} row is

$$987\ldots(10-n).9 + (8-n) = \underset{(n+1)\text{ eight}}{88\ldots8}.$$

$$LHS = 987\ldots\ (10-n).9 + (8-n)$$

$$= 9\left(9.10^{n-1} + 8.10^{n-2} + \ldots + (11-n).10 + (10-n).1\right) + (8-n)$$

$$= (10-1)\left(9.10^{n-1} + 8.10^{n-2} + \ldots + (11-n).10 + (10-n).1\right) + (8-n)$$

$$= 9.10^{n} + 8.10^{n-1} + 7.10^{n-2} + \ldots + (11-n).10^{2} + (10-n).10$$
$$- \left(9.10^{n-1} + 8.10^{n-2} + \ldots + (11-n).10 + (10-n)\right) + (8-n)$$

$$= 9.10^{n} - (10^{n-1} + 10^{n-2} + \ldots + 10) - (10-n) + 8 - n$$

$$= (10-1).10^{n} - 10^{n-1} - 10^{n-2} \ldots -10 - 10 + n + 8 - n$$

$$= 10.10^{n} - 10^{n} - 10^{n-1} - 10^{n-2} \ldots -10 - 1 - 1$$

$$= 10^{n+1} - (10^{n} + 10^{n-1} + 10^{n-2} + \ldots + 10 + 1) - 1$$

$$= 10^{n+1} - \left(\frac{10^{n+1}-1}{10-1}\right) - 1 \qquad \left(\because \sum_{i=0}^{k} r^{i} = \frac{r^{k+1}-1}{r-1}\ (r \neq 1)\right)$$

$$= 10^{n+1} - \left(\frac{10^{n+1}-1}{9}\right) - 1$$

$$= \frac{9.10^{n+1} - 10^{n+1} + 1 - 9}{9} = \frac{8(10^{n+1}-1)}{9}$$

But

$$\underset{(n+1)\text{ nines}}{99\ldots99} = (10^{n+1}-1)$$

So

$$\underbrace{11\ldots11}_{(n+1)\text{ ones}} = \frac{(10^{n+1}-1)}{9}$$

$$\therefore \frac{8(10^{n+1}-1)}{9} = \underset{(n+1)\text{ eights}}{88\ldots88} = RHS$$

Prob. No(3) observing the pattern of numbers write down the formula for the n^{th} row and prove it.

$$1.8+1 = 9$$
$$12.8+2 = 98$$
$$123.8+3 = 987$$
$$1234.8+4 = 9876$$
$$\vdots$$

Sol:- From the given number pattern we find the n^{th} row is

$$123\cdots n\times 8+n = 987\cdots(10-n) \qquad 1\le n\le 9.$$

$$LHS = 123\cdots n.8+n$$
$$= 8(10^{n-1}+2.10^{n-2}+3.10^{n-3}+\cdots+(n-1)10+n.1)+n$$

Let $S = 10^{n-1}+2.10^{n-2}+3.10^{n-3}+\cdots+(n-1)10+n.1$

$$S = n.1+(n-1).10+\cdots+3.10^{n-3}+2.10^{n-2}+10^{n-1} \rightarrow (1)$$

It is an arithmetic geometric series with the common ratio of the G.P part is 10.

multiply (1) by 10.

$$10S = n.10+(n-1)10^2+\cdots+2.10^{n-1}+10^n \rightarrow (2).$$

$$(1)-(2).\quad -9S = n-(10+10^2+\cdots+10^{n-1}+10^n)$$
$$= n-10\left(\frac{10^n-1}{10-1}\right) \qquad \left(\because S_n = \frac{a(r^n-1)}{r-1}, r>1\right)$$
$$= n-\frac{10}{9}(10^n-1)$$
$$9S = \frac{10}{9}(10^n-1)-n$$
$$S = \frac{10}{81}(10^n-1)-\frac{n}{9}$$
$$LHS = 8\left(\frac{10}{81}(10^n-1)-\frac{n}{9}\right)+n$$
$$= \frac{80}{81}(10^n-1)-\frac{8n}{9}+n$$
$$= \frac{80}{81}(10^n-1)+\frac{n}{9}.$$

$RHS = 9876 \cdots (10-n)$ $\quad$ (no. of factors $= 9-(10-n)+1 = n$)

$= 9\cdot10^{n-1} + 8\cdot10^{n-2} + 7\cdot10^{n-3} + \cdots + (11-n)\cdot10 + (10-n)\cdot1$

Let $S = (10-n)1 + (11-n)\cdot10 + \cdots + 8\cdot10^{n-2} + 9\cdot10^{n-1} \rightarrow ①$

this is an arithmetic co-geometric. the common ratio of the G.P part is 10.

multiply by 10.

$10S = (10-n)10 + (11-n)10^2 + \cdots + 8\cdot10^{n-1} + 9\cdot10^n \rightarrow ②$

①-②

$$-9S = (10-n) + (10+10^2+\cdots+10^{n-1}) - 9\cdot10^n$$

$$= (10-n) + (10+10^2+\cdots+10^{n-1}) - (10-1)\cdot10^n.$$

$$= (10-n) + (10+10^2+\cdots+10^{n-1}) - 10^{n+1} + 10^n.$$

$$= (10-n) + (10+10^2+\cdots+10^{n-1}+10^n) - 10^{n+1}$$

$$= 10-n + 10\cdot\left(\frac{10^n-1}{10-1}\right) - 10^{n+1}$$

$$= 10-n + \frac{10}{9}(10^n-1) - 10^{n+1}$$

$$= \frac{1}{9}(90-9n+10^{n+1}-10-10^{n+1}\cdot9)$$

$$= 1/9\,(80 - 8\cdot10^{n+1} - 9n)$$

$$= 1/9\,(80 - 80\cdot10^n - 9n)$$

$$= \frac{80}{9}(1-10^n) - n.$$

$$S = -\frac{80}{81}(1-10^n) + n/9$$

$\therefore R.H.S = \frac{80}{81}(10^n-1) + n/9.$

$\therefore$ LHS = R.H.S

Prob. No 4 Using the number pattern

$$1^2-0^2=1$$
$$2^2-1^2=3$$
$$3^2-2^2=5$$
$$\vdots$$

Make a conjecture about row n and prove the conjecture.

Sol:- From the given number pattern, we find the n^{th} row is

$$n^2-(n-1)^2=(2n-1)$$

∴ the conjecture is

$$n^2-(n-1)^2=2n-1 \quad \forall\, n\geq 0$$

$$\begin{aligned} LHS &= n^2-(n-1)^2 \\ &= n^2-(n^2-2n+1) \\ &= 2n-1 \\ &= RHS \end{aligned}$$

Prob.No 5. Establish the validity of the number pattern.

$$1\cdot 1=1$$
$$11\cdot 11=121$$
$$111\cdot 111=12321$$
$$\vdots$$

Sol:- $$\underbrace{11111\cdots1}_{n\text{-ones}}\cdot\underbrace{1111\cdots1}_{n\text{-ones}}=(1\times10^{n-1}+1\times10^{n-2}+\cdots+1)^2$$

$$=(1\times10^{n-1}+1\times10^{n-2}+\cdots+1)\times(1\times10^{n-1}+1\times10^{n-2}+\cdots+1).$$

$$\begin{aligned}=1\times10^{2n-2}&+1\times10^{2n-3}+\cdots+1\times10^{n+1}+1\times10^{n}+1\times10^{n-1}\\ &+1\times10^{2n-3}+\cdots+1\times10^{n+1}+1\times10^{n}+1\times10^{n-1}+1\times10^{n-2}\\ &+\cdots+1\times10^{4}+1\times10^{3}+1\times10^{2}\\ &+1\times10^{3}+1\times10^{2}+1\times10^{1}\\ &+1\times10^{2}+1\times10^{1}+1.\end{aligned}$$

$$\overline{1\times10^{2n-2}+2\times10^{2n-3}+\cdots+4\times10^{3}+3\times10^{2}+2\times10^{1}+1\times10^{0}}$$

$$=1\,2\,3\,4\cdots n\,(n-1)\cdots\,4\,3\,2\,1$$

The Egyptian method of Multiplication

Problems

Prob. No ① Multiply 23.45 using Egyptian method.

Sol:- Given 23.45

First, express one of the factors say 23 as a sum of powers of 2.

$$23 = 1 + 2 + 4 + 16$$

then $23.45 = 1.45 + 2.45 + 4.45 + 16.45$.

Next construct a table consisting of two rows, one headed by 1 and the other by 45, each successive column is obtained by doubling the preceding column.

1	2	4	8	16
45*	90*	180*	360	720*

To find the desired result, add the starred numbers in the second row. These correspond to the terms in the binary expansion of 23.

$$23.45 = 45 + 90 + 180 + 720$$
$$= 1035.$$

Alternate method

2 | 23
2 | 11 − 1
2 | 5 − 1
2 | 2 − 1
1 − 0

$$(10111)_2 = 1(2^0) + 1(2^1) + 1(2^2) + 0(2^3) + 1 \times 16$$

	1	1	1	0	1
23	1	2	4	8	16
45	45*	90*	180*	360	720*

(* for the numbers corresponds to binary expansion)

$$\therefore 45 + 90 + 180 + 720 = 1035.$$

Prob. No ② Multiply 24·43 using Russian Peasant algorithm.

Sol:-

24	12	6	3	1
43	86	172	344*	688*

* - only for odd quotients

$\therefore 24 \cdot 43 = 344 + 688 = 1032$

Prob. No ③ Multiply 29.49 using Russian Peasant method.

Sol:- Given 29. 49

29	14	7	3	1
49*	98	196*	392*	784*

* - only for odd quotients

$784 + 392 + 196 + 49 = 1421.$

Prob. No ④ Divide 256 by 23 using Egyptian method.

Sol:-

$2 \,|\, 23$
$2 \,|\, 11 - 1$
$2 \,|\, 5 - 1$
$2 \,|\, 2 - 1$
$1 - 0$

$(10111)_{two} = 1(2^0) + 1(2^1) + 1(2^2) + 0(2^3) + 1(2^4)$

	1	1	1	0	1
23	1	2	4	8	16
23	23*	46*	92	184*	368

↑ exceeds 256

$256 = 184 + 72$
$= 184 + 46 + 26$
$= (184 + 46 + 23) + 3$

So Remainder is 3.

$\therefore$ quotient $= 1 + 2 + 8 = 11$

Prime and Composite Numbers

Defn:- A Positive integer $p>1$ is called a prime if its only positive factors are 1 and P.

If $p>1$ is not a prime, then it is called a composite number

It is obvious, the integer 'n' is composite if and only if there exists an integer 'a' such that a/n and $1<a<n$.

For example: 5 is prime because its only positive factors are 1 and 5.

But 6 is a composite number because its has 2 and 3 as factors

Note ① By definition the integer 1 is neither a prime nor a composite number. 1 is just the multiplicative identity or unit.

theorem ①. Every integer $n \geq 2$ has a prime factor.

Proof:- We prove the theorem by strong principle of induction on n.

If $n=2$, then the statement is true. Since 2 is a prime and 2 is a factor of 2

Assume the statement is true for all integers upto $k, k>2$

To prove it is true for $k+1$

If $k+1$ is a prime, then $k+1$ is a prime factor of $k+1$.

If $k+1$ is not a prime, then $k+1$ must be a composite number.

So, it must have a factor d, where $d \leq k$. Then by the induction hypothesis, d has a prime factor P.

Since P/d and $d/k+1$, we have $P/k+1$. So P is a factor of $k+1$.

Hence by Second principle of induction the statement is true for every integer >1

ie every integer ≥ 2 has a prime factor.

Theorem ②: (Euclid) There are infinitely many primes

Proof:- We prove by contradiction method

Assume that there are only n primes $P_1P_2\cdots P_n$ where n is finite

Now consider the integer $m = P_1P_2P_3\cdots P_{n+1}$. Since $m>1$

By theorem ① 'm' has a prime factor P.

But none of the primes $P_1, P_2, \cdots P_n$ divide m

For, if $P|m$ and since $P_i | P_1P_2\cdots P_i \cdots P_n$

we get $P|m-P_1P_2\cdots P_n \Rightarrow P_i|1$ which is not true and

hence a contradiction $P_i|m$.

So, we have a prime P which is not in the list of n primes

Thus we have n+1 primes $P_1P_2\cdots P_n, P$ which contradicts the assumption there are only 'n' primes.

So, our assumption of finiteness is wrong

Hence the number of primes is infinite.

Theorem ③: Every composite number 'n' has a prime factor $\leq [\sqrt{n}]$

Proof:- Given 'n' is a composite number then there exist positive integers 'a' and 'b' such that

$n = ab$, where $1<a<n$, $1<b<n$.

We will now prove $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Suppose $a > \sqrt{n}$ and $b > \sqrt{n}$

then $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n \Rightarrow n > n$, which is impossible

either $a \leq \sqrt{n}$ or $b \leq \sqrt{n} \Rightarrow a \leq [\sqrt{n}]$ or $b \leq [\sqrt{n}]$

($\because$ a, b are integers)

We know that every positive integer ≥ 2 has a prime factor

Any such factor of 'a' or 'b' is also a factor $a \times b = n$.

So, n must have a factor $\leq [\sqrt{n}]$

Note (1) From this theorem it follows that if n has no prime factor $\leq [\sqrt{n}]$, then n is a prime

Problems

Prob. No (1) Determine whether the following is a prime

(i) 101 (ii) 1601 (iii) 1001

Sol:- (i) Given 101

First we find all primes $\leq [\sqrt{101}] = 10$.

the primes are 2, 3, 5, 7. Since none of these is a factor of 101 $\therefore$ 101 is a prime

(ii) Given 1601

First we find all primes $\leq [\sqrt{1601}] = 40$.

the primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 and 37.

we can verify that none of them is a factor of 1601. $\therefore$ 1601 is a prime

(iii) Given 1001

First we find all primes $\leq [\sqrt{1001}] = 31$.

the primes are 2, 3, 5, 7, 11, 13, 19, 23, 29, 31.

we find $7 / 1001$

Hence 1001 is not a prime.

Prob. No (2) Find the smallest prime factor of 119

Sol:- Given 119

we have to find the smallest prime factor of 119.

First we find all primes $\leq [\sqrt{119}] = 10$.

the primes are 2, 3, 5, 7

we find that $7 / 119$

So, the smallest prime dividing 119 is 7.

Defn:- Let x be a positive real number. Then $\pi(x)$ denote the number of primes $\leq x$

for example $\pi(10) = 4$ (∵ 2, 3, 5, 7 are the primes ≤ 10)

$\pi(18.75) = 7$ (∵ 2, 3, 5, 7, 11, 13, 17 are the primes ≤ 18.75).

If n is a positive integer, then by using inclusion-exclusion principle we state a formula for $\pi(n)$, the number of primes $\leq n$.

Theorem (4): Let $p_1 p_2 \ldots p_r$ be the primes $\leq [\sqrt{n}]$. Then the number of primes $\leq n$ is $\pi(n)$ and

$$\pi(n) = n-1+\pi(\sqrt{n}) - \sum_{i}\left[\frac{n}{p_i}\right] + \sum_{i<j}\left[\frac{n}{p_i p_j}\right] - \sum_{i<j<k}\left[\frac{n}{p_i p_j p_k}\right]$$
$$+ \cdots + (-1)^r\left[\frac{n}{p_1 p_2 \cdots p_r}\right]$$

Prob. No (1) Find the number of primes ≤ 47

Sol:- We have to find the number of primes ≤ 47.

Here $n = 47$, then $\sqrt{n} = \sqrt{47} = 6.8$

The primes $\leq (\sqrt{47})$ are 2, 3, 5

$\pi(\sqrt{47}) = 3$.

We know $\pi(n) = n-1+\pi(\sqrt{n}) - \sum\left[\frac{n}{p_i}\right] + \sum\left[\frac{n}{p_i p_j}\right] - \sum\left[\frac{n}{p_i p_j p_k}\right]$

$$\pi(47) = 47-1+\pi(\sqrt{47}) - \left(\left[\frac{47}{2}\right]+\left[\frac{47}{3}\right]+\left[\frac{47}{5}\right]\right)$$
$$+\left(\left[\frac{47}{2\cdot 3}\right]+\left[\frac{47}{2\cdot 5}\right]+\left[\frac{47}{3\cdot 5}\right]\right) - \left[\frac{47}{2\cdot 3\cdot 5}\right]$$

$= 46+3 - (23+15+9) + (7+4+3) - 1$

$= 49 - 47 + 14 - 1$

$= 15.$

Prob.No ② Using the formula for $\pi(n)$ find the number of primes ≤ 100

Sol:- Here $n=100$, $\sqrt{n} = \sqrt{100} = 10$

the primes ≤ 10 are $2, 3, 5, 7$

$\therefore \pi(\sqrt{100}) = 4.$

we know $\pi(n) = n-1+\pi(\sqrt{n}) - \sum\left[\frac{n}{p_i}\right] + \sum\left[\frac{n}{p_i p_j}\right] - \sum\left[\frac{n}{p_i p_j p_k}\right] + \cdots$

$$\pi(100) = 100-1+4 - \left(\left[\frac{100}{2}\right] + \left[\frac{100}{3}\right] + \left[\frac{100}{5}\right] + \left[\frac{100}{7}\right]\right) + \left(\left[\frac{100}{2\cdot3}\right] + \left[\frac{100}{2\cdot5}\right] + \left[\frac{100}{2\cdot7}\right] + \left[\frac{100}{3\cdot5}\right] + \left[\frac{100}{3\cdot7}\right] + \left[\frac{100}{5\cdot7}\right]\right) - \left(\left[\frac{100}{2\cdot3\cdot5}\right] + \left[\frac{100}{2\cdot5\cdot7}\right] + \left[\frac{100}{2\cdot3\cdot7}\right] + \left[\frac{100}{3\cdot5\cdot7}\right]\right) - \left[\frac{100}{2\cdot3\cdot5\cdot7}\right]$$

$$= 103 - (50+33+20+14) + (16+10+7+6+4+2) - (3+1+2+0)$$
$$-0$$
$$= 25.$$

$\therefore$ the number primes ≤ 100 is 25.

Note ① though the formula for $\pi(n)$ gives the exact value of the number of primes, when 'n' is large it is practically impossible to find the value of $\pi(n)$.

② the Prime number theorem is one of the important results in number theory, which gives an approximate value of $\pi(n)$, when 'n' is large.

theorem:⑤: Prime number theorem

If $x>0$, then $\lim\limits_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = 1$. this means as x becomes very large $\pi(x)$ approaches $\left(\frac{x}{\ln x}\right)$.

Theorem (6): For every positive integer n, there are n consecutive integers that are composite numbers.

Proof:- Let n be a positive integer and $n \geq 1$

To prove the existence, we have to construct suitably consider the 'n' consecutive integers

$$(n+1)! + 2\ (n+1)! + (n+1)!, 3 + \dots (n+1)! + (n+1)$$

where $n \geq 1$

Suppose k is an integer such that $2 \leq k \leq n+1$, then k is a factor of $(n+1)!$ ($\because (n+1)! = 1, 2, 3, 4, \dots k \dots (n+1)$).

