

MA 8551 - Algebra and Number Theory

Department: Mathematics

Batch/Year: CSE/ III

Created by: Mr.J.Leo Amalraj

Date: 28.07.2020

SYLLABUS

MA8551	ALGEBRA AND NUMBER THEORY	L	T	P	C
		4	0	0	4

UNIT I GROUPS AND RINGS 12

Groups : Definition - Properties - Homomorphism - Isomorphism - Cyclic groups - Cosets - Lagrange's theorem. Rings: Definition - Sub rings - Integral domain - Field - Integer modulo n - Ring homomorphism.

UNIT II FINITE FIELDS AND POLYNOMIALS 12

Rings - Polynomial rings - Irreducible polynomials over finite fields - Factorization of polynomials over finite fields.

UNIT III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS 12

Division algorithm – Base - b representations – Number patterns – Prime and composite numbers – GCD – Euclidean algorithm – Fundamental theorem of arithmetic – LCM.

UNIT IV DIOPHANTINE EQUATIONS AND CONGRUENCES 12

Linear Diophantine equations – Congruence's – Linear Congruence's - Applications: Divisibility tests - Modular exponentiation-Chinese remainder theorem – 2×2 linear systems.

UNIT V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS 12

Wilson's theorem – Fermat's little theorem – Euler's theorem – Euler's Phi functions – Tau and Sigma functions.

TOTAL: 60 PERIODS

View the lecture on YouTube: https://youtu.be/PN-cro0J_v8

Groups:

Definition: A non empty set G together with the binary operation $*$ is said to be Group $(G,*)$ provided the following conditions are satisfied

Closure : For all $a, b \in G \Rightarrow a * b \in G$

Associative: For all $a, b, c \in G$
 $\Rightarrow a * (b * c) = (a * b) * c$

Identity : There exist an $e \in G$ with
 $a * e = a = e * a$ for all $a \in G$

Inverse : For each $a \in G$, there is an element $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$

Definition (Abelian Group):

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

Example 1: Determine whether $\{-1,1\}$ is a group under multiplication?

Solution : **Closure:** Let $-1, 1 \in G \Rightarrow (-1) \cdot 1 = -1 \in G$ (Closure exist)

Identity: Let $-1 \in G$ an identity element $1 \in G$
such that $(-1) \cdot 1 = -1 = 1 \cdot (-1)$ (Identity exist)

Inverse: Let $-1 \in G$, inverse of -1 is -1

Let $1 \in G$, inverse of 1 is 1

such that $(-1) \cdot (-1) = 1 = (-1) \cdot (-1)$ (Inverse exist)

There fore, $\{-1,1\}$ is a group under multiplication.

Example 2: Determine whether $\{-1, 1\}$ is a group under addition?

Solution : Let $-1, 1 \in G \Rightarrow (-1) + 1 = 0 \notin G$ closure is not exist

There fore, $\{-1, 1\}$ is a not a group under addition.

Example 3: Under ordinary addition Z, Q, R, C are abelian groups, whereas they are not groups under usual multiplication. Since 0 has no inverse with respect to multiplication.

Definition Order of a group:

The number of elements in a group $(G, *)$ is called order of the group and it is denoted by $o(G)$ or $|G|$.

G is called finite group if $o(G)$ is finite.

Elementary Properties of Groups

View the lecture on YouTube: <https://youtu.be/9K6rXgxZAgs>

Theorem 1:

For all $a \in G$, Prove that the identity element in a group is unique

Proof:

Given : Let $(G, *)$ be a group

W.K.T, the identity axiom in a group G is

For all $a, e \in G$, $a * e = a = e * a$

To Prove: Identity Element in a group G is unique

Let e and e' are the identities in G

$$(i.e) \quad e * e' = e \text{ and} \quad (1)$$

$$e' * e = e' \quad (2)$$

from (1) and (2), we have $e = e'$

There fore, the identity element in a group $(G, *)$ is unique.

Theorem 2: Let $a \in G$, Prove that the inverse of each element of G is unique.

Proof:

Given: Let $a \in G$. Let $(G, *)$ be a group.

Inverse axiom in group G is $a * a^{-1} = e = a^{-1} * a$

To Prove: The inverse of each element of G is unique

Let b and c are the inverses of a in G

(i.e) $a * b = e = b * a$ also $a * c = e = c * a$

Therefore, it is enough to prove that $b = c$.

$$\begin{aligned}
 \text{Let } b &= b * e \text{ by } b * e = b \\
 &= b * (a * c) \quad \text{w.k.t } (a * c) = e \\
 &= (b * a) * c \quad \text{by Associative} \\
 &= e * c \\
 &= c
 \end{aligned}$$

We proved that $b = c$

Therefore, the inverse of each element of G is unique

Theorem 3: Prove that the Cancellation laws holds in group $(G, *)$

[Or]

Prove that (i) $a * b = a * c \Rightarrow b = c$ [LCL]

(ii) $b * a = c * a \Rightarrow b = c$ [RCL]

Proof (i):**Given:** Let $(G, *)$ be a groupFor all $a, b, c \in G$

$$\text{Also, } a * b = a * c \quad (1)$$

To Prove: $b = c$ Let $a^{-1} \in G$, Pre multiply a^{-1} on both side in equation (1)

$$(i.e) \quad a^{-1} * (a * b) = a^{-1} * (a * c)$$

$$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c \quad \text{by Associative}$$

$$\Rightarrow e * b = e * c$$

$$\Rightarrow b = c$$

Left Cancellation Law Holds in G **Proof (ii):**Let $a^{-1} \in G$, Post multiply a^{-1} on both side in equation (1)

$$(i.e) \quad (b * a) * a^{-1} = (c * a) * a^{-1}$$

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

$$\Rightarrow b * e = c * e$$

$$\Rightarrow b = c$$

Right Cancellation Law Holds in G .

Theorem 4: Let $(G, *)$ be a group then for all $a, b \in G$,

Prove that (i) $(a^{-1})^{-1} = a$

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

Proof:

Given: Let $(G, *)$ be a group. Let $a \in G$

By inverse axiom $a * a^{-1} = e = a^{-1} * a$

Also, w.k.t a^{-1} is the inverse of a and $(a^{-1})^{-1}$ is the inverse of a^{-1}

To Prove: $(a^{-1})^{-1} = a$

By inverse axiom $a * a^{-1} = e = a^{-1} * a$

Let a^{-1} is the inverse of a and $(a^{-1})^{-1}$ is the inverse of a^{-1}

w.k.t $(a^{-1})^{-1} * a^{-1} = e = a^{-1} * (a^{-1})^{-1}$

(ie) $a^{-1} * a = a^{-1} * (a^{-1})^{-1}$

$a = (a^{-1})^{-1}$ by [LCL]

(ii) Consider, $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$

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

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

$$= e$$

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

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

Example 4: Show that the set of all non-zero real numbers is an abelian

group under the operation $*$ defined by $(a * b) = \frac{ab}{2}, \forall a, b \in G$

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

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

Closure : $a * b = \frac{ab}{2} \quad \forall a, b \in G$ where a and b are non-zero real

Hence G is closed under $*$

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

$$a * (b * c) = a * \frac{bc}{2} = \frac{a(\frac{bc}{2})}{2} = \frac{a(bc)}{4} \quad (1)$$

$$(a * b) * c = \frac{ab}{2} * c = \frac{(\frac{ab}{2})c}{2} = \frac{a(bc)}{4} \quad (2)$$

$$\Rightarrow a * (b * c) = (a * b) * c$$

Hence G is Associative under $*$

Identity: There exist an $e \in G$ with

$$a * e = a = e * a \quad \forall a \in G$$

$$\frac{ae}{2} = a$$

$$\Rightarrow \frac{e}{2} = 1$$

$$\Rightarrow e = 2, \text{identity element is } 2$$

Inverse: For each $a \in G$, Let b is an inverse of a

$$\text{such that } a * b = e = b * a$$

$$\frac{ab}{2} = 2 \Rightarrow b = \frac{4}{a}$$

The inverse axiom is satisfied

Commutative: Let a and b are the elements of G

$$\text{then } a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

Commutative holds under $*$

Therefore, it is an abelian group.

View the lecture on YouTube: <https://youtu.be/uqMFcwi8PsY>

<https://drive.google.com/file/d/1WjGL0tL3OiC2K9bG-TQ71ZPutTb40AmW/view>

Definition: Subgroup

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

Theorem 5: A non-empty proper subset H of a group G is a subgroup of G if and only if, for all $a, b \in H \Rightarrow a * b^{-1} \in H$.

Proof:

Let $(G, *)$ be a group.

Let $(H, *)$ be a subgroup of G .

Then for all $a, b \in H \Rightarrow a * b^{-1} \in H$.

Converse,

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

Claim : H is a subgroup of G .

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

Then $a * a^{-1} \in H \Rightarrow e \in H$.

Inverse: Let $a \in H$, then $a, e \in H \Rightarrow e * a^{-1} \in H \Rightarrow a^{-1} \in H$.

Closure: For all $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$.

Since $H \subseteq G$, associative axiom is holds in H .

Hence H is a subgroup of G .

Theorem 6: If H_1 and H_2 are subgroups of a group $(G, *)$ then $H_1 \cap H_2$ is a subgroup of $(G, *)$.

Proof:

Given:

Let H_1 and H_2 are subgroups of a group G .

To prove: $H_1 \cap H_2$ is a subgroup of G

Let $a, b \in H_1 \cap H_2$

$\Rightarrow a, b \in H_1$ and $a, b \in H_2$

$\Rightarrow a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$

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

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

Example 5: Find all the non-trivial subgroup of $(\mathbb{Z}_6, +_6)$.

Solution: Let $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$

Cayley's Table:

$+_6$	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

The divisors of 6 are 2 and 3

∴ There are two subgroups for \mathbb{Z}_6

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

Definition: Permutation

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

Example 6:

If $S = \{a, b\}$ then the two possible permutations of S are

$$P_1 = \begin{pmatrix} a & b \\ a & b \end{pmatrix}, P_2 = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

Note: If there are n elements in the set $S = \{a_1, a_2, \dots, a_n\}$ then there are $n!$ permutations of S .

Example 7:

Prove that (S, \circ) , where $S = \{1, 2, 3\}$ is a group under the operation of right composition of permutations.

Let f and g be the permutations of the elements of $\{1, 2, 3, 4, 5\}$ given

$$\text{by } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}.$$

Find gf^2g^{-1} and $g^{-1}fgf^{-1}$

Solution:

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

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

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

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

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

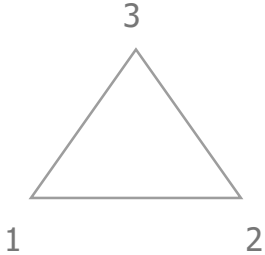
$$g^{-1}fgf^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

Example 8: Let G be the set of all rigid motions of a equilateral triangle. Identity the elements of G . Show that it is a non-abelian group of order 6.

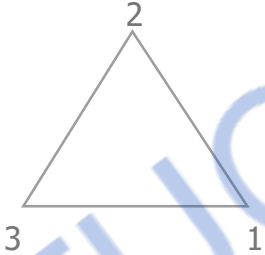
Solution:

Consider an equilateral triangle with vertices named as 1,2,3.
Let ρ_0, ρ_1, ρ_2 denote the rotations of the triangle in the counter clockwise direction about an axis through the center of triangle.

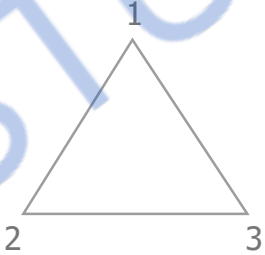
Rotations:(Counter Clockwise)

$\rho_0:$ 

$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

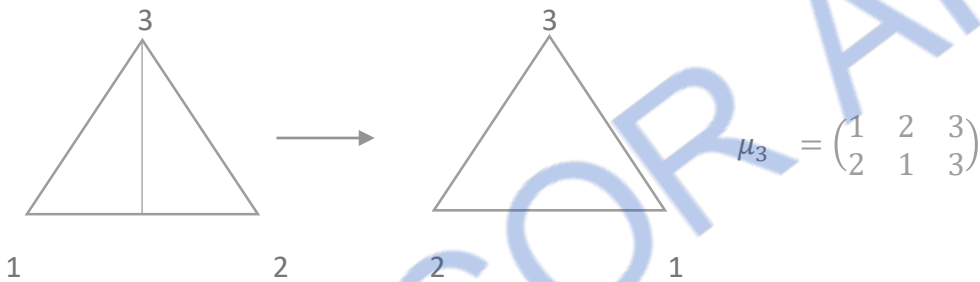
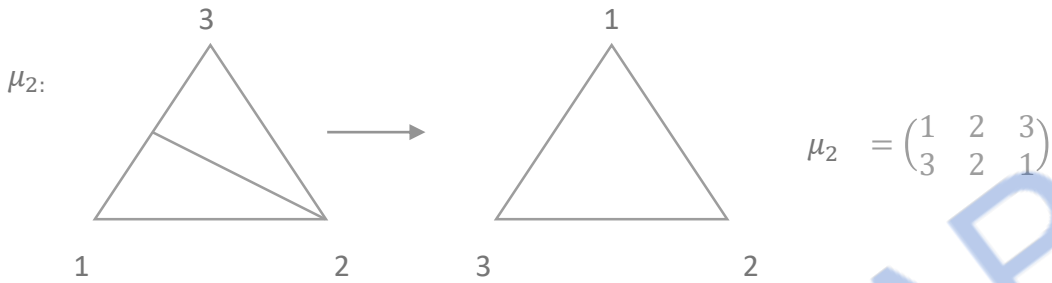
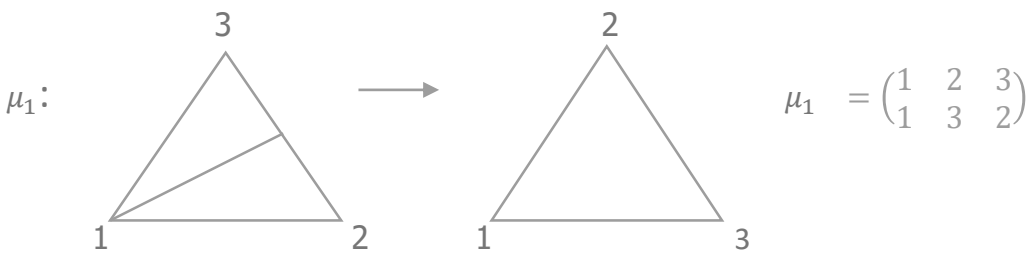
$\rho_1:$ 

$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\rho_2:$ 

$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Reflections: Let μ_1, μ_2, μ_3 denote the reflections along the lines joining vertices 3,1,2 and the midpoints of the opposite sides



Let G be the set of all permutations of an equilateral triangle.

The elements of G are $G = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$.

The Cayley's table of G is given by

\circ	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Now we have to prove the axioms

Closure: The body of the table contains only all the elements of G

Therefore, G is closed under the composition

Associative: In general, Composition of function is associative

Therefore, Associative holds in G

Identity : ρ_0 is an identity element from the Cayley's table

Inverse :	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
	<hr/>					
Inverse	ρ_0	ρ_2	ρ_1	μ_1	μ_2	μ_3

Commutative: $\rho_1 \circ \mu_1 = \mu_3 \neq \mu_1 \circ \rho_1 = \mu_2$

Commutative is not exist.

It is a non-abelian group of order 6.

Definition: Cyclic group

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

Example 9:

$(\mathbb{Z}, +)$ is a cyclic group generated by 1, since any element is $n1$ for some integer n . It can be seen easily that -1 is another generator. $(n\mathbb{Z}, +)$ is a cyclic group with n and $-n$ are the generators of this group.

Example 10:

Prove that $G = \{1, \omega, \omega^2\}$ is a cyclic group under usual multiplication.

Solution:

The generators of G are $\langle \omega \rangle$ and $\langle \omega^2 \rangle$.
Since $1 = (\omega)^3, \omega = (\omega)^1, \omega^2 = (\omega)^5$ and $1 = (\omega^2)^3, \omega = (\omega^2)^2, \omega^2 = (\omega^2)^4$.
Hence $G = \{1, \omega, \omega^2\}$ is a cyclic group under usual multiplication.

Theorem 7: Any cyclic group is abelian.**Proof:**

Let $(G, *)$ be a cyclic group with generator 'a'.

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

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

Commutative law is satisfied.

Hence $(G, *)$ is abelian.

Theorem 8: Every subgroup of a cyclic group is cyclic.**Proof:**

Let G be a cyclic group generated by a .

Let H be a subgroup of G .

Claim: H is a cyclic group

Clearly every element of H is of the form a^n for some integer n .

Let m be the least positive integer such that $a^m \in H$

We claim that a^m is the generator of H .

Let $b \in H$. Then $b = a^n$ for some integer n .

Let $n = mq + r, 0 \leq r < m$.

Then $b = a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r$.

$\therefore a^r = (a^m)^{-q} b$ -----(1)

Now, $a^m \in H$. Since H is a subgroup, $(a^m)^{-q} \in H$.

Also, $b \in H$.

By (1), $a^r \in H$ and $0 \leq r < m$.

But m is the least positive integer such that $a^m \in H$.

$\therefore r = 0$. Hence $b = a^n = a^{mq} = (a^m)^q$.

\therefore Every element of H is a power of a^m .

$\therefore H = \langle a^m \rangle$ and hence H is cyclic.

COSETS AND LAGRANGE'S THEOREM

View the lecture on YouTube:

<https://youtu.be/XzEgrCwPJ8A>

Definition: (Cosets)

Let $(H, *)$ be a subgroup of $(G, *)$. Let $a \in G$ be any element then $aH = \{a * h / h \in H\}$ is called left coset of H in G determined by a .

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

Note:

In general $aH \neq Ha$, but if G is abelian then $aH = Ha$.

Example 1:

Find all the distinct left cosets of the subgroup $H = \{[0], [3]\}$ of the group $(Z_6, +_6)$. Also, find their union.

Solution:

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

Given $H = \{[0], [3]\}$ is a subgroup of $(Z_6, +_6)$.

The left cosets of H are:

$$[0] + H = \{[0], [3]\} = H$$

$$[1] + H = \{[1], [4]\} = H_1 \text{ (say)}$$

$$[2] + H = \{[2], [5]\} = H_2 \text{ (say)}$$

$$[3] + H = \{[3], [0]\} = H$$

$$[4] + H = \{[4], [1]\} = H_1$$

$$[5] + H = \{[5], [2]\} = H_2$$

The distinct left cosets H are: H, H_1, H_2

Also, $H \cup H_1 \cup H_2 = \{[0], [1], [2], [3], [4], [5]\} = Z_6$.

Theorem 1: Let H be a subgroup of G . Then

(i) any two left cosets of H are either identical or disjoint.

(ii) union of all the left cosets of H is G .

(iii) the number of elements in any left coset aH is the same as the number of elements in H .

Proof:

Given H is a subgroup of G .

Let aH and bH be two left cosets of H .

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

Suppose $aH \cap bH \neq \emptyset$, then there exists an element

$$x \in aH \cap bH$$

$$\Rightarrow x \in aH \text{ and } x \in bH$$

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

$$\therefore a * h_1 = b * h_2$$

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

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

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

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

If x is any element in aH then

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

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

$$\therefore aH \subseteq bH.$$

Similarly, we can prove that $bH \subseteq aH$

Hence $aH = bH$.

Let $a \in G$. Then $a = a * e \in aH$.

\therefore Every element of G belongs to a left coset of H .

\therefore The union of all the left cosets of H is G .

i.e. $G = \bigcup_{a \in G} aH$

The map $f: H \rightarrow aH$ defined by $f(h) = a * h, \forall h \in H$ is clearly a bijection.

Hence every left coset aH has the same number of elements as H .

Theorem 2: [Lagrange's Theorem]

The order of a subgroup of a finite group divides the order of a group.

Proof:

Let G be a finite group of order n , i.e. $o(G) = n$

Let H be a subgroup of G of order m , i.e. $o(H) = m$

Let k be the number of left cosets of H in G .

Let the k left cosets be $\{a_1H, a_2H, \dots, a_kH\}$

Then by Theorem 1, these k left cosets are mutually disjoint, they have the same number of elements in H namely m and their union is G .

$$\therefore G = a_1H \cup a_2H \cup \dots \cup a_kH$$

$$\therefore o(G) = o(a_1H \cup a_2H \cup \dots \cup a_kH)$$

$$\Rightarrow o(G) = o(a_1H) + o(a_2H) + \dots + o(a_kH)$$

$$\Rightarrow n = m + m + \dots + m \quad (k \text{ times})$$

$$\Rightarrow n = km$$

$$\Rightarrow k = \frac{n}{m}$$

$$\text{i.e. } \frac{o(G)}{o(H)}$$

Hence the proof.

NORMAL SUBGROUPS

View the lecture on YouTube:

https://youtu.be/o_TFzzTNFjI

Definition: (Normal subgroup)

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

Note: $aH = Ha$ does not mean that $a * h = h * a$, for any $h \in H$. But $a * h_1 = h_2 * a$, for some $h_1, h_2 \in H$.

Theorem 1: A subgroup $(H,*)$ of a group $(G,*)$ is a normal subgroup if and only if $a^{-1} * h * a \in H$, for any $a \in G, h \in H$.

Proof:

Given $(H,*)$ is a normal subgroup of $(G,*)$

Then $aH = Ha, \forall a \in G$

Now for $h \in H$,

$h * a \in aH = Ha$

$\therefore h * a = a * h_1$, for some $h_1 \in H$

$\Rightarrow a^{-1} * h * a = h_1 \in H$

i.e. $a^{-1} * h * a \in H$

Converse,

Assume $a^{-1} * h * a \in H$, for every $a \in G$ and $h \in H$

Then $a * (a^{-1} * h * a) \in aH$

$\Rightarrow (a * a^{-1}) * (h * a) \in aH$

$\Rightarrow e * (h * a) \in aH$

$\Rightarrow h * a \in aH$

i.e. $Ha \subseteq aH$

----- (1)

Now,

Let $b = a^{-1} \in G$

Then $b^{-1} * h * b \in H$

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

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

$\Rightarrow (a * h * a^{-1}) * a \in Ha$

$\Rightarrow (a * h) * (a^{-1} * a) \in Ha$

$\Rightarrow (a * h) * e \in Ha$

$\Rightarrow a * h \in Ha$

i.e. $aH \subseteq Ha$

------(2)

from (1) & (2),

$aH = Ha$

Hence H is a normal subgroup of G .

Theorem 2: Show that intersection of two normal subgroups of G is also normal subgroup of G .

Proof:

Let H_1 and H_2 be two normal subgroups of a group G

Then H_1 and H_2 are subgroups of G

WKT, "The intersection of two subgroups of a group G is also a subgroup of G "

$\therefore H_1 \cap H_2$ are subgroups of G

Let $a \in G$ and $h \in H_1 \cap H_2$

Then $h \in H_1$ and $h \in H_2$

Since H_1 and H_2 are normal subgroups of G .

$\therefore a^{-1} * h * a \in H_1$ and $a^{-1} * h * a \in H_2$

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

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

GROUP HOMOMORPHISM

View the lecture on YouTube: <https://youtu.be/l3tJXbgJXoE>

<https://youtu.be/EQvHsfvhbbc>

Definition: If (G, o) and $(G', *)$ are the groups and $f: G \rightarrow G'$, then the mapping f is called a group homomorphism if

$$f(a o b) = f(a) * f(b) \quad \forall a, b \in G$$

Example 1:

Let (G, o) and $(G', *)$ be any two groups e and e' be the identity elements of G and G' respectively. Define by $f: G \rightarrow G'$ $f(a) = e'$. Then f is a homomorphism.

Solution:

Let $a, b \in G$. We have to verify that $f(a o b) = f(a) * f(b)$

$a, b \in G \Rightarrow a o b \in G$. So $f(a o b) = e'$. Also $f(a) = e'$, $f(b) = e'$

$$f(a) * f(b) = e' * e' = e' = f(a o b)$$

Hence f is a homomorphism.

This homomorphism is called a trivial homomorphism.

Example 2:

Let G be then group of additive integers and define $f: G \rightarrow G$ by

$f(a) = 2a \quad \forall a \in G$. Then f is homomorphism.

Solution:

Let $a, b \in G$. We have to verify that $f(a + b) = f(a) + f(b)$

$a, b \in G \Rightarrow a + b \in G$. So $f(a + b) = 2(a + b)$

$$= 2a + 2b$$

$$= f(a) + f(b)$$

Hence f is a homomorphism.

Properties of Homomorphisms:

If f is a homomorphism of the groups (G, o) into $(G', *)$, then

(i) $f(e) = e'$ where e and e' are the identities of G and G'

(ii) For any $a \in G$, $f(a^{-1}) = [f(a)]^{-1}$

(iii) For any $a \in G$, $f(a^n) = [f(a)]^n$, $n \in \mathbb{Z}$

Proof:

For any $a \in G$,

$$\begin{aligned} a \circ e &= a \\ f(a \circ e) &= f(a) \end{aligned}$$

$$f(a) * f(e) = f(a) * e' \quad (\text{Since, } f \text{ is a homomorphism})$$

$$f(e) = e' \quad (\text{By Left Cancellation Law})$$

(ii) For any $a \in G$ there exist $a^{-1} \in G \ni a \circ a^{-1} = a^{-1} \circ a = e$

$$\text{Now, } f(a \circ a^{-1}) = f(a) * f(a^{-1})$$

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

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

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

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

$$e' = f(a^{-1}) * f(a) \text{ -----(2)}$$

From the equations (1) & (2), we see that

$f(a^{-1})$ is an inverse of $f(a)$

$$\text{Hence, } f(a^{-1}) = [f(a)]^{-1}.$$

(iii) We shall prove this result by induction on n

$$f(a^1) = f(a) = [f(a)]^1$$

Therefore, the result is true for $n=1$

Let us assume that the result is true for $n=K$

$$f(a^K) = [f(a)]^K$$

$$\text{Now } f(a^{K+1}) = f(a^K \circ a)$$

$$= f(a^K) * f(a) \quad (\text{Since } f \text{ is a homomorphism})$$

$$= [f(a)]^K * f(a) \quad \text{by induction hypothesis}$$

$$= [f(a)]^{K+1}$$

Therefore, the result is true for $n=K+1$

Thus the result is true for all positive integers.

For $n = 0$; $a^0 = e$.

$$f(a^0) = f(e) = e' \text{ and } e' = [f(a)]^0$$

$$\text{and } f(a^0) = [f(a)]^0$$

Thus the result is true for $n = 0$

When n is a negative integer

put $n = -m$, where m is a positive integer.

Now, for $x \in G$,

$$\begin{aligned} f(x^n) &= f(x^{-m}) \\ &= f[(x^{-1})^m] \\ &= [f(x^{-1})]^m \\ &= \{[f(x)]^{-1}\}^m \\ &= [f(x)]^{-m} \\ &= [f(x)]^n \end{aligned}$$

Thus the result is true for negative integers.

Hence we proved that the result is true for any integer.

Definition:

Let (G, o) and $(G', *)$ be any two groups e and e' be the identity elements of G and G' respectively. If $f: G \rightarrow G'$ is a group homomorphism, then the subset K of G defined by $K = \{x \in G \mid f(x) = e'\}$ is called the Kernel of f and is denoted by $\ker f$.

Theorem 1:

Let f be a homomorphism of a group (G, o) into a group $(G', *)$ with Kernel K . Then

(i) K is a subgroup of G .

(ii) K is a normal subgroup of G

Proof:

Let e and e' be the identity elements of G and G' respectively.

Now, $K = \{x \in G \mid f(x) = e'\}$

(i) Since $e \in G$, we have $f(e) = e' \Rightarrow e \in K$

K is non-empty

$a, b \in K$. Then $f(a) = e'$ and $f(b) = e'$

$$\begin{aligned} f(a \circ b^{-1}) &= f(a) * f(b^{-1}) \\ &= f(a) * [f(b)]^{-1} \\ &= e' * (e')^{-1} \\ &= e' * e' \\ &= e' \end{aligned}$$

$a \circ b^{-1} \in K$ and hence K is a subgroup of G .

(ii) For any $g \in G$ and $k \in K$

We have

$$\begin{aligned} f(g \circ k \circ g^{-1}) &= f(g) * f(k) * f(g^{-1}) \\ &= f(g) * e' * f(g^{-1}) \\ &= f(g) * f(g^{-1}) \\ &= f(g) * [f(g)]^{-1} \\ &= e' \end{aligned}$$

$g \circ k \circ g^{-1} \in K$, for all $g \in G$ and $k \in K$

Hence K is a normal subgroup of G .

Theorem 2:

Let f be a homomorphism of a group (G, \circ) into a group $(G', *)$ with Kernel K .

Then f is one-one if and only if $K = \{e\}$

Proof:

Necessary Part:

Let f be a one-one mapping.

Let us take $a \in K$ which implies $f(a) = e'$

$$= f(e)$$

$$\Rightarrow a = e \quad [\text{Since } f \text{ is one-one}]$$

$$K = \{e\}$$

Sufficient Part:

Let $K = \{e\}$

We have to show that f is one-one mapping.

Now $f(a) = f(b)$

$$f(a) * [f(b)]^{-1} = f(b) * [f(b)]^{-1}$$

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

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

$$a \circ b^{-1} \in K = \{e\}$$

$$\text{Let } a \circ b^{-1} = e$$

$$a = b$$

Hence we proved that f is one-one mapping.

Definition:

If (G, o) and $(G', *)$ are the groups and $f: G \rightarrow G'$ is a homomorphism. The function f is called an **epimorphism** if it is onto mapping.

Definition:

If (G, o) and $(G', *)$ are the groups and $f: G \rightarrow G'$ is a homomorphism. The function f is called an **monomorphism** if it is one - one mapping.

Definition:

If (G, o) and $(G', *)$ are the groups and $f: G \rightarrow G'$ is a homomorphism. The function f is called an **isomorphism** if it is both one – one and onto mapping. In this case G, G' are said to be isomorphic groups.

Example 3:

Let $f: (Z, +) \rightarrow (2Z, +)$ be defined by

$f(a) = 2a \quad \forall a \in Z$. Then f is isomorphism.

Solution:

Let $a, b \in Z$. First we have to verify that $f(a + b) = f(a) + f(b)$

$$\begin{aligned} a, b \in Z &\Rightarrow a + b \in Z. \text{ So } f(a + b) = 2(a + b) \\ &= 2a + 2b \\ &= f(a) + f(b) \end{aligned}$$

Hence f is a homomorphism.

$$\begin{aligned} \text{Now } f(a) &= f(b) \\ \Rightarrow 2a &= 2b \\ \Rightarrow a &= b \end{aligned}$$

f is one -one

For every $2a \in 2Z \exists a \in Z$
such that $f(a) = 2a$
 f is onto

Hence f is isomorphism.

Example 4:

Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping

$f: R^+ \rightarrow R$ defined by $f(x) = \log_{10} x \quad \forall x \in R^+$ is an isomorphism.