Now $k/(n+1)!$ and $k/k \Rightarrow k/(n+1)!+k$ for every k.

$\therefore$ $(n+1)!+k$ is a consecutive composite numbers are

$$(n+1)!+2, (n+1)!+3, (n+1)!+ \dots (n+1)!+(n+1)$$

Problems

Prob. No (1) Find Five consecutive composite numbers

Sol:- Here $n=5$

We know that 5 consecutive composite integers are

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, (n+1)!+5, (n+1)!+6$$

put $n=5$

$$(n+1)!+2 = 6!+2 = 720+2 = 722$$
$$(n+1)!+3 = 6!+3 = 720+3 = 723$$
$$(n+1)!+4 = 6!+4 = 720+4 = 724$$
$$(n+1)!+5 = 6!+5 = 720+5 = 725$$
$$(n+1)!+6 = 6!+6 = 720+6 = 726$$

$\therefore$ The five consecutive composite numbers are 722, 723, 724, 725, 726.

Prob. No ②. obtain six consecutive integers that are composite numbers.

Sol:- Here $n=6$

Then the six consecutive composite numbers are

$(n+1)!+2,\ (n+1)!+3,\ (n+1)!+4,\ (n+1)!+5,\ (n+1)!+6,\ (n+1)!+7.$

Put $n=6$

$$(n+1)!+2 = 7!+2 = 5040+2 = 5042$$
$$(n+1)!+3 = 7!+3 = 5040+3 = 5043$$
$$(n+1)!+4 = 7!+4 = 5040+4 = 5044$$
$$(n+1)!+5 = 7!+5 = 5040+5 = 5045$$
$$(n+1)!+6 = 7!+6 = 5040+6 = 5046$$
$$(n+1)!+7 = 7!+7 = 5040+7 = 5047.$$

∴ The six consecutive composite numbers are 5042, 5043, 5044, 5045, 5046, 5047.

Prob. No ③. Find five consecutive integers <100 that are composite numbers

Sol:- Since $5! = 120 > 100$

We consider $4!,\ 4!+1,\ 4!+2,\ 4!+3,\ 4!+4.$

$\Rightarrow$ 24, 25, 26, 27, 28 are five consecutive composite numbers <100.

Greatest common divisor

The greatest common divisor (gcd) of two integers 'a' and 'b', not both zero, is the largest positive integer that divides both 'a' and 'b' it is denoted by (a,b)

For example: $(12,18)=6$ $(12,25)=1$, $(11,19)=1$ $(-15,25)=5$ and $(3,0)=3$

Note ① Since $(a,-b)=(-a,b)=(-a,-b)=(a,b)$ we confine one discussion of gcd to positive integers

Defn:- A positive integer d is the gcd of integers 'a' and 'b' if (i) d/a and d/b and (ii) If c/a and c/b, then c/d, where c is a positive integer.

Theorem: The gcd of two positive integers 'a' and 'b' is a linear combination of 'a' and b
ie if $d=(a,b)$, then $d=la+mb$ for some integers 'l' and 'm'.

Proof:- Let $S=\{xa+yb \,/\, xa+yb>0,\ x,y\in Z\}$

If $a>0$ then $a=1a+0b\in S$

So, S is non-empty set of positive integers

Hence by well ordering principle S has a least positive integer d

$\therefore$ $d=la+mb$ for some integers 'l' and 'm'.

We shall now prove $d=\gcd(a,b)$

Since $d>0$, by division algorithm to 'a' and 'd' we can find integers 'q' and 'r' such that

$$a=qd+r,\quad 0\le r<d$$

$$r=a-qd$$

$$=a-q(la+mb)$$

$= (1-ql)a + (-qm)b$

This shows that r is a linear combination of 'a' and 'b'.

If $r \neq 0$, then $r > 0$ and so $r \in S$. Further $r < d$

Hence we get a contradiction to the fact d is the least element of S

$\therefore r = 0$. so, $a = qd \Rightarrow d/a$.

III'ly we can prove d/b

Thus d is a common divisor of 'a' and 'b'

If c/a and c/b then $c/la+mb \Rightarrow c/d$

Hence d is gcd of 'a' and $b \Rightarrow d = (a,b)$.

Defn:- (Relatively prime)

Two positive integers 'a' and 'b' are relatively prime if their gcd is 1 ie $(a,b) = 1$

For example the gcd $(6,25) = 1$ and so 6 and 25 are relatively prime.

corollary ①. Two positive integers 'a' and 'b' are relatively prime if and only if there exist integers α and β such that $\alpha a + \beta b = 1$.

Proof:- If a and b are relatively prime, then $(a,b) = 1$ then by previous theorem, there exist integers α and β such that $\alpha a + \beta b = 1$.

conversely, let $\alpha a + \beta b = 1$

To prove $(a,b) = 1$

If $d = (a,b)$, then d/a and d/b

$\Rightarrow d/\alpha a + \beta b \Rightarrow d/1$

$\Rightarrow d = 1$

$\therefore$ $(a,b)=1 \Rightarrow$ 'a' and 'b' are relatively prime.

Corollary ②: If a/c and b/c and $(a,b)=1$, then prove that ab/c

Proof:- Given a/c and b/c

$\therefore$ $c = ma$ and $c = nb$ for some integers m,n

Also given $(a,b)=1 \Rightarrow \alpha a+\beta b=1$

$$\Rightarrow \alpha ac+\beta bc=c$$

$$\Rightarrow \alpha a(nb)+\beta b(ma)=c$$

$$\Rightarrow (\alpha n+\beta m)ab=c$$

$$\Rightarrow ab/c.$$

Corollary ③: If 'a' and 'b' are relatively prime and if a/bc then a/c

Proof:- Given $(a,b)=1 \Rightarrow \alpha a+\beta b=1$ for some integers α,β

Since $a/\alpha ac$ and a/bc, we get $a/\alpha ac+\beta bc$

$$\Rightarrow a/(\alpha a+\beta b)c$$

$$\Rightarrow a/c.$$

Theorem: (Euclid's lemma)

If p is a prime and p/ab then p/a or p/b.

Proof:- Given p is a prime and p/ab

If p/a there is nothing to prove

If $p\nmid a$, then we have to prove p/b

Since p is a prime and $p\nmid a$ then $(p,a)=1$

$\alpha p+\beta a=1$ for some integers α and β

Multiply by b, then $\alpha pb+\beta ab=b$

Since p/ab and p/pb

we have $p/\alpha pb+\beta ab \Rightarrow p/b$

Corollary : If p is a prime and $p/a_1a_2\dots a_n$ where $a_1a_2\dots a_n$ are positive integers, then p/a_i for some i, $1\le i\le n$.

Proof:- We prove by first principle of induction

Let $p(n)$ denote the statement $p/a_1a_2\dots a_n \Rightarrow p/a_i$ for some a_i

If $n=1$, $p(1)$ is p/a_1 which is true

Assume $p(k)$ is true an arbitrary $k>1$

ie $p/a_1a_2\dots a_k \Rightarrow p/a_i$ for some i, $1\le i\le k$.

To prove $p(k+1)$ is true

ie to prove $p/a_1a_2\dots a_k\, a_{k+1} \Rightarrow p/a_i$ for some a_i

Consider $p/(a_1a_2\dots a_k)a_{k+1}$

then $p/(a_1a_2\dots a_k)$ (or) p/a_{k+1} by Euclid lemma

If $p/a_1a_2\dots a_k$ then by induction hypothesis

p/a_i for some a_i, $1\le i\le k$

Thus p/a_i, $1\le i\le k$ or p/a_{k+1}

Hence p/a_i $1\le i\le k+1 \Rightarrow p(k+1)$ is true

Thus $p(k)$ is true $\Rightarrow p(k+1)$ is true

Hence by first principle of induction $p(n)$ is true for all $n\ge 1$.

Theorem: (Fundamental theorem of Arithmetic)

Every integer $n(\ge 2)$ is either a prime or can be written as a product of primes in only one way, except for the order of the factors.

Proof:- We prove by second principle of induction on n

Let $p(n)$ denote the proposition n is a prime or can be expressed as a product of primes

To prove $p(n)$ is true for all $n \geq 2$.

Basic step: Here $n_0 = 2$

$\therefore$ $p(2)$ is 2, which is a prime

thus $p(2)$ is true.

Inductive step: Assume that the proposition is true for all integers upto k, $k > 2$

ie $p(3), p(4) \ldots p(4)$ are true.

To prove $p(k+1)$ is true

ie To prove $k+1$ is either a prime or is a product of primes

If $k+1$ is a prime, then $p(k+1)$ is true

If $k+1$ is not a prime, then it is a composite number

$k+1 = xy$ where $1 < x < k+1$, $1 < y < k+1$

ie the integers x, y are $\leq k$

so, by our induction hypothesis x and y are primes or product of primes

$\therefore$ $k+1 = xy$ is a product of two or more primes

$\therefore$ $p(k+1)$ is true.

Hence by Second Principle or Strong principle of induction $p(n)$ is true for all $n \geq 2$

thus every integer $n (\geq 2)$ is either a prime or product of primes.

Next we prove uniqueness of the product

Let $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ be two factorisation of n into product of primes

we shall prove $r=s$ and every p_i is some q_j

$$1 \leq i \leq r, \quad 1 \leq j \leq r$$

we have $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$

Suppose $r < s$

Since $p_1 / p_1 p_2 \cdots p_r$ we have $p_1 / q_1 q_2 \cdots q_s$ and p_1 is a prime

$\therefore$ p_1 must divide some q_j $\Rightarrow$ $p_1 = q_j$ as they are primes

Divide both sides by p_1 we get

$$p_2 p_3 \cdots p_r = q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_s$$

Repeat this argument with $p_2, p_3, \cdots p_r$

Since $r < s$ finally we get $1 =$ a product of q's

ie $1 =$ a product of primes which is a contradictions

$\therefore$ our assumption $r < s$ is wrong $\Rightarrow$ $r \geq s$

|||ly if $s < r$ (arguing with q's instead of p's)

we get a contradiction

$s \geq r$ and hence $r = s$

Hence the primes $p_1 p_2 \cdots p_r$ are the same as $q_1 q_2 \cdots q_r$ in some order

Thus the factorization is unique, except for the order.

Defn:- (Canonical decomposition)

The canonical decomposition of a positive integer 'n' is of the form $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1 p_2 \cdots p_k$ are distinct primes with $p_1 < p_2 < \cdots < p_k$ and $\alpha_1 \alpha_2 \cdots \alpha_k$ are positive integers

Problems

Prob. No ① Find the canonical decompositions of (i) 999 (ii) 1024 (iii) 2520

Sol:- (i) $999 = 3.3.3.37 = 3^3.37$

(ii) $1024 = 2^5.32 = 2^5.2^5 = 2^{10}$

(iii) $2520 = 2^3.3^3.7$

$$\begin{array}{r|l} 3 & 999 \\ \hline 3 & 333 \\ \hline 3 & 111 \\ \hline & 37 \end{array} \qquad \begin{array}{r|l} 2 & 1024 \\ \hline 2 & 512 \\ \hline 2 & 256 \\ \hline 2 & 128 \\ \hline 2 & 64 \\ \hline & 32 \end{array}$$

These are canonical decompositions

$$\begin{array}{r|l} 2 & 2520 \\ \hline 2 & 1260 \\ \hline 2 & 630 \\ \hline 3 & 315 \\ \hline 3 & 63 \\ \hline 3 & 21 \\ \hline & 7 \end{array}$$

Prob. No ②. Find the gcd of the following using canonical decompositions (i) (414, 662) (ii) (175, 192) (iii) (168, 180) (iv) (120, 500)

Sol:-
(i) To find gcd of 414, 662

$414 = 2.3^2.23$

$662 = 2.231$

$\therefore$ gcd(414, 662) = 2

$$\begin{array}{r|l} 2 & 414 \\ \hline 3 & 207 \\ \hline 3 & 69 \\ \hline & 23 \end{array} \qquad \begin{array}{r|l} 2 & 662 \\ \hline & 331 \end{array}$$

(ii) To find $(175, 192)$

First we find the canonical decompositions

$$\begin{array}{r|l} 5 & 175 \\ \hline 5 & 35 \\ \hline & 7 \end{array} \qquad \begin{array}{r|l} 2 & 192 \\ \hline 2 & 96 \\ \hline 2 & 48 \\ \hline 2 & 24 \\ \hline 2 & 12 \\ \hline 2 & 6 \\ \hline & 3 \end{array}$$

$175 = 5^2 . 7$

$192 = 2^6 . 3$

we notice that there is no common factor except 1

$\therefore (175, 192) = 1$

(iii) To find gcd of 168, 180

First we find the canonical decompositions

$$\begin{array}{r|l} 2 & 168 \\ \hline 2 & 84 \\ \hline 2 & 42 \\ \hline 3 & 21 \\ \hline & 7 \end{array} \qquad \begin{array}{r|l} 2 & 180 \\ \hline 2 & 90 \\ \hline 3 & 45 \\ \hline 3 & 15 \\ \hline & 5 \end{array}$$

$168 = 2^3 . 3 . 7$

$180 = 2^2 . 3^2 . 5$

$\therefore \gcd(168, 180) = 2^2 . 3 = 12$

(iv). To find gcd of 120 and 500

First we find the canonical decompositions

$$\begin{array}{r|l} 2 & 120 \\ \hline 2 & 60 \\ \hline 2 & 30 \\ \hline 3 & 15 \\ \hline & 5 \end{array} \qquad \begin{array}{r|l} 2 & 500 \\ \hline 2 & 250 \\ \hline 5 & 125 \\ \hline 5 & 25 \\ \hline & 5 \end{array}$$

$120 = 3 . 5 . 2^3$

$500 = 2^2 . 5^3$

$\gcd(120, 500) = 2^2 . 5 = 20$

Prob. No ③. Use recursion to evaluate (i) $(12, 36, 60, 108)$ (iv) $(15, 24, 28, 45)$. (ii) $(18, 30, 60, 75, 132)$ (iii) $(12, 18, 28, 38, 44)$

Sol:- (i) To evaluate $(12, 36, 60, 108)$ we isolate each terms from the right and find gcd of the inner groups as below

$$(12, 36, 60, 108) = ((12, 36, 60), 108)$$
$$= (((12, 36)\ 60), 108)$$

Now $(12, 36) = 12$ $(\because 12$ is a factor of $36)$

$((12, 36), 60) = (12, 60) = 12$ $(\because 12$ is a factor of $60)$

$(((12, 36), 60), 108) = (12, 108) = 12$ $(\because 12$ is a factor of $108)$

$\therefore (12, 36, 60, 108) = 12.$

(ii) To evaluate $(18, 30, 60, 75, 132)$ we isolate each term from the right and then find the gcd of inner groups

$$(18,30,60,75,132) = ((18,30,60,75),132)$$
$$= (((18,30,60),75),132)$$
$$= ((((18,30),60),75),132)$$

$$\begin{array}{r|l} 2 & 18, 30 \\ \hline 3 & 9, 15 \\ \hline & 3, 5 \end{array}$$

No common factor

Now $(18,30) = 2\cdot 3 = 6$

$((18,30),60) = (6,30) = 6$

$(((18,30),60),75) = (6,75) = 3$

$$\begin{array}{r|l} 2 & 6, 75 \\ \hline & 2, 25 \end{array}$$

No common factor

$\therefore (18,30,60,75,132) = (3,132)$

$= 3$ $\quad$ $(\because 3$ is a factor of $132)$

(iii) To evaluate $(12, 18, 28, 38, 44)$ we isolate each term from the right and then find the gcd of inner groups as below

$$(12,18,28,38,44) = ((12,18,28,38),44)$$
$$= (((12,18,28),38),44)$$
$$= ((((12,18),28),38),44)$$

$$\begin{array}{r|l} 2 & 12, 18 \\ \hline 3 & 6, 9 \\ \hline & 2, 3 \end{array}$$

$$\begin{array}{r|l} 2 & 6, 28 \\ \hline & 3, 14 \end{array}$$

Now $(12,18) = 2\cdot 3 = 6$

$((12,18),28) = (6,28) = 2$

$(((12,18),28),38) = (2,38) = 2$

$(12,18,28,38,44) = (2,44) = 2$

(iv) To evaluate $(15, 24, 28, 45)$ we isolate each term from the right and then find the gcd of inner groups as below

$$\begin{array}{r|l} 3 & 15, 24 \\ \hline & 5, 8 \end{array}$$

$$(15,24,28,45) = ((15,24,28),45)$$
$$= (((15,24),28),45)$$

$$= (15, 24) = 3$$

$$((15,24), 28) = (3, 28) = 1$$

$$(((15, 24), 28), 45) = (1, 45) = 1$$

$$\therefore (15, 24, 28, 48) = 1.$$

Prob. No (4) Find the gcd of $a = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2$ and $b = 2^{11} \cdot 3^9 \cdot 5^3 \cdot 11$.

Sol:- Given $a = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2$

and $b = 2^{11} \cdot 3^9 \cdot 5^3 \cdot 11$

$$(a, b) = 2^2 \cdot 3^3 \cdot 5^2 \cdot 11 = 29,700$$

Prob. No (5). Find the gcd of 92928 and 123552.

Sol:- We have to find the gcd of 92928 and 123552

$$\begin{array}{r|l}
2 & 92928, \ 123552 \\ \hline
2 & 46464, \ 61776 \\ \hline
2 & 23232, \ 30888 \\ \hline
2 & 11616, \ 15444 \\ \hline
2 & 5808, \ 7722 \\ \hline
3 & 2904, \ 3861 \\ \hline
11 & 986 \quad 1287 \\ \hline
 & 88 \quad 117
\end{array}$$

$117 \rightarrow$ No factor

$$\therefore \text{g.c.d}(92928, 123552) = 2^5 \cdot 3 \cdot 11 = 1056.$$

The gcd and the Euclidean algorithm

Theorem: Let 'a' and 'b' be two positive integers such that $a = qb + r$, $0 \le r < b$ then $\gcd(a, b) = \gcd(b, r)$

Proof:- Given 'a' and 'b' are positive integers such that

$$a = qb + r, \ 0 \le r < b \rightarrow (1)$$

$$a - qb = r$$

Let $d = \gcd(a,b)$ and $d' = \gcd(b,r)$

To prove $d = d'$

Since $d = \gcd(a,b)$, d/a and $d/b \Rightarrow d/a - qb \Rightarrow d/r$

Thus d/b and d/r and so $d/\gcd(b,r) \Rightarrow d/d'$

Since $d' = \gcd(b,r)$, d'/b and d'/r

① $\Rightarrow$ d'/a

Thus d'/a and d'/b and so $d'/\gcd(a,b) \Rightarrow d'/d$

Hence $d = d' \Rightarrow \gcd(a,b) = \gcd(b,r)$.

The Euclidean Algorithm

Suppose 'a' and 'b' are positive integers with $a \geq b$.

If $a = b$, then $(a,b) = a$

So assume $a > b$

Then by successive application of division algorithm.

we get

$$\begin{aligned} a &= q_1 b + r_1 & 0 &\leq r_1 < b \\ b &= q_2 r_1 + r_2 & 0 &\leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 &\leq r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n & 0 &\leq r_n < r_{n-1} \end{aligned}$$

and $$r_{n-1} = q_{n+1} r_n + 0$$

where $b > r_1 > r_2 > \cdots \geq 0$. The sequence of remainders terminate with remainder 0.

$\therefore \gcd(a,b) = \gcd(b,r) = \gcd(r_1, r_2) \ldots = \gcd(r_{n-1}, r_n) = r_n$

Thus $(a,b) = r_n$ where r_n is the last non-zero remainder in the sequence of divisions

Problems

Prob. No ① Find the gcd of the following using Euclidean algorithm (i) (414, 662) (ii) (2076, 1776) (iii) (3076, 1976)

Sol:- (i) Here 662 > 414

Applying division algorithm successively we get

$662 = 1(414) + 248$

$414 = 1(248) + 166$

$248 = 1(166) + 82$

$166 = 2(82) + 2$

$82 = 41(2) + 0$

$$\begin{array}{r|l} & 1 \\ 414 & 662 \\ & 414 \\ \hline & 248 \end{array} \quad \begin{array}{r|l} & 1 \\ 248 & 414 \\ & 248 \\ \hline & 166 \end{array} \quad \begin{array}{r|l} & 1 \\ 166 & 248 \\ & 166 \\ \hline & 82 \end{array} \quad \begin{array}{r|l} & 2 \\ 82 & 166 \\ & 164 \\ \hline & 2 \end{array}$$

$$\begin{array}{r|l} & 41 \\ 2 & 82 \\ & 8 \\ \hline & 2 \\ & 2 \\ \hline & 0 \end{array}$$

The last non zero remainder is 2

$\therefore$ gcd (662, 414) = 2

(ii) Here 2076 > 1776

Applying division algorithm successively we get

$2076 = 1(1776) + 300$

$1776 = 5(300) + 276$

$300 = 1(276) + 24$

$276 = 11(24) + 12$

$24 = 2(12) + 0$

$$\begin{array}{r|l} & 1 \\ 1776 & 2076 \\ & 1776 \\ \hline & 300 \end{array} \quad \begin{array}{r|l} & 1 \\ 300 & 1776 \\ & 1500 \\ \hline & 276 \end{array} \quad \begin{array}{r|l} & 11 \\ 24 & 276 \\ & 24 \\ \hline & 36 \\ & 24 \\ \hline & 12 \end{array}$$

$$\begin{array}{r|l} & 1 \\ 276 & 300 \\ & 276 \\ \hline & 24 \end{array}$$

The last non zero remainder is 12

$\therefore$ gcd (2076, 1776) = 12

(iii) Here 3076 > 1976

Applying the division algorithm successively we get

$3076 = 1(1976) + 1100$

$1976 = 1(1100) + 876$

$1100 = 1(876) + 224$

$876 = 3(224) + 204$

$224 = 1(204) + 20$

$204 = 10(20) + 4$

$20 = 5(4) + 0$

$$\begin{array}{r} 1 \\ 1976\overline{)3076} \\ 1976 \\ \hline 1100 \\ \hline \end{array} \qquad \begin{array}{r} 1 \\ 1100\overline{)1976} \\ 1100 \\ \hline 876 \\ \hline \end{array} \qquad \begin{array}{r} 1 \\ 876\overline{)1100} \\ 876 \\ \hline 224 \\ \hline \end{array}$$

$$\begin{array}{r} 3 \\ 224\overline{)876} \\ 672 \\ \hline 204 \\ \hline \end{array} \qquad \begin{array}{r} 1 \\ 204\overline{)224} \\ 204 \\ \hline 20 \\ \hline \end{array} \qquad \begin{array}{r} 10 \\ 20\overline{)204} \\ 200 \\ \hline 4 \\ \hline \end{array}$$

the last non-zero remainder is 4

$\therefore \gcd(3076, 1976) = 4$

Prob. No ②. Apply Euclidean algorithm to express the following gcd as a linear combination of them

(i) $(1976, 1776)$ (ii) $(4076, 1024)$.

Sol:- (i) Here $1976 > 1776$

Applying division algorithm successively, we get

$1976 = 1(1776) + 200$

$1776 = 8(200) + 176$

$200 = 1(176) + 24$

$176 = 7(24) + 8$

$24 = 3(8) + 0$

$$\begin{array}{r} 1 \\ 1776\overline{)1976} \\ 1776 \\ \hline 200 \\ \hline \end{array} \qquad \begin{array}{r} 8 \\ 200\overline{)1776} \\ 1600 \\ \hline 176 \\ \hline \end{array} \qquad \begin{array}{r} 1 \\ 176\overline{)200} \\ 176 \\ \hline 24 \end{array}$$

$$\begin{array}{r} 3 \\ 8\overline{)24} \\ 24 \\ \hline 0 \\ \hline \end{array}$$

the last non-zero remainder is 8

$\therefore \gcd(1976, 1776) = 8$

using the above equation in reverse order substituting for remainder each time, we get the linear combination.

$$\begin{aligned} (1976, 1776) &= 8 \\ &= 176 - 7(24) \\ &= 176 - 7(200 - 1(176)) \\ &= 8(176) - 7(200) \end{aligned}$$

$= 8(1776 - 8(200)) - 71(200)$

$= 8(1776 - 71(200)$

$= 8(1776) - 71(1976 - 1(1776))$

$= 79(1776) - 71(1976)$

$= 79(1776) + (-71)(1976).$

$\therefore$ gcd is a linear combination of the numbers 1776 and 1976.

(ii). Here $4076 > 1024$

By applying division algorithm successively, we get

$4076 = 3(1024) + 1004$

$1024 = 1(1004) + 20$

$1004 = 50(20) + 4$

$20 = 5(4) + 0$

$$\begin{array}{r|l} & \;3 \\ 1024 & 4076 \\ & 3072 \\ \hline & 1004 \end{array} \qquad \begin{array}{r|l} & \;1 \\ 1004 & 1024 \\ & 1004 \\ \hline & \;\;20 \end{array} \qquad \begin{array}{r|l} & \;50 \\ 20 & 1004 \\ & \;100 \\ \hline & \quad 4 \end{array} \qquad \begin{array}{r|l} & \;5 \\ 4 & 20 \\ & 20 \\ \hline & \;0 \end{array}$$

$\therefore$ the last non zero remainder is 4 $\therefore$ gcd$(4076, 1024) = 4$.

using the above equation in reverse order substituting successively for remainder each time, we get

$(4076, 1024) = 4$

$= 1004 - 50(20)$

$= 1004 - 50(1024 - 1(1004))$

$= 51(1004) - 50(1024)$

$= 51(4076 - 3(1024)) - 50(1024)$

$= 51(4076) - 203(1024)$

$= 51(4076) + (-203)(1024).$

$\therefore$ gcd is a linear combination of the numbers 1024 and 4076.

Theorem: There are infinitely many primes of the form $4n+3$

Proof: We prove by contradiction method

Suppose there are only finite number of primes of the form $4n+3$, say $P_0 P_1, P_2, \dots P_k$ where $P_0=3$ and P_k is the largest prime.

Consider the positive integer $m=4P_1P_2\dots P_k+3$

clearly $m>P_k$ and is of the form $4n+3$ (Here $n=P_1P_2\dots P_k$)

If m is a prime, then m is a prime larger than the largest prime P_k. which is a contradiction.

If m is not a prime, then m is a composite number

clearly m is an odd number.

So, every factor of m is of the form $4n+1$ or $4n+3$

Suppose every factor is of the form $4n+1$, then their product will be of the form $4n+1$.

$\therefore$ m will be of the $4n+1$ ($\because (4l+1)(4m+1)=16m+4(l+m)+1=4(4lm+l+m)+1$)

Since m is of the form $4n+3$, at least one of the factors of m, say P is of the form $4n+3$.

If $P=P_0=3$, then $3/m$ and $3/3 \Rightarrow 3/m-3$

$\therefore 3/4P_1P_2\dots P_k \Rightarrow 3/4$ or $3/$ some P_i ($\because$ by Euclid lemma)

But both are impossible and hence a contradiction

If $P=P_i$ for some P_i then P/m and $P/P_1P_2\dots P_k$

$\therefore P/m-P_1P_2\dots P_k \Rightarrow P/3$ is a contradiction

$\therefore$ in both the cases, we get a contradiction

This means our assumption of finiteness is wrong

Hence there are infinitely many primes of the form $4n+3$

Problems

Prob. No ① For any positive integer, Prove that $8n+3$ and $5n+2$ are relatively prime

$$5n+2\,\overset{1}{\overline{)\,8n+3}}\qquad 3n+2\,\overset{1}{\overline{)\,5n+2}}$$
$$\frac{5n+2}{3n+1}\qquad\qquad \frac{3n+1}{2n+1}$$

Sol:- To Prove $(8n+3, 5n+2)=1$

when $n=1$, $8n+3=11$ and $5n+2=7$

$\gcd(11,7)=1$

Hence it is true when $n=1$

For $n\geq 2$, we have $8n+3>5n+2$

$$8n+3 = 1\cdot(5n+2)+(3n+1),\ 0<3n+1<5n+2$$
$$5n+2 = 1\cdot(3n+1)+(2n+1),\ 0<2n+1<3n+1$$
$$3n+1 = 1\cdot(2n+1)+n$$
$$2n+1 = 2(n)+1.$$
$$n = 1\cdot n+0$$

$\therefore$ the last nonzero remainder is 1

$\therefore$ $\gcd(8n+3, 5n+2)=1$ $\forall n\geq 2$

So, $8n+3$ and $5n+2$ are relatively prime for any positive integer.

Prob. No ②. Prove that $(a, a-b)=1$ if and only if $(a,b)=1$.

Sol:- Let $(a,b)=1$

then there exist integers l and m such that

$$la+mb=1$$
$$\Rightarrow la+ma+mb-ma=1$$
$$\Rightarrow (l+m)a-m(a-b)=1$$
$$\Rightarrow (l+m)a+(-m)(a-b)=1$$
$$\Rightarrow (a, a-b)=1$$

Conversely, let $(a, a-b)=1$

then there exist integers α and β such that

$$\alpha a+\beta(a-b)=1$$

$\Rightarrow \alpha a + \beta a - \beta b = 1$

$\Rightarrow (\alpha+\beta)a + (-\beta)b = 1$

$\Rightarrow (a, b) = 1$

Prob. No ③. If the square of an integer is odd, then prove that the integer is odd.

Sol:- Let 'n' be an integer such that n^2 is odd

To prove 'n' is odd

Suppose 'n' is not odd, then 'n' is even

$\therefore n = 2m$ for some integer m

$n^2 = 4m^2 = 2(2m^2)$

which is even and hence a contradiction

$\therefore$ 'n' is odd

Similarly, we can prove that if n^2 is even, then 'n' is even.

Prob. No ④ If $(a,b)=1$, then prove that $(a^2, b^2) = 1$.

Sol:- Given $(a,b)=1$

To prove $(a^2, b^2)=1$

Suppose $(a^2,b^2) \neq 1$, then a^2 and b^2 have a common factor and hence have a prime factor P

$\therefore P/a^2$ and $P/b^2 \Rightarrow P/a.a$ and $P/b.b$

$\Rightarrow P/a$ and P/b ($\because$ P is a prime and $P/ab \Rightarrow P/a$ or P/a).

$\therefore$ P/ the greatest common divisor of 'a' and 'b'

$\Rightarrow P/(a,b) \Rightarrow P/1$

which is not possible and hence a contradiction

$\Rightarrow (a^2, b^2) = 1$.

Prob. No ⑤. If 'a' and 'b' are positive integers such that b/a and b/a+2, prove that b=1 or 2

Sol:- Given b/a and b/a+2

$\therefore \; b/la+m(a+2)$ for all integers l,m

$\Rightarrow b/(l+m)a+2m$ for all, l,m

In particular, it is true for $l=-1, m=1$

$\Rightarrow b/0(a)+2 \Rightarrow b/2$

Since b is a positive integer $b/2 \Rightarrow b=1$ or 2

Prob. No (6). If a, b are odd positive integers, prove that $2/a^2+b^2$ but $4\nmid a^2+b^2$

Sol:- Given 'a' and 'b' are odd positive integers

then $a = 2m+1$ and $b = 2n+1$ where m, n are integers ≥ 0

$$a^2+b^2 = (2m+1)^2+(2n+1)^2$$
$$= 4m^2+4m+1+4n^2+4n+1$$
$$= 4m^2+4n^2+4m+4n+2$$
$$= 2(2m^2+2n^2+2m+2n+1)$$

$\therefore \; 2/a^2+b^2$ but $4\nmid a^2+b^2$

($\because$ $2m^2+2n^2+2m+2n+1$ is an odd integer).

Prob. No (7). Prove that the product of any two integers of the form $4n+1$ is also the same form.

Sol:- Let $a=4m+1$, $b=4n+1$ be two integers

Then
$$a\cdot b = (4m+1)(4n+1)$$
$$= 16mn+4m+4n+1$$
$$= 4(4mn+m+n)+1$$
$$= 4k+1$$

which of the same form.

Least common Multiple (lcm)

Defn:- The least common multiple of two positive integers 'a' and 'b' is the smallest positive integer that is divisible by both 'a' and 'b'

The lcm of 'a' and 'b' is denoted by [a,b] (or) lcm (a,b)

We can use canonical decomposition to find lcm.

If $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}$, where $\alpha_i \beta_i$ are non-negative integers. then

$$[a,b] = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)} .$$

Problems

Prob.No ① Find the lcm of the following (i) 1050 and 2574 (ii) 120 and 500 (iii) 504 and 540.

Sol:- (i) we have to find lcm of 1050 and 2574

First we find the canonical decompositions

$$\begin{array}{r|l} 2 & 1050 \\ \hline 5 & 525 \\ \hline 5 & 105 \\ \hline 3 & 21 \\ \hline & 7 \end{array} \qquad \begin{array}{r|l} 2 & 2574 \\ \hline 3 & 1287 \\ \hline 3 & 429 \\ \hline 11 & 143 \\ \hline & 13 \end{array}$$

$1050 = 2.3.5^2.7 = 2.3.5^2.7.11^0.13^0$

$2574 = 2.3^2.11.13$

$= 2.3^2.5^0.7^0.11.13$

$\therefore$ lcm $[a,b]$ = Product of factors with maximum indices

$= 2.3^2.5^2.7.11.13$

$= 450,450$

(ii) we have to find lcm of 120 and 500

First we find the canonical decompositions

$$\begin{array}{r|l} 2 & 120 \\ \hline 2 & 60 \\ \hline 2 & 30 \\ \hline 3 & 15 \\ \hline & 5 \end{array} \qquad \begin{array}{r|l} 2 & 500 \\ \hline 2 & 250 \\ \hline 5 & 125 \\ \hline 5 & 25 \\ \hline & 5 \end{array}$$

$120 = 2^3.3.5 = 2^3.3.5$

$500 = 2^2.5^3 = 2^2.3^0.5^3$

lcm (120, 500) = factors with maximum powers

$= 2^2 . 3 . 5^3$

$= 3000$

(iii) we have to find lcm of 504 and 540

First we find the canonical decompositions

$\therefore 504 = 2^3 . 3^2 . 7 = 2^3 . 3^2 . 5^0 . 7$

and $540 = 2^2 . 3^3 . 5 = 2^2 . 3^3 . 5 . 7^0$

$$\begin{array}{r|l} 2 & 504 \\ \hline 2 & 252 \\ \hline 2 & 126 \\ \hline 3 & 63 \\ \hline 3 & 21 \\ \hline & 7 \end{array} \qquad \begin{array}{r|l} 2 & 540 \\ \hline 2 & 270 \\ \hline 3 & 135 \\ \hline 3 & 45 \\ \hline 3 & 15 \\ \hline & 5 \end{array}$$

$\therefore$ lcm (504, 540) = factors with maximum powers

$= 2^2 . 3^2 . 5 . 7$

$= 7560 .$

Theorem: If 'a' and 'b' are positive integers, then

$$[a, b] = \frac{a \cdot b}{(a, b)}$$

Proof:- Let $a = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ be the canonical decompositions of 'a' and 'b'

then $(a, b) = p_1^{\min(\alpha_1 \beta_1)} p_2^{\min(\alpha_2 \beta_2)} \ldots p_k^{\min(\alpha_k \beta_k)}$

and $[a, b] = p_1^{\max(\alpha_1 \beta_1)} p_2^{\max(\alpha_2 \beta_2)} \ldots p_k^{\max(\alpha_k, \beta_k)}$

$\therefore (a, b)[a, b] = p_1^{\min(\alpha_1 \beta_1) + \max(\alpha_1 \beta_1)} . p_2^{\min(\alpha_1 \beta_1) + \max(\alpha_2 \beta_2)}$

$\ldots p_k^{\min(\alpha_k \beta_k) + \max(\alpha_k \beta_k)}$

$= p_1^{\alpha_1 + \beta_1} . p_2^{\alpha_2 + \beta_2} \ldots p_k^{\alpha_k + \beta_k}$

$= p_1^{\alpha_1} . p_1^{\beta_1} . p_2^{\alpha_2} . p_2^{\beta_2} \ldots p_k^{\alpha_k} . p_k^{\beta_k}$

$= (p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}) . (p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k})$

$= a . b \qquad \therefore [a, b] = \dfrac{a \cdot b}{(a, b)} .$

Note: ① This theorem gives another method for finding lcm

②. If 'a' and 'b' are relatively prime, then $(a,b)=1$

$$\therefore [a,b] = \frac{a \cdot b}{1} = a \cdot b$$

Thus lcm of relatively prime numbers is their product.

Problems

Prob. No ① Find the lcm of 504 and 540 using their gcd.

Sol:- We have to find the lcm of 504 and 540

First we have the canonical decompositions as

$$504 = 2^3 \cdot 3^2 \quad \text{and} \quad 540 = 2^2 \cdot 3^3 \cdot 5$$

$$\gcd(504, 540) = 2^2 \cdot 3^2 = 36$$

$$\text{lcm}(504, 540) = \frac{504 \cdot 540}{36} = 14 \cdot 540 = 7560$$

Prob. No ②. Use recursion to find the following (i) $[24, 28, 36, 40]$ (ii) $[15, 18, 24, 30]$.

Sol:- (i) we have to find $[24, 28, 36, 40]$

we isolate each term from the right and find the lcm of the inner groups as below

$$\begin{array}{r|l} 2 & 24, 28 \\ \hline 2 & 12, 14 \\ \hline & 6, 7 \end{array}$$

$$\therefore [24, 28, 36, 40] = [[24, 28, 36], 40]$$

$$= [[[24, 28], 36], 40]$$

$$\begin{array}{r|l} 2 & 168, 36 \\ \hline 2 & 84, 18 \\ \hline 3 & 42, 9 \\ \hline & 14, 3 \end{array}$$

But $[24, 28] = 168 = 2 \cdot 2 \cdot 6 \cdot 7$

$$[[24, 28], 36] = [168, 36] = 2 \cdot 2 \cdot 3 \cdot 14 \cdot 3 = 504$$

$$\begin{array}{r|l} 2 & 504, 40 \\ \hline 2 & 252, 20 \\ \hline 2 & 126, 10 \\ \hline & 63, 5 \end{array}$$

$$\therefore [24, 28, 36, 40] = [504, 40]$$

$$= 2^3 \cdot 5 \cdot 65$$

$$= 2520.$$

(ii) we have to find $[15, 18, 24, 30]$

$$[15,18,24,30] = [[15,18,24],30]$$
$$= [[[15,18],24],30]$$

$$3 \,\underline{|\, 15, 18}$$
$$5, 6$$

But $[15,18] = 3\cdot5\cdot6 = 90$

$$3 \,\underline{|\, 90, 24}$$
$$2 \,\underline{|\, 30, 8}$$
$$15, 4$$

$$[[15,18],24] = [90,24]$$
$$= 3\cdot2\cdot15\cdot4 = 360$$

$$[15,18,24,30] = [360,30]$$
$$= 360$$

Prob. No ③. Find the positive integer 'a' if $[a, a+1] = 132$.