Solution:

First, let us show that f is a homomorphism.

Let $a, b \in R^+$.

$$\begin{aligned} \text{Now, } f(a.b) &= \log_{10}(a.b) \\ &= \log_{10} a + \log_{10} b \\ &= f(a) + f(b) \end{aligned}$$

$\Rightarrow f$ is a homomorphism.

Next, let us prove that f is a Bijection.

For any $a, b \in R^+$, Let, $f(a) = f(b)$

$$\Rightarrow \log_{10} a = \log_{10} b$$

$$\Rightarrow a = b$$

Therefore, f is one –one

Next, take any $c \in R$.

Then $10^c \in R^+$ and $f(10^c) = \log_{10} 10^c = c$.

\Rightarrow Every element in R has a pre image in R^+ .

i.e., f is onto.

$\Rightarrow f$ is a bijection.

Hence f is an isomorphism.

Definition:

A homomorphism of a group G to itself is called an endomorphism.

Definition:

An isomorphism of a group G onto itself is called an automorphism of the group.

Example 5:

Let $(G, .)$ be any group. The identity map $I_G: G \rightarrow G$ defined by $I_G(a) = a$, $\forall a \in G$ is an automorphism.

Solution:

Let $a, b \in G \Rightarrow a.b \in G$

so $I_G(a.b) = a.b$

$$= I_G(a) . I_G(b)$$

Therefore, the mapping I_G is homomorphism.

We see that, clearly the identity mapping I_G is Bijective.

Hence I_G is an automorphism.

QUOTIENT GROUPS

Definition:

Let N be a normal subgroup of G . Let $\frac{G}{N}$ denotes the collection of all distinct right Cosets of N in G .

$$\text{i.e } \frac{G}{N} = \{Na \mid a \in G\}$$

Then $\frac{G}{N}$ is a group under coset multiplication. It is called a quotient group or factor group of $\frac{G}{N}$.

Theorem 3:

Let N be a normal subgroup of G . Then $\frac{G}{N}$ is a group under the operation is defined by $Na Nb = Nab$.

Proof:

$$\frac{G}{N} = \{Na \mid a \in G\}$$

(i) Let Na, Nb be the two right Cosets in G . Then the product $Na Nb = Nab$.

The above product is well defined.

i.e for every $Na, Nb \in \frac{G}{N}$ and $a, b \in G$

We have $Nab \in \frac{G}{N}$ and $a, b \in G$

$\frac{G}{N}$ is closed.

(ii) $Na, Nb, Nc \in \frac{G}{N}$ and $a, b, c \in G$

$$\begin{aligned}
 \text{Now } (Na Nb)Nc &= Nab Nc \\
 &= Nabc \\
 &= Na(bc) \\
 &= Na Nbc \\
 &= Na (Nb Nc)
 \end{aligned}$$

Associative property is true in $\frac{G}{N}$.

(iii) $Ne = N \in \frac{G}{N}$ and

$$\begin{aligned}
 Na Ne &= Nae \\
 &= Ne \\
 &= Nae \\
 &= Ne Na
 \end{aligned}$$

Ne is the identity element

(iv) For every $Na \in \frac{G}{N}$

There exists $Na^{-1} \in \frac{G}{N}$ such that

$$\begin{aligned}
 Na Na^{-1} &= Naa^{-1} \\
 &= Ne
 \end{aligned}$$

$$\begin{aligned}
 \text{Also } Na^{-1}Na &= Na^{-1}a \\
 &= Ne
 \end{aligned}$$

Na^{-1} is the inverse of Na in $\frac{G}{N}$

Hence $\frac{G}{N}$ is a group under coset multiplication.

Theorem 4:

If G is a group and N is a normal subgroup of G . Then the mapping $\varphi: G \rightarrow \frac{G}{N}$ defined by $\varphi(a) = Na \quad \forall a \in G$ is a homomorphism of G onto $\frac{G}{N}$.

Proof:

Let $a, b \in G$ be any two elements.

$$\text{Then } \varphi(ab) = Nab$$

$$= Na Nb \quad [\text{Since } Na \text{ is normal in } G]$$

$$= \varphi(a)\varphi(b)$$

φ is a homomorphism.

Let Na be any element of $\frac{G}{N}$

Then we have $a \in G$ such that $\varphi(a) = Na$

φ is onto.

This homomorphism is called Natural or Canonical homomorphism.

FUNDAMENTAL THEOREM OF GROUP HOMOMORPHISM:**Theorem 5:**

Let G and G' be two groups. Let $f: G \rightarrow G'$ be a onto homomorphism with Kernel K . Then $\frac{G}{K} \cong G'$

Proof:

We define $\varphi: \frac{G}{K} \rightarrow G'$ by $\varphi(Ka) = f(a)$

We have to show that φ is well defined.

$$\text{Let } Ka = Kb$$

$$\Rightarrow a \in Kb$$

$$\Rightarrow ab^{-1} \in K$$

$$\Rightarrow f(ab^{-1}) = e'$$

$$\Rightarrow f(a) f(b^{-1}) = e' \quad [\text{Since } \varphi \text{ is homomorphism}]$$

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

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

$$\Rightarrow \varphi(Ka) = \varphi(Kb)$$

φ is well defined.

To prove $\frac{G}{K} \cong G'$, we have to show that the mapping φ is homomorphism, one-one and onto.

$$\text{Now, } \varphi(Ka Kb) = \varphi(Kab)$$

$$= f(ab)$$

$$= f(a) f(b) \quad [\text{Since } f \text{ is homomorphism}]$$

$$= \varphi(Ka) \varphi(Kb)$$

φ is homomorphism

$$\text{Let } \varphi(Ka) = \varphi(Kb)$$

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

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

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

$$\Rightarrow f(ab^{-1}) = e'$$

$$\Rightarrow ab^{-1} \in K$$

$$\Rightarrow a \in Kb$$

$$\Rightarrow Ka = Kb$$

φ is one-one mapping.

Let $a' \in G'$. Since f is onto

there exist $a \in G$ such that $f(a) = a'$

$$\text{Hence } \varphi(Ka) = f(a) = a'$$

φ is onto

Hence we proved $\frac{G}{K} \cong G'$.

RINGS

View the lecture on YouTube: <https://youtu.be/yKRbG9Y5pYY>

RING EXAMPLES

Definition 1: Rings: A non –empty set R together with two binary operations denoted by $+$ and \cdot are called addition and multiplication which satisfy the following conditions is called a ring.

- i. $(R, +)$ is an abelian group.
- ii. Multiplication is an associative binary operation on R .
 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for all $a, b, c \in R$
- iii. Multiplication is distributive over addition.
 $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, $(a + b) \cdot c = a \cdot c + b \cdot c \forall a, b, c \in R$

Example 1: Prove that the set F of all real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$ is a field under usual addition and multiplication of real numbers.

We have to show that F is a commutative ring with identity in which every non zero element has multiplicative inverse.

1. Closure: $a + b\sqrt{2}, c + d\sqrt{2}$ where $a, b, c, d \in \mathbb{Q}$
 Then $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in F$.
 $\therefore F$ is closed under $+$
2. Associativity: Since $+$ is associative in the set of real numbers and F is a subset, $+$ is associative in F .
3. Identity: $0 = 0 + 0\sqrt{2} \in F$ is the identity for $+$.
4. Inverse: For any element $a + b\sqrt{2} \in F$, there exists $-a - b\sqrt{2} \in F$ such that
 $(a + b)\sqrt{2} + (-a - b)\sqrt{2} = a - a + (b - b)\sqrt{2} = 0 + 0\sqrt{2}$.

Hence, the inverse of $a + b\sqrt{2}$ is $-a - b\sqrt{2}$.

Also, $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (c + d\sqrt{2}) + (a + b\sqrt{2})$ for all $a + b\sqrt{2}, c + d\sqrt{2} \in F$.

$\therefore (F, +)$ is an abelian group.

Now, let $a + b\sqrt{2}$, and $c + d\sqrt{2} \in F$.

Then $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in F$.

Thus F is closed under multiplication.

$1 = 1 + 0\sqrt{2} \in F$ and is the multiplicative identity.

Since the two binary operations are the usual addition and multiplication of real numbers, multiplication is associative and commutative and the two distributive laws are true.

$$\begin{aligned}\text{Since, } (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2} \\ &= (ca + 2db) + (da + cb)\sqrt{2} \\ &= (c + d\sqrt{2}) \cdot (a + b\sqrt{2})\end{aligned}$$

Hence multiplication is commutative. The verification of associative and distributive law are straight forward.

To prove that multiplicative inverse exists for every non zero element of F .

Now let $a + b\sqrt{2} \in F - 0$. Then a and b are not simultaneously 0.

$$\text{Also, } \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2}.$$

We claim that $a^2 - 2b^2$.

Case (i) $a \neq 0$ and $b = 0$, then $a^2 - 2b^2 = a^2 \neq 0$.

Case (ii) $a = 0$ and $b \neq 0$, then $a^2 - 2b^2 = -2b^2 \neq 0$.

Case (iii) $a \neq 0$ and $b \neq 0$. Suppose $a^2 - 2b^2 = 0$,

Then $a^2 = 2b^2 \Rightarrow \frac{a^2}{b^2} = 2$. Hence $\frac{a}{b} = \pm\sqrt{2}$.

Now, $\frac{a}{b} \in Q$ and $\sqrt{2} \notin Q$. This is a contradiction.

Hence, $a^2 - 2b^2 \neq 0$

$$\therefore \frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b\sqrt{2}}{a^2-2b^2} \in F \text{ and is the inverse of } a + b\sqrt{2}.$$

Hence F is a field.

Example 2: In $Z_6 = \{0,1,2,3,4,5\}$, $2 \neq 0, 3 \neq 0$. But $2 \times_6 3 = 0$.

$\therefore 2$ and 3 are zero divisor. Hence Z_6 is a ring with zero divisors.

Example 3: $(Q, +, \cdot), (R, +, \cdot), (C, +, \cdot)$ are field.

But $(Z, +, \cdot)$ is an integral domain but not a field.

Practice Example: Prove that $R = \{a + b\sqrt{2}, a, b \in Z\}$ is an integral domain, but not a field under addition and multiplication.

Theorem 1: A ring R has no zero- divisors iff cancellation law is valid for multiplication in R .

Proof: Let R be a ring without zero-divisors. $ab = 0$

Let $ax = ay$ and $a \neq 0$.

$\therefore ax - ay = 0$. Hence $a(x - y) = 0$ and $a \neq 0$.

Since R has no zero-divisors, $x - y = 0$.

$\therefore x = y$. Thus cancellation law is valid in R .

Conversely, let the cancellation law be valid in R .

Let $ab = 0$ and $a \neq 0$, $ab = 0 \Rightarrow b = 0$, by cancellation law.

Hence R has no zero divisors.

Theorem 2: Every field is an integral domain.

Proof: Let R be a field.

To prove R is an integral domain, it is enough to prove that it has no zero divisors.

Suppose $a, b \in R$ with $ab = 0, a \neq 0$, then there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.

$ab = 0 \Rightarrow a^{-1}.ab = a^{-1}.0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow b = 0$.

If $b \neq 0$, then we can prove that $a = 0$.

$\therefore a.b = 0 \Rightarrow a = 0$ or $b = 0$.

$\therefore R$ has no zero divisors.

Hence R is an integral domain.

Theorem 3: Every 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.

Claim: To prove R is a field, it is enough to prove that every non-zero element in R has multiplicative inverse.

Let $R = \{0, 1, a_2, a_3, \dots, a_n\}, a \in R$ and $a \neq 0$.

Multiplying the non-zero elements of R by a , we get the set $\{a.1, aa_2, aa_3, \dots, aa_n\}$.

These elements are non-zero and they are distinct.

Suppose $a.a_j = a.a_k, j \neq k$, then $a.(a_j - a_k) = 0$. Since $a \neq 0, a_j \neq a_k$,

which is a contradiction to the fact that a_k are distinct elements in R .

$\therefore a.a_j \neq a.a_k$

Since R is finite, these n elements are same as the n non-zero element in R in some order by pigeon hole principle.

$\therefore 1 = a \cdot a_i$ for some $a_i \in R$. Since R is commutative, $a \cdot a_i = a_i \cdot a = 1$.

\therefore Every non- zero element in R has multiplicative inverse.

Hence any finite integral domain is a field.

Definition 2: Let $(R, +, \cdot)$ be a ring with unity 1. An element $u \in R$ is called a unit in R if there exists a $v \in R$ such that $u \cdot v = v \cdot u = 1$.

Example 4: In Z_4 , 1 and 3 are the units.

In Z_5 , $\{1, 2, 3, 4\}$ are the set of units.

Theorem 4: Z_n is an integral domain if and only if n is a prime.

Proof: Clearly Z_n is a commutative ring with identity. To prove that n is a prime.

Suppose n is a composite number.

Then there exists $1 < a < n$, $1 < b < n$ such that $a \cdot b = n$.

Let $a, b \in Z_n$, and $a \neq 0, b \neq 0$,

$a \odot b = 0$. $\therefore n$ is a prime.

Conversely suppose n is a prime.

To prove that Z_n has no zero divisor.

Suppose Z_n has zero divisors.

Then there exists $a, b \in Z_n$, $a \neq 0, b \neq 0$ such that $a \odot b = 0$.

$1 \leq a, b \leq n$ and n divides $a \cdot b$. That is, n divides a or n divides b .

Which is a contradiction. Since n is a prime.

$\therefore Z_n$ has no zero divisor.

Hence, Z_n is an integral domain.

Definition 3: Let $(R, +, \cdot), (S, \oplus, \odot)$ be two rings. These two rings are said to be isomorphic if there exists a map $f: R \rightarrow S$ such that

(i) f is one-one.

(ii) f is onto.

(iii) $f(a + b) = f(a) \oplus f(b)$ and $f(a \cdot b) = f(a) \odot f(b)$ for all $a, b \in R$.

Theorem 5: Let R and S be two isomorphic rings, then the following hold:

- (i) If R is commutative, then S is commutative.
- (ii) If R has multiplicative identity, then S has multiplicative identity.
- (iii) If R is an integral domain, so is S .
- (iv) If R is a field, so is S .

Proof:

(i) Let $f: R \rightarrow S$ be an isomorphism between the two rings R and S let $a', b' \in S$. Since f is onto, there exists $a, b \in R$ such that $f(a) = a'$, and $f(b) = b'$.

Now, $a' b' = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = b' a'$.

$\therefore S$ is a commutative ring.

(ii) Let $1 \in R$ be the identity element of R .

Let $a' \in S$. Then there exists $a \in R$ such that $f(a) = a'$.

Now, $f(1) = a' = f(1)f(a) = f(1 \cdot a) = f(a) = a'$.

Similarly, $a' f(a) = a'$ and hence $f(1)$ is identity element in S .

$\therefore S$ is a ring with identity.

(iii) Let R be an integral domain. Then by (i) and (ii) S is a commutative ring with identity.

To prove that S has no zero divisors.

Let $a', b' \in S$ and let $a' \cdot b' = 0$.

Since f is onto there exists $a, b \in R$ such that $f(a) = a'$ and $f(b) = b'$

$\therefore a' b' = f(a)f(b) = f(ab) = 0 \Rightarrow ab = 0$. (Since f is $1-1$.)

$a = 0$ or $b = 0$ (since R is an integral domain).

$f(a)=0$ or $f(b) = 0 \Rightarrow a' = 0$ or $b' = 0$

S is an integral domain.

(iv) To prove that every non zero element in S has an inverse.

Let $a' \in S$ and $a' \neq 0$. There exists $a \in R - \{0\}$ such that $f(a) = a'$.

Now, $f(a^{-1})a' = f(a^{-1})a = f(a^{-1}a) = f(1)$.

Hence $f(a^{-1})$ is the inverse of a' in S

$\therefore S$ is a field.

Definition 1: Let $(R, +, \cdot)$ be a ring. A non-empty subset S of R is called a subring of R if S is a ring with respect to the same binary operations $+$ and \cdot defined in R .

Examples:

(i) $(2\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Z}, +, \cdot)$.

(ii) $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Q}, +, \cdot)$.

(iii) $(2\mathbb{Z}, +, \cdot)$ with $a * b = \frac{ab}{2}$ is a ring but not a subring of $(\mathbb{Z}, +, \cdot)$.

Theorem 6: Let $(R, +, \cdot)$ be a ring. A non-empty subset S of R is called a subring of R if and only if $a - b \in S$ and $a \cdot b \in S$.

Proof: Let $(R, +, \cdot)$ be a ring. Then S itself is a ring under the same operations $+$, \cdot as defined in R .

If $a, b \in S$, then $-b \in S$. Since S is a subring.

Hence $a + (-b) = a - b \in S$. Also $a \cdot b \in S$.

Conversely, let S be a non-empty subset of R such that $a, b \in S \Rightarrow a - b \in S$ and $a \cdot b \in S$.

Since S is non-empty, take any element $x \in S$. Then $x, x \in S \Rightarrow x - x \in S$ i.e. $0 \in S$.

Let a be any element in S .

Then $0, a \in S \Rightarrow 0 - a \in S \Rightarrow -a \in S$. Clearly, $+$ in S is closed, associative and commutative. Also, \cdot in S is associative and distributive over $+$.

Hence $(S, +, \cdot)$ is a subring of R .

Theorem 7: The intersection of two subrings of a ring R is again a subring of R .

Proof: Let S_1, S_2 be two subrings of a ring R .

To prove that $S_1 \cap S_2$ is a subring of R .

Since $0 \in S_1$ and $0 \in S_2$, we get $0 \in S_1 \cap S_2$.

$\therefore S_1 \cap S_2$ is non-empty.

Let $a, b \in S_1 \cap S_2$. Then $a, b \in S_1$ and $a, b \in S_2$.

$\therefore a - b, a \cdot b \in S_1$ and $a - b, a \cdot b \in S_2 \Rightarrow a - b, a \cdot b \in S_1 \cap S_2$

Hence $S_1 \cap S_2$ is a subring of R .

Note: The union of two subrings of a ring need not be a subring.

Theorem 8: Let $(R, +, \cdot)$ be a ring. Let S_1, S_2 be two subrings of a ring R . Then $S_1 \cup S_2$ is a subring of R iff $S_1 \subset S_2$ or $S_2 \subset S_1$.

Definition : Left Ideal

Let R be a ring. A non- empty subset I of R is called a left ideal of R if

- (i) $a, b \in I \Rightarrow a - b \in I$.
- (ii) $r \in R, a \in I \Rightarrow ra \in I$.

Definition : Right Ideal

Let R be a ring. A non- empty subset I of R is called a right ideal of R if

- (i) $a, b \in I \Rightarrow a - b \in I$.
- (ii) $r \in R, a \in I \Rightarrow ar \in I$.

Definition : Ideal

Let R be a ring. A non- empty subset I of R is called an ideal of R if

- (i) $a, b \in I \Rightarrow a - b \in I$.
- (ii) $r \in R, a \in I \Rightarrow ra \in I$ and $ar \in I$.

Theorem 9: Every left ideal of R is a subring of R .

Proof: Let I be a left ideal of the ring R . Let $a, b \in I$.

Then by definition $a - b \in I$ and $a, b \in I$.

Hence I is a subring of R .

Remark : A subring of a ring R need not be an ideal of R .

Example: Z is subring of Q , but Z is not an ideal of Q .

Since $8 \in Z$ and $\frac{1}{3} \in Q \Rightarrow 8 \cdot \frac{1}{3} \notin Z$.

Note: For any ring R , $\{0\}$ and R are always ideal of R called improper ideals. Other ideals are called proper ideals.

Theorem 10: A field has no proper ideals.

Proof: Let I be an ideal of the field F . Suppose $I \neq \{0\}$.

We shall prove that $I = F$. Since $I \neq \{0\}$, there exists a non-zero element $a \in I$. Also $a^{-1} \in F$ such that $a \cdot a^{-1} = 1 \in I$.

Let $r \in F, 1 \in I \Rightarrow r \cdot 1 \in I$. Thus $F \subseteq I$.

But, $I \subseteq F$.

Hence, $I = F$.

HOMOMORPHISM OF RINGS

View the lecture on YouTube: <https://youtu.be/yasOkiWTFrE>

Definition: Let R and R' be rings. A function $f: R \rightarrow R'$ is called a homomorphism if.

- (i) $f(a + b) = f(a) + f(b)$ and
- (ii) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

Note 1: If f is 1-1, then f is monomorphism. If f is onto, then f is epimorphism.

A homomorphism of a ring onto itself is called an endomorphism.

Note 2: A 1-1, onto homomorphism is an isomorphism.

Example 1: $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$ defined by $f(x) = r$, where $x = an + r$, $0 < r < n$ is a homomorphism.

Solution: For, let $a, b \in \mathbb{Z}$.

Let $a = q_1n + r_1$, where $0 < r_1 < n$.

Let $b = q_2n + r_2$, where $0 < r_2 < n$.

$r_1 + r_2 = q_3n + r_3$, where $0 < r_3 < n$ and

$r_1r_2 = q_4n + r_4$, where $0 < r_4 < n$.

Now, $a + b = (q_1 + q_2)n + r_1 + r_2 = (q_1 + q_2 + q_3)n + r_3$.

$f(a + b) = r_3 = f(a) + f(b)$.

Also, $ab = (q_1n + r_1)(q_2n + r_2) = n(q_1q_2n + r_1q_2 + r_2q_1) + r_1r_2$.

$ab = n(q_1q_2n + r_1q_2 + r_2q_1 + q_4) + r_4$.

$f(ab) = r_4 = r_1 \odot r_2 = f(a) \odot f(b)$.

Hence, f is a homomorphism.

Definition: The kernel of a homomorphism f of a ring R to a ring R' is defined by $\{a / a \in R \text{ and } f(a) = 0\}$ and is denoted by $\text{Ker } f$.

Theorem : Let R and R' be two rings. Let $f: R \rightarrow R'$ be a homomorphism. Then $\text{Ker } f$ is an ideal of R .

Proof: By definition, $\text{Ker } f = f^{-1}(\{0\})$.

Since $\{0\}$ is an ideal of $f(R)$, $\text{Ker } f = f^{-1}(\{0\})$ is an ideal of R .

Theorem 1: (The fundamental theorem of homomorphism)

Let R and R' be rings and $f: R \rightarrow R'$ an epimorphism. Let K be the kernel of f . Then $R/K \cong R'$.

Proof: Define $\phi: R/K \rightarrow R'$ by $\phi(K + a) = f(a)$.

(i) To prove ϕ is well defined.

Let $K + b = K + a$, Then $b \in K + a$.

$\therefore b = k + a$, where $k \in K$.

$$f(b) = f(k + a) = f(k) + f(a) = 0 + f(a) = f(a).$$

$$\phi(K + b) = f(b) = f(a) = \phi(K + a).$$

(ii) Claim: ϕ is 1-1.

For, $\phi(K + a) = \phi(K + b) \Rightarrow f(a) = f(b)$.

$$\Rightarrow f(a) - f(b) = 0 \Rightarrow f(a) + f(-b) = 0.$$

$$f(a - b) = 0. \Rightarrow a - b \in K.$$

$$a \in K + b \Rightarrow K + a = K + b.$$

(iii) Claim: ϕ is onto.

For, let $a' \in R'$.

Since f is onto, there exists $a \in R$ such that $f(a) = a'$.

$$\text{Hence, } \phi(K + a) = f(a) = a'.$$

(iv) Claim: ϕ is homomorphism.

$$\phi[(K + a) + (K + b)] = \phi[K + (a + b)] = f(a + b) = f(a) + f(b).$$

$$\therefore \phi[(K + a) + (K + b)] = \phi(K + a) + \phi(K + b).$$

$$\phi[(K + a)(K + b)] = \phi[K + (ab)] = f(ab) = f(a)f(b).$$

$$\therefore \phi[(K + a)(K + b)] = \phi(K + a)\phi(K + b).$$

Hence, ϕ is an isomorphism.

INTEGER MODULO n

Definition: Integer modulo n (Congruence modulo 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 .

Properties of Congruences:

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$(i) \ a + c \equiv b + d \pmod{n}.$$

$$(ii) \ a - c \equiv b - d \pmod{n}.$$

$$(iii) \ ac \equiv bd \pmod{n}.$$

Definition: Euclidean Division Algorithm

If a is any integer and b is a positive integer then there exists unique integers q and r such that $a = qb + r$, $0 \leq r < b$, where q is called the quotient and r is the remainder when a is divided by b . Then we write $a \equiv r \pmod{b}$.

Theorem 3: Z_n is a field if and only if n is prime.

Proof:

Assume Z_n is a field.

Claim: n is prime.

Suppose n is not a prime.

Then $n = a \cdot b$, where a and b are primes.

$$\Rightarrow a|n \text{ and } b|n$$

$$\Rightarrow n = ka \text{ and } n = mb, \text{ for some } k, m \in \mathbb{Z}^+.$$

$$\therefore ka = mb$$

$$\Rightarrow a = \frac{m(b)}{k}, \text{ where } \frac{m}{k} \in \mathbb{Q}.$$

Which is a contradiction to the fact that a and b are prime.

$\therefore n$ is a prime.

Conversely, Assume n is a prime.

Claim: Z_n is a field.

Let $a \in \mathbb{Z}_n$.

Since n is prime.

Then $\gcd(a, n) = 1, 0 < a < n$.

\therefore There exist $s, t \in \mathbb{Z}$ such that $as + tn = 1$ (By Division algorithm)

$$\Rightarrow as - 1 = (-t)n$$

$\therefore as - 1$ is divisible by n .

$$\Rightarrow as \equiv 1 \pmod{n}$$

$$\Rightarrow [as] = [1]$$

$$\Rightarrow [a][s] = [1]$$

$\therefore [a]$ is a unit of \mathbb{Z}_n .

Hence \mathbb{Z}_n is a field.

Theorem 4: In \mathbb{Z}_n , $[a]$ is a unit if and only if $\gcd(a, n) = 1$.

Proof:

Assume $[a]$ is a unit of \mathbb{Z}_n .

$$\Rightarrow [a][s] = [1]$$

$$\Rightarrow as \equiv 1 \pmod{n}$$

$\Rightarrow as - 1$ is divisible by n .

$$\Rightarrow as - 1 = tn \text{ for some } t \in \mathbb{Z}.$$

$$\Rightarrow as + (-t)n = 1.$$

$$\therefore \gcd(a, n) = 1.$$

Conversely, Assume $\gcd(a, n) = 1$.

Then there exists integers s and t such that $as + nt = 1$.

$$\Rightarrow as - 1 = (-t)n.$$

$\Rightarrow as - 1$ is divisible by n .

$$\Rightarrow as \equiv 1 \pmod{n}.$$

$$\therefore [a][s] = [1].$$

$$\Rightarrow [a]^{-1} = [s].$$

Hence $[a]$ is a unit of \mathbb{Z}_n .

Example 1: Find $[100]^{-1}$ in the ring Z_{1009} .

Solution:

Since 100 and 1009 are relatively prime.

$$\therefore \gcd(100, 1009) = 1.$$

By Euclidean Algorithm, $1009 = 10(100) + 9$

$$100 = 11(9) + 1.$$

$$9 = 3(3) + 0.$$

As 1 is the last non-zero remainder.

$$\therefore 1 = 100 - 11(9).$$

$$= 100 - 11[1009 - 10(100)].$$

$$= 111(100) - 11(1009).$$

$$\Rightarrow 1 - 111(100) = -11(1009).$$

$\Rightarrow 1 - 111(100)$ is divisible by 1009.

$$\therefore 1 \equiv 111(100) \pmod{1009}.$$

$$\Rightarrow [1] = [111][100] \text{ in the ring } Z_{1009}.$$

$$\therefore [100]^{-1} = [111] \text{ in the ring } Z_{1009}.$$

Example 2: Find $[100]^{-1}$ in the ring Z_{72} .

Solution:

Since $\gcd(25, 72) = 1$.

By Euclidean algorithm,

$$72 = 2(25) + 22$$

$$25 = 1(22) + 3$$

$$22 = 7(3) + 1$$

As 1 is the last non-zero remainder.

$$\therefore 1 = 22 - 7(3)$$

$$= 22 - 7(25 - 22)$$

$$= 8(22) - 7(25)$$

$$= 8(72 - 2(25)) - 7(25).$$

$$1 = 8(72) - 23(25)$$

$$\Rightarrow 1 + 23(25) = 8(72)$$

$\Rightarrow 1 + 23(25)$ is divisible by 72

$$\therefore 1 \equiv (-23)(25) \pmod{72}.$$

$$\therefore \Rightarrow [1] = [-23][25].$$

$$\therefore [25]^{-1} = [-23] \text{ in the ring } Z_{72}.$$

$$\Rightarrow [25]^{-1} = [49] \text{ in the ring } Z_{72}. \text{ (since } -23 \equiv 49 \pmod{72}\text{)}.$$

Example 3: Find $[17]^{-1}$ in the ring Z_{1009} .

Solution:

Since 17 and 1009 are relatively prime, the $\gcd(17, 1009) = 1$.

By Euclidean Algorithm, $1009 = 59(17) + 6$

$$17 = 2(6) + 5.$$

$$6 = 1(5) + 1.$$

As 1 is the last non-zero remainder.

$$\therefore 1 = 6 - 1(5).$$

$$= 6 - 1[17 - 2(6)].$$

$$= 3(6) - 17 = 3[1009 - 59(17)] - 17.$$

$$1 = 3(1009) - 178(17).$$

$$\therefore 1 \equiv -178(17) \pmod{1009}.$$

$$\Rightarrow [1] = [-178][17].$$

$$\therefore [17]^{-1} = [-178] \text{ in the ring } Z_{1009}.$$

$$\therefore \text{Since } -178 \equiv 831 \pmod{1009}.$$

$$\therefore [17]^{-1} = [-178] \text{ in the ring } Z_{1009}.$$

$$\therefore -178 \equiv 831 \pmod{1009}.$$

$$\therefore [-178] = [831].$$

$$\therefore \text{Hence, } [17]^{-1} = [831] \text{ in the ring } Z_{1009}.$$

PRACTICE QUIZ: GROUPS AND RINGS

- If G is a group of order p , where p is a prime number. Then the number of subgroups of G is
 a) 1 b) 2 c) $p - 1$ d) p
- The set of all real numbers under the usual multiplication operation is not a group since
 a) multiplication is not a binary operation b) multiplication is not associative
 c) identity element does not exist d) zero has no inverse
- If (G, \cdot) is a group such that $a^2 = e$, for all $a \in G$, then G is
 a) semi group b) abelian group
 c) non-abelian group d) none of these
- The set of integers Z with the binary operation $*$ defined as $a * b = a + b + 1$ for $a, b \in Z$, is a group. The identity element of this group is
 a) 0 b) 1 c) -1 d) 12
- In the group (G, \cdot) , the value of $(a^{-1}b)^{-1}$ is
 a) ab^{-1} b) $b^{-1}a$ c) $a^{-1}b$ d) ba^{-1}
- The set of integers Z with the binary operation $*$ defined as $a * b = a + b + 1$ for $a, b \in Z$, is a group. The inverse of a is
 a) 0 b) -2 c) $a - 2$ d) $-a - 2$
- Which of the following is TRUE ?
 a) Set of all rational negative numbers forms a group under multiplication
 b) Set of all non-singular matrices forms a group under multiplication
 c) Set of all matrices forms a group under multiplication
 d) Both b) and c)
- Let R be any non zero ring. Choose all the correct statements. Z denotes the ring of integers
 a) Suppose every proper ideal of R is prime, then R is a field.
 b) Every non-zero proper ideal of Z is maximal
 c) Every non-zero proper ideal of $Z[x]$ is prime.
 d) Every integral domain is a field.
- Select all the true statements. Note that, by definition, any ring homomorphism $R_1 \rightarrow R_2$ sends 1 to 1. Z denotes the ring of integers; Q and C denote the fields of rationals and complex respectively.
 a) There are atleast two homomorphisms $Z \rightarrow Q$.
 b) There are exactly one homomorphism $Q \rightarrow Q$.
 c) If R is any ring $\phi: C \rightarrow R$ is a ring homomorphism, then ϕ is injective.
 d) If R is any non zero ring $\phi: Z \rightarrow R$ is a ring homomorphism, then ϕ is injective.