Sol:- Given $[a, a+1] = 132$

Since a and a+1 are consecutive integers, they are relatively prime

$$(a, a+1) = 1$$

Hence $[a, a+1] = a(a+1)$

$$132 = a(a+1)$$
$$a(a+1) = 11 \cdot 12$$
$$a = 11$$

Note ① If p is a prime and $p/n!$, then the highest power of p dividing n! in its canonical decomposition is

$$= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

It is a finite sum because $\left[\frac{n}{p^m}\right] = 0$ if $p^m > n$.

Prob. No ④. Find the canonical decomposition of 23!

Sol:- The primes dividing 23! are

$$2, 3, 5, 7, 11, 17, 19, 23$$

the power of 2 dividing 23! is $=\left[\frac{23}{2}\right]+\left[\frac{23}{2^2}\right]+\left[\frac{23}{2^3}\right]+\left[\frac{23}{2^4}\right]$

$= 11+5+2+1=19$

the power of 3 dividing 23! is $=\left[\frac{23}{3}\right]+\left[\frac{23}{3^2}\right]=7+2=9.$

the power of 5 dividing 23! is $=\left[\frac{23}{5}\right]+\left[\frac{23}{5^2}\right]=4+0=4$

the power of 7 dividing 23! is $=\left[\frac{23}{7}\right]=3$

the power of 11 dividing 23! is $=\left[\frac{23}{11}\right]=2$

the power of 13 dividing 23! is $=\left[\frac{23}{13}\right]=1$

the power of 17 dividing 23! is $=\left[\frac{23}{17}\right]=1$

the power of 19 dividing 23! is $=\left[\frac{23}{19}\right]=1$

the power of 23 dividing 23! is $=\left[\frac{23}{23}\right]=1$

∴ the canonical form of $23! = 2^{19}.3^{9}.5^{4}.7^{3}.11^{2}.13.17.19.23$

Prob. No ⑤. Find the largest power of 2 that divides 97!

Sol:- we know 2/97!

∴ the largest power is

$=\left[\frac{97}{2}\right]+\left[\frac{97}{2^2}\right]+\left[\frac{97}{2^3}\right]+\left[\frac{97}{2^4}\right]+\left[\frac{97}{2^5}\right]+\left[\frac{97}{2^6}\right]$

$= 48+24+12+6+3+1$ $\quad (\because 2^7>97, \left[\frac{97}{2^7}\right]=0).$

$= 94$

∴ 2^{94} is the highest power of 2 dividing 97!

Prob. No ⑥. The number of trailing zeros in the decimal value of 260!

Sol:- The number of zeros in which 260! is ending with is the same as the highest power of 10 dividing 260!

Now $10 = 2 \cdot 5 \Rightarrow 10^n = 2^n \cdot 5^n$

∴ the highest power of 10 is the same as highest power of 5.

The highest power of 5 dividing 260! is

$$= \left[\frac{260}{5}\right] + \left[\frac{260}{5^2}\right] + \left[\frac{260}{5^3}\right]$$

$$= 52 + 10 + 2$$

$$= 64$$

∴ 10^{64} is the highest power of 10 dividing 260!

∴ the number of zeros in the decimal form is 64.

Prob. No ⑦. Find the number of trailing zero in 234!

Sol:- The number of zeros in which 234! is ending with is the same as the highest power of 10 dividing 234!

Now $10 = 2 \cdot 5$

So, the highest power of 10 is the same as the highest power of 5 dividing 234!

The highest power of 5 dividing 234! is

$$= \left[\frac{234}{5}\right] + \left[\frac{234}{5^2}\right] + \left[\frac{234}{5^3}\right] \quad (\because 5^4 > 234)$$

$$= 46 + 9 + 1$$

$$= 56$$

∴ 264! ends with 56 zeros.

Unit 5. CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

In this chapter we will discuss three important classical results in number theory namely Wilson's theorem, Fermat's little theorem and Euler's theorem. These theorems are important milestones in the development of the theory of congruence and illustrate the significance of congruence.

Result ① $ax \equiv 1 \pmod{p} \Leftrightarrow$ (has a unique solution)
ie $(a,p)=1$ and x is the inverse of 'a'.

Note ① For p, all the numbers $1,2,3,\ldots(p-1)$ has inverse based on above.

Lemma ①: 'a' is self invertible modulo $p \Leftrightarrow a \equiv \pm 1 \pmod{p}$

Proof:- Nec part: If 'a' is self invertible

$$a \cdot a \equiv 1 \pmod{p}$$

$\Rightarrow a^2-1$ is divisible by p

$\Rightarrow p/(a-1)(a+1) \Rightarrow p/(a-1)$ or $p/(a+1)$

$\Rightarrow a \equiv 1 \pmod{p}$ (or) $a \equiv -1 \pmod{p}$

$\Rightarrow a \equiv \pm 1 \pmod{p}$

Suffi part: If $a \equiv \pm 1 \pmod{p}$

$$a^2 \equiv 1 \pmod{p}$$

ie 'a' is self invertible modulo p.

Note ① From the above we conclude. For a prime 'p' 1 and $(p-1)$ only are self invertible.

For example $p=7$

$$(p-1)! = 6! = 1 \times 2 \times 3 \times 4 \times 5 \times 6$$

$$6! = \underset{\substack{\downarrow \\ \text{Self} \\ \text{invertible}}}{1} \times \underbrace{2\times3\times4\times5}_{\substack{\text{group these} \\ \text{elements with} \\ \text{their inverse}}} \times \underset{\substack{\downarrow \\ \text{self} \\ \text{invertible}}}{6}$$

$$= 1\times(2\times4)\times(3\times5)\times6$$

$$= 1\times1\times1\times6$$

$$\equiv -1 \pmod 7.$$

$$\equiv 1 \pmod 7$$

Wilson's theorem

If p is a prime, then $(p-1)! \equiv -1 \pmod p$

Proof:- when $p=2$, $(p-1)! = 1 \equiv -1 \pmod 2$

So, let $p>2$ (note that p is an odd number $(p-1)$ is an even number).

$$(p-1)! = \underset{\substack{\downarrow \\ \text{Self} \\ \text{invertible}}}{1} \times \underbrace{2\times3\times4\times5\times\cdots\times(p-2)}_{\substack{\text{group each of these} \\ \text{elements} \\ \Downarrow \\ \text{since it is an even number} \\ \text{we can pair the elements}}} \times \underset{\substack{\downarrow \\ \text{self invertible.}}}{(p-1)}$$

$$= 1\times 1\times1\times1\times1\cdots\times1\times(p-1)$$

$$\equiv -1 \pmod p$$

Problems

Prob. No ① Find the self invertible least residue modulo for each prime (i) 7 and (ii) 13

Sol:- (i) $p=7$ $\quad (7-1)! \equiv -1 \pmod 7$

$\equiv 1 \pmod 7$

ie $1\times1 \equiv 1 \pmod 7$ and $6\times6 \equiv 1 \pmod 7$

(ii) $p=13$ $\quad (13-1)! \equiv -1 \pmod{13}$

$\equiv 1 \pmod{13}$

ie $1\times1 \equiv 1 \pmod{13}$ and $12\times12 \equiv 1 \pmod{13}$

Prob. No ②. Solve $x^2 \equiv 1 \pmod{m}$ when $m = 8$ equivalently find self invertible modulo m.

Sol:- Given $m = 8$ $1^2 \equiv 1 \pmod{8}$ $2^2 \equiv 4 \pmod{8}$ $3^2 \equiv 1 \pmod{8}$

$4^2 \equiv 0 \pmod{8}$ $5^2 \equiv 1 \pmod{8}$ $6^2 \equiv 4 \pmod{8}$ $7^2 \equiv 1 \pmod{8}$

So, $x = 1, 3, 5, 7$ are self invertibles.

Prob. No ③. Solve $x^2 \equiv 1 \pmod{15}$

Sol:- Given $m = 15$

$1^2 \equiv 1 \pmod{15}$ $2^2 = 4 \pmod{15}$ $3^2 \equiv 9 \pmod{15}$ $4^2 \equiv 1 \pmod{15}$

$5^2 \equiv 10 \pmod{15}$ $6^2 = 6 \pmod{15}$ $7^2 \equiv 4 \pmod{15}$

$8^2 \equiv 4 \pmod{15}$ $9^2 \equiv 6 \pmod{15}$ $10^2 \equiv 10 \pmod{15}$ $11^2 \equiv 1$ (mod15

$12^2 \equiv 4 \pmod{15}$ $13^2 \equiv 4 \pmod{15}$ $14^2 \equiv 1 \pmod{15}$.

So, $x = 1, 4, 11, 14$ are self invertibles.

Prob. No ④. Prove or disprove. The congruence $x^2 \equiv 1 \pmod{m}$ has exactly two solutions, then m is prime

Sol:- $x^2 \equiv 1 \pmod{4}$ has exactly two solutions $x = 1, 3$

but 4 is not a prime.

So the above result is not true.

Prob. No ⑤. If $x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$ does it follow that $x^2 \equiv 1 \pmod{pq}$, where p and q are distinct primes.

Sol:- $x^2 \equiv 1 \pmod{p} \Rightarrow x = 1, p-1$ are self invertible elts

$x^2 \equiv 1 \pmod{q} \Rightarrow x = 1, q-1$ are self invertible elts

but $p \neq q \Rightarrow (p-1) \neq (q-1)$

$\therefore x = 1$ is the only element satisfying both eqns

$\therefore\ x^2 \equiv 1^2 \equiv 1 \pmod{pq}$ is true (and is true only for $x=1$).

Prob. No 6. Let 'a' be a solution of the congruence $x^2 \equiv 1 \pmod{m}$. Show that $(m-a)$ is also a solution.

Sol:- $a^2 \equiv 1 \pmod{m}$

$\Rightarrow m/(a^2-1) \Rightarrow m/(a-1)(a+1)$

$(a-1) = mq$ (or) $(a+1) = mq'$

$a \equiv mq+1$ (or) $a \equiv mq'-1$

$m-a = m-mq-1$ (or) $m-a = m-mq'+1$

$\Rightarrow m/(m-a)+1$ (or) $m/(m-a)-1$

$\Rightarrow m/((m-a)+1)((m-a)-1)$

$\Rightarrow m/((m-a)^2-1) \Rightarrow (m-a)^2 \equiv 1 \pmod{m}$

$\Rightarrow (m-a)$ is a solution for the equation $x^2 \equiv 1 \pmod{m}$.

Prob. No 7. Verify that $(p-1)! = -1$ when $p = 13$

Sol:- $(p-1)! = 12! = 1\times2\times3\times4\times5\times6\times7\times8\times9\times10\times11\times12$

$= 1\times(2\times7)\times(3\times9)\times(4\times10)\times(5\times8)\times(6\times11)\times12$

$= 1\times1\times1\times1\times1\times1\times12$

$= -1 \pmod{13}$.

Prob. No 8. Let p be odd then prove that $2(p-3)! \equiv -1 \pmod{p}$

Sol:- $2 \times (p-3)! = 2 \times 1 \times 2 \times 3 \times \cdots \times (p-4) \times (p-3) \rightarrow ①$

By Wilson's theorem, 1 and $(p-1)$ are self invertible $(p-2)$ is not self-invertible and is not available in the above product.

So, there is a value x in the above product $1 \leq x < p-2$ whose inverse is $(p-2)$.

$$(p-2)x \equiv 1 (\mod p)$$

$$xp - 2x \equiv 1 (\mod p)$$

$$(-2x) \equiv 1 (\mod p) \quad (\because \text{we know that } p/xp).$$

(or) equivalently $2x \equiv -1 (\mod p) \rightarrow ②$

Now take the product ①

$$2 \times (p-3)! = 2 \times (1 \times 2 \times 3 \times \cdots \times (p-4) \times (p-3))$$

$\Downarrow$

even number of terms regroup the elts with their inverse

So x alone is left without inverse whose inverse is $(p-2)$

$$= 2 \times (1 \times (2 \times 2^{-1}) \times (3 \times 3^{-1}) \times \cdots) \times x$$

$$= 2 \times (1 \times 1 \times 1 \times 1 \cdots 1) \times x$$

$$= 2x$$

$$= -1 (\mod p) \quad (\because \text{by } ②).$$

Prob. No ⑨ Prove that $(p-1)(p-2)\cdots(p-k) \equiv (-1)^k k! (\mod p)$ where $1 \leq k < p$.

Sol:-

$$p-1 \equiv -1 (\mod p)$$

$$p-2 \equiv -2 (\mod p)$$

$$\vdots$$

$$p-k = -k (\mod p)$$

$$(p-1)(p-2)\cdots(p-k) \equiv (-1)(-2)\cdots(-k) (\mod p)$$

$$\equiv (-1)^k k! (\mod p).$$

Prob. No (10) Let p be a prime, n positive integers. Prove that

$$\frac{(np)!}{n!\,p^n} \equiv (-1)^n \pmod p$$

Sol:- First, we can make an observation. Let 'a' be any positive integer congruent to 1 modulo p. Then by wilson's theorem

$$a(a+1)\cdots(a+(p-2)) \equiv (p-1)! \pmod p$$

In other words, the product of the $(p-1)$ integers between any two consecutive multiples of p is congruent to -1 modulo p. Then

$$\frac{(np)!}{n!\,p^n} = \frac{(1\times2\times3\times\cdots\times(p-1))p\,((p+1)(p+2)\cdots(p+p-1))2p\,((2p+1)(2p+2)\cdots(2p+p-1))3p\cdots((n-1)p+1)\,((n-1)p+2)\cdots((n-1)p+p-1))np}{(1\times2\times3\times3\times\cdots n)\,(p.p.p\ldots p)\,(n \text{ times})}$$

Cancelling Numerator and denominator each product inside the each paranthesis is $\equiv -1 \pmod p$ (∵ by Wilson's theorem)

$$\equiv (-1)(-1)\cdots(-1)\ (n \text{ times}) \pmod p$$

$$\equiv (-1)^n \pmod p.$$

Note (1) Evaluate $\frac{(230)!}{46!\,5^{46}} \pmod 5$

Sol:- $\frac{(230)!}{46!\,5^{46}} = \frac{(46\times5)!}{46!\,5^{46}} \equiv (-1)^{46} \pmod 5$

$\equiv 1 \pmod 5$.

Prob. No 11. p be odd. then $1^2\cdot3^2\cdot5^2\cdots(p-2)^2 \equiv (-1)^{\frac{p+1}{2}}$ (mod p)

Sol:- $(1^2\cdot3^2\cdot5^2\cdots(p-2)^2) \equiv (1\cdot3\cdot5\cdots(p-2))(1\cdot3\cdot5\cdots(p-2))$

$$= (1\cdot3\cdot5\cdots(p-2))((p-2)(p-4)\cdots(p-(p-1))(p-(p-3)))$$

$$= (1\cdot3\cdot5\cdots(p-2))\cdot((-2)(-4)\cdots(-1)(p-5)(-1)(p-3)(-1)(p-1))$$

$$= (1\cdot3\cdot5\cdots(p-2))\cdot((-1)(2)(-1)(4)\cdots(-1)(p-5)(-1)(p-3)(-1)(p-1))$$

$$=(-1)^{\frac{p-1}{2}}(1\cdot2\cdot3\cdot4\cdot5\cdots(p-3)(p-2)(p-1))$$

$$= (-1)^{\frac{p-1}{2}}(p-1)! \pmod p$$

$$= (-1)^{\frac{p-1}{2}}(-1) \pmod p$$ (∵ by Wilson's theorem)

$$= (-1)^{\frac{p+1}{2}} \pmod p.$$

Prob. No 12. Let p be odd $2^2\cdot4^2\cdots(p-1)^2 \equiv (-1)^{\frac{p+1}{2}}$ (mod p).

Sol:- $(1^2\cdot2^2\cdot3^2\cdots(p-2)^2)(2^2\cdot4^2\cdots(p-1)^2) = 1^2\cdot2^2\cdots(p-1)^2$ (mod p)

$$= ((p-1)!)^2 \pmod p.$$

$$= (-1)^2 \pmod p$$

$$(-1)^{\frac{p+1}{2}}(2^2\cdot4^2\cdots(p-1)^2) \equiv 1 \pmod p$$

∴ $2^2\cdot4^2\cdots(p-1)^2$ must be $(-1)^{\frac{p+1}{2}}$ (mod p).

Converse of Wilson's theorem

If 'n' is positive integer such that $(n-1)! \equiv -1 \pmod n$ then 'n' is prime

Proof:- Suppose 'n' is not a prime

then $n = ab$ for some $1 < a < n$ and $1 < b < n$.

'a' is a number from 2 to $(n-1)$

$\therefore \quad a/(n-1)!$

Also a/n where $n/(n-1)!+1$ (by given condition)

$\therefore \quad a/(n-1)!+1$

now combining these two

a divides the difference of these two

ie $a/(n-1)!+1-(n-1)!$

ie $a/1 \Rightarrow a=1$ which is contradiction

to the fact ie $1<a<n$.

$\therefore$ 'n' must be a prime.

Problems

Prob.No ① A positive integer $n \geq 2$ is a prime if and only if $(n-2)! \equiv 1 \pmod{n}$

Sol:- Suppose 'n' is a prime

By Wilson's theorem $(n-1)! \equiv -1 \pmod{n}$.

ie $(n-2)!\,(n-1) \equiv -1 \pmod{n}$

Now $(\,n-1 \equiv -1 \pmod{n})$

$\therefore \quad (n-2)!\,(-1) \equiv (-1) \pmod{n}$

$\therefore \quad (n-2)! \equiv 1 \pmod{n}$

conversely, if $(n-2)! \equiv 1 \pmod{n}$

then $(n-1)! = (n-2)!\,(n-1)$

$= (1)\,(-1) \pmod{n}$

$(n-1)! = (-1) \pmod{n}$.

By converse of Wilson's theorem 'n' must be a prime

Prob. No 2. Let r be a positive integer $< p$ such that $r! \equiv (-1)^r \pmod{p}$ then $(p-r-1)! \equiv (-1) \pmod{p}$.

Sol:- By Wilson's theorem

$$(p-1)! \equiv (-1) \pmod{p}$$

$$(1\times2\times3\times\cdots\times(p-r-1))((p-r)(p-r+1)(p-r+2)\cdots(p-r+(r-1))$$

$$\equiv(-1) \pmod{p}$$

$$(p-r-1)! \times ((-r)(-r+1)(-r+2)\cdots(-1)) \equiv (-1)\pmod{p}$$

$$(p-r-1)! \times (-1)^r (1\times2\times3\cdots r) \equiv (-1)\pmod{p}$$

$$(p-r-1)!\ (-1)^r(-1)^r \equiv (-1)\pmod{p} \quad (\because \text{by given condition})$$

$$(p-r-1)! \times 1 \equiv (-1)\pmod{p}$$

$$(p-r-1)! \equiv (-1)\pmod{p}$$

Prob. No 3 $\dfrac{1\cdot3\cdot5\cdots(p-2)}{2\cdot4\cdot6\cdots(p-1)} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ when $p>2$.

Sol:- $$\frac{1\cdot3\cdot5\cdots(p-2)}{2\cdot4\cdot6\cdots(p-1)} = \frac{1\cdot2\cdot3\cdot4\cdot5\cdots(p-2)(p-1)}{(2\cdot4\cdot6\cdots(p-1))(2\cdot4\cdot6\cdots(p-1))}$$

$$= \frac{(p-1)!}{2^2\cdot4^2\cdot6^2\cdots(p-1)^2}$$

$$\equiv \frac{(-1)}{2^2\cdot4^2\cdot6^2\cdots(p-1)^2} \pmod{p} \quad (\because \text{by Wilson's theorem})$$

$$\equiv \frac{(-1)}{(-1)^{\frac{p+1}{2}}} \pmod{p}$$

$$\equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Fermat's little theorem

Result ①: Let p be a prime and a be any integer such that $p \nmid a$. Then the least residues of the integers $a, 2a, 3a, \dots (p-1)a$ modulo p are a permutation of the integers $1, 2, 3, \dots (p-1)$.

Theorem ① Fermat's little theorem (or) Fermat's theorem

If p is a prime and 'a' is any integer not divisible by p then $a^{p-1} \equiv 1 (\mod p)$

Proof:- Given p is a prime and 'a' is any integer not divisible by p ie $p \nmid a$

when an integer is divided by p, the set of possible remainders are $0, 1, 2, 3 \dots (p-1)$

Consider the set of integers

$$1.a, 2.a, 3.a \dots (p-1)a \rightarrow ①$$

Suppose $ia \equiv 0 (\mod p)$, then p/ia. But $p \nmid a$

$\therefore$ p/i is impossible, since $i < p$

$\therefore$ $ia \not\equiv 0 (\mod p)$ for $i = 1, 2, 3 \dots (p-1)$.

So, no term of ① is zero

Next we prove they are all ditinct

Suppose $ia \equiv ja (\mod p)$ where $1 \le i, j \le (p-1)$

then $(i-j)a \equiv 0 (\mod p) \Rightarrow p/(i-j)a$

Since $p \nmid a$, $p/i-j$ and $i, j < p \Rightarrow |i-j| < p$

$i-j=0 \Rightarrow i \equiv j (\mod p)$

$i \neq j \Rightarrow ia \not\equiv ja$

This means, no two of the integers in ① are congruent modulo p.

$\therefore$ the least residues (or remainders) of the integers $a, 2a, 3a \dots (p-1)a$ modulo p are the same as the integers $1, 2, 3 \dots (p-1)$ in some order.

So, their products are congruent modulo p.

$$\therefore\ a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

$$\Rightarrow\ 1 \cdot 2 \cdot 3 \cdots (p-1) a^{p-1} \equiv (p-1)! \pmod p.$$

$$\Rightarrow\ (p-1)!\, a^{p-1} \equiv (p-1)! \pmod p.$$

$$\Rightarrow\ a^{p-1} \equiv 1 \pmod p$$

the result $a^{p-1} \equiv 1 \pmod p$ is equivalent to $a^p \equiv a \pmod p$

Problems

Prob. No (1). Find the remainder when 24^{1947} is divided by 17.

Sol:- We have to find the remainder when 24^{1947} is divided by 17.

Here $a = 24$, $p = 17$

we know that 17 is a prime and $17 \nmid 24$.

$\therefore$ by Fermat's theorem, $24^{17-1} \equiv 1 \pmod{17}$.

$$\begin{array}{r|l} & 121 \\ 16 & 1947 \\ & 16 \\ \hline & 34 \\ & 32 \\ \hline & 27 \\ & 16 \\ \hline & 11 \end{array}$$

$$\Rightarrow 24^{16} \equiv 1 \pmod{17}$$

$$\Rightarrow (24^{16})^{121} \equiv 1^{121} \pmod{17}.$$

$$24^{1936} \equiv 1 \pmod{17}$$

Now $24^{1947} = 24^{1936+11} = 24^{1936} \cdot 24^{11}$

$$24^2 = 576 \equiv -2 \pmod{17}$$

$$(24^2)^2 \equiv (-2)^2 \pmod{17}$$

$$24^4 \equiv 4 \pmod{17}.$$

$$(24^4)^2 \equiv 4^2 \pmod{17}$$

$$24^8 \equiv 16 \pmod{17}$$
$$\equiv -1 \pmod{17}$$
$$24^{11} = 24^8 \cdot 24^2 \cdot 24 \equiv (-1)(-2)7 \pmod{17}$$
$$\equiv 14 \pmod{17}$$
$$24^{1947} \equiv 1 \cdot 14 \pmod{17}.$$
$$\equiv 14 \pmod{17}.$$

$$\begin{array}{r|l} & 34 \\ 17 & 576 \\ & 51 \\ \hline & 66 \\ & 68 \\ \hline & -2 \\ \hline \end{array}$$

∴ the remainder is 14 when 24^{1947} is divided by 17.

alternate way $24 \equiv a7 \pmod{17}$

$$24^{1947} \equiv 7^{1947} \pmod{17}$$

$$\begin{array}{r|l} & 121 \\ 16 & 1947 \\ & 16 \\ \hline & 34 \\ & 32 \\ \hline & 27 \\ & 16 \\ \hline & 11 \\ \hline \end{array}$$

Now by Fermat's little theorem

$$7^{16} \equiv 1 \pmod{17}.$$
$$1947 = 16 \times 121 + 11$$
$$24^{1947} \equiv 7^{16 \times 121 + 11} \pmod{17}$$
$$\equiv (7^{16})^{121}\, 7^{11} \pmod{17}.$$
$$\equiv 1 \times 7^{11} \pmod{17}.$$
$$7^2 \equiv 49 \equiv (-2) \pmod{17}.$$
$$7^{11} \equiv (7^2)^5 \times 7 \pmod{17}$$
$$\equiv (-2)^5 \times 7 \pmod{17}$$
$$\equiv -32 \times 7 \pmod{17}$$
$$\equiv +2 \times 7 \pmod{17}$$
$$\therefore 24^{1947} \equiv 7^{11} \pmod{17} \equiv 14 \pmod{17}.$$

∴ the remainder is 14 when 24^{1947} is divided by 17.

Prob. No ② Find primes p for which $\frac{2^{p-1}-1}{p}$ is a square

Sol:- $\frac{2^{p-1}-1}{p} = n^2$ for some positive integer 'n'

then $2^{p-1}-1 = pn^2$ clearly LHS is odd $\Rightarrow$ RHS is odd

∴ both p and n^2 must be odd

Assume $p = 2k+1$ for some positive integer k.

then $2^{2k}-1 = pn^2 \Rightarrow (2^k-1)(2^k+1) = pn^2$

$\Rightarrow (2^k-1)\ (2^k+1)$ are both consecutive odd integers and relatively prime

So either (2^k-1) (or) (2^k+1) are both consecutive odd integers must be a perfect square.

case (i) If 2^k-1 is a perfect square r^2

$$2^k-1 = r^2 \Rightarrow 2^k = r^2+1$$

ie $2^{p-1} = (2^{2k}) = (2^k)^2 = (r^2+1)^2$

Since r is odd so $r = 2i+1$

∴ $2^{p-1} = ((2i+1)^2+1) = 2(2i^2+2i+1)$

ie $2^{p-2} = 2i^2+2i+1$ is possible only if $i=0$

then $r=1$ we have

$$2^{p-1} = (1^2+1)^2 = 4 = 2^2 \Rightarrow p=3.$$

case (ii) If 2^k+1 is a perfect square s^2

$$2^k+1 = s^2 \Rightarrow 2^k = s^2-1 = (s-1)(s+1)$$

$$2^{p-1} = 2^{2k} = (2^k)^2 = (s-1)^2(s+1)^2$$

Since $s \geq 3$ and s is odd $s = 2i+1$, $i \geq 1$.

$$2^k = (2i+1)^2-1 = 4i(i+1)$$

ie $2^{k-2} = i(i+1)$ is possible only if $i=1$

$$\therefore \quad 2^{p-1} = 2^{6} \Rightarrow p = 7.$$

Theorem: let p be a prime and 'a' be any integer such that $p \nmid a$. then a^{p-2} is an inverse of a modulo p.

Proof: By Fermat's little theorem $a^{p-1} \equiv 1 \pmod{p}$

$$a^{p-2} \cdot a \equiv 1 \pmod{p}$$

So a^{p-2} is an inverse of a modulo p.

Result ①: let p be a prime and a be any integer such that $p \nmid a$. then the solution of the linear congruence $ax \equiv b \pmod{p}$ is given by $x \equiv a^{p-2} b \pmod{p}$

Proof:- Given $ax \equiv b \pmod{p}$

$$a^{p-2}(ax) \equiv a^{p-2} b \pmod{p}$$

$$a^{p-1} x \equiv a^{p-2} b \pmod{p}$$

$$x \equiv a^{p-2} b \pmod{p} \quad (\because a^{p-1} \equiv 1 \pmod{p}$$

by Fermat's theorem)

Result ②: Fermat's little theorem is extended to all positive integers

ie p is a prime 'a' is a positive integer then $a^{p} \equiv a \pmod{p}$

(i) If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ (∵ by Fermat's little theorem)

$$a^{p} \equiv a \pmod{p}$$

(ii) If p/a, then $a \equiv 0 \pmod{p} \Rightarrow a^{p} \equiv 0 \pmod{p}$

$$\text{So } a^{p} \equiv a \equiv 0 \pmod{p}$$

Result ③: The pollard $(p-1)$ factoring method.

$$2^{k!} = 2^{m(p-1)!} = (2^{(p-1)})^{m} \equiv 1^{m} \equiv 1 \pmod{p}.$$

Problems

Prob. No ① Find the inverse of $12^5 (\text{mod } 7)$

Sol:- Here $p=7$ $a=12$ By Fermat's theorem

$$12^6 \equiv 1 (\text{mod } 7)$$

$$12^5 . 12 \equiv 1 (\text{mod } 7)$$

So inverse of 12^5 is $12 (\text{mod } 7) \equiv 5 (\text{mod } 7)$.

Prob. No ②. Solve the congruence equation $12x \equiv 6 (\text{mod } 7)$

Sol:- By Fermat's theorem

$p=7$ $a=12$ $12^6 \equiv 1 (\text{mod } 7)$

12^5 is the inverse of $12 (\text{mod } 7)$

$$12x \equiv 6 (\text{mod } 7)$$

Multiplying 12^5 on both the sides

$$12 \cdot 12^5 . x \equiv 12^5 . 6 (\text{mod } 7)$$

$$x \equiv (12^5) 6 (\text{mod } 7)$$

$$\equiv (-2)^5 \, 6 (\text{mod } 7)$$

$$\equiv (-32) \, 6 (\text{mod } 7)$$

$$\equiv 3 \cdot 6 (\text{mod } 7)$$

$$x \equiv 4 (\text{mod } 7)$$

Prob. No ③ Solve the congruence equation $24x \equiv 11 (\text{mod } 17)$ using Fermat's little theorem

Sol:- $24x \equiv 11 (\text{mod } 17)$ is equivalent to $7x \equiv 11 (\text{mod } 17)$

Take $p=17$ $a=7$ By Fermat's little theorem

$$7^{16} \equiv 1 (\text{mod } 17)$$

$\therefore$ 7^{15} is the inverse of 7

Multiplying both sides by 17^{15}

$7^{15}.\,7x \equiv 7^{15}.\,11 \pmod{17}$

$x \equiv 7^{15}.\,11 \pmod{17}$

$\equiv (7^2)^7.\,11.\,7 \pmod{17}$

$\equiv (-2)^7.\,11.\,7 \pmod{17}$ $(\because 7^2 = 49 \equiv -2 \pmod{17})$

$\equiv (-2)^5.\,(-2)^2.\,11.\,7 \pmod{17}$.

$\equiv (-32)\,4.\,11.\,7 \pmod{17}$

$\equiv 2.\,10.\,7 \pmod{17}$

$\equiv 3.\,7 \pmod{17}$.

$\therefore\ x \equiv 4 \pmod{7}$

Prob. No (4) using pollard (p-1) factoring method, find a non-trivial factor of $n = 2813$

Sol:- Using the fact that $2^{k!} = (2^{(k-1)!})^k$, we continue computing the least positive residue $r \equiv 2^{k!} \pmod{2813}$ and the gcd $(r-1, n)$ until a non trivial factor of n appear, where $k \geq 1$.

$2^{1!} = 2 \equiv 2 \pmod{2813}$ $(1, 2813) = 1$

$2^{2!} = 2^2 \equiv 4 \pmod{2813}$ $(3, 2813) = 1$

$2^{3!} = 4^3 \equiv 64 \pmod{2813}$ $(63, 2813) = 1$

$2^{4!} = 64^4 \equiv 484 \pmod{2813}$ $(483, 2813) = 1$

$2^{5!} = 484^5 \equiv 1648 \pmod{2813}$ $(1647, 2813) = 1$.

$2^{6!} = 1648^6 \equiv 777 \pmod{2813}$ $(776, 2813) = 97$.

Thus $97 / 2813$

Exercise 7.2 (Koshy)

Prob. No ① Compute the remainder when the first integer is divided by the second

(i) $7^{1001}, 17$ (ii) $30^{2020}, 19$ (iii) $15^{1976}, 23$ (iv) $43^{5555}, 31$.

Sol:- (i) $p = 17$ $a = 7$

By Fermat's theorem $a^{p-1} = 7^{16} \equiv 1 \pmod{17}$

we have $7^2 = 49 \equiv -2 \pmod{17}$

$\therefore (7^2)^2 \equiv (-2)^2 \pmod{17}$

$\Rightarrow 7^4 \equiv 4 \pmod{17}$

$\therefore (7^4)^2 \equiv 4^2 \equiv 16 \pmod{17}$

$\Rightarrow 7^8 \equiv -1 \pmod{17}$

$\therefore (7^8)^2 \equiv (-1)^2 \pmod{17}$

$7^{16} \equiv 1 \pmod{17}$

$(7^{16})^{62} \equiv 1^{62} \pmod{17}$

$7^{992} \equiv 1 \pmod{17}$

$7^{1001} = 7^{992+8+1}$

$= 7^{992}.7^{8}.7$

$\equiv 1.(-1).7 \pmod{17}$

$\equiv -7 \pmod{17}$

$\equiv 10 \pmod{17}$

(ii) $p = 19$ $a = 30$

By Fermat's theorem $a^{p-1} = 30^{18} \equiv 1 \pmod{19}$

$30^{2020} = 30^{18\times112+4} \equiv (30^{18})^{112}.30^4 \pmod{19}$

$\equiv 1\times 11^4 \pmod{19}$

$\equiv 11^2\times 11^2 \pmod{19}$

$\equiv 7\times 7 \pmod{19}$

$\equiv 11 \pmod{19}$

112
18) 2020
18
22
18
40
36
4

(iii) $p = 23$, $a = 15$

By Fermat's theorem $15^{22} \equiv 1 \pmod{23}$

$15^{1976} \equiv 5^{22\times89+18} \equiv (15^{22})^{89}.15^{18} \pmod{23}$

$\equiv 1\times 15^{18} \pmod{23}$

$\equiv (15^2)^9 \pmod{23}$

$\because 15^2 \equiv 225 \pmod{23} \equiv -5 \pmod{23}$

89
22) 1976
176
216
198
18

$\equiv (-5)^9 \pmod{23}$ $\quad (\because (-5)^2 = 25 \equiv 2 \pmod{23})$

$\equiv (-5)^8 \times (-5) \pmod{23}$

$\equiv ((-5^2)^4) \times (-5) \pmod{23}$

$\equiv 2^4 \times (-5) \pmod{23}$

$\equiv -80 \pmod{23}$

$\equiv 12 \pmod{23}$

(iv) $p = 31$, $a = 43$

By Fermat's theorem $a^{p-1} \equiv 43^{30} \equiv 1 \pmod{31}$

$$\begin{array}{r|l} & 185 \\ \hline 30 & 5555 \\ & 30 \\ \hline & 255 \\ & 240 \\ \hline & 155 \\ & 150 \\ \hline & 5 \\ \hline \end{array}$$

$43^{5555} \equiv 43^{30\times185+5}$

$\equiv ((43)^{30})^{185} \times 43^5 \pmod{31}$

$\equiv 1 \times 43^5 \pmod{31}$

$\equiv 12^5 \pmod{31}$

$(\because 12^2 \equiv 144 \pmod{31} \equiv 20 \pmod{31})$

$\equiv 12^2 \times 12^2 \times 12 \pmod{31}$

$\equiv 20 \times 20 \times 12 \pmod{31}$

$\equiv 480 \pmod{31}$

$\equiv 15 \pmod{31}$.

Prob. No ② Find the ones digit in the base-seven expansion of each decimal number

(i) 5^{101} (ii) 12^{1111} (iii) 29^{2076} (iv) 37^{3434}.

Sol:- (i) we have to find $5^{101} \pmod{7}$, 7 is a prime so use Fermat's theorem

$a = 5$ $p = 7$

$5^6 \equiv 1 \pmod{7}$

$5^{101} \equiv 5^{16*6+5} = (5^6)^{16} 5^5 \equiv 1 \times 5^5 \pmod{7}$

$\equiv 5^2 \times 5^2 \times 5 \pmod 7$

$\equiv 4 \times 4 \times 5 \pmod 7$

$\equiv 4 \times (-1) \pmod 7$

$\equiv -4 \pmod 7$

$\equiv 3 \pmod 7$.

$$6\overline{)101}^{\,16}$$
96
5

(ii) we have to find $12^{1111} \pmod 7$ 7 is a prime so use fermat's theorem

$a = 12 \quad p = 7$.

$12^6 \equiv 1 \pmod 7$

$12^{1111} \equiv (12^6)^{185} \times 12 \pmod 7$

$\equiv 5 \pmod 7$

$$6\overline{)1111}^{\,185}$$
6
51
48
31
30
1

(iii) we have to find $29^{2076} \pmod 7$ 7 is a prime so use fermat's theorem

$a = 29 \quad p = 7$

$29^6 \equiv 1 \pmod 7$

$29^{2076} \equiv (29^6)^{346} \equiv 1 \pmod 7$

$$6\overline{)2076}^{\,346}$$
18
27
24
36
36
0

(iv) we have to find $37^{3434} \pmod 7$, 7 is a prime so use fermat's theorem

$a = 37 \quad p = 7$

$37^6 \equiv 1 \pmod 7$

$37^{3434} \equiv (37^6)^{572} \times (37)^2 \pmod 7$

$\equiv 2^2 \pmod 7$

$\equiv 4 \pmod 7$.

$$6\overline{)3434}^{\,572}$$
30
43
42
14
12
2

Prob. No ③ Solve each linear congruence by using Fermat's little theorem.