Answers to the Practice Quiz:

1. b) 2. d) 3. b) 4. c) 5. b) 6. d) 7. b) 8. a) 9. b)

STUCOR APP

Answers to the Practice Quiz:

1. a) 2. c) 3. a) & d) 4. d) 5. b) 6. d) 7. b) 8. a)

STUCOR APP

ASSIGNMENTS: UNIT I

1. Why is the set of integers not a group under subtraction?
2. What are the zero divisors in the ring Z_{12} (with respect to the operations addition modulo 12 and multiplication modulo 12).
3. Let $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Show that $A = \{A, A^2, A^3, A^4\}$ is a group under matrix multiplication and is isomorphic to $(Z_4, +)$ under addition modulo 4.
4. Show that subgroup of a cyclic group is cyclic.
5. Prove that every group of prime order is cyclic.
6. Let G be the set of all rigid motions of an equilateral triangle. Identify the elements of G . Show that it is a non abelian group of order 6.
7. Prove that every finite integral domain is a field.
8. Find $[777]^{-1}$ in the ring Z_{1009} .

PART A QUESTIONS AND ANSWERS: UNIT I

1. Define Groups.

(K1, CO1)

A non empty set G together the binary operation $*$ is said to be Group $(G,*)$ provided the following conditions are satisfied

Closure : For all $a, b \in G \Rightarrow a * b \in G$

Associative: For all $a, b, c \in G$

$$\Rightarrow a * (b * c) = (a * b) * c$$

Identity : There exist an $e \in G$ with

$$a * e = a = e * a \text{ or all } a \in G$$

Inverse : For each $a \in G$, there is an element

$$a^{-1} \in G \text{ such that } a * a^{-1} = e = a^{-1} * a$$

2. Define abelian group.

(K1, CO1)

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

3. Determine whether $\{-1,1\}$ is a group under addition?

(K2, CO1)

Solution : Let $-1, 1 \in G \Rightarrow (-1) + 1 = 0 \notin G$ closure is not exist

There fore, $\{-1,1\}$ is a not a group under addition.

4. Determine whether $\{-1,1\}$ is a group under multiplication? (K2, CO1)

Solution : **Closure:** Let $-1, 1 \in G \Rightarrow (-1) \cdot 1 = -1 \in G$ (Closure exist)

Identity: Let $-1 \in G$ an identity element $1 \in G$

$$\text{such that } (-1) \cdot 1 = -1 = 1 \cdot (-1) \text{ (Identity exist)}$$

Inverse: Let $-1 \in G$, inverse of -1 is -1

$$\text{Let } 1 \in G, \text{ inverse of } 1 \text{ is } 1$$

such that $(-1) \cdot (-1) = 1 = (-1) \cdot (-1)$ (Inverse exist)

There fore $\{-1, 1\}$ is a group under multiplication

5. Define Subgroup. (K1, CO1)

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

6. Define Cyclic group. (K1, CO1)

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

7. Prove that $G = \{1, \omega, \omega^2\}$ is a cyclic group under usual multiplication.

(K2, CO1)

Solution:

The generators of G are $\langle \omega \rangle$ and $\langle \omega^2 \rangle$.

Since $1 = (\omega)^3$, $\omega = (\omega)^1$, $\omega^2 = (\omega)^5$ and $1 = (\omega^2)^3$, $\omega = (\omega^2)^2$, $\omega^2 = (\omega^2)^4$.

Hence $G = \{1, \omega, \omega^2\}$ is a cyclic group under usual multiplication.

8. Find the left cosets of the subgroup $H = \{[0], [1]\}$ of the group $(Z_6, +_6)$.

(K2, CO1)

Solution:

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

$$H = \{[0], [3]\} \text{ is a subgroup of } Z_6$$

The left cosets of H are given by,

$$[0] + H = \{[0], [3]\}$$

$$[1] + H = \{[1], [4]\}$$

$$[2] + H = \{[2], [5]\}$$

Hence, H , $[1] + H$, $[2] + H$ are distinct left cosets.

9. Find all the subgroups of $(Z_9, +_9)$.

(K2, CO1)

Solution:

$$Z_9 = \{ [0], [1], [2], [3], \dots, [8] \}$$

$(Z_9, +_9)$ is a cyclic group of order 9

Converse of the Lagrange's theorem is true for any finite cyclic group.

The divisors of 9 are 1, 3 and 9

So, we have three subgroups H_1, H_2, H_3 of order 1, 3, 9 respectively

$$H_1 = \{ [0] \}$$

$$H_2 = \{ [0], [3], [6] \}$$

$$H_3 = Z_9$$

10. Define the term Normal Subgroup of a group.

(K1, CO1)

Solution:

A subgroup N of a group G is said to be a normal subgroup of G if $gng^{-1} \in N \quad \forall g \in G \text{ and } n \in N$.

11. Define Simple subgroup and give an example.

(K1, CO1)

Solution:

A group having no proper normal subgroup is called a simple group.

Example:

Every group of prime order is simple for it does not possess any proper subgroup.

12. Define Quotient group.

(K1, CO1)

Solution:

Let N be a normal subgroup of G . Let $\frac{G}{N}$ denotes the collection of all distinct right cosets of N in G .

$$\text{i.e., } \frac{G}{N} = \{ Na \mid a \in G \}$$

Then $\frac{G}{N}$ is a group under cosets multiplication. It is called a quotient group or factor group of $\frac{G}{N}$.

13. If f is a homomorphism of the groups (G, o) into $(G', *)$, then show that $f(a^{-1}) = [f(a)]^{-1}$. (K2, CO1)

Solution:

For any $a \in G$ there exist $a^{-1} \in G \ni a o a^{-1} = a^{-1} o a = e$

$$\text{Now, } f(a o a^{-1}) = f(a) * f(a^{-1})$$

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

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

$$f(a^{-1} o a) = f(a^{-1}) * f(a)$$

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

$$e' = f(a^{-1}) * f(a) \text{ -----(2)}$$

From the equations (1) & (2), we see that

$f(a^{-1})$ is an inverse of $f(a)$

$$\text{Hence, } f(a^{-1}) = [f(a)]^{-1}.$$

14. Define Kernel of a homomorphism.

(K1, CO1)

Solution:

Let (G, o) and $(G', *)$ be any two groups e and e' be the identity elements of G and G' respectively. If $f: G \rightarrow G'$ is a group homomorphism, then the subset K of G defined by $K = \{x \in G \mid f(x) = e'\}$ is called the Kernel of f and is denoted by $\ker f$.

15. If Kernel K of a homomorphism is a subgroup of G then show that K is a normal subgroup of G . (K2, CO1)

Solution:

Let f be a homomorphism of a group (G, o) into a group $(G', *)$ with Kernel K .

Given that Kernel K is a subgroup of G .

For any $g \in G$ and $k \in K$

We have

$$\begin{aligned}
 f(g \circ k \circ g^{-1}) &= f(g) * f(k) * f(g^{-1}) \\
 &= f(g) * e' * f(g^{-1}) \\
 &= f(g) * f(g^{-1}) \\
 &= f(g) * [f(g)]^{-1} \\
 &= e'
 \end{aligned}$$

Therefore, $g \circ k \circ g^{-1} \in K$ for all $g \in G$ and $k \in K$

Hence K is a normal subgroup of G .

16. If $f: (Z, +) \rightarrow (2Z, +)$ be defined by $f(a) = 2a \forall a \in Z$. Then show that f is isomorphism. (K2, CO1)

Solution:

Let $a, b \in Z$. First we have to verify that $f(a + b) = f(a) + f(b)$

$$\begin{aligned}
 a, b \in Z &\Rightarrow a + b \in Z. \text{ So } f(a + b) = 2(a + b) \\
 &= 2a + 2b \\
 &= f(a) + f(b)
 \end{aligned}$$

Hence f is a homomorphism.

$$\begin{aligned}
 \text{Now } f(a) &= f(b) \\
 &\Rightarrow 2a = 2b \\
 &\Rightarrow a = b
 \end{aligned}$$

Therefore, f is one –one

For every $2a \in 2Z \exists a \in Z$

such that $f(a) = 2a$

Therefore, f is onto.

Hence f is isomorphism.

17. Define automorphism and give an example.

(K2, CO1)

Solution:

An isomorphism of a group G to itself is called an automorphism of the group.

Example:

Let $(G, .)$ be any group. The identity map $I_G: G \rightarrow G$ defined by $I_G(a) = a$, $\forall a \in G$ is an automorphism.

Solution:

Let $a, b \in G \Rightarrow a.b \in G$

so $I_G(a.b) = a.b$

$= I_G(a) . I_G(b)$

Therefore, the mapping I_G is homomorphism.

We see that, clearly the identity mapping I_G is Bijective.

Hence I_G is an automorphism.

18. Give an example of a ring which is not a field.

(K2, CO2)

Solution: The set of integers Z with respect to addition and multiplication is a ring but not a field.

19. Define integral domain and give an example.

(K1, CO2)

Solution: A commutative ring $(R, +, .)$ with unity and without zero divisors is called an Integral domain. $(Z, +, .)$ is an integral domain.

20. Prove that the ring $(Z_6, +_6, \times_6)$ is not an Integral domain.

(K3, CO2)

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

Since $[2] \times_6 [3] = 0$

But $[2] \neq 0, [3] \neq 0$

$\therefore [2]$ and $[3]$ are zero divisors in Z_6

Hence $(Z_6, +_6, \times_6)$ is not an integral domain.

21. Define field and give an example.

(K1, CO2)

Solution: A commutative ring $(R, +, \cdot)$ with identity in which every non-zero element has multiplicative inverse is called a field. $(Q, +, \cdot)$ is a field.

22. Does the set R of positive integers and zero form a ring under addition and multiplication of integers? Justify your answer?

(K2, CO2)

Solution: No R is not a ring. Since additive inverse does not exist for every non zero positive integers of R . So, $(R, +)$ is not an abelian group. Hence R is not a ring.

23. Let R be a ring. Show that for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

(K2, CO2)

Solution: Since, $a \cdot 0 = 0 \Rightarrow a(b + (-b)) = 0$, for any $b \in R$

$$\Rightarrow a \cdot b + a \cdot (-b) = 0$$

$$\therefore a \cdot (-b) = -(a \cdot b)$$

(Additive Inverse)

Similarly, we can prove that $(-a) \cdot b = -(a \cdot b)$

$$\therefore a \cdot (-b) = (-a) \cdot b = -(a \cdot b).$$

PART B QUESTIONS: UNIT I

1. Let $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Show that $A = \{A, A^2, A^3, A^4\}$ is a group under matrix multiplication and is isomorphic to $(Z_4, +)$ under addition modulo. (K3,CO1)
2. Let $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Show that $A = \{A, A^2, A^3, A^4\}$ is a group under matrix multiplication and is isomorphic to $Z_5 = \{1, 2, 3, 4\}$ under multiplication modulo 5. What are the subgroups of G ? Verify that orders of the subgroups of G divide order of G . (K3,CO1)
3. Let $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Show that $A = \{A, A^2, A^3, A^4\}$ is an abelian group under matrix multiplication and is isomorphic to (G, \cdot) , where $G = \{1, -1, i, -i\}$ and \cdot is the ordinary multiplication. (K3,CO1)
4. Show that subgroup of a cyclic group is cyclic. (K2,CO1)
5. Prove that every group of prime order is cyclic. (K2,CO1)
6. Let G be the set of all rigid motions of an equilateral triangle. Identify the elements of G . Show that it is a non abelian group of order 6. (K3,CO1)
7. Examine whether $G = \{1, 2, 3, 4\}$ is a group under multiplication modulo 5. What is the order of G ? Determine the order of each element of G and verify that the order of every element divides the order of G . (K3,CO1)
8. State and prove Lagrange's theorem. (K3,CO1)
9. Is the group $(Z_{12}, +)$ cyclic? What are the subgroups? Examine whether the subgroups are cyclic. (K3,CO1)
10. Let k, m be fixed integers. Find all values for k, m for which (Z, \oplus, \odot) is a ring under the binary operations $(x \oplus y) = x + y - k, (x \odot y) = x + y - mxy$, where $x, y \in Z$. (K3,CO2)
11. Prove that every finite integral domain is a field. (K3,CO2)
12. Show that Z_n is a field with respect to addition modulo n and multiplication modulo n if and only if n is a prime. (K3,CO2)
13. Prove that in Z_n , $[a]$ is a unit if and only if $\gcd(a, n) = 1$. (K3,CO2)
14. Find $[777]^{-1}$ in the ring Z_{1009} . (K3,CO2)
15. What are the zero divisors in the ring Z_{12} (with respect to the operations addition modulo 12 and multiplication modulo 12). (K3,CO2)

SUPPORTIVE ONLINE CERTIFICATION COURSES

The following NPTEL and Coursera courses are the supportive online certification courses for the subject Algebra and Number theory.

1. Introduction to Abstract Group Theory (NPTEL course)

<https://nptel.ac.in/courses/111/106/111106113/>

2. Introduction to Rings and Fields (NPTEL course)

<https://nptel.ac.in/courses/111/106/111106131/#>

3. Mathematical Foundations for Cryptography (Coursera online course).

<https://www.coursera.org/learn/mathematical-foundations-cryptography>

View the following lectures on YouTube:

Applications of Groups

<https://youtu.be/vX8J9oqsVfM>

Motivation for Groups:

https://youtu.be/PN-cro0J_v8

Application of Fields

<https://youtu.be/nczJ7Nw41mU>

Construction of Finite Fields: (Application in Coding theory)

<https://youtu.be/GJtNLiG4Hv8>

Applications of Polynomial Rings

https://youtu.be/4WEhfOI_JAA

DOWNLOADED FROM STUCOR APP

CONTENT BEYOND THE SYLLABUS

The topic **Introduction to Vector space** is the content beyond the syllabus for the course Algebra and Number Theory.

View the lecture on YouTube:

<https://youtu.be/YshfZm99wjk>

Value Added Courses:

1. Mathematics for Machine Learning: Linear Algebra (Coursera online course)
2. Mathematical Foundations for Cryptography (Coursera online course)

STUCOR APP

PRESCRIBED TEXT BOOKS & REFERENCE BOOKS

TEXTBOOKS:

1. Grimaldi, R.P and Ramana, B.V., "Discrete and Combinatorial Mathematics", Pearson Education, 5th Edition, New Delhi, 2007.
2. Koshy, T.,—"Elementary Number Theory with Applications", Elsevier Publications, New Delhi, 2002.

REFERENCES:

1. Lidl, R. and Pitz, G, "Applied Abstract Algebra", Springer Verlag, New Delhi, 2nd Edition, 2006.
2. Niven, I., Zuckerman.H.S., and Montgomery, H.L., —"An Introduction to Theory of Numbers", John Wiley and Sons , Singapore, 2004.
3. San Ling and Chaoping Xing, —"Coding Theory – A first Course", Cambridge Publications, Cambridge, 2004.

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

STUCOR APP

STUCOR APP

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

MA 8551 - Algebra and Number Theory

Department: Mathematics

Batch/Year: CSE/ III

Created by: Mr.J.Leo Amalraj

Date: 28.07.2020

Table of Contents

Contents		
1	Course Objectives	1
2	Pre Requisites	2
3	Syllabus	3
4	Course Outcomes	4
5	CO – PO/PSO Mapping	5
6	Lecture Plan: Unit I Groups and Rings	6
7	Lecture Plan: Unit II Finite Fields And Polynomials	7
8	Activity Based Learning	8
9	Lecture Notes: Unit I Groups and Rings	9
10	Groups	10
11	Properties of Groups	11
12	Subgroups	16
13	Cosets and Lagrange's Theorem	23
14	Normal subgroups	26
15	Group Homomorphism	28
16	Quotient groups	35
17	Rings	39
18	Homomorphism of Rings	46
19	Integer modulo n	48
20	Practice Quiz: Groups and Rings	52
21	Lecture Notes: Unit II Finite Fields And Polynomials	54
22	Polynomial rings	55
23	Division Algorithm	68
24	Irreducible polynomials over finite fields	70
25	Greatest Common Divisor	73
26	Characteristic of a Ring	76
27	Congruence Relation in $F[x]$	78
28	Practice Quiz: Finite Fields And Polynomials	82
29	Assignments: Unit I	84
30	Assignments: Unit II	85
31	Part A Questions and Answers: Unit I	86

Contents

32	Part A Questions and Answers: Unit II	93
33	Part B Questions: Unit I	98
34	Part B Questions: Unit II	99
35	Supportive online Certification courses	100
36	Real time Applications	101
37	Content beyond the Syllabus	102
38	Prescribed Text Books & Reference Books	103

...

...

STUCOR APP

COURSE OBJECTIVES

To introduce the basic notions of groups, rings, fields which will then be used to solve related problems.

To introduce and apply the concepts of rings, finite fields and polynomials.

To understand the basic concepts in number theory.

To examine the key questions in the Theory of Numbers.

To give an integrated approach to number theory and abstract algebra, and provide a firm basis for further reading and study in the subject.

PRE REQUISITES

Pre Requisites for the subject Algebra and Number Theory is
MA 8351 - Discrete Mathematics.

STUCOR APP

DOWNLOADED FROM STUCOR APP

SYLLABUS

MA8551	ALGEBRA AND NUMBER THEORY	L	T	P	C
		4	0	0	4

UNIT I GROUPS AND RINGS 12

Groups : Definition - Properties - Homomorphism - Isomorphism - Cyclic groups - Cosets - Lagrange's theorem. Rings: Definition - Sub rings - Integral domain - Field - Integer modulo n - Ring homomorphism.

UNIT II FINITE FIELDS AND POLYNOMIALS 12

Rings - Polynomial rings - Irreducible polynomials over finite fields - Factorization of polynomials over finite fields.

UNIT III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS 12

Division algorithm – Base - b representations – Number patterns – Prime and composite numbers – GCD – Euclidean algorithm – Fundamental theorem of arithmetic – LCM.

UNIT IV DIOPHANTINE EQUATIONS AND CONGRUENCES 12

Linear Diophantine equations – Congruence's – Linear Congruence's - Applications: Divisibility tests - Modular exponentiation-Chinese remainder theorem – 2 x 2 linear systems.

UNIT V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS 12

Wilson's theorem – Fermat's little theorem – Euler's theorem – Euler's Phi functions – Tau and Sigma functions.

TOTAL: 60 PERIODS

COURSE OUTCOMES

CO 1: Apply the basic notions of groups which will be used to solve group theory related problems.

CO 2: Apply the basic notions of rings, fields which will then be used to solve related problems.

CO 3: Demonstrate accurate and efficient use of advanced algebraic techniques such as finite fields and polynomials.

CO 4: Explain the fundamental concepts of number theory, advanced algebra and their role in modern mathematics.

CO 5: Demonstrate the number theory concepts by solving non - trivial related problems.

CO 6: Apply integrated approach to number theory and abstract algebra and prove simple theorems.

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
CO2	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
CO3	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
CO4	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
CO5	3	2	-	-	-	-	-	-	-	-	-	-	-	-	-
CO6	3	2	1	-	-	-	-	-	-	-	-	-	1	-	-

LECTURE PLAN**UNIT II FINITE FIELDS AND POLYNOMIALS**

S. No	Topic	No. of Periods	Proposed date	Actual date	Pretaining CO	Taxonomy level	Mode of Delivery
1.	Rings - Polynomial rings	1			CO3	K2	PPT
2.	Theorems in Polynomial rings	2			CO3	K3	PPT
3.	Division algorithm for polynomials	1			CO3	K2	PPT
4.	Irreducible polynomials over finite fields	2			CO3	K2	PPT
5.	Problems in irreducible polynomials	2			CO3	K3	PPT
6.	Factorization of polynomials over finite fields.	1			CO3	K3	PPT
7.	Problems in Factorization of polynomials	1			CO3	K3	PPT
8.	Congruence Relation in $F[x]$	1			CO3	K3	PPT
9.	Characteristic of a ring	1			CO3	K3	PPT

ACTIVITY BASED LEARNING

Activity based learning helps students express and embrace their curiosity. Once the students become curious, they tend to explore and learn by themselves. To evoke curiosity in students, Practice quiz is designed for all the five units.

STUCOR APP

LECTURE NOTES**UNIT I GROUPS AND RINGS**

Group theory is one of the most important fundamental concepts of modern algebra. Groups can be considered as the starting point of the study of various algebraic structures. In this chapter, we shall first define groups and study some of their basic properties. In addition, we shall study an algebraic structure equipped with two binary operations, called rings.

Groups : Definition - Properties - Homomorphism - Isomorphism - Cyclic groups -

Cosets - Lagrange's theorem. Rings: Definition - Sub rings - Integral domain -

Field -Integer modulo n - Ring homomorphism.

E- Book Reference:

<http://www2.math.umd.edu/~jcohen/402/Pinter%20Algebra.pdf>

LECTURE NOTES**UNIT II FINITE FIELDS AND POLYNOMIALS**

In this chapter, we shall define polynomials which have coefficients from a ring R and show that the collection of all such polynomials form a ring called polynomial rings. Furthermore, we shall study in detail the algebraic properties of this polynomial rings.

Rings - Polynomial rings - Irreducible polynomials over finite fields - Factorization of polynomials over finite fields.

E- Book Reference:

<http://www2.math.umd.edu/~jcohen/402/Pinter%20Algebra.pdf>

View the lecture on YouTube: <https://youtu.be/5NzDN1M6qic>

Definition: Polynomials

Let $(R, +, \cdot)$ be a ring. An expression of the form

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

Where n is the non negative integers and $a_0, a_1, a_2 \cdots a_n \in R$ is called a Polynomial over R in the indeterminate x .

Definition: If $a_n \neq 0$ then a_n is called leading coefficient of $f(x)$ and we say that $f(x)$ has degree n . Hence the degree of the polynomial is the highest power of x . a_0 is called the constant term of $f(x)$.
The set of all polynomials in x over R is denoted by $R[x]$.

Definition: Equal Polynomials

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 $f(x) = g(x)$ if $m = n$, $a_i = b_i$.
 $\forall i = 0, 1, 2, \dots, n$ is called equal polynomials.

Definition: Zero Polynomial

A polynomial in $R[x]$ with all coefficients zero is called zero polynomial.
Zero polynomial has no degree.

Definition: Constant Polynomial

A polynomial of the form $f(x) = a_0$, where a_0 is a constant is called a constant polynomial.

The degree of non-zero constant polynomial is zero.

Definition: Monic Polynomial

A polynomial in which the leading coefficient is 1 is called the monic polynomial.

Definition: 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, $f(x) + g(x) = C_0 + C_1x + C_2x^2 + \cdots + C_sx^s$

$$C_i = a_i + b_i, \quad \forall i$$

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m) \\ &= C_0 + C_1x + C_2x^2 + \cdots + C_kx^k \end{aligned}$$

Where $C_0 = a_0 b_0$

$$C_1 = a_0 b_1 + a_1 b_0$$

$$C_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$\vdots$$

$$C_r = a_0 b_1 + a_1 b_{r-1} + \cdots + a_r b_0.$$

Example 1:

Let $f(x), g(x) \in \mathbb{Z}_7[x]$, where $f(x) = 2x^4 + 2x^3 + 3x^2 + x + 4$ and $g(x) = 3x^3 + 5x^2 + 6x + 1$, determine the values of $f(x) + g(x)$, $f(x) - g(x)$, $f(x) * g(x)$.

Solution:

$$\begin{aligned}
 f(x) + g(x) &= (2x^4 + 2x^3 + 3x^2 + x + 4) + (3x^3 + 5x^2 + 6x + 1) \\
 &= 2x^4 + 5x^3 + 8x^2 + 7x + 5, (8 \equiv 1(\text{mod } 7)), (7 \equiv 0(\text{mod } 7)) \\
 &= 2x^4 + 5x^3 + 1x^2 + 5
 \end{aligned}$$

$$\begin{aligned}
 f(x) - g(x) &= (2x^4 + 2x^3 + 3x^2 + x + 4) - (3x^3 + 5x^2 + 6x + 1) \\
 &= 2x^4 + 5x^3 + 1x^2 + 0x + 5 \\
 &= 2x^4 - x^3 - 2x^2 - 5x + 3, (-1 \equiv 6(\text{mod } 7)), (-2 \equiv 5(\text{mod } 7)), \\
 &\quad (-5 \equiv 2(\text{mod } 7)) \\
 &= 2x^4 + 6x^3 + 5x^2 + 2x + 3
 \end{aligned}$$

$$\begin{aligned}
 f(x) * g(x) &= (2x^4 + 2x^3 + 3x^2 + x + 4) * (3x^3 + 5x^2 + 6x + 1) \\
 &= (6x^7 + 10x^6 + 12x^5 + 2x^4) + (6x^6 + 10x^5 + 12x^4 + 2x^3) \\
 &\quad + (9x^5 + 15x^4 + 18x^3 + 3x^2) + (3x^4 + 5x^3 + 6x^2) \\
 &= 6x^7 + 16x^6 + 31x^5 + 32x^4 + 37x^3 + 29x^2 + 25x + 4 \\
 &= 6x^7 + 2x^6 + 3x^5 + 4x^4 + 2x^3 + x^2 + 4x + 4
 \end{aligned}$$

$$\begin{aligned}
 &\text{Since } 16 \equiv 2(\text{mod } 7), 31 \equiv 3(\text{mod } 7), 32 \equiv 4(\text{mod } 7), 37 \equiv 2(\text{mod } 7), \\
 &\quad 29 \equiv 1(\text{mod } 7).
 \end{aligned}$$

Definition: Roots of the Polynomial

Let R the ring with identity 1

Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

Let $a \in R$, If $f(a) = 0$, then a is the root of $f(x)$.

Example 1: Find all the roots of the polynomial $f(x) = x^2 + 4x$ in $\mathbb{Z}_{12}[x]$.

Solution : We know that $\mathbb{Z}_{12}[x] = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$$f(0) = 0 + 0 = 0 \quad \therefore 0 \text{ is the root of } f(x)$$

$$f(1) = 1 + 4 = 5 \neq 0 \quad \therefore 1 \text{ is not the root of } f(x)$$

$$f(2) = 2^2 + 4(2) = 4 + 8 = 12 = 0(\text{mod } 12)$$

$$f(3) = 9 + 12 = 21 = 9(\text{mod } 12) \neq 0$$

$$f(4) = 16 + 16 = 32 = 8(\text{mod } 12) \neq 0$$

$$f(5) = 25 + 20 = 45 = 9(\text{mod } 12) \neq 0$$

$$f(6) = 36 + 24 = 60 = 0(\text{mod } 12)$$

$$f(7) = 49 + 28 = 77 = 5(\text{mod } 12) \neq 0$$

$$f(8) = 64 + 32 = 96 = 0(\text{mod } 12)$$

$$f(9) = 81 + 36 = 117 = 9(\text{mod } 12) \neq 0$$

$$f(10) = 100 + 40 = 140 = 8(\text{mod } 12) \neq 0$$

$$f(11) = 121 + 44 = 165 = 9(\text{mod } 12) \neq 0$$

Therefore the roots of the Polynomial $x = 0, 2, 6, 8$.

Example 2: Find all the roots of the polynomial $f(x) = x^2 + 3x + 2$ in $\mathbb{Z}_6[x]$.

Solution: We know that $\mathbb{Z}_6[x] = \{0, 1, 2, \dots, 5\}$

$$f(0) = 0 + 0 + 2 = 2$$

$$f(1) = 1 + 3 + 2 = 6 = 0(\text{mod } 6)$$

$$f(2) = 4 + 6 + 2 = 12 = 0(\text{mod } 6)$$

$$f(3) = 9 + 9 + 2 = 20 = 2(\text{mod } 6).$$

$$f(4) = 16 + 12 + 2 = 30 = 0(\text{mod } 6)$$

$$f(5) = 25 + 15 + 2 = 42 = 0(\text{mod } 6)$$

Therefore, the roots of the polynomials are $x = 1, 2, 4, 5$.

Theorem 1:

Let $(R, +, \cdot)$ be a commutative ring with identity 1 then R is an integral domain then prove that

$$\deg((f(x), g(x))) = \deg(f(x)) + \deg(g(x)).$$

Proof: Let $(R, +, \cdot)$ be a commutative ring with identity 1 then R is an integral domain

To prove: $\deg((f(x), g(x))) = \deg(f(x)) + \deg(g(x)).$

Let R is an integral domain

Then R is a commutative ring with identity and without zero divisors.

$$(i.e) \quad a \neq 0, b \neq 0 \Rightarrow ab \neq 0$$

$$\text{Let} \quad f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, a_n \neq 0$$

$$\text{then } \deg(f(x)) = n$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, b_m \neq 0$$

$$\text{then } \deg(g(x)) = m$$

Since R is an integral domain, $a_n \cdot b_m \neq 0$.

$$f(x)g(x) = (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)$$

$$= C_0 + C_1x + C_2x^2 + \cdots + C_{n+m}x^{n+m}$$

$$\text{Then } c_{n+m} = a_n \cdot b_m \neq 0$$

$$\deg(f(x)g(x)) = n + m$$

$$= \deg(f(x)) + \deg(g(x)).$$

Theorem 2: If R is a ring under usual addition and multiplication
Show that $[R[x], +, \cdot]$ is a ring of polynomial over R .

Proof: R is a ring under usual addition and multiplication.

To Prove : $[R[x], +, \cdot]$ is a ring of polynomial over R .

Given R is a ring, and let $f(x), g(x) \in R[x]$ such that

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, a_n \neq 0 \text{ and}$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, a_m \neq 0$$

where $a_i, b_j \in R$ for all $0 \leq i \leq n, 0 \leq j \leq m$ for $n \geq m$

Closure under addition:

Given R is a ring, and let $f(x), g(x) \in R[x]$ such that

$$\text{Consider } f(x) + g(x) = C_0 + C_1x + C_2x^2 + \cdots + C_sx^s$$

$$\text{where } C_i = a_i + b_i, \quad \forall i$$

$$\text{since, } a_i + b_i \in R, \quad C_i \in R$$

$$\Rightarrow f(x) + g(x) \in R[x]$$

Associative: Since addition $+$ and multiplication \cdot are associative in R ,

therefore addition and multiplication of polynomials are associative in $R[x]$.

Identity:

The zero element or zero polynomial in $R[x]$ is the identity for addition

$$\begin{aligned} f(x) + 0 &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) + (0 + 0x^1 + 0x^2 + \cdots + 0x^m) \\ &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) \\ &= f(x). \end{aligned}$$

Inverse: Let $f(x) \in R[x]$

$$f(x) + (-f(x)) = (a_0 + a_1x + a_2x^2 + \dots + a_nx^n) + (-a_0 - a_1x - a_2x^2 - \dots - a_nx^n) = 0$$

Therefore, $-f(x)$ is the additive inverse of $R[x]$.

Commutative: Further $f(x) + g(x) = g(x) + f(x) \quad \forall f(x), g(x) \in R[x]$

$$\text{since } a_i + b_i = b_i + a_i \quad \forall a_i, b_i \in R$$

$(R[x], +)$ is an abelian group.

(ii) To Prove : $(R[x], \cdot)$ is a semi group.

Closure: Let $f(x), g(x) \in R[x]$

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1x + a_2x^2 + \dots + a_nx^n)(b_0 + b_1x + b_2x^2 + \dots + b_mx^m) \\ &= C_0 + C_1x + C_2x^2 + \dots + C_kx^k \end{aligned}$$

$$\text{Where } C_0 = a_0 b_0$$

$$C_1 = a_0 b_1 + a_1 b_0$$

$$C_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$\vdots$$

$$C_r = a_0 b_r + a_1 b_{r-1} + \dots + a_r b_0 \in R$$

Therefore, $f(x) \cdot g(x) \in R[x]$.

Associative:

Let $f(x), g(x), h(x) \in R[x]$.

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$$

$$h(x) = c_0 + c_1x + c_2x^2 + \dots + c_kx^k$$

Then the coefficient of x^i in the expansion of $(f(x)g(x))h(x)$ is the sum of products of the form $(a_rb_s)c_t$ where r, s, t are the non negative integers $r + s + t = i$

Again the coefficient of x^i in the expansion of $f(x)(g(x)h(x))$ is the sum of products of the form $a_r(b_sc_t)$ where r, s, t are the non negative integers $r + s + t = i$.

since multiplication is associative in R .

$$(a_rb_s)c_t = a_r(b_sc_t)$$

\therefore the coefficient of x^i in the expansion of $(f(x)g(x))h(x)$ is equal to the coefficient of x^i in the expansion of $f(x)(g(x)h(x))$

\therefore Multiplication of polynomials is associative

$(R[x], \cdot)$ is a semi group.

Distributive Law:

$$\text{Now } f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$$

$$\text{Since } a_r(b_s + c_t) = a_rb_s + a_rc_t$$

Distributive axiom is satisfied.

$\therefore [R[x], +, \cdot]$ is a ring of polynomial over R .

Theorem 3:

$R[x]$ is an integral domain if and only if R is an integral domain.

Proof:

Assume that R be an integral domain. The R is a commutative ring with identity and without zero divisors.

Hence $R[x]$ is commutative ring with identity 1, since $f(x) \cdot 1 = f(x)$.

To prove that $R[x]$ is an integral domain.

i.e., $R[x]$ has no zero divisors.

i.e., $f(x) \neq 0, g(x) \neq 0, f(x)g(x) \neq 0$

Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$,

$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$ with $a_n \neq 0, b_m \neq 0$

$f(x)g(x) = (a_0 + a_1x + a_2x^2 + \dots + a_nx^n)$

$(b_0 + b_1x + b_2x^2 + \dots + b_mx^m)$

$= a_0b_0 + (a_1b_0 + a_0b_1)x + \dots + (a_nb_m)x^{m+n}$

Since R has no zero divisors,

$\Rightarrow a_nb_m \neq 0$.

Therefore, $f(x)g(x) \neq 0$.

$\Rightarrow R[x]$ is an integral domain.

Conversely let $R[x]$ is an integral domain,

To prove that R is an integral domain.

We know that R is commutative and has no proper divisor of zero.

Theorem 4: Remainder Theorem**Statement:** Let F be a field and $a \in F$. Let $f(x) \in F(x)$ **Then $f(a)$ is the remainder when $f(x)$ is divided by $(x - a)$.****Proof:**Given: Let F be a field and $a \in F$. Let $f(x) \in F(x)$

By division algorithm, we know that

$$f(x) = q(x)(x - a) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg(x - a)$

$$\therefore \deg r(x) = 0$$

$$r(x) = r \text{ (a constant)}$$

$$\therefore f(x) = q(x)(x - a) + r$$

$$\text{Put } x = a, \quad f(a) = q(a) \cdot 0 + r = r$$

$$\Rightarrow r = f(a)$$

$$\therefore f(x) = q(x)(x - a) + f(a).$$

 $f(a)$ is the remainder when $f(x)$ is divided by $(x - a)$.**Example 1: Find the remainder when $f(x) = x^{100} + x^{90} + x^{80} + x^{70} + x^{50} + 1$ is divided by $g(x) = x - 1$ in $\mathbb{Z}_2[x]$.****Solution:** we have $f(x) = x^{100} + x^{90} + x^{80} + x^{70} + x^{50} + 1$ and $g(x) = x - 1$.Here $a = 1$

$$\text{Therefore } f(1) = 1 + 1 + 1 + 1 + 1 + 1 = 6 \equiv 0 \pmod{2}$$

The remainder is 0.

Example 2:

If $f(x) = 3x^5 - 8x^4 + x^3 - x^2 + 4x - 7$ and $g(x) = x + 9$, such that $f(x), g(x) \in \mathbb{Z}_{11}[x]$. Find the remainder when $f(x)$ is divided by $g(x)$.

Solution: Given $g(x) = x + 9 \Rightarrow x = -9$

$$\begin{aligned} f(-9) &= 3(-9)^5 - 8(-9)^4 + (-9)^3 - (-9)^2 + 4(-9) - 7 \\ &= -177147 - 52488 - 729 - 124 \\ &= -230488 \\ &= 6(\text{mod } 11) \end{aligned}$$

$\Rightarrow \text{Remainder} = 6.$

Example 3:

If $f(x) = x^8 + 7x^5 - 4x^4 + 3x^3 + 5x^2 - 4$ and $g(x) = x - 3$, such that $f(x), g(x) \in \mathbb{Q}[x]$. Find the remainder when $f(x)$ is divided by $g(x)$.

Solution: Given $g(x) = x - 3 \Rightarrow x = 3.$

$$\begin{aligned} f(3) &= 3^8 + 7(3)^5 - 4(3)^4 + 3(3)^3 + 5(3)^2 - 4 \\ &= 6561 + 7(243) - 4(81) + 3(27) + 5(9) - 4 \\ &= 8060. \end{aligned}$$

Theorem 5: Factor Theorem

Statement: Let F be a field and $a \in F$. Let $f(x) \in F[x]$
 then a is the root of $f(x)$ iff $(x - a)$ is a factor of $f(x)$.

Proof: Assume that $x - a$ is a factor of $f(x)$.

To prove a is a root of $f(x)$.

If $(x - a)$ is a factor of $f(x)$, then there exists a polynomial $q(x) \in F[x]$ such that $f(x) = q(x)(x - a)$.

For $x = a$, we have $f(a) = 0 \Rightarrow a$ is a root of $f(x)$

Conversely, let a be the root of the polynomial $f(x)$

we need to prove that $(x - a)$ is a factor of $f(x)$

Since a is a root of $f(x)$, we have $f(a) = 0$.

By division algorithm we have

$$f(x) = q(x)(x - a) + r.$$

$$\text{At } x = a, f(a) = q(a)(a - a) + r$$

$$\Rightarrow f(a) = r = 0.$$

This shows that remainder $r = 0$ and $x - a$ is a factor of $f(x)$.

Theorem 6:

If $f(x) \in F[x]$ has degree $n \geq 1$, then $f(x)$ has at most n roots in F .

Proof: Given $f(x) \in F[x]$ is of degree n , $n \geq 1$.

We prove the theorem by mathematical induction on n .

Basis step:

If $n = 1$, then $f(x) = ax + b$, $a, b \in F$.

Clearly $-a^{-1}b \in F$, since $f(-a^{-1}b) = a(-a^{-1}b) + b = -b + b = 0$

Therefore $f(x)$ has at least one root in F .

In case if c_1, c_2 are two roots, then we have

$$f(c_1) = ac_1 + b = 0, f(c_2) = ac_2 + b = 0$$

$$\Rightarrow ac_1 + b = ac_2 + b$$

$$\Rightarrow c_1 = c_2.$$

So $f(x)$ has exactly only one root in F

Induction hypothesis:

Now assume that the theorem is true for all polynomials of degree k in $F[x]$. That is any polynomial of degree k has at most k roots in F .

Induction Step:

To prove that it is true for all polynomials of degree $k+1$ has at most $k+1$ 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).

By Factor theorem we have $f(x) = q(x)(x-r)$, where $q(x)$ is of degree k . By induction hypothesis $q(x)$ has at most k roots in F and $r \in F$ is a root of $f(x)$.

Therefore, $f(x)$ has at most $k+1$ roots.

Hence by Induction, the theorem is true for all $n \geq 1$.

DIVISION ALGORITHM

View the lecture on YouTube: <https://youtu.be/khoUNagU6Kk>

Theorem: Let F be a field. Let $f(x)$ and $g(x)$ be two polynomials in $F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $a_n \neq 0$ and

$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, $b_m \neq 0$.

Consider the set $S = \{f(x) - g(x)s(x)/s(x) \in F[x]\}$.

Let $r(x)$ be an element of minimal degree in S .

Clearly, $r(x) = f(x) - g(x)q(x)$ for some $q(x) \in F[x]$.

$\therefore f(x) = g(x)q(x) + r(x)$.

We claim that either $r(x) = 0$ or $\deg r(x) < \deg g(x) = m$.

Let $r(x) = c_0 + c_1x + c_2x^2 + \cdots + c_tx^t$, $c_t \neq 0$ and $t \geq m$.

Now, consider the polynomial,

$$r_1(x) = r(x) - c_tb_m^{-1}x^{t-m}g(x)$$

$$= r(x) - c_tb_m^{-1}x^{t-m}(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)$$

$$= r(x) - (c_tb_m^{-1}b_0x^{t-m} + \cdots + c_tx^t) = \text{a polynomial of degree} < t.$$

Hence, $\deg r_1(x) < \deg r(x)$.

$$r_1(x) = r(x) - c_tb_m^{-1}x^{t-m}g(x)$$

$$= f(x) - g(x)q(x) - c_tb_m^{-1}x^{t-m}g(x)$$

$$= f(x) - g(x)[q(x) + c_tb_m^{-1}x^{t-m}] \in S.$$

Therefore, $r_1(x) \in S$ and $\deg r_1(x) < \deg r(x)$ which is a contradiction.

Since $r(x)$ is an element of minimal degree in S . Hence $\deg r(x) < m$.

Thus $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Now, we prove the uniqueness.

Suppose $f(x) = q_1(x)g(x) + r_1(x)$, where $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$.

$$0 = g(x)[q(x) - q_1(x)] + r(x) - r_1(x).$$

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x).$$

Since $\deg [r_1(x) - r(x)] < \deg g(x)$,

the above equation holds good only if $q(x) - q_1(x) = 0$.

Therefore $q(x) = q_1(x)$ and $r(x) = r_1(x)$.

Note: The polynomials $q(x)$ and $r(x)$ in the division algorithm are called the quotient and remainder in the division of $f(x)$ by $g(x)$.

Example 1: If $f(x) = x^2 + 1$ and $g(x) = x^4 + x^3 + x^2 + x + 1$ such that $f(x), g(x) \in \mathbb{Z}_2[x]$, determine the quotient $q(x)$ and remainder $r(x)$ such that $g(x) = q(x)f(x) + r(x)$.

Solution: We divide $g(x)$ by $f(x)$.

$$\begin{array}{r} x^2 + x \\ x^2 + 1 \overline{) x^4 + x^3 + x^2 + x + 1} \\ \underline{x^4 + x^2} \\ x^3 + x + 1 \\ \underline{x^3 + x} \\ 1 \end{array}$$

Hence quotient $q(x) = x^2 + x$ and remainder $r(x) = 1$.

Example 2: If $f(x) = 2x^4 + 5x^2 + 2$ and $g(x) = 6x^2 + 4$, then determine $q(x)$ and $r(x)$ in $\mathbb{Z}_7[x]$, when $f(x)$ is divided by $g(x)$.

Solution: Given $f(x) = 2x^4 + 5x^2 + 2$ and $g(x) = 6x^2 + 4$.

Since $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ is a field. We can find $q(x)$ and $r(x)$ by usual long division method.

While perform long division, keeping in mind the addition and multiplication are done under modulo 7.

Since $30 \equiv 2 \pmod{7}$, $20 \equiv 6 \pmod{7}$, and $-1 \equiv 6 \pmod{7}$.

Also, $-2 \equiv 5 \pmod{7}$,

Hence, $q(x) = 5x^2 + 1$ and $r(x) = 5$.

In addition, $2x^4 + 5x^2 + 2 = (5x^2 + 1)(6x^2 + 4) + 5$.

IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Definition:

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.

i.e., $\deg g(x) \geq 1$ and $\deg h(x) \geq 1$.

If $f(x)$ is not reducible, then we call it irreducible (or prime) over F .

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 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 $1 \leq \deg h(x) < \deg f(x)$

$$\text{therefore } ax + b = g(x)h(x)$$

$$\text{therefore } \deg(ax + b) = \deg g(x) + \deg h(x)$$

$$\Rightarrow 1 = \deg g(x) + \deg h(x)$$

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 one of $g(x)$ and $h(x)$ has degree 1.

Let $\deg g(x) = 1 \Rightarrow g(x) = ax + b, \quad a \neq 0.$

$$\begin{aligned} \text{Now } -a^{-1}b \in F \text{ and } g(-a^{-1}b) &= a(-a^{-1}b) + b \\ &= -(a \cdot a^{-1})b + b \\ &= -(1 \cdot b) + b \\ &= -b + b \\ &= 0 \end{aligned}$$

Therefore $-a^{-1}b$ is a root of $g(x)$

Hence $-a^{-1}b$ is a root of $f(x)$ in F

So, $f(x)$ has a root in F .

Conversely, let $f(x)$ have a root $a \in F$.

Then $(x - a)$ is a factor of $f(x)$.

Therefore $f(x) = (x - a)g(x), \quad g(x) \in F[x].$

Hence $f(x)$ is reducible over F .

Example 1:

Test whether the polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ & \mathbb{C} .

Solution:

Given, $f(x) = 2x^2 + 4$

$$\begin{aligned} f(x) = 0 &\Rightarrow 2x^2 + 4 = 0 \\ &\Rightarrow x^2 + 2 = 0 \\ &\Rightarrow x^2 = -2 \\ &\Rightarrow x = \pm i\sqrt{2} \end{aligned}$$

Therefore the roots do not belong to \mathbb{Z}, \mathbb{Q} and \mathbb{R}

Hence $f(x) = 2x^2 + 4$ is irreducible over \mathbb{Z}, \mathbb{Q} and \mathbb{R}

But the roots $i\sqrt{2}$ and $-i\sqrt{2}$ belong to \mathbb{C}

Hence $f(x) = 2x^2 + 4$ is reducible over \mathbb{C} .

Example 2:

Let $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ is it irreducible or reducible? If reducible find the other factor.

Solution:

Given $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$

and $\mathbb{Z}_2 = \{0, 1\}$

Now $f(0) = 1 \neq 0$

$$f(1) = 4 \equiv 0 \pmod{2}$$

Therefore 1 is a root in \mathbb{Z}_2

Hence $x - 1$ is a factor of $f(x)$ in $\mathbb{Z}_2[x]$

Therefore $f(x)$ is reducible

By division algorithm $\exists q(x), r(x) \in \mathbb{Z}_2[x]$

Such that,

$$x^3 + x^2 + x + 1 = (x^2 + 1)(x - 1) + 0$$

$$\text{Hence } x^3 + x^2 + x + 1 = (x^2 + 1)(x - 1).$$

Example 3:

Test the polynomial $f(x) = x^2 + x + 4$ in $\mathbb{Z}_7[x]$ is irreducible over \mathbb{Z}_7 .

Solution:

Given $f(x) = x^2 + x + 4$

and $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

We search for an element $a \in \mathbb{Z}_7 \ni f(a) = 0$

$$f(0) = 4 \neq 0$$

$$f(1) = 6 \neq 0$$

$$f(2) = 10 \equiv 3 \pmod{7} \neq 0$$

$$f(3) = 16 \equiv 2 \pmod{7} \neq 0$$

$$f(4) = 24 \equiv 3 \pmod{7} \neq 0$$

$$f(5) = 34 \equiv 6 \pmod{7} \neq 0$$

$$f(6) = 46 \equiv 4 \pmod{7} \neq 0$$

Therefore there is no root for $f(x)$ in \mathbb{Z}_7

Hence $f(x)$ is irreducible over \mathbb{Z}_7 .

GREATEST COMMON DIVISOR

Definition: (Greatest Common Divisor)

Let F be a field and $f(x), g(x) \in F[x]$. A Greatest Common Divisor of $f(x)$ and $g(x)$ is a non-zero polynomial $d(x)$ such that (i) $d(x)$ divides $f(x)$ and $g(x)$ (ii) $c(x)$ is a divisor of $f(x)$ and $g(x)$ then $c(x)$ divides $d(x)$.

Theorem 1: Let F be a field and $f(x), g(x) \in F[x]$ with at least one of them is non-zero polynomial. Then their GCD $d(x)$ 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 $S = \{s(x)f(x) + t(x)g(x) : s(x), t(x) \in F[x]\}$

Then $S \neq \emptyset$, since $f(x) \in S$.

Let $d(x)$ be a polynomial of least degree in S .

Then $d(x) = a(x)f(x) + b(x)g(x)$, for some $a(x), b(x) \in F[x]$. -----(1)

First we prove that $d(x)$ is the g.c.d of $f(x)$ and $g(x)$

Now consider $f(x), d(x)$

By division algorithm, there exists $q(x)$ and $r(x)$ such that

$$f(x) = q(x)d(x) + r(x) \text{ -----(2)}$$

Where either $r(x) = 0$ (or) $\deg r(x) < \deg d(x)$

$$\begin{aligned} \therefore r(x) &= f(x) - q(x)d(x) \\ &= f(x) - q(x)[a(x)f(x) + b(x)g(x)] \\ &= [1 - q(x)a(x)]f(x) - q(x)b(x)g(x) \\ &= [1 - q(x)a(x)]f(x) + [-q(x)b(x)]g(x) \end{aligned}$$

This is of the form $s(x)f(x) + r(x)g(x)$

$$\therefore r(x) \in S$$

If $r(x) \neq 0$, then $\deg r(x) < \deg d(x)$, which contradicts the choice of $d(x)$.

$$\therefore r(x) = 0 \Rightarrow f(x) = q(x)d(x) \quad \text{(using (2))}$$

$\therefore d(x)$ 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 $d(x)$
(using (1))

$\therefore d(x)$ is the gcd of $f(x)$ and $g(x)$

Note: Suppose $d(x)$ is Monic then it will be unique

Suppose $d(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, a_n \neq 0$

Then $a_n^{-1}d(x) = a_n^{-1}a_0 + a_n^{-1}a_1x + a_n^{-1}a_2x^2 + \cdots + a_n^{-1}a_nx^n$

$= b_0 + b_1x + b_2x^2 + \cdots + x^n$ is a Monic polynomial.

and $a_n^{-1}d(x)$ is also a gcd of $f(x)$ and $g(x)$.

Suppose $d_1(x)$ and $d_2(x)$ be two monic polynomials which are the gcd's of $f(x)$ and $g(x)$

Then $d_1(x)$ divides $d_2(x)$
(treating $d_2(x)$ as gcd)

and $d_2(x)$ divides $d_1(x)$
(treating $d_1(x)$ as gcd)

$\therefore d_1(x) = u d_2(x)$ for some $u \neq 0$ in F

Since both $d_1(x)$ and $d_2(x)$ are monic polynomials by using equality of polynomial and by equating the leading coefficient's, we get $u = 1$

$\therefore d_1(x) = d_2(x)$

Hence the gcd is unique, when it is monic.

Definition:

If the gcd of $f(x)$ and $g(x) \in F$ 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 exists polynomials $a(x)$ and $b(x)$ in $F[x]$ such that $a(x)f(x) + g(x)b(x) = 1$.

Theorem 2: Let F be a field and $f(x), g(x) \in F[x]$, where $g(x) \neq 0$ and $\deg r(x) \leq \deg d(x)$.

Applying the division algorithm, we write

$$f(x) = q_1(x)g(x) + r_1(x), \quad \deg r_1(x) < \deg g(x)$$

$$g(x) = q_2(x)r_1(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x)$$

$$r_1(x) = q_3(x)r_2(x) + r_3(x), \quad \deg r_3(x) < \deg r_2(x)$$

.

.

.

.

$$r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x), \deg r_n(x) < \deg r_{n-1}(x)$$
$$r_{n-1}(x) = q_{n+1}(x)r_n(x) + r_{n+1}(x), r_{n+1}(x) = 0$$

Then $r_n(x)$ is the last non-zero remainder.

It can be seen that $r_n(x)$ is the gcd of $f(x)$ and $g(x)$.

Example 1: Find the gcd of $x^4 + x^3 + 2x^2 + x + 1$ and $x^3 - 1$ over \mathbb{Q} .

Solution:

Let $f(x) = x^4 + x^3 + 2x^2 + x + 1$ and $g(x) = x^3 - 1$

And $\deg g(x) < \deg f(x)$

Divide $f(x)$ by $g(x)$ by division algorithm successively.

$\therefore f(x) = (x + 1)(x^3 - 1) + 2(x^2 + x + 1), \deg(2x^2 + 2x + 2) < \deg(x^3 - 1).$

$$x^3 - 1 = \left(\frac{x}{2} - \frac{1}{2}\right)(2x^2 + 2x + 2) + 0$$
$$= (x - 1)(x^2 + x + 1)$$

\therefore The last non-zero remainder is $(x^2 + x + 1)$

$$\therefore f(x) = (x + 1)(x - 1)(x^2 + x + 1) + (x^2 + x + 1)$$
$$= (x^2 + x + 1)((x + 1)(x - 1) + 1)$$

\therefore The gcd of $f(x)$ and $g(x)$ is $(x^2 + x + 1)$.

$x^3 - 1$	$x + 1$		$\frac{1}{2}x - \frac{1}{2}$
	$x^4 + x^3 + 2x^2 + x + 1$		
	$x^4 - x$		
	<hr/>		
	$x^3 + 2x^2 + 2x + 1$		
	$x^3 - 1$		
	<hr/>		
	$2x^2 + 2x + 2$		

$2x^2 + 2x + 2$	$\frac{1}{2}x - \frac{1}{2}$
	$x^3 - 1$
	$x^3 + x^2 + x$
	<hr/>
	$-x^2 - x - 1$
	$-x^2 - x - 1$
	<hr/>
	0

View more GCD examples on YouTube:

<https://youtu.be/82nmtNxPaXE>

<https://youtu.be/q9lKz-cicWI>

CHARACTERISTIC OF A RING

CHARACTERISTIC OF A RING

Definition: The characteristic of a ring R is the least positive integer n such that $n \cdot a = 0$ for all $a \in R$ and is denoted by $\text{Char}(R) = n$. If no such positive integer exists, then R is said to have characteristic 0.

Examples:

- The ring $(\mathbb{Z}_3, +, \cdot)$ has characteristic 3.
- The ring $(\mathbb{Z}_4, +, \cdot)$ has characteristic 4.
- The ring $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$ both have characteristic 0.
- The characteristic of a field $(F, +, \cdot)$ is either 0 or a prime number.
- The characteristic of a finite field is a prime number p .

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 $\text{Char}(F) \neq 0$, then let $\text{Char}(F) = n$.

To prove n is prime.

Suppose n is not a prime, then $n = pq$, where $1 < p < n, 1 < q < n$.

i.e p and q are proper factors of n .

Since $\text{Char}(F) = n$, we have $na = 0 \forall a \in F$.

Take $a = 1$, then $n \cdot 1 = 0$. (1 is the identity of F)

$$\Rightarrow (pq) \cdot 1 = 0 \Rightarrow (p \cdot 1)(q \cdot 1) = 0$$

$$[\because (pq) \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{p \text{ terms}} = \underbrace{(1 + 1 + \dots + 1)}_{p \text{ terms}} \underbrace{(1 + 1 + \dots + 1)}_{q \text{ terms}}]$$

Since F is a field, F is an integral domain and so, it has no divisor of zero,

\therefore either $p \cdot 1 = 0$ or $q \cdot 1 = 0$.

Since p and q are less than n , it contradicts the definition of characteristics of F .

$\therefore n$ is a prime number.

Note:

1. The characteristic of a ring need not be a prime. For example $\text{Char}(\mathbb{Z}_6) = 6$, 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 and n is a positive integer.

Proof: For a prime p , Z_p is field having p elements and $\text{Char}(Z_p) = p$, since $p \cdot a = 0$ for all $a \in Z_p$.

Consider the polynomial $f(x) = x^{p^n} - x$ in $Z_p[x]$.

Now, the derivative $x^{p^n} x^{p^n-1} - 1 = f'(x)$.

Since, $\text{Char}(Z_p) = p$, $\text{Char}(Z_p[x]) = p$. $\therefore p \cdot g(x) = 0$ for all $g(x) \in Z_p[x]$.

Hence $p \cdot x^{p^n-1} = 0 \Rightarrow p^n \cdot x^{p^n-1} = 0$.

Thus $f'(x) = -1 = \text{a constant polynomial}$.

So, $f(x)$ and $f'(x)$ have no common root.

Hence $f(x)$ has no multiple roots. i.e all the roots of $f(x)$ are distinct.

If K is the smallest extension field (splitting field) containing all the roots of $f(x)$. Then $f(x)$ has p^n distinct roots in K .

In K , let F be the set of all elements satisfying $f(x)$.

$F = \{a \in K / a^{p^n} = a\} \subset K$.

Hence F has only p^n elements.

Claim: To prove that F is a field.

Let $a, b \in F$. Then $a^{p^n} = a$ and $b^{p^n} = b$.

$(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n} = a \cdot b \Rightarrow a \cdot b \in F$.

$(a + b)^{p^n} = a^{p^n} + p^n C_1 a^{p^n-1} b + p^n C_2 a^{p^n-2} b^2 + \dots + p^n C_r a^{p^n-r} b^r + \dots b^{p^n}$.

Since $\text{Char}(K) = p$, $p \cdot a^{p^n-r} b^r = 0$, $r = 1, 2, 3 \dots$

$\therefore (a \cdot b)^{p^n} = a^{p^n} + b^{p^n} = a + b \Rightarrow a + b \in F$.

Similarly, $(a - b)^{p^n} = a - b \Rightarrow a - b \in F$.

Hence, F is a subfield of K .

In addition the field F consisting of p^n elements, where p is a prime and n is a positive integer

CONGRUENCE RELATION IN $F[x]$ **Definition:**

Let $s(x) \in F[x]$ and $s(x) \neq 0$ and $f(x), g(x) \in F[x]$. We say that $f(x)$ is congruent to $g(x)$ modulo $s(x)$ and write

$$f(x) \equiv g(x) \pmod{s(x)} \text{ if } s(x) \text{ divides } f(x) - g(x)$$

i.e., $f(x) - g(x) = q(x)s(x)$ for some $q(x) \in F[x]$

This relation congruence of polynomial is an equivalence relation on $F[x]$

The equivalence class of $f(x)$ is denoted by $[f(x)]$

$$[f(x)] = \{ t(x) \in F[x] \mid f(x) \equiv t(x) \pmod{s(x)} \}$$

We define addition and multiplication of congruence classes as in \mathbb{Z}_n

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$

$$[f(x)] \cdot [g(x)] = [f(x) \cdot g(x)]$$

Definition:

Let R be a commutative ring with unity and $a \in R$, then the ideal generated by single element a is called a principal ideal and it is denoted by $\langle a \rangle$

$$\text{Thus } \langle a \rangle = \{ ra \mid r \in R \}$$

Now, we state a theorem without proof for polynomials.

Theorem:

Let $F = \mathbb{Z}_p$, p is a prime and $f(x)$ be an irreducible polynomial of degree n over \mathbb{Z}_p . Then the quotient ring $\frac{F[x]}{\langle f(x) \rangle}$ is a field having p^n elements, Where $\langle f(x) \rangle$ is the ideal generated by $f(x)$.

Example 1:

In $Z_2[x]$, $s(x) = x^2 + x + 1$. show that $s(x)$ is irreducible over $\frac{Z_2[x]}{\langle s(x) \rangle}$ and construct the field.

Solution:

Given $s(x) = x^2 + x + 1$ in $Z_2[x]$

and $Z_2 = \{0, 1\}$

Now,

$$s(0) = 1 \neq 0$$

$$s(1) = 3 \equiv 1 \pmod{2} \neq 0$$

Therefore $s(x)$ has no root in $Z_2[x]$

Hence $s(x)$ is irreducible in $Z_2[x]$.

Therefore $\frac{Z_2[x]}{\langle s(x) \rangle}$ is a field

Since degree of $s(x) = 2$, this field has $2^2 = 4$ elements.

This field consists of 4 different equivalence classes $(\text{mod } s(x))$

Let $s(x), f(x) \in F[x]$

Then by division algorithm, we have

$$f(x) = q(x)(x^2 + x + 1) + r(x)$$

where $r(x) = 0$ or $\deg r(x) = 0 < \deg (x^2 + x + 1)$

Therefore degree of $r(x)$ is either 0 or 1

Here, $r(x) = ax + b$, $a, b \in Z_2$

Since $f(x) - r(x) = q(x)(x^2 + x + 1)$

$$f(x) \equiv r(x) \pmod{(x^2 + x + 1)}$$

Therefore $[f(x)] = [r(x)]$

Therefore the different equivalence classes $\text{mod } (x^2 + x + 1)$ correspond to the different values of $r(x)$

Each of a and b can take two values from Z_2 and so $2 \cdot 2 = 4$ values for $r(x)$

They are,

- (i) If $a = 0, b = 0$, then $r(x) = 0$
- (ii) If $a = 0, b = 1$, then $r(x) = 1$
- (iii) If $a = 1, b = 0$, then $r(x) = x$
- (iv) If $a = 1, b = 1$, then $r(x) = x + 1$

Therefore four elements of the field are If $[0], [1], [x], [x + 1]$

Therefore $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1 \rangle} = \{[0], [1], [x], [x + 1]\}$

Example 2:

If $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1 \rangle} = \{[0], [1], [x], [x + 1]\}$ is a field, then find $[x]^{-1}$.