(i) $8x \equiv 3 \pmod{11}$ (ii) $15x \equiv 7 \pmod{13}$ (iii) $26x \equiv 12 \pmod{17}$ (iv) $43x \equiv 17 \pmod{23}$.

Sol:- (i) By Fermat's little theorem we have

$8^{10} \equiv 1 \pmod{11}$. Here $a = 8$, $p = 11$

Multiply both sides by 8^9

$$8^9(8x) \equiv 8^9 \times 3 \pmod{11}$$

$$x \equiv 8^9 \times 3 \pmod{11}$$

$$\equiv (-3)^9 \times 3 \pmod{11}$$

$$\equiv (-3)^2 \times (-3)^2 \times (-3)^2 \times (-3)^2 \times (-3) \times 3 \pmod{11}$$

$$\equiv -2 \times -2 \times -2 \times -2 \times -3 \times 3 \pmod{11}.$$

$$\equiv 5 \times -3 \times 3 \pmod{11}$$

$$\equiv -15 \times 3 \pmod{11}$$

$$\equiv 7 \times 3 \pmod{11}$$

$$\equiv 10 \pmod{11}.$$

(ii) $a = 15$ $p = 13$ By Fermat's little theorem we have $15^{12} \equiv 1 \pmod{13}$

Multiply both sides by 15^{11}

$$15^{11}(15x) \equiv 15^{11} \times 7 \pmod{13}$$

$$x \equiv 15^{11} \times 7 \pmod{13}$$

$$\equiv 12^{11} \times 7 \pmod{13}$$

$$\equiv 2^4 \times 2^4 \times 2^3 \times 7 \pmod{13}$$

$$\equiv 3 \times 3 \times 56 \pmod{13}$$

$$\equiv 9 \times 4 \pmod{13}$$

$$\equiv 10 \pmod{13}.$$

(iii) $a = 26$ $p = 17$ By Fermat's theorem we have

$$26^{16} \equiv 1 \pmod{17}$$

Multiply both sides by 26^{15}

$$26^{15}(26x) \equiv 26^{15} \times 12 \pmod{17}$$

$$x \equiv 26^{15} \times 12 \pmod{17}$$

$$\equiv 9^{15} \times 12 \pmod{17}$$

$$9^2 \equiv -4 \pmod{17}$$

$$x \equiv (9^2)^7 \times 9 \times 12 \pmod{17}$$

$$x \equiv (-4)^7 \times 6 \pmod{17}$$

$$\equiv (-4)^2 \times (-4)^2 \times (-4)^2 \times (-4) \times 6 \pmod{17}$$

$$\equiv (-1) \times (-1) \times (-1) \times (7) \pmod{17}.$$

$$\therefore x \equiv 7 \pmod{17}$$

(iv). $a = 43$, $p = 23$ By Fermat's theorem we have

$$43^{22} \equiv 1 \pmod{23}$$

Multiply both sides by 43^{21}

$$43^{21}(43x) \equiv 43^{21} \times 17 \pmod{23}$$

$$x \equiv 43^{21} \times 17 \pmod{23}$$

$$\equiv (-3)^{21} \times 17 \pmod{23}$$

$$\equiv ((-3)^3)^7 \times 17 \pmod{23}$$

$$\equiv (-4)^7 \times 17 \pmod{23}$$

$$\equiv (-4)^3 \times (-4)^3 \times (-4 \times 17) \pmod{23}$$

$$\equiv 5 \times 5 \times (1) \pmod{23}$$

$$\equiv 2 \pmod{23}.$$

Prob. No ④ compute the residue of $2^{340} (\text{mod } 341)$

Sol:- $341 = 31 \times 11$

By Fermat's little theorem $2^{30} \equiv 1 (\text{mod } 31)$ and $2^{10} \equiv 1 (\text{mod } 11)$.

$$2^{340} \equiv (2^{10})^{34} \equiv 1 (\text{mod } 11)$$

$$2^{340} \equiv (2^{30})^{11} \times 2^{10} \equiv 1 \times 1 (\text{mod } 31)$$

$$\therefore 2^{340} \equiv 1 \times 1 (\text{mod } (11 \times 31))$$

$$\therefore 2^{340} \equiv 1 (\text{mod } 341).$$

Prob. No ⑤. compute the least residue of (i) $11^{16} + 17^{10} (\text{mod } 187)$ and (ii) $13^{18} + 19^{12} (\text{mod } 247)$.

Sol: (i) By Fermat's little theorem $11^{16} \equiv 1 (\text{mod } 17)$ and $17^{10} \equiv 1 (\text{mod } 11)$.

$$\therefore 11^{16} + 17^{10} \equiv 1 + 0 \equiv 1 (\text{mod } 17) \quad (\because 17 / 17^{10}).$$

$$17^{10} + 11^{16} \equiv 1 + 0 \equiv 1 (\text{mod } 11) \quad (\because 11 / 11^{16}).$$

$$\therefore 11^{16} + 17^{10} \equiv 1 \times 1 (\text{mod } (17 \times 11))$$

$$\equiv 1 (\text{mod } 187).$$

(ii) $247 = 13 \times 19$

By Fermat's little theorem $13^{18} \equiv 1 (\text{mod } 19)$ and $19^{12} \equiv 1 (\text{mod } 13)$

$$\therefore 13^{18} + 19^{12} \equiv 1 + 0 (\text{mod } 19) \quad (\because 19 / 19^{12})$$

$$19^{2} + 13^{18} \equiv 1 + 0 (\text{mod } 13) \quad (\because 13 / 13^{18})$$

$$13^{18} + 19^{12} \equiv 1 \times 1 (\text{mod } (13 \times 19))$$

$$\equiv 1 (\text{mod } 247).$$

Prob. No 6 Let $a^p \equiv a \pmod{q}$. and $a^q \equiv a \pmod{p}$. then Prove that $a^{pq} \equiv a \pmod{pq}$

Sol:- we know that $a^p \equiv a \pmod{p}$ and

$$a^q \equiv a \pmod{q}$$

$$a^{pq} \equiv (a^p)^q \pmod{p} \equiv a^q \pmod{p} \equiv a \pmod{p}$$

$$a^{pq} \equiv (a^q)^p \pmod{q} \equiv a^p \pmod{q} \equiv a \pmod{q}$$

Now $a^{pq} \equiv a \pmod{(p \times q)} \Rightarrow a^{pq} \equiv a \pmod{pq}$

Prob. No 7. Prove that $a^{pq} - a^p - a^q + a \equiv 0 \pmod{pq}$

Sol:- $a^p \equiv a \pmod{p}$

$$a^{pq} \equiv a^q \pmod{p}$$

$$a^{pq} \equiv (a^p - a) + a^q = a^p + a^q - a \pmod{p}.$$

ie $p / a^{pq} - a^p - a^q + a$

IIIly $q / a^{pq} - a^p - a^q + a$

Now p and q are relatively primes and $(p, q) = pq$

$\therefore pq / a^{pq} - a^p - a^q + a$

$\therefore a^{pq} - a^p - a^q + a \equiv 0 \pmod{pq}$.

Prob. No 8. $a^p \equiv b^p \pmod{p}$ Prove that $a \equiv b \pmod{p}$.

Sol:- $a^p \equiv a \pmod{p}$ and $b^p \equiv b \pmod{p}$

$p / a^p - a$ and $p / b^p - b$

$$p / (a^p - a - b^p + b)$$

$p / (a^p - b^p) + (a - b)$ $\quad$ ($\because a^p = b^p \Rightarrow p / a^p - b^p$

$\Rightarrow p / (a - b) \Rightarrow a \equiv b \pmod{p}$

Prob. No 9 Prove that $1^{p-1}+2^{p-1}+3^{p-1}+\dots+(p-1)^{p-1} \equiv -1 \pmod{p}$

Sol:- By Fermat's theorem

$$a^{p-1} \equiv 1 \pmod{p} \text{ if } (p,a)=1.$$

∴ it is true for $a = 1,2,3,4 \dots (p-1)$

∴ $1^{p-1} \equiv 1 \pmod{p}$, $2^{p-1} \equiv 1 \pmod{p} \dots (p-1)^{p-1} \equiv 1 \pmod{p}$

adding all these congruences we get

$$1^{p-1}+2^{p-1}+3^{p-1}+\dots+(p-1)^{p-1} \equiv (1+1+1+\dots+1) \pmod{p}.$$
$$\equiv (p-1) \pmod{p}.$$

But $p-1 \equiv -1 \pmod{p}$

∴ $1^{p-1}+2^{p-1}+3^{p-1}+\dots+(p-1)^{p-1} \equiv -1 \pmod{p}$.

Euler's theorem and Euler's phi function.

To evaluate $a^n \pmod{p}$ we shall use Fermat's little theorem if p is prime

Suppose p is not prime then we shall use Euler's theorem

ie $a^n \pmod{m}$

Defn:- (Euler's phi function)

$\phi(n)$ is the numbers from 1 to $(n-1)$ that are relatively prime to 'n'.

Ex 1. Compute $\phi(11)$ and $\phi(18)$.

Sol:- $\phi(11)$ of the numbers $\{1,2,3,4,5,6,7,8,9,10\}$ the numbers $1,2,3,4,5,6,7,8,9,10$ are relatively prime to 11. So $\phi(11)=10$.

$\phi(18)$ of the numbers $\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\}$

the numbers are $1,5,7,11,13,17$

∴ $\phi(18)=6$.

Result ①: A positive integer p is a prime if and only if $\phi(p) = p-1$

Proof:- If p is prime, all the numbers $1, 2, 3, 4 \cdots (p-1)$ are relatively prime to p. So $\phi(p) = p-1$

conversely, if p is not a prime then $p = a \cdot b$ for some $1 < ab < p$.

$\therefore$ $(a, p) \neq 1$ a is not relatively prime to p

$(b, p) \neq 1$ b is not relatively prime to p.

consequently $\phi(p) < p-1$

Result ②: let m be a positive integer, a is an integer relatively prime to m. $r_1, r_2 \cdots r_{\phi(m)}$ are the integers relatively prime to m (each $\leq m$). then $ar_1, ar_2, \cdots ar_{\phi(m)}$ are just a re-arrangement (permutation) of the integers $r_1, r_2 \cdots r_m$.

Proof:- Step ①. claim ar_i is relatively prime to m

Suppose not that is gcd of $ar_i, m > 1$ (in notation $(ar_i, m) > 1$) $d = (ar_i, m)$ and d is written as

$d = p \cdot d'$ (any no shall be written as product of primes)

Since d/ar_i $\quad p/ar_i \Rightarrow p/a$ (or) p/r_i

$\Rightarrow d/m \quad p/m$

If p/r_i then combining p/r_i and p/m. we get p is a common divisor for r_i and m

$\therefore$ $(r_i, m) > p$ r_i and m are not relatively prime which is contradiction to the hypothesis.

$\therefore$ we get p/a and p/m

p is a common divisor for a, m

$(a,m) > p$ a, m are not relatively prime which is contradiction to the given hypothesis.

$\therefore$ ar_i is relatively prime to m.

Step ②: No two integers ar_i and ar_j are equal

ie $ar_i \not\equiv ar_j \pmod{m}$

Suppose not ie $ar_i \equiv ar_j \pmod{m}$.

Since 'a' is relatively prime to 'm' we shall cancel 'a' and get $r_i \equiv r_j \pmod{m}$ which is contradiction

$\therefore$ $ar_i \not\equiv ar_j$.

Step ③: Also $ar_1, ar_2 \ldots ar_{\phi(m)}$ are relatively prime to m they are equal to any of $r_1 r_2 \ldots r_{\phi(m)}$ (which are also least residues of m relatively prime to m) in some order.

Euler's theorem: Let m be a positive integer and a any integer with $(a,m)=1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof:- Let $r_1, r_2 \ldots r_{\phi(m)}$ be least residues of m that are relatively prime to m.

Then by result ②

$ar_1, ar_2 \ldots a r_m$ are also relatively prime to m in some order.

and equal to $r_1 r_2 \ldots r_{\phi(m)}$ in some order.

$\therefore$ $ar_1\, ar_2 \ldots ar_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m}$

$a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m}$

Since $r_1, r_2 \ldots r_{\phi(m)}$ are relatively prime to m we can cancel them and get

$$a^{\phi(m)} \equiv 1(\mod m).$$

Result ③: Equivalent to fermat's little theorem we have $a^{\phi(m)} \equiv 1(\mod m) \Rightarrow a^{\phi(m)-1}$ is inverse of a modulo m

Result ④: the congruence $ax \equiv b(\mod m)$ has solutions $x \equiv a^{\phi(m)-1} b(\mod m)$.

Problems

Prob. No ①. Find the remainder when 245^{1040} is divided by 18

Sol: By Euler's theorem $a^{\phi(18)} \equiv 1(\mod 18)$ if a is relatively prime to 18.

$$245 \equiv 11 (\mod 18)$$

$$245^{1040} \equiv 11^{1040} (\mod 18)$$

$$\begin{array}{r} 13 \\ 18\overline{)245} \\ 18 \\ \hline 65 \\ 54 \\ \hline 11 \end{array}$$

By Euler's theorem, $11^6 \equiv 1 (\mod 18)$ since $\phi(18)=6$

$$245^{1040} \equiv 11^{1040} (\mod 18)$$

$$\equiv ((11)^6)^{173} 11^2 (\mod 18)$$

$$\equiv 1 \times 11^2 (\mod 18)$$

$$\equiv 121 (\mod 18)$$

$$\equiv 13 (\mod 18)$$

$$\begin{array}{r} 173 \\ 6\overline{)1040} \\ 6 \\ \hline 44 \\ 42 \\ \hline 20 \\ 18 \\ \hline 2 \end{array} \qquad \begin{array}{r} 6 \\ 18\overline{)121} \\ 108 \\ \hline 13 \end{array}$$

Prob. No②. Solve the congruence $35x \equiv 47 (\mod 24)$ Euler's theorem

Sol: 24 is not prime so use Euler's theorem

$\phi(24) = 8$ (∵ $\{1, 5, 7, 11, 13, 17, 19, 23\}$)

$11^8 \equiv 1 (\mod 24)$ (∵ By Euler's theorem)

$$35x \equiv 47 (\mod 24)$$

is reduced to $11x \equiv 23 \pmod{24}$ or equivalently

$11x \equiv -1 \pmod{24}$

$\therefore$ 11^7 is inverse of $11 \pmod{24}$

$$11x \equiv 23 \pmod{24}$$

$$x \equiv 11^7 \times 23 \pmod{24}$$

$$x \equiv 11^7 \times (-1) \pmod{24}.$$

$$11^2 \equiv 121 \equiv 1 \pmod{24}$$

$$\equiv (11^2)^3 \times 11 \times (-1) \pmod{24}$$

$$x \equiv -11 \pmod{24}$$

$$\therefore x \equiv 13 \pmod{24}.$$

Exercise 7.4 Koshy.

Prob. No ① compute (i) $\phi(21)$ (iii) $\phi(28)$.

Sol:- (i) $21 = 3 \times 7$

$\phi(3) = 2$ and $\phi(7) = 6$.

$\phi(21) = \phi(3) . \phi(7) = 12$

or equivalently

No relatively prime to 21 are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

So $\phi(21) = 12$.

(ii) $28 = 4 \times 7$ that are relatively prime

$\phi(4) = 2$ and $\phi(7) = 6$

$\therefore \phi(28) = \phi(4) \cdot \phi(7) = 12$

Verification 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27 are relatively prime to 28.

Prob. No ②. Find the remainder when the first integer is divided by the second (i) $7^{1020}, 15$ (ii) $25^{2550}, 18$ (iii) $79^{1776}, 24$ (iv) $199^{2020}, 28$.

Sol:- (i) $7^{1020}, 15$

15 is not prime. So use Euler's theorem

$$\phi(15) = \phi(3)\,\phi(5) = 8$$

By Euler's theorem $7^8 \equiv 1 \pmod{15}$

$$7^{1020} \equiv (7^8)^{127} \times 7^4 \pmod{15}$$
$$\equiv 1 \times 7^4 \pmod{15}$$
$$\equiv 7^2 \times 7^2 \pmod{15}$$
$$\equiv 4 \times 4 \pmod{15}$$
$$\equiv 1 \pmod{15}.$$

$$\begin{array}{r|l} & 127 \\ \hline 8 & 1020 \\ & \underline{8} \\ & 22 \\ & \underline{16} \\ & 60 \\ & \underline{56} \\ & \underline{4} \end{array}$$

(ii) $25^{2550}, 18$

18 is not a prime. So use Euler's theorem

$$\phi(18) = \phi(2)\,\phi(9) = 1 \times 6 = 6$$

By Euler's theorem $7^6 \equiv 1 \pmod{18}$

$$25^{2550} \equiv 7^{2550} \pmod{18}$$
$$\equiv (7^6)^{425} \pmod{18}$$
$$\equiv 1 \pmod{18}$$

$$\begin{array}{r|l} & 425. \\ \hline 6 & 2550 \\ & \underline{24} \\ & 15 \\ & \underline{12} \\ & 30 \\ & \underline{30} \\ & \underline{0} \end{array}$$

(iii) $79^{1776}, 24$

24 is not a prime. So use Euler's theorem

$$\phi(24) = \phi(3).\phi(8) = 2 \times 4 = 8$$

By Euler's theorem $a^8 \equiv 1 \pmod{24}$ if a is relatively prime to 24

$$79^{1776} \equiv 7^{1776} \pmod{24}$$

$\equiv (7^8)^{222} (\bmod 24)$

$\equiv 1 (\bmod 24)$

$$8 \overline{)1776}\ \ 222$$
16
17
16
16
16
0

(iv) $199^{2020}, 28$

28 is not a prime. So, use Euler's theorem

$\phi(28) = \phi(4) \cdot \phi(7) = 2 \times 6 = 12$

$\therefore$ By Euler's theorem $a^{12} \equiv 1 (\bmod 28)$ if a is relatively prime to 28

$199^{2020} \equiv 3^{2020} (\bmod 28)$

$\equiv (3^{12})^{168} \times 3^4 (\bmod 28)$

$\equiv 1 \times 81 (\bmod 28)$

$\equiv 25 (\bmod 28)$

$$12 \overline{)2020}\ \ 168$$
12
82
72
100
96
4

Prob. No ③ Find the one's digit in the decimal value of (i) 17^{6666} and (ii) 23^{7777}

Sol:- (i) Find the remainder when 17^{6666} is divided by 10.

10 is not a prime so use Euler's theorem

$\phi(10) = 4 \quad (\because \{1, 3, 7, 9\})$

$\therefore$ By Euler's theorem $a^4 \equiv 1 (\bmod 10)$ if a is relatively prime to 10.