Solution:

Since $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1 \rangle} = \{[0], [1], [x], [x + 1]\}$ is a field

The non zero elements $[1], [x]$ and $[x + 1]$ form a group under multiplication,

We write $[a]$ as a

Therefore, $[1] = 1$

$$[x] = x$$

$$[x + 1] = x + 1$$

Now,

$$1 \cdot 1 = 1$$

$$1 \cdot x = x$$

$$1 \cdot (x + 1) = x + 1$$

$$x \cdot 1 = x$$

$$x \cdot x = x^2$$

Also,

$$x^2 = 1 \cdot (x^2 + x + 1) + (x + 1) \text{ in } \mathbb{Z}_2[x]$$

Therefore, $x \cdot x = x^2 \equiv x + 1 \pmod{(x^2 + x + 1)}$.

$$x.(x+1) = x^2 + x$$

Also, $x^2 + x = 1(x^2 + x + 1) + 1$ in $Z_2[x]$

Therefore, $x.(x+1) = x^2 + x \equiv 1(mod(x^2 + x + 1))$

$$(x+1).1 = x+1$$

$$(x+1).x = x^2 + x \equiv 1(mod(x^2 + x + 1))$$

$$(x+1).(x+1) = x^2 + 1 \text{ in } Z_2[x]$$

Also,

$$x^2 + 1 = 1.(x^2 + x + 1) + x \text{ in } Z_2[x]$$

Therefore $(x+1).(x+1) = x^2 + 1 \equiv x(mod(x^2 + x + 1))$

.	1	x	x + 1
1	1	x	x + 1
x	x	x + 1	1
x + 1	x + 1	1	x

Since 1 is the multiplicative identity.

We find $x.(x+1) = 1$

Therefore inverse of x is $(x+1)$

Hence $[x]^{-1} = [x+1]$.

PRACTICE QUIZ: FINITE FIELDS AND POLYNOMIALS

- Choose all the correct statements. Z denotes the ring of integers, R denotes the field of real numbers.
 - There are infinitely many units in the polynomial ring $R[x]$.
 - There are infinitely many units in the polynomial ring $Z[x]$.
 - If $f(x) \in Z[x]$ is a unit, then the degree of $f(x)$ is one.
 - If $f(x) \in R[x]$ has no roots in R , then $f(x)$ is a unit.
- Let R be a ring. An element $x \in R$ is a zero divisor if $x \neq 0$ and $xy = 0$ for element $0 \neq y \in R$. Choose the correct statements. Z denotes the ring of integers.
 - The ring Z contains zero divisors
 - A field contains zero divisors
 - The ring $Z[x]$ does not contain any zero divisors
 - A field contains at least one zero divisor.
- Let $f(x) = 3x^5 + 11x^4 - 25x^3 - 59x^2 + 94x - 24 \in Q[x]$, where Q denotes the field of rational numbers. Which of the following polynomials divide $f(x)$.
 - $x - 1$
 - $x + 1$
 - $x + 2$
 - $x^2 + x - 6$.
- Let R denote the field of real numbers. Determine which of the following are ideals in the polynomial ring $R = R[x]$.
 - The set of all polynomials all of whose coefficients are irrational.
 - The set of all polynomials of degree at least 10, along with zero polynomial
 - The set of all polynomials which have 1 as a root.
 - The set of all polynomials divisible by the polynomial $x^2 + 1$.
- Which of the given elements are irreducible in the given ring? Here Z is the ring of integers and Q is the field of rational number.
 - $17 \in Z[i]$, where i denotes a square root of -1
 - $2x + 2 \in Q[x]$
 - $2x + 2 \in Z[x]$
 - None of the above
- Choose all the correct statements. Z denotes the ring of integers. Q and C denote the fields of rational and complex numbers, respectively.
 - A greatest common divisor of 3, 4 in $Z[i]$ is 2.
 - A greatest common divisor of $2x^7 - 4x^4 + 2$ and $x^2 - 1$ in $Z[x]$ is $x + 1$.
 - A greatest common divisor of $2x^2 + 1$ and $2x^5 - 10x^4 + 3x^3 - 15x^2 + x - 5$ in $Q[x]$ is 1.
 - A greatest common divisor of $x - 2$ and $x^4 - 7x^2 + 11x - 10$ in $C[x]$ is $x - 2$.
- If F is a field, then $F[x]$ is a/an
 - Field
 - Integral domain
 - both a) and b)
 - None of the above
- Let $f(x) = 2x + 1$, $g(x) = x^2 + 1$ polynomials in $Z[x]$. Choose all the incorrect statements.
 - We can divide $g(x)$ by $f(x)$ in $Z[x]$.
 - We can not divide $g(x)$ by $f(x)$ in $Z[x]$.
 - We can divide $g(x)$ by $f(x)$ in $Q[x]$.
 - We can divide $g(x)$ by $f(x)$ as long as the leading co-efficient of $f(x)$ is a unit.

Answers to the Practice Quiz:

1. a) 2. c) 3. a) & d) 4. d) 5. b) 6. d) 7. b) 8. a)

STUCOR APP

ASSIGNMENTS: UNIT II

1. If R is a ring under usual addition and multiplication, show that $(R[x], +, \times)$ is a ring of polynomials over R .
2. If $f(x) = x^{100} + x^{90} + x^{80} + x^{50} + 1$, $g(x) = x - 1$, and $f(x), g(x) \in Z_2[x]$ find the remainder when $f(x)$ is divided by $g(x)$.
3. If $f(x) \in F[x]$ has degree $n \geq 1$, then prove that $f(x)$ has at most n roots in F .
4. Prove that every finite field has p^n elements for some prime number p and some positive integer n .
5. Determine whether the polynomial $x^4 + x^2 + 1$ is irreducible over Z_2 . Also give an example of a reducible polynomial of degree 6 over Z_2 having no root in Z_2 . How many polynomials in Z_2 have degree 3?
6. Construct a field consisting of four elements (Hint: use the irreducible binary polynomial $x^2 + x + 1$ over Z_2).
7. Determine whether the following polynomials are irreducible over the given fields
a) $x^2 + x + 1$ over Z_2, Z_5 and Z_7 . b) $x^3 + 3x^2 - x + 1$ over Z_5 .
8. Find the multiplicative inverse of each non-zero element in Z_7 (with respect to the operations addition modulo 7 and multiplication modulo 7). Also, show that the polynomial $x^4 + x^2 + 1$ is irreducible over Z_2 .

PART A QUESTIONS AND ANSWERS: UNIT II

1. Define Greatest common divisor (g.c.d) in polynomials. (K2, CO3)

Solution:

Let F be a field $p(x), q(x) \in F[x]$. The greatest common divisor of $p(x)$ and $q(x)$ is a polynomial $d(x)$ satisfying the following conditions.

- (i) $d(x)|p(x)$ and $d(x)|q(x)$
- (ii) if $c(x)|p(x)$ and $c(x)|q(x)$ then $c(x)|d(x)$

2. Define irreducible polynomials. (K2, CO3)

Solution:

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.

i.e., $\deg g(x) \geq 1$ and $\deg h(x) \geq 1$.

If $f(x)$ is not reducible, then we call it irreducible (or prime) over F .

3. Test whether the polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ & \mathbb{C} . (K3, CO3)

Solution:

Given, $f(x) = 2x^2 + 4$

$$f(x) = 0 \Rightarrow 2x^2 + 4 = 0$$

$$\Rightarrow x^2 + 2 = 0$$

$$\Rightarrow x^2 = -2$$

$$\Rightarrow x = \pm i\sqrt{2}$$

Therefore the roots do not belong to \mathbb{Z}, \mathbb{Q} and \mathbb{R}

Hence $f(x) = 2x^2 + 4$ is irreducible over \mathbb{Z}, \mathbb{Q} and \mathbb{R}

But the roots $i\sqrt{2}$ and $-i\sqrt{2}$ belong to \mathbb{C}

Hence $f(x) = 2x^2 + 4$ is reducible over \mathbb{C} .

4. Let $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ is it irreducible or reducible? If reducible find the other factor. (K3, CO3)

Solution:

Given $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$

and $\mathbb{Z}_2 = \{0, 1\}$

Now $f(0) = 1 \neq 0$

$$f(1) = 4 \equiv 0 \pmod{2}$$

Therefore 1 is a root in \mathbb{Z}_2

Hence $x - 1$ is a factor of $f(x)$ in $\mathbb{Z}_2[x]$

Therefore $f(x)$ is reducible

By division algorithm $\exists q(x), r(x) \in \mathbb{Z}_2[x]$

Such that,

$$x^3 + x^2 + x + 1 = (x^2 + 1)(x - 1) + 0$$

$$\text{Hence } x^3 + x^2 + x + 1 = (x^2 + 1)(x - 1).$$

5. Test the polynomial $f(x) = x^2 + x + 4$ in $\mathbb{Z}_7[x]$ is irreducible over \mathbb{Z}_7 . (K3, CO3)

Solution:

Given $f(x) = x^2 + x + 4$

and $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

We search for an element $a \in \mathbb{Z}_7 \ni f(a) = 0$

$$f(0) = 4 \neq 0$$

$$f(1) = 6 \neq 0$$

$$f(2) = 10 \equiv 3 \pmod{7} \neq 0$$

$$f(3) = 16 \equiv 2 \pmod{7} \neq 0$$

$$f(4) = 24 \equiv 3 \pmod{7} \neq 0$$

$$f(5) = 34 \equiv 6 \pmod{7} \neq 0$$

$$f(6) = 46 \equiv 4 \pmod{7} \neq 0$$

Therefore there is no root for $f(x)$ in \mathbb{Z}_7

Hence $f(x)$ is irreducible over \mathbb{Z}_7 .

6. Define principal ideal.

(K1, CO3)

Solution:

Let R be a commutative ring with unity and $a \in R$, then the ideal generated by single element a is called a principal ideal and it is denoted by $\langle a \rangle$

$$\text{Thus } \langle a \rangle = \{ra \mid r \in R\}.$$

7. What is the GCD of $f(x) = x^4 + x^3 + 1$ and $g(x) = x^2 + x + 1$ in $Z_2[x]$.

(K3, CO3)

Solution:

We know that $Z_2 = \{0, 1\}$.

Given $f(x) = x^4 + x^3 + 1$ and $g(x) = x^2 + x + 1$

Now, $f(0) = 0 + 0 + 1 \neq 0$

$$f(1) = 3 \equiv 1 \pmod{2} \neq 0.$$

Therefore, $f(x)$ has no root for in Z_2

Hence $f(x)$ is irreducible over Z_2 .

$$g(0) = 0 + 0 + 1 \neq 0$$

$$g(1) = 1 + 1 + 1 = 3 \equiv 1 \pmod{2} \neq 0$$

Therefore, there is no root for $g(x)$ in Z_2

Hence $f(x)$ is irreducible over Z_2 .

Thus $f(x)$ and $g(x)$ are irreducible polynomials over Z_2 .

Therefore, GCD of $f(x)$ and $g(x)$ is 1.

8. State division algorithm for polynomials.

(K2, CO3)

Solution:

Let F be a field. Let $f(x)$ and $g(x)$ be two polynomials in $F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

9. State Remainder Theorem.

(K2, CO3)

Solution:

Let F be a field and $a \in F$. Let $f(x) \in F(x)$.

Then $f(a)$ is the remainder when $f(x)$ is divided by $(x - a)$.

10. State Factor Theorem.

(K2, CO3)

Solution:

Let F be a field and $a \in F$. Let $f(x) \in F(x)$

then a is the root of $f(x)$ iff $(x - a)$ is a factor of $f(x)$.

11. Find the remainder when $f(x) = x^{100} + x^{90} + x^{80} + x^{70} + x^{50} + 1$ is divided by $g(x) = x - 1$ in $Z_2[x]$.

(K3, CO3)

Solution: we have $f(x) = x^{100} + x^{90} + x^{80} + x^{70} + x^{50} + 1$ and $g(x) = x - 1$

Here $a = 1$

Therefore $f(1) = 1 + 1 + 1 + 1 + 1 + 1 = 6 \equiv 0 \pmod{2}$

The remainder is 0.

12. If $f(x) = 3x^5 - 8x^4 + x^3 - x^2 + 4x - 7$ and $g(x) = x + 9$, such that $f(x), g(x) \in Z_{11}[x]$. Find the remainder when $f(x)$ is divided by $g(x)$.

(K3, CO3)

Solution: Given $g(x) = x + 9 \Rightarrow x = -9$

$$f(-9) = 3(-9)^5 - 8(-9)^4 + (-9)^3 - (-9)^2 + 4(-9) - 7$$

$$= -177147 - 52488 - 729 - 124$$

$$= -230488$$

$$= 6 \pmod{11}$$

$$\Rightarrow \text{Remainder} = 6.$$

13. Define Polynomial ring.

(K2, CO3)

Solution:

Let $(R, +, \cdot)$ be a ring. An expression of the form

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

Where n is the non negative integers and $a_0, a_1, a_2 \cdots a_n \in R$ is called a Polynomial over R in the indeterminate x .

14. Define monic polynomial.

(K2, CO3)

Solution:

A polynomial in which the leading coefficient is 1 is called the monic polynomial.

15. Define constant polynomial.

(K2, CO3)

Solution:

A polynomial of the form $f(x) = a_0$, where a_0 is a constant is called a constant polynomial.

16. If $f(x) = x^8 + 7x^5 - 4x^4 + 3x^3 + 5x^2 - 4$ and $g(x) = x - 3$,
such that $f(x), g(x) \in \mathbb{Q}[x]$. Find the remainder when $f(x)$ is
divided by $g(x)$. (K3, CO3)

Solution: Given $g(x) = x - 3 \Rightarrow x = 3$

$$\begin{aligned} f(3) &= 3^8 + 7(3)^5 - 4(3)^4 + 3(3)^3 + 5(3)^2 - 4 \\ &= 6561 + 7(243) - 4(81) + 3(27) + 5(9) - 4 \\ &= 8060. \end{aligned}$$

PART B QUESTIONS: UNIT II

1. If R is a ring under usual addition and multiplication, show that $(R[x], +, \times)$ is a ring of polynomials over R . (K2, CO3)
2. Prove that $R[x]$ is an integral domain if and only if R is an integral domain. (K2, CO3)
3. If $f(x) = x^{100} + x^{90} + x^{80} + x^{50} + 1$, $g(x) = x - 1$, and $f(x), g(x) \in \mathbb{Z}_2[x]$ find the remainder when $f(x)$ is divided by $g(x)$. (K3, CO3)
4. If $f(x) \in F[x]$ has degree $n \geq 1$, then prove that $f(x)$ has at most n roots in F . (K3, CO3)
5. Let F be a field and $F[x]$ be the corresponding polynomial ring and $f(x) \in F[x]$ and $a \in F$. Show that $x - a$ is a factor of $F[x]$ if and only if a is a root of $f(x)$. (K3, CO3)
6. Let F be a field and $F[x]$ be the corresponding polynomial ring. Let $f(x), g(x) \in F[x]$ with $f(x)$ not the zero polynomial. Show that there exist unique polynomials $q(x), r(x) \in F[x]$ such that $g(x) = q(x)f(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg f(x)$. (K3, CO3)
7. State and prove remainder theorem for polynomials. (K2, CO3)
8. Determine whether the polynomial $x^4 + x^2 + 1$ is irreducible over \mathbb{Z}_2 . Also give an example of a reducible polynomial of degree 6 over \mathbb{Z}_2 having no root in \mathbb{Z}_2 . How many polynomials in \mathbb{Z}_2 have degree 3? (K3, CO3)
9. Construct a field consisting of four elements (Hint: use the irreducible binary polynomial $x^2 + x + 1$ over \mathbb{Z}_2). (K3, CO3)
10. Determine whether the following polynomials are irreducible over the given fields a) $x^2 + x + 1$ over $\mathbb{Z}_2, \mathbb{Z}_5$ and \mathbb{Z}_7 . b) $x^3 + 3x^2 - x + 1$ over \mathbb{Z}_5 . (K3, CO3)
11. Find the multiplicative inverse of each non-zero element in \mathbb{Z}_7 (with respect to the operations addition modulo 7 and multiplication modulo 7). Also, show that the polynomial $x^4 + x^2 + 1$ is irreducible over \mathbb{Z}_2 . (K3, CO3)
12. Prove that every finite field has p^n elements for some prime number p and some positive integer n . (K3, CO3)

SUPPORTIVE ONLINE CERTIFICATION COURSES

The following NPTEL and Coursera courses are the supportive online certification courses for the subject Algebra and Number theory.

1. Introduction to Abstract Group Theory (NPTEL course)

<https://nptel.ac.in/courses/111/106/111106113/>

2. Introduction to Rings and Fields (NPTEL course)

<https://nptel.ac.in/courses/111/106/111106131/#>

3. Mathematical Foundations for Cryptography (Coursera online course).

<https://www.coursera.org/learn/mathematical-foundations-cryptography>

View the following lectures on YouTube:

Applications of Groups

<https://youtu.be/vX8J9oqsVfM>

Motivation for Groups:

https://youtu.be/PN-cro0J_v8

Application of Fields

<https://youtu.be/nczJ7Nw41mU>

Construction of Finite Fields: (Application in Coding theory)

<https://youtu.be/GJtNLiG4Hv8>

Applications of Polynomial Rings

https://youtu.be/4WEhfOI_JAA

DOWNLOADED FROM STUCOR APP

CONTENT BEYOND THE SYLLABUS

The topic **Introduction to Vector space** is the content beyond the syllabus for the course Algebra and Number Theory.

View the lecture on YouTube:

<https://youtu.be/YshfZm99wjk>

Value Added Courses:

1. Mathematics for Machine Learning: Linear Algebra (Coursera online course)
2. Mathematical Foundations for Cryptography (Coursera online course)

PRESCRIBED TEXT BOOKS & REFERENCE BOOKS

TEXTBOOKS:

1. Grimaldi, R.P and Ramana, B.V., "Discrete and Combinatorial Mathematics", Pearson Education, 5th Edition, New Delhi, 2007.
2. Koshy, T.,—"Elementary Number Theory with Applications", Elsevier Publications, New Delhi, 2002.

REFERENCES:

1. Lidl, R. and Pitz, G, "Applied Abstract Algebra", Springer Verlag, New Delhi, 2nd Edition, 2006.
2. Niven, I., Zuckerman.H.S., and Montgomery, H.L., —"An Introduction to Theory of Numbers", John Wiley and Sons , Singapore, 2004.
3. San Ling and Chaoping Xing, —"Coding Theory – A first Course", Cambridge Publications, Cambridge, 2004.

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

STUCOR APP

STUCOR APP

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

MA8551 - Algebra and Number Theory

Department: Mathematics

Batch/Year: CSE/ III

Created by: Mr. R. Rajaraman

Date: 21.08.2020

Table of Contents

Contents

1	Course Objectives	6
2	Pre-requisites	7
3	Syllabus	8
4	Course Outcomes	9
5	CO – PO/PSO Mapping	10
6	Lecture Plan	11
7	Activity Based Learning	12
8	Lecture Notes: Unit III Divisibility Theory and Canonical Decompositions	13
9	Division Algorithm	14
10	Base - b representations	20
11	Number patterns	27
12	Prime and composite numbers	30
13	Greatest Common Divisor	34
14	Fundamental theorem of arithmetic	40
15	Canonical Decomposition	42
16	Least Common Multiple	44
17	Practice Quiz: Divisibility Theory and Canonical Decompositions	47
18	Assignments: Unit III	48
19	Part A Questions and Answers: Unit III	49
20	Part B Questions: Unit III	55
21	Supportive online Certification courses	56
22	Real time Applications	57
23	Content beyond the Syllabus	58
24	Prescribed Text Books & Reference Books	59

COURSE OBJECTIVES

To introduce the basic notions of groups, rings, fields which will then be used to solve related problems.

To introduce and apply the concepts of rings, finite fields and polynomials.

To understand the basic concepts in number theory.

To examine the key questions in the Theory of Numbers.

To give an integrated approach to number theory and abstract algebra, and provide a firm basis for further reading and study in the subject.

PRE-REQUISITES

Pre-requisites for the subject Algebra and Number Theory is
MA8351 - Discrete Mathematics.

STUCOR APP

MA8551	ALGEBRA AND NUMBER THEORY	L	T	P	C	
		4	0	0	4	
UNIT I GROUPS AND RINGS						12
Groups : Definition - Properties - Homomorphism - Isomorphism - Cyclic groups - Cosets - Lagrange's theorem. Rings: Definition - Sub rings - Integral domain - Field - Integer modulo n - Ring homomorphism.						
UNIT II FINITE FIELDS AND POLYNOMIALS						12
Rings - Polynomial rings - Irreducible polynomials over finite fields - Factorization of polynomials over finite fields.						
UNIT III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS						12
Division algorithm – Base - b representations – Number patterns – Prime and composite numbers – GCD – Euclidean algorithm – Fundamental theorem of arithmetic – LCM.						
UNIT IV DIOPHANTINE EQUATIONS AND CONGRUENCES						12
Linear Diophantine equations – Congruence's – Linear Congruence's - Applications: Divisibility tests - Modular exponentiation-Chinese remainder theorem – 2 x 2 linear systems.						
UNIT V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS						12
Wilson's theorem – Fermat's little theorem – Euler's theorem – Euler's Phi functions – Tau and Sigma functions.						
TOTAL: 60 PERIODS						

COURSE OUTCOMES

CO 1: Apply the basic notions of groups which will be used to solve group theory related problems.

CO 2: Apply the basic notions of rings, fields which will then be used to solve related problems.

CO 3: Demonstrate accurate and efficient use of advanced algebraic techniques such as finite fields and polynomials.

CO 4: Explain the fundamental concepts of number theory, advanced algebra and their role in modern mathematics.

CO 5: Demonstrate the number theory concepts by solving non - trivial related problems.

CO 6: Apply integrated approach to number theory and abstract algebra and prove simple theorems.

Course Out Comes	Program Outcomes												Program Specific Outcomes		
	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6	PO-7	PO-8	PO-9	PO-10	PO-11	PO-12	PSO-1	PSO-2	PSO-3
C01	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C02	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C03	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C04	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C05	3	2	-	-	-	-	-	-	-	-	-	-	-	-	-
C06	3	2	1	-	-	-	-	-	-	-	-	-	1	-	-

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High)

UNIT III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS							
S. No	Topic	No. of Periods	Proposed date	Actual date	Pertaining CO(s)	Taxonomy level	Mode of Delivery
1	Division Algorithm	2			CO4	K2	PPT
2	Inclusion-Exclusion principle	1			CO4	K3	PPT
3	Base - b representations	1			CO4	K3	PPT
4	Number patterns	1			CO4	K3	PPT
5	Prime and composite numbers	2			CO4	K2	PPT
6	GCD	2			CO4	K3	PPT
7	Euclidean algorithm	1			CO4	K3	PPT
8	Canonical decomposition	1			CO4	K3	PPT
9	Fundamental theorem of arithmetic	1			CO4	K3	PPT
10	LCM	1			CO4	K3	PPT

ACTIVITY BASED LEARNING

Activity based learning helps students express and embrace their curiosity. Once the students become curious, they tend to explore and learn by themselves. To evoke curiosity in students, Practice quiz is designed for all the five units.

Quiz – Unit III Divisibility Theory And Canonical Decompositions

<https://quizizz.com/print/quiz/5f34c66c9c163a001cbcdcbce>

Play game Quiz: Divisibility Theory And Canonical Decompositions

<https://quizizz.com/join/quiz/5f34c66c9c163a001cbcdcbce/start?from=soloLinkShare&referrer=5f34c592777326001b2ccd9e>

LECTURE NOTES**UNIT III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS**

This chapter begin to deal with the divisibility theory of integers. Also, this chapter continues the study of properties of integers and explores some classes of positive integers such as prime numbers, which are the building blocks of integers, and composite numbers. We begin by exploring the common factor of two or more positive integers. Finally, we establish the fundamental theorem of arithmetic, and then turn to the common multiples of two or more positive integers.

Division algorithm – Base - b representations – Number patterns – Prime and composite numbers – GCD – Euclidean algorithm – Fundamental theorem of arithmetic – LCM.

E- Book Reference:

<https://drive.google.com/file/d/1frQQxDZ4wWsS78NHZK6xQAZqfXofcIGQ/view?usp=drivesdk>

DIVISION ALGORITHM

View the lecture on YouTube: <https://youtu.be/TJGm1Af25S0>

Well-ordering Principle

Every non-empty subset of Natural numbers has a least element.

The Division Algorithm

The division algorithm is a fine application of the well-ordering principle and is often employed to check the correctness of a division problem.

THEOREM 1: (The Division Algorithm) Let a be any integer and b a positive integer. Then there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$.

Proof: The proof consists of two parts.

Existence proof:

Consider the set $S = \{a - bn : n \in \mathbb{Z} \text{ and } a - bn \geq 0\}$.

Clearly, $S \subseteq \mathbb{W}$. We shall show that S contains a least element.

First we will show that S is a non-empty subset of \mathbb{W} .

Case (i) Suppose $a \geq 0$. Then $a = a - b \cdot 0 \in S$, so S contains an element.

Case (ii) Suppose $a \leq 0$. Since $b \in \mathbb{Z}^+$, $b \geq 1$. \mathbb{W}

Then $ab \leq a \Rightarrow -ba \geq -a \Rightarrow a - ba \geq 0$. i.e. $a - ba \in S$.

In both cases, S contains at least one element. So, S is a non-empty set of \mathbb{W} .

\therefore By well ordering principle, S contains a least element r .

Since $r \in S$, an integer q exists such that $r = a - bq$, where $r \geq 0$.

To show that $r < b$.

Assume $r \geq b$. Then $r - b \geq 0$.

But $r - b = (a - bq) - b = a - b(q + 1)$

Since $a - b(q + 1)$ is of the form $a - bn$ and ≥ 0

$a - b(q + 1) \in S$ i.e. $r - b \in S$

Since $b > 0$, $r - b < r$. Thus $r - b$ is smaller than r and is in S .

This contradicts our choice of r , so $r < b$.

Thus, there are integers q and r such that $a = bq + r$, where $0 \leq r < b$. ----(1)

Uniqueness Proof:

Suppose $a = bq_1 + r_1$, where $0 \leq r_1 < b$

Then $bq + r = bq_1 + r_1$ by (1)

$$\Rightarrow (q - q_1)b = r_1 - r \Rightarrow b/r_1 - r$$

If $r_1 - r \neq 0$, then $b/r_1 - r$. Which is a contradiction. (since $|r_1 - r| < b$)

$$\therefore r_1 - r = 0 \Rightarrow r_1 = r$$

Hence $(q - q_1)b = 0 \Rightarrow q - q_1 = 0 \Rightarrow q_1 = q$.

$\therefore a = bq + r$, where $0 \leq r < b$ is unique.

Hence the proof.

Example 1: Find the quotient q and the remainder r when

(i) 207 is divided by 15.

(ii) -23 is divided by 5.

Solution:

(i) $207 = 15 \cdot 13 + 12$; so $q = 13$ and $r = 12$.

(ii) $-23 = 5 \cdot (-5) + 2$; so $q = -5$ and $r = 2$.

The Pigeonhole Principle and the Division Algorithm

The pigeonhole principle is also known as the Dirichlet box principle after the German mathematician Gustav Peter Lejeune Dirichlet who used it extensively in his work on number theory. It can be applied to variety of situations.

Suppose m pigeons fly into n pigeonholes to roost, where $m > n$. What is your conclusion? Because there are more pigeons than pigeonholes, at least two pigeons must roost in the same pigeonhole; in other words, there must be a pigeonhole containing two or more pigeons.

THEOREM 2: (The Pigeonhole Principle) If m pigeons are assigned to n pigeonholes, where $m > n$, then at least two pigeons must occupy the same pigeonhole.

Proof: (By Contradiction)

Suppose the given conclusion is false; that is, no two pigeons occupy the same pigeonhole. Then every pigeon must occupy a distinct pigeonhole, so $n > m$, which is a contradiction. Thus, two or more pigeons must occupy some pigeonhole.

Example 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 .

Solution:

Let q be the quotient and r the remainder when an integer a is divided by b .

Then, by the division algorithm, $a = bq + r$, where $0 \leq r < b$.

The $b + 1$ integers yield $b + 1$ remainders (pigeons), but there are only b possible remainders (pigeonholes).

Therefore, by the pigeonhole principle, two of the remainders must be equal.

Let x and y be the corresponding integers.

Then $x = bq_1 + r$ and $y = bq_2 + r$ for some quotients q_1 and q_2 .

$$\therefore x - y = (bq_1 + r) - (bq_2 + r) = b(q_1 - q_2)$$

Thus, $x - y$ is divisible by b .

The Divisibility Relation

Suppose we let $r = 0$ in the division algorithm. Then $a = bq + 0 = bq$. We then say that b divides a , b is a factor of a , a is divisible by b , or a is a multiple of b , and write $b|a$. If b is not a factor of a , we write $b \nmid a$.

THEOREM 2: Let a and b be positive integers such that $a|b$ and $b|a$. Then $a = b$.

Proof:

Let a and b be positive integers such that $a|b$ and $b|a$.

Claim: $a = b$

Since $a|b \Rightarrow b = aq$, for some $q \in \mathbb{Z}$. -----(1)

Also, $b|a \Rightarrow aq|a \Rightarrow q = 1$

Substitute in (1), we have $a = b$.

Hence the proof.

THEOREM 3: Let a, b, c, α and β be any integers. Then,

(i) If $a|b$ and $b|c$, then $a|c$. (transitive property)

(ii) If $a|b$ and $a|c$, then $a|(\alpha b + \beta c)$.

(iii) If $a|b$, then $a|bc$.

Proof:

(i) $a|b \Rightarrow b = q_1 a \Rightarrow c = q_2 b$, where $a \neq 0, b \neq 0$ in \mathbb{Z} , q_1, q_2 are some integers.

$$\therefore c = q_2(q_1 a) = (q_1 q_2) a \Rightarrow a|c.$$

(ii) $a|b \Rightarrow b = q_1a$ and $a|c \Rightarrow c = q_2a$, for some integers q_1, q_2

$$\therefore \alpha b + \beta c = \alpha(q_1a) + \beta(q_2a)$$

$$= (\alpha q_1)a + (\beta q_2)a$$

$$= (\alpha q_1 + \beta q_2)a, \alpha q_1 + \beta q_2, \text{ is an integer.}$$

$$\Rightarrow a|(\alpha b + \beta c).$$

(iii) $a|b \Rightarrow b = q_1a$

$$\therefore bc = (q_1a)c = q_1(ac) = q_1(ca) = (q_1c)a$$

$$\Rightarrow a|bc, \forall b \in \mathbb{Z}.$$

Note:

The expression $\alpha b + \beta c$ is called a linear combination of b and c . Thus, by part 2, if a is a factor of b and c , then a is also a factor of any linear combination of b and c . In particular, $a|(b + c)$ and $a|(b - c)$.

The floor function can be used to determine the number of positive integers less than or equal to a positive integer a and divisible by a positive integer b , as the next theorem shows.

THEOREM 4: Let a and b be any positive integers. Then the number of positive integers $\leq a$ and divisible by b is $\lceil a/b \rceil$.

Proof:

Suppose there are k positive integers $\leq a$ and divisible by b .

we need to show that $k = \lceil a/b \rceil$.

The positive multiples of b less than or equal to a are $b, 2b, \dots, kb$.

Clearly, $kb \leq a$, i.e. $k \leq a/b$.

Further, $(k + 1)b > a$. Thus, $k + 1 > a/b$ or $a/b - 1 < k$.

$$\therefore a/b - 1 < k \leq a/b.$$

Thus, k is the largest integer less than or equal to a/b , so $k = \lceil a/b \rceil$.

Hence the proof.

For example, the number of positive integers ≤ 2076 and divisible by 19 is $\lceil 2076/19 \rceil = \lceil 109.26316 \rceil = 109$.

Union, Intersection and Complement

Let A be a finite set and $|A|$ the number of elements in A .

For example, if $A = \{3, 5, 8, 17\}$, then $|A| = 4$.

Let A and B be any two sets. Their union $A \cup B$ is the set of elements belonging to A or B ; their intersection $A \cap B$ consists of the common elements; A' denotes the complement of A , that is, the set of elements in the universal set that are not in A .

Principle of Inclusion and Exclusion:

Let A and B be finite sets. Let $|A \cup B| = |A| + |B| - |A \cap B|$

Likewise, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$

THEOREM 6: (The Inclusion-Exclusion Principle)

Let A_1, A_2, \dots, A_n be n finite sets. Then $|\bigcup_{i=1}^n A_i| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n+1} |\bigcap_{i=1}^n A_i|$.

Example 3: Find the number of positive integers ≤ 2076 and divisible by neither 4 nor 5.

Solution:

Let $A = \{x \in \mathbb{N} : x \leq 2076 \text{ and divisible by } 4\}$ and

$B = \{x \in \mathbb{N} : x \leq 2076 \text{ and divisible by } 5\}$. Then

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$= \left\lfloor \frac{2076}{4} \right\rfloor + \left\lfloor \frac{2076}{5} \right\rfloor - \left\lfloor \frac{2076}{20} \right\rfloor$$

$$= 519 + 415 - 103 = 831.$$

Thus, among the first 2076 positive integers, there are $2076 - 831 = 1245$ integers not divisible by 4 or 5.

Example 4: Find the number of positive integers ≤ 3000 and divisible by 3, 5 or 7.

Solution:

Let A, B and C denote the sets of positive integers ≤ 3000 and divisible by 3, 5 or 7.

By the inclusion-exclusion principle.

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

$$= \left\lfloor \frac{3000}{3} \right\rfloor + \left\lfloor \frac{3000}{5} \right\rfloor + \left\lfloor \frac{3000}{7} \right\rfloor - \left\lfloor \frac{3000}{15} \right\rfloor - \left\lfloor \frac{3000}{35} \right\rfloor - \left\lfloor \frac{3000}{21} \right\rfloor + \left\lfloor \frac{3000}{105} \right\rfloor$$

$$= 1000 + 600 + 428 - 200 - 85 - 142 + 28$$

$$= 1629.$$

Principle of Mathematical Induction:

Let $P(n)$ be the given statement.

Base Step: $P(n_0)$ is true for some integer n_0 .

Inductive Step: $P(k)$ is true for an arbitrary integer $k \geq n_0$.

Then $P(k + 1)$ is true.

Hence $P(n)$ is true for every integer $n \geq n_0$.

Example 5: Prove by induction $2n^3 + 3n^2 + n$ is divisible by 6, $\forall n \geq 0$.

Solution:

Let $P(n) = 2n^3 + 3n^2 + n$ is divisible by 6, $\forall n \geq 0$.

Base Step:

$P(0) = 0$ is divisible by 6.

Inductive Step:

Assume $P(k)$ is true for all $k \geq 0$.

i.e. $2k^3 + 3k^2 + k$ is divisible by 6, $\forall k \geq 0$

i.e. $2k^3 + 3k^2 + k = 6m$ (say), $m > 0$. -----(1)

To Prove: $P(k + 1)$ is true.

i.e. $2(k + 1)^3 + 3(k + 1)^2 + (k + 1)$ is divisible by 6.

Consider $2(k + 1)^3 + 3(k + 1)^2 + (k + 1)$.

$$= 2(k^3 + 1 + 3k^2 + 3k) + 3(k^2 + 2k + 1) + (k + 1)$$

$$= 2k^3 + 6k^2 + 6k + 2 + 3k^2 + 6k + 3 + k + 1$$

$$= (2k^3 + 3k^2 + k) + (6k^2 + 12k + 6)$$

$$= 6m + 6(k^2 + 2k + 1)$$

$$= 6(k^2 + 2k + 1 + m)$$

Which is divisible by 6.

Thus $P(k + 1)$ is true.

Hence $P(n)$ is true.

BASE – b REPRESENTATIONS**Definition:** (Base – b Representations)

If n is a positive integer and $b \geq 2$ and $n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$,

where a_0, a_1, \dots, a_k are non negative integers then the above expression is called base b of the integer n . We then write $n = (a_k a_{k-1} \dots a_1 a_0)_b$.

Example:

$$(345)_{10} = 3(10)^2 + 4(10) + 5.$$

Note:

- (i) The number system with base 2 is called binary system and it has the digits 0, 1.
- (ii) The number system with base 8 is called octal system and it has the digits 0, 1, 2, 3, 4, 5, 6, 7.
- (iii) The number system with base 10 is called decimal system and it has the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
- (iv) The number system with base 16 is called hexadecimal system and it has the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 with letters A, B, C, D, E, F. The letters A, B, C, D, E, F denotes the digits 10, 11, 12, 13, 14, 15 respectively.

Conversion of Binary, Octal, Hexadecimal systems to Decimal system**Example 1:**

Express $(101011)_2$ in base 10.

Solution:

$$\begin{aligned}(101011)_2 &= 1(2)^5 + 0(2)^4 + 1(2)^3 + 0(2)^2 + 1(2)^1 + 1(2)^0 \\ &= 32 + 8 + 2 + 1 \\ &= 43.\end{aligned}$$

Therefore $(101011)_2 = (43)_{10}$.

Example 2:

Express $(347)_8$ in base 10.

Solution:

$$\begin{aligned}(347)_8 &= 3(8)^2 + 4(8)^1 + 7(8)^0 \\ &= 192 + 32 + 7 \\ &= 231\end{aligned}$$

Therefore $(347)_8 = (231)_{10}$.

Example 3

Express $(3AB0E)_{16}$ in base 10.

Solution:

$$\begin{aligned}(3AB0E)_{16} &= 3(16)^4 + A(16)^3 + B(16)^2 + 0(16)^1 + E(16)^0 \\ &= 3(16)^4 + 10(16)^3 + 11(16)^2 + 0(16)^1 + 14(16)^0 \\ &= 196608 + 40960 + 2816 + 14 \\ &= 240398.\end{aligned}$$

Therefore $(3AB0E)_{16} = (240398)_{10}$.

Conversion of Decimal system to Binary, Octal and Hexadecimal systems

Example 1:

Express $(134)_{10}$ in binary system.

Solution:

$$\begin{aligned}134 &= 67(2) + 0 \\ 67 &= 33(2) + 1 \\ 33 &= 16(2) + 1 \\ 16 &= 8(2) + 0 \\ 8 &= 4(2) + 0 \\ 4 &= 2(2) + 0 \\ 2 &= 1(2) + 0 \\ 1 &= 0(2) + 1\end{aligned}$$

Therefore $(134)_{10} = (10000110)_2$.

Example 2:

Express $(1543)_{10}$ in octal system.

Solution:

$$\begin{aligned}1543 &= 192(8) + 7 \\ 192 &= 24(8) + 0 \\ 24 &= 3(8) + 0 \\ 3 &= 0(8) + 3\end{aligned}$$

Therefore $(1543)_{10} = (3007)_8$.

Example 3:

Express $(15036)_{10}$ in hexadecimal system.

Solution:

$$15036 = 939(16) + 12 (= C)$$

$$939 = 58(16) + 11 (= B)$$

$$58 = 3(16) + 10 (= A)$$

$$3 = 0(16) + 3$$

Therefore $(15036)_{10} = (3ABC)_{16}$.

We have seen the conversions of base b systems to decimal system and decimal system to base b systems.

Conversion of Binary system to Octal system

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 zeroes at the left most block and replace each group with the corresponding octal digit.

Example 1:

Convert the binary number $(1110011)_2$ into octal digit.

Solution:

Given 1 110 011 .

We group the digits in blocks of three digits from right to left.

Here the blocks are 001, 110, 011 (adding zeroes to the left most block to get three digits).

$$001 = 0.(2)^2 + 0.(2)^1 + 1.(2)^0 = 1$$

$$110 = 1.(2)^2 + 1.(2)^1 + 0.(2)^0 = 6$$

$$011 = 0.(2)^2 + 1.(2)^1 + 1.(2)^0 = 3$$

Therefore $(1110011)_2 = (163)_8$.

Example 2:

Convert the binary number $(111010)_2$ into octal digit.

Solution:

Given 111 010.

We group the digits in blocks of three digits from right to left.

Here the blocks are 111, 010.

$$111 = 1(2)^2 + 1(2)^1 + 1(2)^0 = 7$$

$$010 = 0(2)^2 + 1(2)^1 + 0(2)^0 = 2$$

Therefore $(111010)_2 = (72)_8$.

Conversion of Binary system to Hexadecimal system

To convert a binary system number to hexadecimal system, we group the binary digits into blocks of four bits from right to left and adding if necessary initial zeroes at the left most block and replace each group with the corresponding hexadecimal digit.

Example 1:

Convert the binary number $(11111010111100)_2$ into hexadecimal digit.

Solution:

Given 11 1110 1011 1100.

We group the digits in blocks of four digits from right to left.

Here the blocks are 0011, 1110, 1011, 1100 (adding zeroes to the left most block to get four digits).

$$0011 = 0(2)^3 + 0(2)^2 + 1(2)^1 + 1(2)^0 = 3$$

$$1110 = 1(2)^3 + 1(2)^2 + 1(2)^1 + 0(2)^0 = 14 (= E)$$

$$1011 = 1(2)^3 + 0(2)^2 + 1(2)^1 + 1(2)^0 = 11 (= B)$$

$$1100 = 1(2)^3 + 1(2)^2 + 0(2)^1 + 0(2)^0 = 12 (= C)$$

Therefore $(11111010111100)_2 = (3EBC)_{16}$.

Example 2:

Convert the binary number $(1110101)_2$ into hexadecimal digit.

Solution:

Given 111 0101.

We group the digits in blocks of four digits from right to left.

Here the blocks are 0111, 0101 (adding zero to the left most block to get four digits).

$$0111 = 0(2)^3 + 1(2)^2 + 1(2)^1 + 1(2)^0 = 7$$

$$0101 = 0(2)^3 + 1(2)^2 + 0(2)^1 + 1(2)^0 = 5$$

Therefore $(1110101)_2 = (75)_{16}$.

Conversion of Octal system to Binary system

To convert an octal system number to binary system, we write each digits from left to right as block of three bits, then grouping all those block of three bits from top to bottom as left to right gives the corresponding binary value.

Example 1:

Convert the octal digit $(3450)_8$ into binary number.

Solution:

Given $(3450)_8$.

We write each digits as a block of three bits.

$$3 = 0(2)^2 + 1(2)^1 + 1(2)^0 = 011$$

$$4 = 1(2)^2 + 0(2)^1 + 0(2)^0 = 100$$

$$5 = 1(2)^2 + 0(2)^1 + 1(2)^0 = 101$$

$$0 = 0(2)^2 + 0(2)^1 + 0(2)^0 = 000$$

Therefore $(3450)_8 = (011100101000)_2$.

$$= (11100101000)_2.$$

Example 2:

Convert the octal digit $(12376)_8$ into binary number.

Solution:

Given $(12376)_8$.

We write each digits as a block of three bits.

$$1 = 0(2)^2 + 0(2)^1 + 1(2)^0 = 001$$

$$2 = 0(2)^2 + 1(2)^1 + 0(2)^0 = 010$$

$$3 = 0(2)^2 + 1(2)^1 + 1(2)^0 = 011$$

$$7 = 1(2)^2 + 1(2)^1 + 1(2)^0 = 111$$

$$6 = 1(2)^2 + 1(2)^1 + 0(2)^0 = 110$$

Therefore $(12376)_8 = (001010011111110)_2$.

$$= (1010011111110)_2.$$

Conversion of Hexadecimal system to Binary system

To convert an hexadecimal system number to binary system, we write each digits from left to right as block of four bits, then grouping all those block of four bits from top to bottom as left to right gives the corresponding binary value.

Example 1:

Convert the hexadecimal digit $(3AD)_{16}$ into binary number.

Solution:

Given $(3AD)_{16}$.

We write each digits as a block of four bits.

$$3 = 0(2)^3 + 0(2)^2 + 1(2)^1 + 1(2)^0 = 0011$$

$$A = 10 = 1(2)^3 + 0(2)^2 + 1(2)^1 + 0(2)^0 = 1010$$

$$D = 13 = 1(2)^3 + 1(2)^2 + 0(2)^1 + 1(2)^0 = 1101$$

$$\begin{aligned}\text{Therefore } (3AD)_{16} &= (001110101101)_2. \\ &= (1110101101)_2.\end{aligned}$$

Example 2:

Convert the hexadecimal digit $(25)_{16}$ into binary number.

Solution:

Given $(25)_{16}$.

We write each digits as a block of four bits.

$$2 = 0(2)^3 + 0(2)^2 + 1(2)^1 + 0(2)^0 = 0010$$

$$5 = 0(2)^3 + 1(2)^2 + 0(2)^1 + 1(2)^0 = 0101$$

$$\begin{aligned}\text{Therefore } (25)_{16} &= (00100101)_2. \\ &= (100101)_2.\end{aligned}$$

Example 3:

Find the number of ones in the binary expansion of $2^4 - 1$.

Solution:

$$\begin{aligned}2^4 - 1 &= 15 = 1(2)^3 + 1(2)^2 + 1(2)^1 + 1(2)^0 \\ &= (1111)_2.\end{aligned}$$

Hence the number of ones in the binary expansion of $2^4 - 1$ is 4.

Remark:

More generally the number of ones in the binary expansion of $2^n - 1$ is n .

Finding base b values**Example 1:**

Find the value of base b if $(1001)_b = 9$.

Solution:

Given that $(1001)_b = 9$.

$$\Rightarrow 1(b)^3 + 0(b)^2 + 0(b)^1 + 1(b)^0 = 9$$

$$\Rightarrow b^3 + 1 = 9$$

$$\Rightarrow b^3 = 8$$

$$\Rightarrow b = 2.$$

Example 2:

Find the value of base b if $(144)_b = 49$.

Solution:

Given that $(144)_b = 49$.

$$\Rightarrow 1(b)^2 + 4(b)^1 + 4(b)^0 = 49$$

$$\Rightarrow b^2 + 4b + 4 = 49$$

$$\Rightarrow b^2 + 4b - 45 = 0$$

$$\Rightarrow (b + 9)(b - 5) = 0$$

$$\Rightarrow b = -9, 5$$

Since $b \geq 2$, we have $b = 5$.

NUMBER PATTERNS

In drawing scientific conclusions, there are two fundamental processes of reasoning that are commonly used.

One is the process of deduction, which is the process of reasoning from general to particular.

The other process of reasoning is the process of induction, which is the process of reasoning from particular to general. This process may lead to true or false conclusion. To succeed in the art of inductive reasoning one must be good at studying pattern. Observing particular cases or pattern a general statement is usually made. Such a statement is called a conjecture or educated guess. A conjecture remains a conjecture until it is proved or disproved.

Example 1:

From the pattern

$$\begin{aligned} 1.9 + 2 &= 11 \\ 12.9 + 3 &= 111 \\ 123.9 + 4 &= 1111 \\ 1234.9 + 5 &= 11111 \\ &\vdots \\ &\vdots \\ &\vdots \end{aligned}$$

Write down the n^{th} row and prove the validity of the number pattern.

Solution:

From the given pattern we find the n^{th} row is

$$1.2.3.4.5 \dots n.9 + (n + 1) = 1 \ 1 \ 1 \dots 1 \ \{n + 1\} \text{ones.}$$

$$\begin{aligned} L.H.S &= 1.2.3.4.5 \dots n.9 + (n + 1) \\ &= 9.1.2.3.4.5 \dots n + (n + 1) \\ &= 9 [1(10)^{n-1} + 2(10)^{n-2} + 3(10)^{n-3} + \dots + (n-1)10 + n.1] + (n + 1) \\ &= (10 - 1) [(10)^{n-1} + 2(10)^{n-2} + 3(10)^{n-3} + \dots + (n-1)10 + n] + (n + 1) \\ &= [10^n + 2.(10)^{n-1} + 3.(10)^{n-2} + \dots + (n-1).10^2 + n.10] \\ &\quad - [(10)^{n-1} + 2(10)^{n-2} + \dots + (n-2)10^2 + (n-1)10 + n] + (n + 1) \\ &= 10^n + 10^{n-1} + 10^{n-2} + \dots + 10^2 + 10 - n + (n + 1) \\ &= 10^n + 10^{n-1} + 10^{n-2} + \dots + 10^2 + 10 + 1 \\ &= 111 \dots 1 \ \{n + 1\} \text{ones.} \\ &= R.H.S. \end{aligned}$$

Example 2:

Using the number pattern

$$1^2 - 0^2 = 1$$

$$2^2 - 1^2 = 3$$

$$3^2 - 2^2 = 5$$

$$4^2 - 3^2 = 7$$

.

.

.

Make a conjecture about row n and prove the conjecture.

Solution:

From the given number pattern, we find the n^{th} row is

$$n^2 - (n - 1)^2 = 2n - 1$$

Therefore the conjecture is

$$n^2 - (n - 1)^2 = 2n - 1 \quad \forall n \geq 0$$

$$\begin{aligned} L.H.S &= n^2 - (n - 1)^2 \\ &= n^2 - (n^2 - 2n + 1) \\ &= 2n - 1 \\ &= R.H.S. \end{aligned}$$

Example 3:

Given the pattern

$$9.9 + 7 = 88$$

$$98.9 + 6 = 888$$

$$987.9 + 5 = 8888$$

.

.

.

Find the formula for the n^{th} row and prove it.

Solution:

Observing the pattern, we find the n^{th} is

$$987 \dots (10 - n).9 + (8 - n) = 888 \dots 8, \{n + 1 \text{ eights}\} \quad 1 \leq n \leq 8$$

$$L.H.S = 987 \dots (10 - n).9 + (8 - n)$$

$$= 9.987 \dots (10 - n) + (8 - n)$$

$$= 9.[9.(10)^{n-1} + 8.(10)^{n-2} + \dots + (11 - n).10 + (10 - n).1] + (8 - n)$$

$$= (10 - 1)[9.(10)^{n-1} + 8.(10)^{n-2} + \dots + (11 - n).10 + (10 - n).1] + (8 - n)$$

$$= [9.(10)^n + 8.(10)^{n-1} + 7.(10)^{n-2} + \dots + (11 - n).10^2 + (10 - n).10]$$

$$- [9.(10)^{n-1} + 8.(10)^{n-2} + \dots + (11 - n).10 + (10 - n)] + (8 - n)$$

$$= 9.10^n - [10^{n-1} + 10^{n-2} + \dots + 10^2 + 10] - (10 - n) + (8 - n)$$

$$= 10.10^n - [10^n + 10^{n-1} + 10^{n-2} + \dots + 10^2 + 10] - 2$$

$$= 10.10^n - [10^n + 10^{n-1} + 10^{n-2} + \dots + 10^2 + 10 + 1] - 1$$

$$= 10^{n+1} - \left[\frac{10^{n+1} - 1}{10 - 1} \right] - 1$$

$$= 10^{n+1} - \left[\frac{10^{n+1} - 1}{9} \right] - 1$$

$$= \frac{1}{9}[9.10^{n+1} - 10^{n+1} + 1 - 9]$$

$$= \frac{1}{9}[8.10^{n+1} - 8]$$

$$= \frac{8}{9}[10^{n+1} - 1]$$

$$= 888 \dots 8 \{n + 1 \text{ eights}\}$$

$$= R.H.S.$$

PRIME AND COMPOSITE NUMBERS

View the lecture on YouTube: <https://youtu.be/6So-0z4zxs4>

View motivational speech from Adam Spencer on YouTube to understand the nature of prime numbers: <https://youtu.be/B4xOFsygwr4>

Definition: Any positive integer > 1 is prime if and only if its factors are 1 and itself, and the positive integer that is not prime is called composite number.

If x is a positive real number then $\pi(x)$ denotes the number of primes $\leq x$.

Theorem 1: Every integer $n \geq 2$ has a prime factor.

Proof: This proof involves strong induction.

For $n = 2$, the statement is true since 2 is a prime number. Assume that all integers between 2 and k ($2 \leq x \leq k$) has a prime factor.

TPT the integer $k + 1$ also has a prime factor

(i) If $k + 1$ is prime then it is a factor of itself

(ii) If $k + 1$ is not prime then $k + 1$ has factors between $2 \leq x \leq k \Rightarrow (k + 1)$ has a prime factor.

Hence by induction all integers $n \geq 2$ has a prime factor.

Theorem 2: Prove that there are infinitely many primes.

Proof: Assume the contradiction, that is there is only a finite number of primes i.e., $p_1, p_2, p_3 \dots p_n$

Now, consider an integer $N = p_1 p_2 p_3 \dots p_n + 1$ since $N \geq 2$, N is divisible by some prime $p_i, 0 \leq i \leq n$.

Since $p_i | N \Rightarrow p_i | (p_1 p_2 p_3 \dots p_n)$

$$\Rightarrow p_i | (N - p_1 p_2 p_3 \dots p_n) = p_i | 1.$$

which is a contradiction that it is divided by only one term.

Hence the assumption is false.

\Rightarrow There are infinitely many primes.

Theorem 3: Prove that there are infinitely many prime of the form $4n + 3$.

Proof: To prove this assume the contradiction. i.e., there are only finite number of primes of the form $4n + 3$ and let them be $p_1, p_2, p_3 \dots p_n$.

Let $N = 4(p_1 p_2 p_3 \dots p_n) - 1$, then $N \equiv -1 \pmod{4} \Rightarrow N \equiv 3 \pmod{4}$.

Let the prime factorization of N be given as $N = q_1 q_2 q_3 \dots q_l$.

Since N is odd $\Rightarrow q_1, q_2, q_3 \dots q_l$ are all odd.

Note that any q_i satisfies one of the residues

$$q_i \equiv 1(\text{mod}4), q_i \equiv 2(\text{mod}4), q_i \equiv 3(\text{mod}4), q_i \equiv 0(\text{mod}4).$$

Since q_i is odd, $q_i \equiv 2(\text{mod}4), q_i \equiv 0(\text{mod}4)$ is not possible.

Therefore, we have $q_i \equiv 1(\text{mod}4)$ or $q_i \equiv 3(\text{mod}4)$.

Claim 1: At least for one i , $q_i \equiv 3(\text{mod}4)$.

To prove this claim assume the contrary that $q_i \equiv 1(\text{mod}4)$ for each $i = 1, 2, \dots, l$.

$$q_1 q_2 q_3 \dots q_l \equiv 1 \cdot 1 \cdot 1 \dots 1 (\text{mod}4)$$

$N \equiv 1(\text{mod}4)$, which is a contradiction. Hence the claim.

Claim 2: q_i is different from each of $p_1, p_2, p_3 \dots p_n$.

To prove this assume the contradiction, i.e., $q_i = p_j$ for some j .

Therefore, $p_j / (4p_1 p_2 p_3 \dots p_n) \Rightarrow p_j / (N + 1)$ by definition of N .

$$\Rightarrow q_i / N \Rightarrow p_j / N, \text{ since } q_i = p_j.$$

Now, $p_j / (N + 1)$ and $p_j / N \Rightarrow p_j / N + 1 - N \Rightarrow p_j / 1$ which

is contradiction that p_j is prime. Hence the Claim.

Claim 1 and 2 contradicts the assumption that there are finite number of prime.

Hence, there are infinitely many primes.

Theorem 4: For every positive integer n there are n consecutive integers that are composite.

Proof: Consider a n consecutive integers of the form

$$(n + 1)! + 2, (n + 1)! + 3, \dots, (n + 1)! + n + 1.$$

For any integer k ,

such that $2 \leq k \leq n + 1$ and by previous theorem, we have $k / (n + 1)!$ and also k / k , therefore $k / (n + 1)! + k$ for every k .

\Rightarrow each of them is composite.

Theorem 5: Every composite number n has a prime factor $\leq \sqrt{n}$.

Proof: Consider a composite number n . Then n can be written as a product of integers.

So for $a, b \in N$, let $n = ab$ be the composite number.

If suppose $a > \sqrt{n}$, $b > \sqrt{n}$, then $n = ab > \sqrt{n}\sqrt{n} > n$, which is a contradiction.

Therefore, $a \leq \sqrt{n}$, $b \leq \sqrt{n}$.

We know that, every positive integer ≥ 2 has a prime factor. Any such factor of a or b is also a factor of $ab = n$. So n must have a prime factor.

Important Results:

1. Let $p_1, p_2, p_3 \dots p_t$ be the prime $\leq \sqrt{n}$, then

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i < j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i < j < k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \dots + (-1)^n \left\lfloor \frac{n}{p_1 p_2 p_3 \dots p_t} \right\rfloor$$

2. If x approaches ∞ , $\pi(x)$ approaches $\frac{x}{\log x}$ for $x \geq 2$. i.e

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Example 1: Determine whether the following are prime or composite

a) 129 b) 1729 c) 1601 d) 1001

Solution: a) It's composite since 3 is a factor

b) Given 1729.

The prime factors $\leq \sqrt{1729} = 41.58$ are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.

In this 7 is a factor of 1729 ($7|1729$). Therefore, it is a composite number

c) 1601. The prime factors $\leq \sqrt{1601} = 40.01$ are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.

In this none of the numbers divide 1601.

Therefore, 1601 is a prime number.

d) 1001. The prime factors $\leq \sqrt{1001} = 31$ are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

In this 7 is a factor of 1001 ($7|1001$). Therefore, it is a composite number

Example 2: Find the number of primes ≤ 61 using $\pi(x)$.

Solution:

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i < j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i < j < k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \dots$$

$$+ (-1)^n \left\lfloor \frac{n}{p_1 p_2 p_3 \dots p_t} \right\rfloor$$

$$\pi(61) = 61 - 1 + \pi(\sqrt{61}) - \left(\frac{61}{2} + \frac{61}{3} + \frac{61}{5} + \frac{61}{7} \right)$$

$$+ \left(\frac{61}{6} + \frac{61}{10} + \frac{61}{14} + \frac{61}{15} + \frac{61}{21} + \frac{61}{35} \right)$$

$$\begin{aligned}
& -\left(\frac{61}{30} + \frac{61}{42} + \frac{61}{70} + \frac{61}{105}\right) + \left(\frac{61}{210}\right) \\
& = 60 + 4 - (30 + 20 + 12 + 8) + (10 + 6 + 4 + 4 + 2 + 4) \\
& \quad - (1 + 2 + 0 + 0) + (0) \\
& = 21.
\end{aligned}$$

Example 3: Find the number of primes ≤ 100 using $\pi(x)$.

Solution:

$$\begin{aligned}
\pi(n) &= n - 1 + \pi(\sqrt{n}) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i < j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i < j < k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \dots \\
& \quad + (-1)^n \left\lfloor \frac{n}{p_1 p_2 p_3 \dots p_t} \right\rfloor \\
\pi(100) &= 100 - 1 + \pi(\sqrt{100}) - \left(\frac{100}{2} + \frac{100}{3} + \frac{100}{5} + \frac{100}{7}\right) \\
& \quad + \left(\frac{100}{6} + \frac{100}{10} + \frac{100}{14} + \frac{100}{15} + \frac{100}{21} + \frac{100}{35}\right) \\
& \quad - \left(\frac{100}{30} + \frac{100}{42} + \frac{100}{70} + \frac{100}{105}\right) + \left(\frac{100}{210}\right) \\
&= 99 + 4 - (50 + 33 + 20 + 14) - (16 + 10 + 7 + 6 + 4 + 2) \\
&= 25.
\end{aligned}$$

Example 4: Find five consecutive integers that are composite.

Solution: Here, $n = 5$, We know that the consecutive composite numbers are given by $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$

$$\begin{aligned}
\text{For } n = 5 \text{ we have } 6! + 2, 6! + 3, 6! + 4, 6! + 5, 6! + 6 \\
= 722, 723, 724, 725, 726 \text{ are composite.}
\end{aligned}$$

Example 5: Find six consecutive integers that are composite.

Solution: We know that the consecutive composite numbers are given

$$\text{By } (n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$$

$$\begin{aligned}
\text{For } n = 6 \text{ we have } 7! + 2, 7! + 3, 7! + 4, 7! + 5, 7! + 6, 7! + 7 \\
= 5042, 5043, 5044, 5045, 5046, 5047 \text{ are composite.}
\end{aligned}$$

Example 6: Find five consecutive integers < 100 that are composite numbers.

Solution: Since $5! = 120 > 100$,

$$\text{We consider } 4!, 4! + 1, 4! + 2, 4! + 3, 4! + 4,$$

Therefore, 24, 25, 26, 27, 28 are 5 consecutive composite numbers < 100 .

View the lecture on YouTube: <https://youtu.be/IfLqUhTNQ3c>

Greatest Common Divisor (GCD)

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 $(3, 0) = 3$.

Important Results

A positive integer d is the gcd of two positive integers a and b , if

- (i) $d|a$ and $d|b$.
- (ii) If $c|a$ and $c|b$ then $c|d$, where c is the positive integer.

Theorem 1: The GCD of positive integers a and b is the linear combination with respect to a and b .

Proof:

Let $S = \{xa + yb \mid xa + yb > 0, x, y \in \mathbb{Z}\}$.

For $x = 1$ and $y = 0$, $S = a \Rightarrow S$ is non empty.

Therefore by well ordering principle, let S has the least positive integer d .

$d = la + mb$ for some positive integers l and m .

To Prove: $d = \gcd(a, b)$.

Since $d > 0$, by the division algorithm a and d , there exist an integers q and r such that

$$a = qd + r, \quad 0 \leq r < d \quad (1)$$

$$r = a - qd$$

$$= a - q(la + mb)$$

$$= (1 - ql)a + (-qm)b.$$

This shows r is the linear combination of a and b .

If $r \neq 0$, then $r > 0$, and so $r \in S$. Further $r < d$.

Which is a contradiction that d is the least positive integer of S .

Put $r = 0$, in equation (1), so $a = qd \Rightarrow d|a$.

similarly we can prove that $d|b$.