$17^{6666} \equiv 7^{6666} (\bmod 10)$

$\equiv (7^4)^{1666} \times 7^2 (\bmod 10)$

$\equiv 1 \times 7^2 (\bmod 10)$

$\equiv 9 (\bmod 10)$.

$$4 \overline{)6666}\ \ 1666$$
4
26
24
26
24
26
24
2

(ii) Find the remainder when 7^{1030} is divided by 16.

16 is not a prime So use Euler's theorem

$\phi(16) = 8$ $(\because \{1, 3, 5, 7, 9, 11, 13, 15\})$

$\therefore$ By Euler's theorem $a^8 \equiv 1 \pmod{16}$ if a is relatively prime to 16

$$7^{1030} \equiv (7^8)^{128} \times 7^6 \pmod{16}$$
$$\equiv 7^2 \times 7^2 \times 7^2 \pmod{16}$$
$$\equiv 1 \times 1 \times 1 \pmod{16}$$
$$\equiv 1 \pmod{16}$$

128
8) 1030
8
23
16
70
64
6

Prob. No (4). Find one's digit in the hexadecimal value of (i) 7^{1030} and (ii) 13^{4444}.

Sol:- (i) Find the remainder when 23^{7777} is divided by 10

10 is not a prime. So, use Euler's theorem

$\phi(10) = 4$ $a^4 \equiv 1 \pmod{10}$ If a is relatively prime to 10

$$23^{7777} \equiv 3^{7777} \pmod{10}$$
$$\equiv (3^4)^{1944} \times 3 \pmod{10}$$
$$\equiv 3 \pmod{10}$$

1944
4) 7777
4
37
36
17
16
17
16
1

(ii) Find the remainder when 13^{4444} is divided by 16.

16 is not a prime So use Euler's theorem

$\phi(16) = 8$, $a^8 \equiv 1 \pmod{16}$ if 'a' is relatively prime to 16

$$13^{4444} \equiv (13^8)^{555} \, 13^4 \pmod{16}$$
$$\equiv 1 \times 13^2 \times 13^2 \pmod{16}$$

555
8) 4444
40
44
40
44
40
4

$\equiv 9\times 9 \pmod{16}$

$\equiv 1 \pmod{16}$.

Prob. No (5). Solve the linear congruence (i) $7x\equiv 8 \pmod{10}$ and (ii) $17x \equiv 20 \pmod{24}$.

Sol:- (i) $7x\equiv 8 \pmod{10}$

10 is not a prime so use Euler's theorem

$\phi(10) = \phi(2)\cdot\phi(5) = 1\times 4$

$7^4 \equiv 1 \pmod{10}$

$\therefore 7^3$ is the inverse of $7 \pmod{10}$.

Multiply by 7^3 both sides

$7^3(7x) \equiv 7^3\times 8 \pmod{10}$

$x \equiv 7^3\times 8 \pmod{10}$

$x \equiv 7^2\times 7\times 8 \pmod{10}$

$\equiv 9\times 7\times 8 \pmod{10}$

$\equiv 3\times 8 \pmod{10}$

$x \equiv 4 \pmod{10}$.

(ii) $17x \equiv 20 \pmod{24}$

24 is not a prime so use Euler's theorem

$\phi(24) = \phi(3)\cdot\phi(8) = 2\times 4 = 8$

$17^8 \equiv 1 \pmod{24}$

So 17^7 is the inverse of $17 \pmod{24}$

Multiply by 17^7 both sides

$17^7(17x) \equiv 17^7\times 20 \pmod{24}$

$x \equiv 17^7\times 20 \pmod{24}$

$\equiv 17\times 17^2\times 17^2\times 17^2\times 17^2\times 20 \pmod{24}$

$\equiv 17\times 1\times 1\times 1\times 1\times 20 \pmod{24}$

$x \equiv 4 \pmod{24}$.

Prob. No 6. Solve the linear congruence (i) $23x \equiv 17 \pmod{12}$ is reduced to $11x \equiv 5 \pmod{12}$ (ii) $25x \equiv 13 \pmod{18}$ is reduced to $7x \equiv 13 \pmod{18}$

Sol: (i) 12 is not a prime so use Euler's theorem

$$\phi(12) = \phi(3).\phi(4) = 2\times2 = 4$$

By Euler's theorem $11^4 \equiv 1 \pmod{12}$ so 11^3 is the inverse of $11 \pmod{12}$

Multiply by 11^3 both sides

$$11^3(11x) \equiv 11^3\times5 \pmod{12}$$

$$x \equiv 11^2\times11\times5 \pmod{12}$$

$$\equiv 1\times7 \pmod{12}$$

$$\equiv 7 \pmod{12}$$

(ii) 18 is not a prime so use Euler's theorem

$$\phi(18) = \phi(2).\phi(9) = 1\times6 = 6$$

By Euler's theorem $7^6 \equiv 1 \pmod{18}$ So 7^5 is the inverse of $7 \pmod{18}$

Multiply by 7^5 both sides

$$7^5(7x) \equiv 7^5\times13 \pmod{18}$$

$$x \equiv 7^2\times7^2\times7\times13 \pmod{18}$$

$$\equiv (-5)(-5)\times1 \pmod{18}$$

$$\equiv 25 \pmod{18}$$

$$x \equiv 7 \pmod{18}$$

Prob. No 7 Evaluate (i) $\phi(105)$ (ii) $\phi(462)$

Sol:- (i) $105 = 3\times5\times7$ all are relatively prime

$$\phi(105) = \phi(3)\phi(5)\phi(7) = 2\times4\times6 = 48$$

(ii) $462 = 7\times6\times11$ all are relatively prime

$$\phi(462) = \phi(7)\,\phi(6)\,\phi(11)$$
$$= 6 \times 2 \times 10$$
$$= 120.$$

Prob. No (8). Verify (i) $1+9+9^2+\cdots+9^{23} \equiv 0 \pmod{35}$

(ii) $1+11+11^2+\cdots+11^{31} \equiv 0 \pmod{51}$

Sol:- (i) 35 is not prime. So let us make use of Euler's theorem

9 and 35 are relatively prime

$$\phi(35) = \phi(5)\cdot\phi(7) = 4 \times 6 = 24$$

$$\therefore \; 9^{24} \equiv 1 \pmod{35}.$$

Now $1+x+x^2+\cdots+x^n = \dfrac{1-x^{n+1}}{1-x} = \dfrac{x^{n+1}-1}{x-1}$

$$1+9+9^2+9^3+\cdots+9^{23} = \frac{9^{24}-1}{9-1} \pmod{35} \equiv 0 \pmod{35}$$

(ii) 51 is not prime. So let us make use of Euler's theorem

$\phi(51) = \phi(17)\cdot\phi(3) = 16 \times 2 = 32$ since 11 and 51 are relatively prime

$$11^{32} \equiv 1 \pmod{51}$$

Now $1+11+11^2+11^3+\cdots+11^{31} \equiv \dfrac{11^{32}-1}{11-1} \pmod{51} \equiv 0 \pmod{51}$.

Prob. No (9) (i) If a and b are relatively prime, then Prove that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$.

(ii) If p and q are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

Sol:- (i) By Euler's theorem $a^{\phi(b)} \equiv 1 \pmod{b}$ and $b^{\phi(a)} \equiv 1 \pmod{a}$

$a^{\phi(b)} + b^{\phi(a)} \equiv 1+0 \pmod{b}$ (since b divides $b^{\phi(a)}$)

$a^{\phi(b)} + b^{\phi(a)} \equiv 0+1 \pmod a$ (since a divides $a^{\phi(b)}$)

$\therefore a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$.

(ii) put $a=p$ $b=q$ in the above

$\phi(a) = \phi(p) = p-1$ since p is prime

$\phi(b) = \phi(q) = q-1$ since q is prime

we get $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

Prob. No ⑩. Every integer 'n' relatively prime to 10 (ie $(n,10)=1$) divides some integer N consisting of all 1's (for eg 3/111 7/111111 etc)

Sol:- Given 'n' is relatively prime to 10. So by Euler's theorem

$10^{\phi(n)} \equiv 1 \pmod n$ So 'n' divides $(10^{\phi(n)} - 1)$

the number $10^{\phi(n)} - 1$ is integer consisting of all 9's which can be written as $9 \times 111111\ldots$

$\therefore n / 10^{\phi(n)} - 1$ ie $n/9999\ldots$ ie $n/9(1111\ldots)$

Case (i) $n > 10$

then 'n' cannot divide 9

$\therefore n/(1111\ldots)$ Hence the proof

ie n divides a no consisting of all 1's

Case (ii) $n \leq 10$

possibility① ie $n=1$ 1/1 possibility② ie $n=3$ 3/111

possibility③ ie $n=7$ 7/111111 possibility④ ie $n=9$

9/111111111 ($\because$ Took only number's that are relatively prime to 10)

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

Proof:- $\left.\begin{array}{l}\text{No. of integers} \\ \text{relatively prime to } p^n \\ \phi(p^n)\end{array}\right\} = \left(\begin{array}{l}\text{No. of positive} \\ \text{integers} \le p^n\end{array}\right) - \left(\begin{array}{l}\text{No of integers that} \\ \text{are not relatively} \\ \text{prime to } p^n\end{array}\right)$

$= p^n - |\{1, p, 2p, 3p, \ldots p^{n-1}, p\}|$

$= p^n - p^{n-1}$

Ex① Compute $\phi(15625)$

Sol:- $\phi(15625) = \phi(5^6) = 5^6 - 5^5 = 12500$

Computational technique

Already we saw $\phi(p^e) = p^e(1-\frac{1}{p})$

So, $\phi(p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}) = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_m})$

Ex① Evaluate $\phi(221)$ and $\phi(6125)$

Sol:- $\phi(221) = \phi(13 \times 17) = 13 \times 17\,(1-\frac{1}{13})(1-1/17)$

$= 13 \times 17\left(\frac{12}{13}\right)\left(\frac{16}{17}\right) = 192.$

$\phi(6125) = \phi(5^3 \times 7^2) = 5^3 \times 7^2(1-\frac{1}{5})(1-\frac{1}{7})$

$= 5^3 \times 7^2 \times \left(\frac{4}{5}\right) \times \left(\frac{6}{7}\right)$

$= 5^2 \times 7 \times 4 \times 6 = 4200$

Ex②. Compute $\phi(666)$ and $\phi(1976)$

Sol:- $\phi(666) = \phi(2 \cdot 3^2 \cdot 37)$

$= 2 \times 3^2 \times 37\,(1-1/2)(1-1/3)(1-1/37)$

$= 2 \times 3^2 \times 37 \times (1/2)(2/3) \times (36/37)$

$= 2 \times 36 \times 3 = 216.$

$\phi(1976) = \phi(2^3 \times 13 \times 19)$

$= 2^3 \times 13 \times 19\,(1-1/2)(1-1/13)(1-1/19)$

$$= 2^3 \times 13 \times 19 \times (1/2) \times (12/13) \times (18/19)$$

$$= 2^2 \times 12 \times 18$$

$$= 864.$$

Euler-phi function.

Result ① let m and n are relatively prime positive integers and r any integer. then the integers $r, m+r, 2m+r \ldots (n-1)m+r$ are congruent to modulo n.to $0,1,2,3 \ldots (n-1)$ in some order.

Proof:- Suppose $km+r \equiv lm+r \pmod{n}$ then $n/(k-l)m$

since n,m are relatively prime $n/k-l$. Since $0 \leq k,l < n$

$\Rightarrow k-l=0$ is the only possibility $\Rightarrow k=l$.

So no two integers of the form $r, m+r, 2m+r \ldots (n-1)m+r$ are equal is congruent modulo n.

Result ②. The Euler phi function ϕ is multiplicative

ie $\phi(m,n) = \phi(m)\cdot\phi(n)$ if m and n are relatively prime.

Proof:- Consider the integers from 1 to mn and arrange them as follows

$$\begin{array}{llllll}
\text{Row } 1: & 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
\text{Row } 2: & 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
\text{Row } 3: & 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\vdots & & \vdots & \vdots & & \vdots \\
\text{Row } r: & r & m+r & 2m+r & & (n-1)m+r \\
\vdots & \vdots & \vdots & \vdots & & \vdots \\
\text{Row } m: & m & m+m & 3m & & nm
\end{array}$$

Argument ①: If r is not relatively prime to m then no element in that row is relatively prime to mn.

Proof:- Since $d = (r, m)$ $d > 1$ then d/r d/m

So $d/km+r$ $\forall k$ and d/mn

So $(km+r)$ and mn have a common factors and are not relatively prime to mn.

So all the elements in that row are not relatively prime to mn.

Observation ①: If at all there is an integer. $km+i$ is relatively prime to mn then it is in i^{th} row where i is relatively prime to m.

Argument ②: There are $\phi(m)$ are rows which are relatively prime to m.

Proof:- It is trivial by the definition of $\phi(m)$.

Note ①: In those row (or in any row) not all the elements are relatively prime to mn.

There are only $\phi(n)$ elements that are relatively prime to mn. (By result ①).

So In total: there are $\phi(m)$ rows that are relatively prime to m and each row has $\phi(n)$ elements that are relatively prime to mn.

Combining these two, we have $\phi(mn) = \phi(m) \cdot \phi(n)$.

Exercise 8.1 Koshy

Prob. No ① Compute (i) $\phi(1105)$ (ii) $\phi(2047)$ (iii) $\phi(16860)$ (iv) $\phi(98865)$ (v) $\phi(183920)$

Sol:- (i) $1105 = 13 \times 17 \times 5$

$\phi(1105) = \phi(13) \times \phi(17) \times \phi(5) = 12 \times 16 \times 4 = 768$

(ii) $2047 = 23 \times 89$

$\phi(2047) = \phi(23) \times \phi(89) = 22 \times 88 = 1936$

(iii) $6860 = 686 \times 10 = 2 \times 343 \times 10 = 2 \times 7^3 \times 2 \times 5 = 2^2 \times 5 \times 7^3$

$\phi(6860) = 2^2 \times 5 \times 7^3 \times (1-1/2) \times (1-1/5) \times (1-1/7)$

$= 2^2 \times 5 \times 7^3 \times (1/2)(4/5)(6/7)$

$= 8 \times 7 \times 6 = 2352.$

(iii) $98865 = 19773 \times 5 = 3 \times 6591 \times 5 = 3^2 \times 2197 \times 5$

$= 3^2 \times 13 \times 169 \times 5 = 3^2 \times 13^3 \times 5$

$\phi(98865) = 3^2 \times 13^3 \times 5 \times (1-1/3) \times (1-1/13) \times (1-1/5)$

$= 3^2 \times 13^3 \times 5 \times 2/3 \times 12/13 \times 4/5$

$= 3 \times 13^2 \times 2 \times 12 \times 4$

$= 48672$

(iv) $183920 = 20 \times 9196 = 5 \times 4 \times 4 \times 2299 = 5 \times 4^2 \times 11 \times 209$

$= 5 \times 2^4 \times 11 \times 11 \times 19 = 2^4 \times 5 \times 11^2 \times 19 \times (1-1/2)(1-1/5)(1-1/11)(1-1/19).$

$= 2^4 \times 5 \times 11^2 \times 19 \times (1/2)(4/5)(10/11)(18/19)$

$\therefore \phi(183920) = 63360.$

Prob. No 2. Compute (i) $\phi(7!)$ (ii) $\phi(11!)$

Sol: (i) $\phi(7!) = \phi(1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7)$

$= \phi(2^4 \times 3^2 \times 5 \times 7)$

$= 2^4 \times 3^2 \times 5 \times 7 \times (1-1/2) \times (1-1/3) \times (1-1/5) \times (1-1/7)$

$= 2^4 \times 3^2 \times 5 \times 7 \times (1/2)(2/3)(4/5)(6/7)$

$= 2^7 \times 3^2 = 1152$

(ii) $\phi(11!) = \phi(2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11)$

$= \phi(2 \times 3 \times 2^2 \times 5 \times 2 \times 3 \times 7 \times 2^3 \times 3^2 \times 2 \times 5 \times 11)$

$= \phi(2^8 \times 3^4 \times 5^2 \times 11 \times 7)$

$= 2^8 \times 3^4 \times 5^2 \times (1-1/2) \times (1-1/3) \times (1-1/5) \times 10 \times 6$

$= 2^8 \times 3^4 \times 5^2 \times (1/2)(2/3)(4/5)\, 10 \times 6$

$= 2^{10} \times 3^3 \times 60$

$= 1658880.$

Prob. No ③. Find the positive integers 'n' such that (i) $\phi(n)=n$ (ii) $\phi(n)=4$ (iii) $\phi(n)=6$ (iv) $\phi(n)=12$.

Sol:- (i) no such integer exists; $\phi(n)$ is maximum when n is a prime except for $n=1$ and $\phi(p)=p-1$

(ii) $\phi(n)=4 \Rightarrow n-1=4$ ($\because n=5$ is a prime)

$\therefore \phi(5)=4.$

(iii) $\phi(n)=6 \Rightarrow n-1=6$ ($\because n=7$ is a prime)

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

(iv) $\phi(n)=12 \Rightarrow n-1=12$ ($\because n=13$ is a prime)

$\therefore \phi(13)=12.$

Prob. No ④ Derive a formula for $\phi(pq)$ where p and q are twin primes

Sol:- Assume $q=p+2$

$\phi(p(p+2)) = \phi(p)\,\phi(p+2) = (p-1)(p+1) = p^2-1.$

Prob. No ⑤ Find the twin primes p and q if (i) $\phi(pq)=120$ (ii) $\phi(pq)=288$

Sol:- (i) By above prob. $p^2-1=120 \Rightarrow p^2=121 \Rightarrow p=11$

$\therefore$ the twin primes are 11 and 13.

(ii) By above prob $p^2-1=288 \Rightarrow p^2=289 \Rightarrow p=17$

$\therefore$ the twin primes are 17 and 19.

Prob. No ⑥ If p and q are twin primes with $p<q$. Show that $\phi(q)=\phi(p)+2$.

Sol:- p is prime $\phi(p) = p-1$

q is prime $\phi(q) = q-1$

and since $q = p+2$

$$\phi(p+2) = (p+2)-1 = p+1 = p-1+2 = \phi(p)+2$$

Prob. No (7) If $n = 2^k$ then prove that $\phi(n) = n/2$

Sol:- $\phi(n) = \phi(2^k) = 2^k(1-1/2) = 2^k \cdot 1/2 = \frac{2^k}{2} = n/2$

Prob. No (8). Let f_n denote a Fermat prime. then prove that $\phi(f_n) = f_n - 1$

Sol:- Assume $f_n = 2^n+1$ is a Fermat's prime.

$$\phi(f_n) = \phi(2^n+1) = 2^n+1-1 = f_n - 1$$

$$\therefore \phi(f_n) = f_n - 1$$

Prob. No (9). (i) Prove that $\phi(4n) = 2\phi(n)$ when 'n' is odd.