Thus, d is the common divisor of a and b .

Hence $d = \gcd(a, b)$.

Theorem 2: Prove that two positive integers a and b are relatively prime iff there exist an integers α and β such that $\alpha a + \beta b = 1$.

Proof:

If a and b are relatively prime then $(a, b) = 1$.

we know that, there exist an integers α and β such that $\alpha a + \beta b = 1$.

Conversely, let $\alpha a + \beta b = 1$.

To Prove: $(a, b) = 1$.

If $d = \gcd(a, b)$, then $d|a$ and $d|b$.

$$\Rightarrow d | \alpha a + \beta b$$

$$\Rightarrow d | 1$$

$$\therefore (a, b) = 1 \Rightarrow a \text{ and } b \text{ are relatively prime.}$$

Theorem 3: If $a|c$ and $b|c$ and $(a, b) = 1$, then prove that $ab|c$.

Proof:

Given: $a|c$ and $b|c$

$$\therefore c = ma \text{ and } c = nb.$$

Also given that $(a, b) = 1 \Rightarrow \alpha a + \beta b = 1$, for some integers α and β .

$$\alpha a c + \beta b c = c$$

$$\alpha a (nb) + \beta b (ma) = c$$

$$(\alpha n + \beta m)ab = c$$

$$\Rightarrow ab|c.$$

Theorem 4: Prove that $(a, a - b) = 1$ iff $(a, b) = 1$.

Proof:

Let $(a, b) = 1$.

To Prove: $(a, a - b) = 1$.

\exists an integer l and m such that $la + mb = 1$.

$$\Rightarrow la + ma + mb - ma = 1$$

$$\Rightarrow (l + m)a - m(a - b) = 1.$$

$$\Rightarrow (l + m)a + (-m)(a - b) = 1.$$

$$\therefore (a, a - b) = 1.$$

Conversely,

Let $(a, a - b) = 1$.

To Prove: $(a, b) = 1$.

\exists an integer α and β such that

$$\alpha a + \beta(a - b) = 1.$$

$$(\alpha + \beta)a + (-\beta)b = 1.$$

Therefore, $(a, b) = 1$.

The Euclidean Algorithm

Suppose a and b are positive integers $a \geq b$.

If $a = b$, then $(a, b) = (a, a) = a$.

So, assume $a > b$

Then by successive application of division algorithm, we have

$$a = q_1 b + r_1, \quad 0 \leq r_1 \leq b$$

$$b = q_2 r_1 + r_2 \quad 0 \leq r_2 \leq r_1$$

\vdots

$$r_{n-1} = q_{n+1} r_n + 0$$

The sequence of remainders terminate with remainder 0.

Thus, $(a, b) = r_n$, where r_n is the non zero remainder.

Example 1: Evaluate $(2076, 1776)$ or Find the GCD of 2076 and 1776.

Solution:

Apply the division algorithm with 2076 (the larger of the two numbers) as the dividend and 1776 as the divisor. Applying the division algorithm successively, continue this procedure until a zero remainder is reached.

$$2076 = 1 \cdot 1776 + 300$$

$$1776 = 5 \cdot 300 + 276$$

$$300 = 1 \cdot 276 + 24$$

$$276 = 11 \cdot 24 + 12$$

$$24 = 2 \cdot 12 + 0$$

$$\therefore (2076, 1776) = 12.$$

Example 2: Using the Euclidean algorithm, express $(4076, 1024)$ as a linear combination of 4076 and 1024.

Solution:

By applying the division algorithm successively,

$$4076 = 3(1024) + 1004$$

$$1024 = 1(1004) + 20$$

$$1004 = 50(20) + 4$$

$$20 = 5(4) + 0$$

The last non zero remainder is 4.

$$\therefore (4076, 1024) = 4.$$

Using the above equations in reverse order, we can express the $\gcd(4076, 1024)=4$ as a linear combination of 1024 and 4076.

$$\begin{aligned}
 4 &= 1004 - 50 \cdot 20 \\
 &= 1004 - 50(1024 - 1 \cdot 1004) \text{ (substitute for 20)} \\
 &= 51 \cdot 1004 - 50 \cdot 1024 \\
 &= 51(4076 - 3 \cdot 1024) - 50 \cdot 1024 \text{ (substitute for 1004)} \\
 &= 51 \cdot 4076 + (-203) \cdot 1024
 \end{aligned}$$

\therefore The gcd 4 is the linear combination of the numbers 1024 and 4076.

Example 3: Apply Euclidean algorithm to express the gcd of 1976 and 1776 as a linear combination of them.

Solution:

Applying the division algorithm successively, we get

$$1976 = 1(1776) + 200$$

$$1776 = 8(200) + 176$$

$$200 = 1(176) + 24$$

$$176 = 7(24) + 8$$

$$24 = 3(8) + 0$$

The last non zero remainder is 8.

$$\therefore \gcd(1976, 1776) = 8.$$

Now we shall express $\gcd(1976, 1776) = 8$ as a linear combination of 1976 and 1776.

.

$$\begin{aligned}
8 &= 176 - 7(24) \\
&= 176 - 7(200 - 1(176)) \\
&= 8(176) - 7(200) \\
&= 8(1776 - 8(200)) - 7(200) \\
&= 8(1776) - 71(200) \\
&= 8(1776) - 71(1976 - 1(1776)) \\
&= 79(1776) - 71(1976) \\
&= 79(1776) + (-71)(1976).
\end{aligned}$$

\therefore The gcd is the linear combination of the numbers 1776 and 1976.

Theorem: (The Euclid's Lemma)

Statement: If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Proof:

Given that p is a prime.

To Prove that either $p|a$ or $p|b$.

Suppose p is not a factor of a .

Then p and a are relatively prime, $(p, a) = 1$

there are integers α and β such that $\alpha p + \beta a = 1$.

Multiply both sides of this equation by b , we get $\alpha pb + \beta ab = b$.

Since $p|p$ and $p|ab \Rightarrow p|\alpha pb + \beta ab$.

$\therefore p|(\alpha p + \beta a)b \Rightarrow p|b$. (since $\alpha p + \beta a = 1$.)

FUNDAMENTAL THEOREM OF ARITHMETIC

Theorem: (The Fundamental theorem of Arithmetic)

Statement:

Every integer $n \geq 2$ either is a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.

Proof:

First, we will show by strong induction that n either is a prime or can be expressed as a product of primes. Then we will establish the uniqueness of such a factorization.

Let $P(n)$ denote the statement that n is a prime or can be expressed as a product of primes.

To show that $P(n)$ is true for every integer $n \geq 2$.

Since 2 is a prime, clearly $P(2)$ is true.

Now assume $P(2), P(3), \dots, P(k)$ are true; that is, every integer ≥ 2 through k either is a prime or can be expressed as a product of primes.

If $k + 1$ is a prime, then $P(k + 1)$ is true.

Suppose $k + 1$ is composite.

Then $k + 1 = ab$ for some integers a and b , where $1 < a, b < k + 1$.

By the inductive hypothesis, a and b either are primes or can be expressed as products of primes.

In any event, $k + 1 = ab$ can be expressed as a product of primes.

Thus, $P(k + 1)$ is also true. Thus, by strong induction, the result holds for every integer $n \geq 2$.

.

To establish the uniqueness of the factorization:

Let n be a composite number with two factorizations into primes.

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s.$$

We will show that $r = s$ and every p_i equals some q_j , where $1 \leq i, j \leq r$;

that is, the primes $q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s$ are a permutation of the primes $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r$.

Assume, for convenience, that $r < s$.

Since, $p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s$. But p_1 must divide some q_j .

(i.e) $p_1 \mid q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s$, and p_1 is prime. p_1 must divide some q_j

$\Rightarrow p_1 = q_j$ as they are primes.

Dividing both sides by p_1 , we get, $p_2 \cdot p_3 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_{j-1} \cdot q_{j+1} \cdot \dots \cdot q_s$.

Repeat this argument with $p_2 \cdot p_3 \cdot \dots \cdot p_r$.

Since $r < s$, we get 1 = a product of q' s.

$\Rightarrow 1 =$ a product of primes.

Which is a contradiction.

Therefore, our assumption $r < s$ is wrong $\Rightarrow r \geq s$. (1)

Similarly, if $s < r \Rightarrow s \geq r$. (2)

For (1) and (2), $r = s$.

Thus, the factorization is unique, except for the order of the factors.

CANONICAL DECOMPOSITION

Canonical Decomposition

Definition: A canonical decomposition of any positive integer n is of the form $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, where $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$ are distinct primes.

Example 1: Find the canonical decomposition of 4312.

Solution: $4312 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 7 \cdot 11 = 2^3 \cdot 7^2 \cdot 11^1$

Example 2: Find the canonical decomposition of 2520.

Solution: $2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 = 2^3 \cdot 3^3 \cdot 5 \cdot 7^1$

Example 3: Find the $(72, 108)$ using canonical decomposition.

Solution:

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$$

$$108 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 = 2^2 \cdot 3^3$$

$$(72, 108) = 2^2 3^2 = 4 \cdot 9 = 36.$$

Example 4: Using recursion, evaluate $(18, 30, 60, 75, 132)$.

Solution:

$$(18, 30, 60, 75, 132) = ((18, 30, 60, 75), 132)$$

$$= (((18, 30, 60), 75), 132)$$

$$= (((((18, 30), 60), 75), 132)$$

$$= (((6, 60), 75), 132)$$

$$= ((6, 75), 132)$$

$$= (3, 132) = 3.$$

Example 5: Using recursion evaluate $(14, 18, 21, 36, 48)$.

Solution:

$$\begin{aligned}
 \text{Consider } (14, 18, 21, 36, 48) &= ((14, 18), 21, 36, 48) \\
 &= (((14, 18), 21), 36, 48) \\
 &= (((((14, 18), 21), 36), 48) \\
 &= (((2, 21), 36), 48) \\
 &= ((1, 36), 48) \\
 &= (1, 48) \\
 &= 1.
 \end{aligned}$$

Example 6: Using recursion evaluate $(12, 18, 28, 34, 44)$.

Solution:

$$\begin{aligned}
 \text{Consider } (12, 18, 28, 34, 44) &= ((12, 18), 28, 34, 44) \\
 &= (((12, 18), 28), 34, 44) \\
 &= (((((12, 18), 28), 34), 44) \\
 &= (((6, 28), 34), 44) \\
 &= ((2, 34), 44) \\
 &= (2, 44) \\
 &= 2.
 \end{aligned}$$

LEAST COMMON MULTIPLE

View the lecture on YouTube:

<https://youtu.be/0iGwZlDcpac>

<https://youtu.be/39h-bbITGII>

Least Common Multiple (LCM)

Definition: The LCM of two positive integers a and b is the least positive integer, which is divisible both by a and b , denoted by $[a, b]$. We can use the canonical decompositions to find lcm.

If $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}$, where α_i and β_i are nonnegative integers, then $[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \dots \cdot p_k^{\max(\alpha_k, \beta_k)}$.

Example 1: Find the LCM of 120 and 500.

Solution:

First we find the canonical decomposition of 120.

$$120 = 2^3 \cdot 3 \cdot 5$$

$$500 = 2^2 \cdot 3 \cdot 5^3 = 2^2 \cdot 3^0 \cdot 5^3$$

$$[120, 500] = \text{Factors with maximum of indices}$$

$$= 2^3 \cdot 3 \cdot 5^3$$

$$= 3000.$$

Example 2: Using the canonical decompositions of 1050 and 2574, Find their lcm.

Solution:

$$1050 = 2 \cdot 3 \cdot 5^2 \cdot 7 \text{ and } 2574 = 2 \cdot 3^2 \cdot 11 \cdot 13$$

$$[1050, 2574] = \text{Factors with maximum indices}$$

$$= 2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$$

$$= 450,450.$$

Theorem: If a and b are positive integers, then $[a, b] = \frac{a \cdot b}{(a, b)}$.

Proof:

Let $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}$ be the canonical decompositions of a and b .

$$\text{Then } (a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \dots \cdot p_k^{\min(\alpha_k, \beta_k)}$$

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \dots \cdot p_k^{\max(\alpha_k, \beta_k)}.$$

$$\begin{aligned} \therefore (a, b) [a, b] &= p_1^{\min(\alpha_1, \beta_1) + \max(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2) + \max(\alpha_2, \beta_2)} \cdot \dots \cdot p_k^{\min(\alpha_k, \beta_k) + \max(\alpha_k, \beta_k)} \\ &= p_1^{\alpha_1 + \beta_1} \cdot p_2^{\alpha_2 + \beta_2} \cdot \dots \cdot p_k^{\alpha_k + \beta_k} \\ &= p_1^{\alpha_1} \cdot p_1^{\beta_1} \cdot p_2^{\alpha_2} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\alpha_k} \cdot p_k^{\beta_k} \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}) (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}) \\ &= a \cdot b \\ \therefore [a, b] &= \frac{a \cdot b}{(a, b)}. \end{aligned}$$

Important Result: If a and b are relatively prime, then $(a, b) = 1$

$$\therefore [a, b] = \frac{a \cdot b}{1} = a \cdot b$$

Example 3: Using $(252, 360)$. Compute $[252, 360]$.

Solution:

$$\text{W.K.T } 252 = 2^2 \cdot 3^2 \cdot 7$$

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$(252, 360) = 2^2 \cdot 3^2 = 36.$$

$$\text{W.K.T } [a, b] = \frac{a \cdot b}{(a, b)}$$

$$[252, 360] = \frac{252 \cdot 360}{36}$$

$$= 2520.$$

Example 4: Find the positive integer a if $[a, a + 1] = 132$.

Solution:

Given $[a, a + 1] = 132$.

Since a and $a+1$ are the consecutive integers, they are relatively prime.

$$\therefore (a, a + 1) = 1$$

Hence, $[a, a + 1] = a(a + 1)$

$$132 = a(a + 1)$$

$$11 \cdot 12 = a(a + 1)$$

$$\therefore a = 11.$$

PRACTICE QUIZ: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS

Divisibility Theory and Canonical Decompositions

Practice Quiz – 18 questions

<https://quizizz.com/print/quiz/5f34c66c9c163a001cbcdbee>

STUCOR APP

ASSIGNMENTS: UNIT III

1. Let a and b be positive integers. Show that there exist integers m and n such that $ma + nb = \gcd(a, b)$.
2. Show that every composite integer n has a prime factor $\leq \sqrt{n}$.
3. Prove that there are infinitely many primes of the form $4n + 3$.
4. Let b be an integer ≥ 2 . Suppose that $b + 1$ integers are randomly selected, Prove that the difference of two of them is divisible by 5.
5. Show that for every positive integer n , there are n consecutive composite integers.
6. Apply Euclidean algorithm to compute $(3076, 1976)$.
7. Apply Euclidean algorithm to express the gcd of 1976 and 1776 as a linear combination of themselves.
8. State and prove Fundamental theorem of arithmetic.
9. Using recursion evaluate $(18, 30, 60, 75, 132)$.
10. If a and b are positive integers, then prove that $[a, b] = \frac{ab}{(a, b)}$.
11. Using $(252, 360)$ compute $[252, 360]$.
12. Prove that $\gcd(a, a - b) = 1$ if and only if $\gcd(a, b) = 1$.

PART A QUESTIONS AND ANSWERS: UNIT III**1. State the Pigeonhole Principle.**

(K2,CO4)

Solution:

If m pigeons are assigned to n pigeonholes, where $m > n$, then at least two pigeons must occupy the same pigeonhole.

2. State the Division Algorithm.

(K2, CO4)

Solution:

Let a be any integer and b a positive integer. Then there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$.

3. If a and b are positive integers such that $a|b$ and $b|a$. Then prove that $a = b$.

(K3, CO4)

Solution:

Let a and b be positive integers such that $a|b$ and $b|a$.

Claim: $a = b$

Since $a|b \Rightarrow b = aq$, for some $q \in \mathbb{Z}$. -----(1)

Also, $b|a \Rightarrow aq|a \Rightarrow q = 1$

Substitute in (1), we have $a = b$.

Hence the proof.

4. Let a, b , and c be any integers. If $a|b$ and $b|c$, then prove that $a|c$. (transitive property)

(K3, CO4)

Solution:

$a|b \Rightarrow b = q_1a \Rightarrow c = q_2b$, where $a \neq 0, b \neq 0$ in \mathbb{Z} , q_1, q_2 are some integers.

$\therefore c = q_2(q_1a) = (q_1 q_2)a \Rightarrow a|c$.

5. Determine whether 1601 is a prime.

(K2, CO4)

Solution:

Given 1601.

First we find all primes $\leq \lfloor \sqrt{1601} \rfloor = 40$.

The primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, and 37.

None of the above is a factor of 1601.

Hence 1601 is a prime.

6. Prove that 101 is a prime.

(K2, CO4)

Solution:

Given 101.

First we find all primes $\leq \lfloor \sqrt{101} \rfloor = 10$.

The primes are 2, 3, 5, and 7.

Since, none of them is a factor of 101.

Hence 101 is a prime.

7. Determine whether 1001 is a prime.

(K2, CO4)

Solution:

Given 1001.

To prove that 1001 is a prime.

First we find all primes $\leq \lfloor \sqrt{1001} \rfloor = 31$.

The primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, and 31.

We have $7 \mid 1001$.

Hence 1001 is not a prime.

8. Find the largest power of 2 that divides 97!.

(K3, CO4)

Solution:

We know that $2 \mid 97!$.

Therefore, the largest power is

$$= \left\lfloor \frac{97}{2} \right\rfloor + \left\lfloor \frac{97}{2^2} \right\rfloor + \left\lfloor \frac{97}{2^3} \right\rfloor + \left\lfloor \frac{97}{2^4} \right\rfloor + \left\lfloor \frac{97}{2^5} \right\rfloor + \left\lfloor \frac{97}{2^6} \right\rfloor, \text{ since } 2^7 > 97, \text{ all other terms are omitted.}$$

$$= 48 + 24 + 12 + 6 + 3 + 1 = 94.$$

Hence, 2^{94} is the highest power of 2 dividing 97!.

9. What is Principle of Mathematical Induction?

(K2, CO4)

Solution:

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 $n \geq n_0$.

10. State Well Ordering Principle.

(K2, CO4)

Solution:

Every non empty set of positive integers has a least number.

11. Find the number of positive integers ≤ 3076 that are not divisible by 24.

(K3, CO4)

Solution:

The number of positive integers ≤ 3076 that are divisible by 24 is

$$\left\lfloor \frac{3076}{24} \right\rfloor = \lfloor 128.1 \rfloor = 128$$

The number of integers not divisible by 24 is = Total number of integers - 128
 $= 3076 - 128$
 $= 2498.$

12. Define base b representation.

(K2, CO4)

Solution:

If n is a positive integer and $b \geq 2$ and

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$$

where a_0, a_1, \dots, a_k are non negative integers then the above expression is called base b of the integer n .

We then write $n = (a_k a_{k-1} \dots a_1 a_0)_b$.

Example:

$$(345)_{10} = 3(10)^2 + 4(10) + 5.$$

13. Express $(101011)_2$ in base 10.

(K3, CO4)

Solution:

$$\begin{aligned}
 (101011)_2 &= 1(2)^5 + 0(2)^4 + 1(2)^3 + 0(2)^2 + 1(2)^1 + 1(2)^0 \\
 &= 32 + 8 + 2 + 1 \\
 &= 43
 \end{aligned}$$

Therefore $(101011)_2 = (43)_{10}$.**14. Express $(1543)_{10}$ in octal system.**

(K3, CO4)

Solution:

$$\begin{aligned}
 1543 &= 192(8) + 7 \\
 192 &= 24(8) + 0 \\
 24 &= 3(8) + 0 \\
 3 &= 0(8) + 3
 \end{aligned}$$

Therefore $(1543)_{10} = (3007)_8$.**15. Convert the binary number $(1110101)_2$ into hexadecimal digit.** (K3, CO4)**Solution:**

Given 111 0101 .

We group the digits in blocks of four digits from right to left.

Here the blocks are 0111, 0101 (adding zero to the left most block to get four digits).

$$0111 = 0(2)^3 + 1(2)^2 + 1(2)^1 + 1(2)^0 = 7$$

$$0101 = 0(2)^3 + 1(2)^2 + 0(2)^1 + 1(2)^0 = 5$$

Therefore $(1110101)_2 = (75)_{16}$.**16. Convert the octal digit $(12376)_8$ into binary number.**

(K3, CO4)

Solution:Given $(12376)_8$.

We write each digits as a block of three bits.

$$1 = 0(2)^2 + 0(2)^1 + 1(2)^0 = 001$$

$$2 = 0(2)^2 + 1(2)^1 + 0(2)^0 = 010$$

$$3 = 0(2)^2 + 1(2)^1 + 1(2)^0 = 011$$

$$7 = 1(2)^2 + 1(2)^1 + 1(2)^0 = 111$$

$$6 = 1(2)^2 + 1(2)^1 + 0(2)^0 = 110$$

Therefore $(12376)_8 = (001010011111110)_2 = (1010011111110)_2$.

17. Find the value of base b if $(1001)_b = 9$.

(K3, CO4)

Solution:

Given that $(1001)_b = 9$.

$$\Rightarrow 1(b)^3 + 0(b)^2 + 0(b)^1 + 1(b)^0 = 9$$

$$\Rightarrow b^3 + 1 = 9$$

$$\Rightarrow b^3 = 8$$

$$\Rightarrow b = 2.$$

18. Find the value of base b if $(144)_b = 49$.

(K3, CO4)

Solution:

Given that $(144)_b = 49$.

$$\Rightarrow 1(b)^2 + 4(b)^1 + 4(b)^0 = 49$$

$$\Rightarrow b^2 + 4b + 4 = 49$$

$$\Rightarrow b^2 + 4b - 45 = 0$$

$$\Rightarrow (b + 9)(b - 5) = 0$$

$$\Rightarrow b = -9, 5$$

Since $b \geq 2$, we have $b = 5$.

19. Define the Greatest Common Divisor (GCD).

(K2, CO4)

Solution:

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) .

20. Find the canonical decomposition of 4312.

(K2, CO4)

Solution: $4312 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 7 \cdot 11 = 2^3 7^2 11^1$

21. Find the canonical decomposition of 2520.

(K2, CO4)

Solution: $2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 = 2^3 3^3 7^1$

22. Find the GCD of 2076 and 1776.

(K3, CO4)

Solution:

Apply the division algorithm with 2076 (the larger of the two numbers) as the dividend and 1776 as the divisor. Applying the division algorithm successively, continue this procedure until a zero remainder is reached.

$$2076 = 1 \cdot 1776 + 300$$

$$1776 = 5 \cdot 300 + 276$$

$$300 = 1 \cdot 276 + 24$$

$$276 = 11 \cdot 24 + 12$$

$$24 = 2 \cdot 12 + 0$$

$$\therefore (2076, 1776) = 12.$$

23. Find the (72, 108) using canonical decomposition.

(K3, CO4)

Solution:

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 3^2$$

$$108 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 = 2^2 3^3$$

$$(72, 108) = 2^2 3^2 = 4 \cdot 9 = 36.$$

24. Find the LCM of 120 and 500.

(K3, CO4)

Solution:

First we find the canonical decompositions

$$120 = 2^3 \cdot 3 \cdot 5$$

$$500 = 2^2 \cdot 3 \cdot 5^3 = 2^2 \cdot 3^0 \cdot 5^3$$

$$[120, 500] = \text{Factors with maximum of indices}$$

$$= 2^3 \cdot 3 \cdot 5^3$$

$$= 3000.$$

PART B QUESTIONS: UNIT III

1. Let a be any integer and b be a positive integers. Show that there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$. (K3, CO4)
2. Find the number of positive integers less than or equal to 3000 and divisible by 2, 5 or 7. Also, show that the product of two consecutive integers is even. (K3, CO4)
3. Find the number of positive integers ≤ 3000 and divisible by 3, 5, or 7. (K3, CO4)
4. Find the number of positive integers in the range 1976 through 3776 that are divisible by 13. (K3, CO4)
5. Show that every composite integer n has a prime factor $\leq \sqrt{n}$. (K2, CO4)
6. Show that there are infinitely many primes. (K2, CO4)
7. Prove that there are infinitely many primes of the form $4n + 3$. (K2, CO4)
8. Let b be an integer ≥ 2 . Suppose that $b + 1$ integers are randomly selected, Prove that the difference of two of them is divisible by 5. (K3, CO4)
9. Show that for every positive integer n , there are n consecutive composite integers. (K2, CO4)
10. Obtain the six consecutive integers that are composite. (K2, CO4)
11. Let a and b be positive integers. Show that there exist integers m and n such that $ma + nb = \gcd(a, b)$. (K3, CO4)
12. Prove that two positive integers a and b are relatively prime if and only if there are integers m and n such that $ma + nb = 1$. (K3, CO4)
13. Apply Euclidean algorithm to compute (3076, 1976). (K3, CO4)
14. Apply Euclidean algorithm to compute (2076, 1776). (K3, CO4)
15. Apply Euclidean algorithm to express the gcd of 1976 and 1776 as a linear combination of themselves. (K3, CO4)
16. State and prove Fundamental theorem of arithmetic. (K3, CO4)
17. Using recursion evaluate (18, 30, 60, 75, 132). (K3, CO4)
18. If a and b are positive integers, then prove that $[a, b] = \frac{ab}{(a, b)}$. (K3, CO4)
19. Using (252, 360) compute [252, 360]. (K3, CO4)
20. Prove that $\gcd(a, a - b) = 1$ if and only if $\gcd(a, b) = 1$. (K3, CO4)

SUPPORTIVE ONLINE CERTIFICATION COURSES

The following NPTEL and Coursera courses are the supportive online certification courses for the subject Algebra and Number theory.

1. Introduction to Abstract Group Theory (NPTEL course)

<https://nptel.ac.in/courses/111/106/111106113/>

2. Introduction to Rings and Fields (NPTEL course)

<https://nptel.ac.in/courses/111/106/111106131/#>

3. Mathematical Foundations for Cryptography (Coursera online course)

<https://www.coursera.org/learn/mathematical-foundations-cryptography>

4. Number Theory (NPTEL course)

<https://nptel.ac.in/courses/111/103/111103020/>

5. Computational Number Theory & Cryptography (NPTEL course)

<https://nptel.ac.in/courses/106/103/106103015/>

6. A Basic course in Number Theory (NPTEL course)

<https://nptel.ac.in/courses/111/101/111101137/>

REAL TIME APPLICATIONS

View the lecture on YouTube: <https://youtu.be/c9dG59sEoHI>

The best known application of number theory is public key cryptography, such as the RSA algorithm. Public key cryptography in turn enables many technologies for granted such as the ability to make secure online transactions. In addition to cryptography, number theory has been applied to other areas, such as:

- Military information transmission
- Error correcting codes
- Numerical integration
- Computer Arithmetic
- Random and quasi-random number generation.

STUCOR APP

DOWNLOADED FROM STUCOR APP

CONTENT BEYOND THE SYLLABUS

The topic **Introduction to Vector space** is the content beyond the syllabus for the course Algebra and Number Theory.

View the lecture on YouTube:

<https://youtu.be/YshfZm99wjk>

Value Added Courses:

1. Mathematics for Machine Learning: Linear Algebra (Coursera online course)
<https://www.coursera.org/learn/linear-algebra-machine-learning>

2. Mathematical Foundations for Cryptography (Coursera online course)
<https://www.coursera.org/learn/mathematical-foundations-cryptography>

3. Cryptography and Network Security (NPTEL course)
<https://nptel.ac.in/courses/106/105/106105162/>

PRESCRIBED TEXT BOOKS & REFERENCE BOOKS

TEXTBOOKS:

1. Grimaldi, R.P and Ramana, B.V., "Discrete and Combinatorial Mathematics", Pearson Education, 5th Edition, New Delhi, 2007.
2. Koshy, T,—“Elementary Number Theory with Applications”, Elsevier Publications, New Delhi, 2002.

REFERENCES:

1. Lidl, R. and Pitz, G, "Applied Abstract Algebra", Springer Verlag, New Delhi, 2nd Edition, 2006.
2. Niven, I., Zuckerman.H.S., and Montgomery, H.L., —“An Introduction to Theory of Numbers”, John Wiley and Sons , Singapore, 2004.
3. San Ling and Chaoping Xing, —“Coding Theory – A first Course”, Cambridge Publications, Cambridge, 2004.

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

STUCOR APP

STUCOR APP

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

MA8551 - Algebra and Number Theory

Department: Mathematics

Batch/Year: CSE/ III

Created by: Mr. R. Rajaraman

Date: 31.08.2020

Table of Contents

Contents

1	Course Objectives	6
2	Pre-requisites	7
3	Syllabus	8
4	Course Outcomes	9
5	CO – PO/PSO Mapping	10
6	Lecture Plan	11
7	Activity Based Learning	12
8	Lecture Notes: Unit IV Diophantine Equations and Congruences	13
9	Linear Diophantine Equations	14
10	Congruences	21
11	Modular Exponentiation	26
12	Linear Congruences	27
13	Applications: Divisibility Tests	32
14	Chinese Remainder Theorem	33
15	2×2 Linear Systems	39
16	Practice Quiz: Diophantine Equations and Congruences	44
17	Assignments: Unit IV	45
18	Part A Questions and Answers: Unit IV	46
19	Part B Questions: Unit IV	51
20	Supportive online Certification courses	52
21	Real time Applications	53
22	Content beyond the Syllabus	54
23	Prescribed Text Books & Reference Books	55

COURSE OBJECTIVES

To introduce the basic notions of groups, rings, fields which will then be used to solve related problems.

To introduce and apply the concepts of rings, finite fields and polynomials.

To understand the basic concepts in number theory.

To examine the key questions in the Theory of Numbers.

To give an integrated approach to number theory and abstract algebra, and provide a firm basis for further reading and study in the subject.

PRE-REQUISITES

Pre-requisites for the subject Algebra and Number Theory is
MA8351 - Discrete Mathematics.

STUCOR APP

MA8551	ALGEBRA AND NUMBER THEORY	L	T	P	C
		4	0	0	4
UNIT I GROUPS AND RINGS		12			
Groups : Definition - Properties - Homomorphism - Isomorphism - Cyclic groups - Cosets - Lagrange's theorem. Rings: Definition - Sub rings - Integral domain - Field - Integer modulo n - Ring homomorphism.					
UNIT II FINITE FIELDS AND POLYNOMIALS		12			
Rings - Polynomial rings - Irreducible polynomials over finite fields - Factorization of polynomials over finite fields.					
UNIT III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS		12			
Division algorithm – Base - b representations – Number patterns – Prime and composite numbers – GCD – Euclidean algorithm – Fundamental theorem of arithmetic – LCM.					
UNIT IV DIOPHANTINE EQUATIONS AND CONGRUENCES		12			
Linear Diophantine equations – Congruence's – Linear Congruence's - Applications: Divisibility tests - Modular exponentiation-Chinese remainder theorem – 2 x 2 linear systems.					
UNIT V CLASSICAL FUNCTIONS	THEOREMS	AND	MULTIPLICATIVE		
			12		
Wilson's theorem – Fermat's little theorem – Euler's theorem – Euler's Phi functions – Tau and Sigma functions.					
TOTAL: 60 PERIODS					

COURSE OUTCOMES

CO 1: Apply the basic notions of groups which will be used to solve group theory related problems.