(ii) Prove that $\phi(2n) = \begin{cases} \phi(n) & \text{if } n \text{ is odd} \\ 2\phi(n) & \text{if } n \text{ is even} \end{cases}$

Sol:- (i) $\phi(4n) = \phi(2^2 \cdot n) = \phi(2^2) \cdot \phi(n)$ since 2^2 and n are relatively prime

$$= \phi(n) \cdot 2^2(1-1/2)$$

$$= \phi(n) \cdot 2.$$

(ii) Case (i) if n is odd

$\phi(2n) = \phi(2) \cdot \phi(n)$ since 2 and n are relatively prime

$$= 1 \cdot \phi(n)$$

$$= \phi(n).$$

case (ii) if n is even. Take $n = 2^r m$ where m is odd.

$$\phi(2n) = \phi(2 \cdot 2^r m) = \phi(2^{r+1} \cdot m) = \phi(2^{r+1}) \cdot \phi(m)$$

($\because$ 2^{r+1} and m are relatively prime)

$$= 2^{r+1}(1-1/2)\,\phi(m).$$

$$= 2^r \cdot \phi(m)$$
$$= 2 \cdot 2^{r-1} \phi(m)$$
$$= 2 \cdot 2^r (1 - 1/2) \, \phi(m)$$
$$= 2 \cdot \phi(2^r) \cdot \phi(m)$$
$$= 2 \cdot \phi(2^r \cdot m).$$
$$= 2 \cdot \phi(n)$$

Prob. No ⑩. (i) If $n = 2^j, j \geq 1$ then P.T $n = 2\phi(n)$

(ii) Prove that $\phi(2^{2k+1})$ is a square

(iii) If $\phi(p^l)$ is a square then $p-1$ must be a square and l must be odd.

Sol:- (i) $\phi(2^j) = 2^j(1 - 1/2) = 2^j/2 = n/2$

ie $\phi(n) = n/2 \Rightarrow n = 2\phi(n)$.

(ii) $\phi(2^{2k+1}) = 2^{2k+1}(1 - 1/2) = \dfrac{2^{2k+1}}{2} = 2^{2k} = (2^k)^2$

which is the square of 2^k.

(iii) $\phi(p^l) = p^l(1 - 1/p) = p^l\left(\dfrac{p-1}{p}\right) = p^{l-1}(p-1)$

$\phi(p^l)$ is a square assume $\phi(p^l) = n^2$

$p^{l-1}(p-1) = n^2$

$\therefore p / n^2 \Rightarrow p/n \quad \therefore n = p^r q^m$

$p^{l-1}(p-1) = p^{2r} \cdot q^{2m}$

$\therefore l = 2r+1$ is odd

$\therefore p-1 = (q^m)^2$ is a square.

Prob. No ⑪. Let $(m,n) = p$. then $\phi(m,n) = \dfrac{p}{p-1} \phi(m) \cdot \phi(n)$.

Sol:- $(m,n) = p$ without loss of generality.

Assume $m = p^r . k$ $n = p.l$ k has no factor of P and p,k,l are relatively prime to each other.

$$\phi(n) = \phi(pl) = \phi(p).\phi(l) = (p-1)\phi(l) \rightarrow \textcircled{1}$$

$$\phi(p^r) = p^r - p^{r-1} = p^r(1 - 1/p) \rightarrow \textcircled{2} .$$

$$\phi(mn) = \phi(p^r k . p.l) = \phi(p^{r+1})\phi(k).\phi(l)$$

$$= (p^{r+1} - p^r)\phi(k)\phi(l)$$

$$= p(p^r - p^{r-1})\phi(k)\phi(l)$$

$$= p(\phi(p^r))\phi(k)\phi(l)$$

$$= p \; \phi(p^r k)\phi(l)$$

$$= p.\phi(m).\phi(l)$$

$$= \frac{p}{p-1}\phi(m).(p-1)\phi(l)$$

$$= \frac{p}{p-1}\phi(m)\phi(p).\phi(l)$$

$$= \frac{p}{p-1}\phi(m)\phi(pl).$$

$$= \frac{p}{p-1}\phi(m).\phi(n).$$

Prob. No $\textcircled{12}$. Let $(m,n) = d$ Prove that $\phi(mn) = \frac{d}{\phi(d)}\phi(m).\phi(n)$

Sol:- Step $\textcircled{1}$: $d = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$

$$\phi(d) = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}(1 - 1/p_1)(1 - 1/p_2)\ldots(1 - 1/p_k)$$

$$d^r = p_1^{re_1} p_2^{re_2} \ldots p_k^{re_k}$$

$$\phi(d^r) = p_1^{re_1} p_2^{re_2} \ldots p_k^{re_k}(1 - 1/p_1)(1 - 1/p_2)\ldots(1 - 1/p_k)$$

$$\frac{\phi(d^r)}{\phi(d)} = d^{r-1} \Rightarrow \phi(d^r) = d^{r-1}\phi(d) \rightarrow \textcircled{1}.$$

Step ② $(m,n)=d$

without loss of generality. Assume $n = d\cdot l$ where d and l are relatively prime

$\therefore m = dk$ ($\because$ k has no factor of d) $n = dl$ k and l are relatively prime

$$\phi(n) = \phi(dl) = \phi(d)\cdot\phi(l) \rightarrow ②$$

$$\phi(mn) = \phi(d^{r+1}kl) = \phi(d^{r+1})\,\phi(k).\phi(l).$$

$$= d^{r}\phi(d)\,\phi(k)\,\phi(l)$$

$$= d^{r}\phi(k)\,\phi(dl)$$

$$= d^{r}\phi(k)\,\phi(n).$$

$$= \frac{d^{r}\phi(d).\,\phi(k)\,\phi(n)}{\phi(d)}$$

$$= \frac{d}{\phi(d)}\,d^{r-1}\phi(d).\,\phi(k)\,\phi(n).$$

$$= \frac{d}{\phi(d)}\,\phi(d^{r})\,\phi(k)\,\phi(n).$$

$$= \frac{d}{\phi(d)}\,\phi(d^{r}k)\,\phi(n).$$

$$\phi(m,n) = \frac{d}{\phi(d)}\,\phi(m)\,\phi(n)$$

Prob. No ⑬: Compute (i) $\phi(n^2) = \phi(n).n$ (ii) $\phi(48)$ (iii) $\phi(90)$ (iv) $\phi(375)$ (v) $\phi(1690)$.

Sol:- (i) By known result $\phi(m,n) = \frac{d}{\phi(d)}\,\phi(m).\,\phi(n)$

$(n,n)=n$

$$= \frac{n}{\phi(n)}\,\phi(n).\,\phi(n)$$

$$= n\phi(n).$$

(ii) $48 = \underset{m\ \ n}{12\times 4}$ $(m,n) = 4 = d.$

$\phi(48) = \phi(mn) = \frac{d}{\phi(d)} \phi(m)\cdot\phi(n) = \frac{4}{\phi(4)} \phi(12)\phi(4) \cdot$

$= 4\cdot\phi(12) = 4\phi(4)\cdot\phi(3)$

$= 4\phi(2^2)\cdot\phi(3)$

$= 4(2^2-2)\phi(3)$

$= 8 \times 2 = 16.$

(iii) $90 = \underset{m}{30} \times \underset{n}{3}$ $(30,3) = 3$

$\phi(90) = \phi(mn) = \frac{3}{\phi(3)} \phi(30)\phi(3) = 3\phi(30) = 3\phi(2\times3\times5)$

$= 3\phi(2)\phi(3)\phi(5)$

$= 3\times1\times2\times4$

$= 24.$

(iv) $375 = 25 \times 15$ $(25,15) = 5$

$\phi(375) = \phi(mn) = \frac{5}{\phi(5)} \phi(25)\times\phi(15)$

$= \frac{5}{\phi(5)} \phi(5^2)\phi(3)\phi(5).$

$= 5\times2\times(5^2-5)$

$= 200$

(v) $1690 = \underbrace{13\times5}_{m} \times \underbrace{13\times2}_{n}$ $(m,n) = 13$

$\phi(1690) = \phi(mn) = \frac{13}{\phi(13)} \phi(13\times5)\cdot\phi(13\times2)$

$= \frac{13}{\phi(13)} \phi(13)\phi(5)\phi(13)\phi(2)$

$= 13\times4\times12\times1 = 624.$

The Tau and Sigma Functions

Defn: (Tau and Sigma functions)

Let n be a positive integer

$\tau(n)$ is the number of positive factors of n is given by

$$\tau(n) = \sum_{d/n} 1.$$

$\sigma(n)$ is the sum of positive factors of n is given by

$$\sigma(n) = \sum_{d/n} d.$$

Result ①: If f is a multiplicative function, then $F(n) = \sum_{d/n} f(d)$ is also multiplicative

Proof:- Assume that 'm' and 'n' are relatively prime integers

Take $F(mn) = \sum_{d/mn} f(d)$

Since m and n are relatively prime, there is no common divisor d for both m and n.

So if there is a divisor d for mn it can be written as $d = d_1 d_2$ where d_1/m and d_2/n such that d_1 and d_2 are relatively prime

$\therefore f(d_1 d_2) = f(d_1) f(d_2)$ (as $f(d)$ is multiplicative)

$$F(mn) = \sum f(d_1 d_2) = \sum_{d_1/m} \Big(\sum_{d_2/n} f(d_2) \Big) f(d_1)$$

$$= \sum_{d_1/m} F(n) \cdot f(d_1) = F(n) \sum_{d_1/m} f(d_1)$$

$$\therefore F(mn) = F(n) \cdot F(m).$$

$\therefore F$ is also multiplicative

corollary ① Take $f(d)=1$. then $\sum_{d/n} f(d) = \sum_{d/n} 1 = \tau(n)$

$\tau(n)$ is multiplicative

Take $g(d)=d$. then $\sum_{d/n} g(d) = \sum_{d/n} d = \sigma(n)$

$\sigma(n)$ is multiplicative

Ex ① Find $\tau(36)$ and $\sigma(36)$

Sol:- $36 = 9 \times 4$

$\tau(9) = 3 \quad \tau(4) = 3$ $\quad \{1,3,9\}$

$\sigma(9) = 13 \quad \sigma(4) = 7$ $\quad \{1,2,4\}$

$\therefore \tau(36) = 9$ and $\sigma(36) = 91$

Result ②: let p and prime and l any positive integer. then

Prove that $\tau(p^l) = l+1$; $\sigma(p^l) = \dfrac{p^{l+1}-1}{p-1}$

proof:- For p^l the positive factors are $1, p, p^2, p^3, \ldots, p^l$

ie there are $(l+1)$ factors and $\tau(p^l) = l+1$

and $\sigma(p^l) = 1 + p + p^2 + \cdots + p^l = \dfrac{p^{l+1}-1}{p-1}$.

Result ③ let n be a positive integer $n = p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k}$. then

$\tau(n) = (l_1+1)(l_2+1)\ldots(l_k+1)$ and

$$\sigma(n) = \frac{p_1^{l_1+1}-1}{p_1-1} \cdot \frac{p_2^{l_2+1}-1}{p_2-1} \cdots \frac{p_k^{l_k+1}-1}{p_k-1}$$

proof: $n = p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k}$

By result ①, since $\tau(n)$ is multiplicative

$\tau(n) = \tau(p_1^{l_1})\, \tau(p_2^{l_2}) \ldots \tau(p_k^{l_k})$

$= (l_1+1)(l_2+1)\ldots(l_k+1)$ ($\because$ by result ②).

Similarly, by result ① since $\sigma(n)$ is multiplicative

$$\sigma(n) = \sigma(p_1^{l_1})\,\sigma(p_2^{l_2})\cdots\sigma(p_k^{l_k})$$

$$= \frac{p_1^{l_1+1}-1}{p_1-1}\cdot\frac{p_2^{l_2+1}-1}{p_2-1}\cdots\frac{p_k^{l_k+1}-1}{p_k-1} \quad (\because \text{by result ②}).$$

Ex ②. Compute $\tau(6120)$ and $\sigma(6120)$

Sol:- $6120 = 10\times 612 = 10\times 9\times 68 = 2\times 5\times 3^2\times 2^2\times 17$

$= 2^3\times 3^2\times 5\times 17.$

By result ③

$$\tau(6120) = (3+1)(2+1)(1+1)(1+1) = 48$$

$$\sigma(6120) = \frac{2^4-1}{2-1}\times\frac{3^3-1}{3-1}\times\frac{5^2-1}{5-1}\times\frac{17^2-1}{17-1}$$

$$= 15\times\frac{26}{2}\times\frac{24}{4}\times\frac{288}{16}$$

$$= 21060.$$

Exercise 8.2 (Koshy)

Prob. No ① Compute (i) $\tau(2187)$ and $\sigma(2187)$ and (ii) $\tau(44982)$ and $\sigma(44982)$

Sol:- (i) $2187 = 9\times 243 = 9\times 9\times 27 = 3^2\times 3^2\times 3^3 = 3^7$

$$\tau(2187) = \tau(3^7) = 7+1 = 8.$$

$$\sigma(2187) = \sigma(3^7) = \frac{3^8-1}{3-1} = 3280$$

(ii) $44982 = 2\times 22491 = 2\times 9\times 2499 = 2\times 3^2\times 7\times 357$

$= 2\times 3^2\times 7\times 3\times 119 = 2\times 3^3\times 7\times 7\times 17$

$= 2\times 3^3\times 7^2\times 17$

$$\tau(44982) = (1+1)(3+1)(2+1)(1+1) = 48$$

$$\sigma(44982) = \frac{2^2-1}{2-1}\;\frac{3^4-1}{3-1}\;\frac{7^3-1}{7-1}\;\frac{17^2-1}{17-1}$$

$$= 3 \times \frac{80}{2} \times \frac{48}{6} \times \frac{288}{16}$$

$$= 3 \times 40 \times 8 \times 18$$

$$= 17280.$$

Prob. No (2). (i) Identify positive integers with exactly three positive divisors

(ii) $n = p_1 p_2 \dots p_k$ be a product of distinct prime Find $\tau(n)$ and $\sigma(n)$.

Sol:- (i) $1, p, p^2$ are three factors of p^2

(ii) $\tau(n) = (1+1)(1+1)\dots(1+1)$ k times $= 2k$.

$$\sigma(n) = \frac{p_1^2-1}{p_1-1} \cdot \frac{p_2^2-1}{p_2-1} \cdots \frac{p_k^2-1}{p_k-1}$$

$$= \frac{(p_1-1)(p_1+1)}{(p_1-1)}\;\frac{(p_2-1)(p_2+1)}{(p_2-1)} \cdots \frac{(p_k-1)(p_k+1)}{(p_k-1)}$$

$$= (p_1+1)(p_2+1)\cdots(p_k+1).$$

Prob. No (3). (i) Find $\tau(2^{2l})$ and $\sigma(2^{2l})$

(ii) Find the product of positive factors of p^l.

Sol:- (i) $\tau(2^{2l}) = 2l+1$

$$\sigma(2^{2l}) = \frac{2^{2l+1}-1}{2-1} = 2^{2l+1}-1.$$

(ii) the positive factors are $1, p, p^2, p^3 \dots p^l$

Its product is $1.p.p^2.p^3 \dots p^l = p^{1+2+3+\dots+l}$
$= p^{\frac{l(l+1)}{2}}$.

Prob. No ④. Compute $\tau(2^{p-1}(2^p-1))$ and $\sigma(2^{p-1}(2^p-1))$

Sol:- 2^{p-1} is an even number and 2^p-1 is prime, So they are relatively prime

$$\tau(2^{p-1}(2^p-1)) = (p-1+1)(1+1) = 2p$$

$$\sigma(2^{p-1}(2^p-1)) = \frac{2^p-1}{2-1} \cdot \frac{(2^p-1)^{1+1}-1}{(2^p-1)-1} = \frac{(2^p-1)((2^p-1)^2-1)}{2^p-2}$$

$$= (2^p-1)\frac{(2^p-1-1)(2^p-1+1)}{2^p-2}$$

$$= \frac{(2^p-1)(2^p-2)\,2^p}{2^p-2}$$

$$\therefore \sigma(2^{p-1}(2^p-1)) = 2^p(2^p-1).$$

Prob. No ⑤. Let n be the product of a pair of twin primes, p being the smaller of the two. Compute $\tau(n)$ and $\sigma(n)$. Also show that $\sigma(p+2) = \sigma(p)+2$

Sol:- $p, p+2$ be the twin primes

$$n = p(p+2)$$

$$\tau(n) = (1+1)(1+1) = 4$$

$$\sigma(n) = \frac{p^2-1}{p-1}\,\frac{(p+2)^2-1}{(p+2)-1} = \frac{(p-1)(p+1)}{p-1}\,\frac{((p+2)-1)((p+2)+1)}{(p+2-1)}$$

$$= (p+1)(p+3)$$

$$\sigma(p+2) = \frac{(p+2)^2-1}{(p+2)-1} = (p+1)+2 = \sigma(p)+2$$

($\because$ for a prime p $\sigma(p) = p+1$).

Prob. No ⑥. Find p for which $\sigma(p)$ is odd.

Sol:- For a prime p, $\sigma(p) = p+1$ is odd

ie p is even 2 is the only even prime

$\therefore p = 2$

Prob. No ⑦. Prove that (i) $\sum_{d/n} \frac{1}{d} = \frac{\sigma(n)}{n}$ (ii) $\phi(p)+\sigma(p) = 2p$

Sol:- (i) For any number n, $n = d_1 d_2$

$\frac{n}{d_1} = d_2$ ($\frac{n}{\text{a divisor}}$ gives another divisor)

$\therefore \sum_{d/n} \frac{n}{d} = \sum_{d/n}$ (another divisor of n).

$= \sum_{d/n}$ divisors of n $= \sigma(n)$.

$$\sum_{d/n} n/d = \sigma(n)$$

$$n \cdot \sum_{d/n} 1/d = \sigma(n)$$

$$\therefore \sum_{d/n} 1/d = \frac{\sigma(n)}{n}.$$

(ii) From previous chapter $\phi(p) = p-1$

from this chapter $\sigma(p) = p+1$

$\therefore \phi(p)+\sigma(p) = 2p$.

Prob. No ⑧. If $\tau(n)$ is odd then n is a square.

Sol:- $n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$

$\tau(n) = (l_1+1)(l_2+1)\cdots(l_k+1)$

$\tau(n)$ is odd $\Leftrightarrow$ the product $(l_1+1)(l_2+1)\cdots(l_k+1)$ is odd

$\Leftrightarrow$ each term in the product is odd ie (l_i+1)

$\Leftrightarrow$ each l_i is even

$\Leftrightarrow$ Take $l_i = 2m_i$

$\Leftrightarrow n = p_1^{2m_1} p_2^{2m_2} \cdots p_k^{2m_k} = (p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k})^2$

$\therefore$ n is a Square.

Prob. No 9. If $\tau(n)$ is a prime, then 'n' is of the form p (or) p^{2l}.

Sol:- Take $n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$

$\tau(n) = (l_1+1)(l_2+1) \cdots (l_k+1)$

$\tau(n)$ is prime so it has only one term (otherwise it is not prime)

Assume it $(l+1)$

$\tau(n) = l+1$

$\therefore n = p^{l+1}$ when $l=0$ ie $n=p$.

Prob. No 10 If 'n' is a power of 2. Prove that $\sigma(n)$ is odd.

Sol:- Take $n = 2^m$

$\sigma(n) = \dfrac{2^{m+1}-1}{2-1}$ is odd.