CO 2: Apply the basic notions of rings, fields which will then be used to solve related problems.

CO 3: Demonstrate accurate and efficient use of advanced algebraic techniques such as finite fields and polynomials.

CO 4: Explain the fundamental concepts of number theory, advanced algebra and their role in modern mathematics.

CO 5: Demonstrate the number theory concepts by solving non - trivial related problems.

CO 6: Apply integrated approach to number theory and abstract algebra and prove simple theorems.

Course Out Comes	Program Outcomes												Program Specific Outcomes		
	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6	PO-7	PO-8	PO-9	PO-10	PO-11	PO-12	PSO-1	PSO-2	PSO-3
C01	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C02	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C03	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C04	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C05	3	2	-	-	-	-	-	-	-	-	-	-	-	-	-
C06	3	2	1	-	-	-	-	-	-	-	-	-	1	-	-

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High)

UNIT IV DIOPHANTINE EQUATIONS AND CONGRUENCES							
S. No	Topic	No. of Periods	Proposed date	Actual date	Pertaining CO(s)	Taxonomy level	Mode of Delivery
1	Linear Diophantine equations	2			CO5	K2	PPT
2	Congruence's	1			CO5	K2	PPT
3	Linear Congruence's	2			CO5	K3	PPT
4	Applications: Divisibility tests	1			CO5	K2	PPT
5	Modular exponentiation	2			CO5	K3	PPT
6	Chinese remainder theorem	2			CO5	K3	PPT
7	2 x 2 linear systems	2			CO5	K3	PPT

ACTIVITY BASED LEARNING

Activity based learning helps students express and embrace their curiosity. Once the students become curious, they tend to explore and learn by themselves. To evoke curiosity in students, Practice quiz is designed for all the five units.

Quiz – Unit IV Diophantine Equations and Congruences

<https://quizizz.com/print/quiz/5f48a21d6bafd3001bb11603>

Play game Quiz: Diophantine Equations and Congruences

<https://quizizz.com/join/quiz/5f48a21d6bafd3001bb11603/start?studentShare=true>

LECTURE NOTES**UNIT IV DIOPHANTINE EQUATIONS AND CONGRUENCES**

This chapter begin to deal with the important class of linear diophantine equations. This chapter continues the study of congruence relation, an extremely useful and powerful number-theoretic relation used throughout number theory, and its fundamental properties. We establish congruence applications which include the standard divisibility tests, and interesting puzzles. we shall study systems of linear congruences in a single variable x with pairwise relatively prime moduli, and finally to systems in two variables x and y with the same modulus.

Linear Diophantine equations – Congruence's – Linear Congruence's - Applications: Divisibility tests - Modular exponentiation-Chinese remainder theorem – 2×2 linear systems.

E- Book Reference:

<https://drive.google.com/file/d/1frQQxDZ4wWsS78NHZK6xQAZqfXofcIGQ/view?usp=drivesdk>

View the lecture on YouTube:

<https://youtu.be/TIk3ujphMfk>

<https://youtu.be/5DcoG69NyO0>

<https://youtu.be/B-0ahK4jJUM>

Definition: A Linear Diophantine equation (in 2 variables) is an equation of the form $ax + by = c$ where a, b, c are integers and x, y are unknowns.

Theorem: The LDE $ax + by = c$ is solvable if and only if $d|c$ where $d = (a, b)$. If x_0, y_0 is the Particular solution of linear Diophantine equation, then all its solutions are given by, $x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$, where t is any integer.

Proof:

Case(i): Assume that the LDE $ax + by = c$ is solvable.

To prove: $d|c$

If $x = \alpha$ and $y = \beta$ is a solution .then $a\alpha + b\beta = c$.

Since, $d = (a, b)$, we know that, $d|a$ and $d|b$

$$\Rightarrow d|a\alpha + b\beta$$

$$\Rightarrow d|c.$$

Conversely, Assume $d|c$

To prove: The LDE $ax + by = c$ is solvable.

Since $d|c$, $c = dm$, for some integer m .

Since $d = (a, b)$, then there exist positive integers r and s such that $d = ra + sb$.

Multiplying by m we get,

$$dm = (ra)m + (sb)m$$

$$\Rightarrow c = (rm)a + (sm)b$$

This shows that $x_0=rm$ and $y_0=sm$ is the LDE $ax + by = c$ is solvable.

Case(ii): Next we prove that if (x_0, y_0) is a solution of $ax + by = c$, then $x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$ is a solution for any integer t .

Now,

$$\begin{aligned}
 ax + by &= a \left[x_0 + \left(\frac{b}{d} \right) t \right] + b \left[y_0 - \left(\frac{a}{d} \right) t \right] \\
 &= (ax_0 + by_0) + \frac{ab}{d} t - \frac{ab}{d} t \\
 &= (ax_0 + by_0) \\
 &= c
 \end{aligned}$$

Thus, every solution is of the form $x = x_0 + \left(\frac{b}{d} \right) t$ and $y = y_0 - \left(\frac{a}{d} \right) t$.

This solution is called the general solution of $ax + by = c$.

Example 1: Determine if the linear Diophantine equation $12x + 18y = 30$ is solvable. If so, find the solutions.

Solution: Given LDE is $12x + 18y = 30$ (1)

Here $a = 12, b = 18, c = 30$. (2)

$$\therefore (a, b) = (12, 18) = 6$$

$$\text{So, } d = (a, b) = 6$$

Since $6|30$, we have $d|c$.

So, the LDE is solvable.

Clearly, $x_0=1, y_0=1$ are the solution of (1)

The general solution is given by

$$x = x_0 + \left(\frac{b}{d} \right) t \text{ and } y = y_0 - \left(\frac{a}{d} \right) t$$

Substitute all the values in the above equations

$$\text{we get, } x = 1 + \frac{18}{6} t \text{ and } y = 1 - \left(\frac{12}{6} \right) t$$

$$x = 1 + 3 t \text{ and } y = 1 - 2 t \quad t \in \mathbb{Z}.$$

Example 2: Examine the linear Diophantine equation $12x + 16y = 18$ is solvable. Write the general solution if solvable.

Solution: Given LDE is $12x + 16y = 18$ (1)

Here $a = 12, b = 16, c = 18$. (2)

$$\therefore (a, b) = (12, 16) = 4.$$

$$\text{so, } d = (a, b) = 4.$$

since 4 is doesn't a factor of 18, (i.e) $4 \nmid 18$

We have $d \nmid c$

Hence the LDE is not solvable.

Example 3: Examine if the LDE $15x + 21y = 39$ is solvable. If so, find the solutions.

Solution: Given LDE is $15x + 21y = 39$ (1)

Here $a = 15, b = 21, c = 39$. (2)

$$\therefore (a, b) = (15, 21) = 3$$

$$\text{so, } d = (a, b) = 3$$

since $3 \mid 39$, we have $d \mid c$.

so the LDE is solvable.

By trial and error $x_0 = -3, y_0 = 4$ is the solution of (1).

The general solution is given by

$$x = x_0 + \left(\frac{b}{d}\right)t \text{ and } y = y_0 - \left(\frac{a}{d}\right)t$$

Substitute all the values in the above equations

$$\text{we get, } x = -3 + \frac{21}{3}t \text{ and } y = 4 - \left(\frac{15}{3}\right)t$$

$$x = -3 + 7t \text{ and } y = 4 - 5t \quad t \in \mathbb{Z}.$$

Result: If $(a, b) = 1$, then the LDE $ax + by = c$ is solvable and the general solution is $x = x_0 + bt$ and $y = y_0 - at$, where x_0, y_0 is a particular solution and t is an arbitrary integer.

Example 4: Solve the LDE $97x + 35y = 13$ by Euclidean algorithm and also find the general solution.

Solution: We have $d = (97, 35) = 1$ and $1|13$.

\Rightarrow the equation is solvable. First we find the GCD and then it can be expressed as a linear combination.

$$97 = 35(2) + 27$$

$$35 = 27(1) + 8$$

$$27 = 8(3) + 3$$

$$8 = 3(2) + 2$$

$$3 = 2(1) + 1$$

$$2 = 1(2) + 0$$

$$(97, 35) = 1$$

Now, We have $(97, 35) = 1$

$$1 = 3 - 1(2)$$

$$= 3 - 1(8 - 2(3))$$

$$= 3 - 1(8) + 2(3)$$

$$= 3(3) - 1(8)$$

$$= 3(27 - 3(8)) - 1(8)$$

$$= 3(27) - 9(8) - 1(8)$$

$$= 3(27) - 10(8)$$

$$= 3(27) - 10(35 - 1(27))$$

$$= 3(27) - 10(35) + 10(27)$$

$$= 13(27) - 10(35)$$

$$= 13(97 - 2(35)) - 10(35)$$

$$= 13(97) - 26(35) - 10(35)$$

$$= 13(97) - 36(35).$$

Consider $13(97) - 36(35) = 1$, Multiplying by 13,

we have $169(97) - 468(35) = 13$

$\therefore x_0 = 168, y_0 = -468$ is the particular solution and the general solution is

$$x = 169 + 35t; y = -468 - 97t, t \in \mathbb{Z}.$$

Example 5: Solve the L D E $1076x + 2076y = 3076$ by Euclidean algorithm and also find the general solution.

Solution:

$$2076 = 1076(1) + 1000$$

$$1076 = 1000(1) + 76$$

$$1000 = 76(13) + 12$$

$$76 = 12(6) + 4$$

$$12 = 4(3) + 0$$

$$\therefore (1076, 2076) = 4$$

$$4 = 76 - 6(12)$$

$$= 76 - 6(1000 - 13(76))$$

$$= 76 - 6(1000) + 78(76)$$

$$= 79(76) - 6(1000).$$

$$= 79(1076 - 1(1000)) - 6(1000)$$

$$= 79(1076) - 79(1000) - 6(1000)$$

$$= 79(1076) - 85(1000)$$

$$= 79(1076) - 85(2076 - 1076)$$

$$= 79(1076) - 85(2076) + 85(1076)$$

$$= 164(1076) - 85(2076).$$

Consider $164(1076) - 85(2076) = 4$,

multiplying by 769, we get $126116(1076) - 65365(2076) = 3076$

$\Rightarrow x_0 = 126116, y_0 = -65365$ is the particular solution and the general solution is

$$x = 126116 + 504t; y = -65365 - 269t, t \in \mathbb{Z}.$$

Example 6: Find the general solution of the LDE $6x + 8y + 12z = 10$.

Solution: Given LDE is $6x + 8y + 12z = 10$ (1)

Here, $a_1=6, a_2=8, a_3=12, c=10$

(i.e) $(6, 8, 12)=2 = d$, and $c=10$.

Since $2|10$ then $d|c$.

So, the given LDE is Solvable.

To find the general solution x, y and z .

Since $8y + 12z$ is a linear combination of 8 and 12. $(8, 12)=4$.

$$\therefore 8y + 12z = 4u \quad (2)$$

$$\text{From (1), } 6x + 4u = 10 \quad (3)$$

First we solve LDE (3), (i.e) $(6, 4)=2$.

Since $2|10$ then $d|c$

so, equation (3) is solvable

By trial and error, we find $x_0=1$ and $u_0=1$ is a solution of (3)

Therefore, the general solution of (3) is

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \text{and} \quad u = u_0 - \left(\frac{a}{d}\right)t.$$

$$x = 1 + \left(\frac{4}{2}\right)t \quad \text{and} \quad u = 1 - \left(\frac{6}{2}\right)t.$$

$$x = 1 + (2)t \quad \text{and} \quad u = 1 - (3)t. \quad t \in \mathbb{Z}.$$

Substituting for u in (2), we get $8y + 12z = 4(1 - 3t)$

Since $d = (8, 12) = 4$,

$4 = 2 \cdot 8 + (-1)12$ is a linear combination of 8 and 12.

Multiplying by $(1 - 3t)$ we get,

$$\begin{aligned} 4(1 - 3t) &= 2 \cdot 8(1 - 3t) + (-1)12(1 - 3t) \\ &= (2 - 6t)8 + (-1 + 3t)12 \end{aligned}$$

\therefore a solution of (2) is $y_0 = 2 - 6t$ and $z_0 = -1 + 3t$.

So the general solution of (2) is

$$y = y_0 + \frac{b}{d} t' \quad z = z_0 - \frac{a}{d} t'.$$

$$y = 2 - 6t + 3t' \quad z = -1 + 3t - 2t'.$$

Thus, the general solution of (1) is

$$x = 1 + 2t, y = 2 - 6t + 3t' \text{ and } z = -1 + 3t - 2t' \text{ for any integers } t \text{ and } t'.$$

STUCOR APP

CONGRUENCES

View the lecture on YouTube: <https://youtu.be/4mkrkdhBC5g>

Definition:

Let m be a positive integer. An integer a is congruent to an integer b modulo m if $m|(a - b)$. Symbolically, we write $a \equiv b \pmod{m}$. Here, m is the modulus of the congruence relation.

Example:

- (i). Congruence $\pmod{12}$ to tell the time of the day.
- (ii). Congruence $\pmod{7}$ to tell the day of the week.

Theorem:

$a \equiv b \pmod{m}$ if and only if $a = b + mk$ for some integer k .

Proof:

Let $a \equiv b \pmod{m}$.

Then $m|(a - b)$

$\Rightarrow a - b = mk$ for some integer k .

$\Rightarrow a = b + mk$.

Conversely, let $a = b + mk$.

Then, $a - b = mk$.

$\Rightarrow m|(a - b)$.

$\Rightarrow a \equiv b \pmod{m}$.

Note:

(i). It follows that $a \equiv 0 \pmod{m}$ if and only if $m|a$. Thus $a \equiv 0 \pmod{m}$ and $m|a$ mean exactly the same thing.

(ii). If $a \equiv r \pmod{m}$, where $0 \leq r < m$, then r is the remainder when a is divided by m .

Properties of congruence relation:

- (i). Reflexive Property: $a \equiv a \pmod{m} \quad \forall a \in \mathbb{Z}$.
- (ii). Symmetric Property: If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.
- (iii). Transitive Property: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

Proof:

(i). Since, $m|(a - a = 0) \quad \forall a \in \mathbb{Z}$.

$\Rightarrow a \equiv a \pmod{m} \quad \forall a \in \mathbb{Z}$.

(ii). If $a \equiv b \pmod{m}$ then $m|(a - b)$.

$$\Rightarrow m|-(b - a).$$

$$\Rightarrow m|(b - a).$$

$$\Rightarrow b \equiv a \pmod{m}.$$

(iii). If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m|(a - b)$ and $m|(b - c)$.

$$\text{Therefore } m|[(a - b) + (b - c)].$$

$$\Rightarrow m|(a - c).$$

$$\Rightarrow a \equiv c \pmod{m}.$$

Hence this proof says congruence relation is an equivalence relation.

Theorem:

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$(i). a + c \equiv b + d \pmod{m}.$$

$$(ii). a \cdot c \equiv b \cdot d \pmod{m}.$$

Proof:

Given $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

Therefore $a = b + km$ and $c = d + lm$ for some integers k, l .

$$\Rightarrow a + c = b + d + (k + l)m.$$

$$\Rightarrow a + c \equiv b + d \pmod{m}.$$

Hence (i) is proved.

Now, $a \cdot c = (b + km)(d + lm)$.

$$= bd + (lb + kd)m + lk m^2.$$

$$ac - bd = m(lb + kd + lkm).$$

$$\Rightarrow m|(ac - bd).$$

$$\Rightarrow a \cdot c \equiv b \cdot d \pmod{m}.$$

Hence (ii) is proved.

Corollary:

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$(i). a - c \equiv b - d \pmod{m}.$$

$$(ii). a \cdot c \equiv b \cdot c \pmod{m}.$$

$$(iii). a^r \equiv b^r \pmod{m} \text{ for any positive integer } r.$$

Example 1:

Find the remainder $1! + 2! + 3! + \dots + 100!$ is divided by 15.

Solution:

For divisibility by 15 we consider $\text{mod } 15$.

$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ is divisible by 15.

Therefore $5! \equiv 0 \pmod{15}$.

$\Rightarrow r! \equiv 0 \pmod{15}$ for $r \geq 5$.

Now, $1! + 2! + 3! + \dots + 100! \equiv 1! + 2! + 3! + 4! + 0 + 0 + \dots + 0 \pmod{15}$.

$$\equiv 1 + 2 + 6 + 24 \pmod{15}.$$

$$\equiv 33 \pmod{15}.$$

$$\equiv 3 \pmod{15}.$$

Therefore, when $1! + 2! + 3! + \dots + 100!$ is divided by 15, the remainder is 3.

Example 2:

Find the remainder when 3^{247} is divided by 17.

Solution:

We have $3^3 = 27 \equiv 10 \pmod{17}$.

$$3^6 \equiv 10^2 \pmod{17}.$$

$$\equiv 15 \pmod{17}.$$

$$\equiv -2 \pmod{17}.$$

$$(3^6)^4 \equiv (-2)^4 \pmod{17}.$$

$$3^{24} \equiv 16 \pmod{17}.$$

$$\equiv -1 \pmod{17}.$$

$$(3^{24})^{10} \equiv (-1)^{10} \pmod{17}.$$

$$\equiv 1 \pmod{17}.$$

Now, $3^{247} = 3^{240+6+1} = 3^{240} \cdot 3^6 \cdot 3^1$

$$3^{247} \equiv 1 \cdot (-2) \cdot 3 \pmod{17}.$$

$$\equiv -6 \pmod{17}.$$

$$3^{247} \equiv 11 \pmod{17}.$$

Hence, when 3^{247} is divided by 17 the remainder is 11.

Example 3:

Find the remainder when 13^{218} is divided by 17.

Solution:

We have $13^2 = 169 \equiv 16 \pmod{17}$.

$$13^2 \equiv -1 \pmod{17}.$$

$$(13^2)^{109} \equiv (-1)^{109} \pmod{17}.$$

$$13^{218} \equiv -1 \pmod{17}.$$

$$\Rightarrow 13^{218} \equiv 16 \pmod{17}.$$

Hence, when 13^{218} is divided by 17 the remainder is 16.

Example 4:

Prove that $2^{2^5} + 1$ is divisible by 641.

Solution:

We observe that $640 \equiv -1 \pmod{641}$.

$$5 \cdot 2^7 \equiv -1 \pmod{641}.$$

$$5^4 \cdot (2^7)^4 \equiv (-1)^4 \pmod{641}.$$

$$5^4 \cdot (2^7)^4 \equiv 1 \pmod{641}. \text{-----(i)}$$

But, $5^4 = 625 \equiv -16 \pmod{641}$.

$$\equiv -2^4 \pmod{641}.$$

Therefore, Eqn (i) $\Rightarrow -2^4 \cdot (2^7)^4 \equiv 1 \pmod{641}$.

$$-2^{32} \equiv 1 \pmod{641}.$$

$$\Rightarrow 2^{32} \equiv -1 \pmod{641}.$$

$$\Rightarrow 2^{2^5} \equiv -1 \pmod{641}.$$

$$\Rightarrow 2^{2^5} + 1 \equiv 0 \pmod{641}.$$

Hence, $2^{2^5} + 1$ is divisible by 641.

Theorem:

If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $a \equiv b \pmod{m_3}$, . . . , $a \equiv b \pmod{m_r}$. Then $a \equiv b \pmod{[m_1, m_2, m_3, \dots, m_r]}$.

Proof:

Given $a \equiv b \pmod{m_i}$, $i = 1, 2, 3, \dots, r$

Then $m_i | (a - b)$, $i = 1, 2, 3, \dots, r$

Since, $m_1 | (a - b)$, $m_2 | (a - b)$, $m_3 | (a - b)$, . . . , $m_r | (a - b)$, then their $\text{lcm}[m_1, m_2, m_3, \dots, m_r] | (a - b)$.

$\Rightarrow a \equiv b \pmod{[m_1, m_2, m_3, \dots, m_r]}$.

Corollary:

If $a \equiv b \pmod{m_i}$, $i = 1, 2, 3, \dots, r$ and $m_1, m_2, m_3, \dots, m_r$ are pairwise relatively prime then $a \equiv b \pmod{m_1, m_2, m_3, \dots, m_r}$.

MODULAR EXPONENTIATION

Modular Exponentiation is a less effective method for determining the remainder when b^n is divided by m . It is based on the binary representation of $n = (n_k n_{k-1} \dots n_1 n_0)_{two}$, successive squaring, the least residue of b^{n_i} , where $0 \leq i \leq k$.

$$b^n = b^{n_k 2^k + n_{k-1} 2^{k-1} + \dots + n_0} \equiv b^{n_k 2^k} \cdot b^{n_{k-1} 2^{k-1}} \dots b^{n_0} \pmod{m}.$$

Example 1:

Compute the remainder when 3^{181} is divided by 17.

Solution:

First, notice that $181 = (10110101)_{two}$. Now find the least residues of 3^2 and its successive squares modulo 17.

We have, $3^2 \equiv 9 \pmod{17}$.

$$3^4 \equiv 9^2 = 81 \pmod{17}.$$

$$\equiv 13 \pmod{17}.$$

$$\equiv -4 \pmod{17}.$$

$$3^8 \equiv (-4)^2 \pmod{17}.$$

$$\equiv 16 \pmod{17}.$$

$$\equiv -1 \pmod{17}.$$

$$3^{16} \equiv (-1)^2 \pmod{17}.$$

$$\equiv 1 \pmod{17}.$$

We have, $(3^{16})^2 \equiv 1^2 \pmod{17} \Rightarrow 3^{32} \equiv 1 \pmod{17}$.

$$\Rightarrow 3^{64} \equiv 1 \pmod{17} \text{ and } 3^{128} \equiv 1 \pmod{17}.$$

(128 is the largest power of 2 contained in 181.)

$$\text{Now, } 3^{181} = 3^{128+32+16+4+1} = 3^{128} \cdot 3^{32} \cdot 3^{16} \cdot 3^4 \cdot 3^1$$

Therefore $3^{181} \equiv 1 \cdot 1 \cdot 13 \cdot 3 \pmod{17}$.

$$\equiv 39 \pmod{17}.$$

$$3^{181} \equiv 5 \pmod{17}.$$

Hence, when 3^{181} is divided by 17 the remainder is 5.

LINEAR CONGRUENCES

Definition:

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a, b are the integers and x is a variable, is called a linear congruence.

Definition:

When $(a, m) = 1$, there is unique least residue x such that $ax \equiv 1 \pmod{m}$. Then a is said to be invertible and x is called an inverse of a modulo m , denoted by a^{-1} .

Therefore, $aa^{-1} \equiv 1 \pmod{m}$.

If $a^{-1} = a$, then a is said to be self invertible.

Theorem:

The unique solution of the linear congruence $ax \equiv b \pmod{m}$, where $(a, m) = 1$ is the least residue of $a^{-1}b \pmod{m}$.

Proof:

Given the linear congruence $ax \equiv b \pmod{m}$, where $(a, m) = 1$.

Since $(a, m) = 1$, a has an inverse a^{-1} modulo m .

$$\begin{aligned} ax \equiv b \pmod{m} &\Rightarrow a^{-1}(ax) \equiv a^{-1}b \pmod{m}. \\ &\Rightarrow (a^{-1}a)x \equiv a^{-1}b \pmod{m}. \\ &\Rightarrow 1.x \equiv a^{-1}b \pmod{m}. \\ &\Rightarrow x \equiv a^{-1}b \pmod{m}. \end{aligned}$$

Therefore, the solution is the least residue of $a^{-1}b \pmod{m}$.

Theorem:

The linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $d|b$, where $d = (a, m)$. If $d|b$, then it has d incongruent solutions.

Proof:

Given the linear congruence,

$$ax \equiv b \pmod{m}, \text{ where } m \in \mathbb{Z}^+ \text{ and } a, b \in \mathbb{Z}. \text{ -----(1)}$$

$$ax \equiv b \pmod{m} \text{ if and only if } m|(ax - b). \text{ ----- (2)}$$

$$\text{i.e., } ax - b = my \text{ iff } ax - my = b$$

which is a linear diophantine equation.

Thus, The linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if the linear diophantine equation $ax - my = b$ is solvable.

Let $d = (a, m)$.

Then the linear diophantine equation is solvable if and only if $d|b$.

When $d|b$, there are infinitely many solutions which are given by

$$x = x_0 + \left(\frac{-m}{d}\right)t \quad \text{and} \quad y = y_0 - \left(\frac{a}{d}\right)t, \quad t \in \mathbb{Z}$$

$$x = x_0 + \left(\frac{m}{d}\right)(-t) \quad \text{and} \quad y = y_0 + \left(\frac{a}{d}\right)(-t), \quad t \in \mathbb{Z}$$

$$x = x_0 + \left(\frac{m}{d}\right)t' \quad \text{and} \quad y = y_0 + \left(\frac{a}{d}\right)t', \quad t' = -t \in \mathbb{Z}$$

Where (x_0, y_0) is a particular solution of (2).

Hence the congruence $ax \equiv b \pmod{m}$ has infinitely many solutions given by $x = x_0 + \left(\frac{m}{d}\right)t$, where x_0 is a particular solution of the congruence and t is an arbitrary integer.

When $d|b$, we shall now prove that there are only d incongruent solutions.

Suppose $x_1 = x_0 + \left(\frac{m}{d}\right)t_1$ and $x_2 = x_0 + \left(\frac{m}{d}\right)t_2$ are two solutions of the congruence.

Suppose $x_0 + \left(\frac{m}{d}\right)t_1 \equiv x_0 + \left(\frac{m}{d}\right)t_2 \pmod{m}$, then $\left(\frac{m}{d}\right)t_1 \equiv \left(\frac{m}{d}\right)t_2 \pmod{m}$.

Since $\left(\frac{m}{d}\right)|m$, we get $t_1 \equiv t_2 \pmod{d}$.

Thus x_1 and x_2 are congruent if and only if $t_1 \equiv t_2 \pmod{d}$.

Therefore x_1 and x_2 are incongruent solutions if and only if t_1, t_2 belong to different congruence classes \pmod{d} .

But we know that there are only d congruence classes modulo d .

So, the number of incongruent solutions is d and they are given by

$$x = x_0 + \left(\frac{m}{d}\right)t, \quad 0 \leq t < d.$$

This is the general solutions of the congruence.

Corollary:

The linear congruence $ax \equiv b \pmod{m}$ has unique solution if and only if $(a, m) = 1$.

Example 1:

Determine the number of incongruent solutions of $48x \equiv 144 \pmod{84}$.

Solution:

Given the linear congruence,

$$48x \equiv 144 \pmod{84}.$$

$$\text{Here } a = 48, \quad b = 144, \quad m = 84$$

$$\text{Now, } (a, m) = (48, 84) = 12.$$

$$\text{Therefore } d = 12.$$

Since $12|144$, we have $d|b$ and so the linear congruence is solvable.

Hence it has 12 incongruent solutions.

Example 2:

Determine whether the congruence $12x \equiv 48 \pmod{18}$ is solvable and also find all the solutions if solvable.

Solution:

Given the linear congruence,

$$12x \equiv 48 \pmod{18}.$$

$$\text{Here } a = 12, \quad b = 48, \quad m = 18$$

$$\text{Now, } (a, m) = (12, 18) = 6.$$

$$\text{Therefore } d = 6.$$

Since $6|48$, we have $d|b$ and so the linear congruence is solvable.

Hence it has 6 incongruent solutions.

We find the particular solution $x_0 = 1$ which satisfies $12x \equiv 48 \pmod{18}$.

The general solution is given by

$$x = x_0 + \left(\frac{m}{d}\right)t, \quad 0 \leq t < d.$$

$$\Rightarrow x = 1 + \left(\frac{18}{6}\right)t \quad 0 \leq t < 6.$$

$$\Rightarrow x = 1 + 3t \quad 0 \leq t < 6.$$

Hence the incongruent solutions are 1, 4, 7, 10, 13 & 16.

Example 3:

Solve the linear Diophantine equation $63x - 23y = -7$ using congruence.

Solution:

Given the LDE is $63x - 23y = -7$. -----(1)

From the above equation we get the congruence,

$$63x \equiv -7 \pmod{23} \text{ and } -23y \equiv -7 \pmod{63}.$$

First we solve $63x \equiv -7 \pmod{23}$. -----(2)

Since $63 \equiv -6 \pmod{23}$, eqn (2) becomes $-6x \equiv -7 \pmod{23}$.

$$\Rightarrow 6x \equiv 7 \pmod{23}.$$

Here $a = 6$, $b = 7$, $m = 23$.

Now, $(a, m) = (6, 23) = 1$.

Since $d = 1$, the linear congruence $6x \equiv 7 \pmod{23}$ has unique solution.

Since $30 \equiv 7 \pmod{23}$, we see that $x = 5$ which satisfies $6x \equiv 7 \pmod{23}$.

Now substituting $x = 5$ in eqn (1), we get

$$23y = 63(5) + 7.$$

$$\Rightarrow 23y = 322.$$

$$\Rightarrow y = 14.$$

Hence the required solution (x, y) is $(5, 14)$.

Example 4:

Twenty three weary travellers entered the outskirts of a lush and beautiful forest. They found 63 equal heaps of plantains and seven single fruits, and divided them equally. Find the number of fruits in each heap.

Solution:

Let x be the number of plantains in a heap.

Let y be the number of plantains received by a traveller.

Then the total number of plantains is $63x + 7$.

Since each traveller received y plantains, the total number of plantains received by the travellers is $23y$.

$$\text{Therefore } 63x + 7 = 23y. \Rightarrow 63x - 23y = -7. \text{ -----(1)}$$

Which is a linear Diophantine equation.

From the above equation we get the congruence,

$$63x \equiv -7 \pmod{23} \text{ and } -23y \equiv -7 \pmod{63}.$$

First we solve $63x \equiv -7 \pmod{23}$. -----(2)

Since $63 \equiv -6 \pmod{23}$, eqn (2) becomes $-6x \equiv -7 \pmod{23}$.

$$\Rightarrow 6x \equiv 7 \pmod{23}.$$

Here $a = 6$, $b = 7$, $m = 23$.

Now, $(a, m) = (6, 23) = 1$.

Since $d = 1$, the linear congruence $6x \equiv 7 \pmod{23}$ has unique solution.

Since $30 \equiv 7 \pmod{23}$, we see that $x = 5$ which satisfies $6x \equiv 7 \pmod{23}$.

Now substituting $x = 5$ in eqn (1), we get

$$23y = 63(5) + 7.$$

$$\Rightarrow 23y = 322.$$

$$\Rightarrow y = 14.$$

Hence the required solution (x, y) is $(5, 14)$.

Example 5:

Using inverse find the incongruent solutions of the linear congruence $5x \equiv 3 \pmod{6}$

Solution:

Given the linear congruence,

$$5x \equiv 3 \pmod{6}.$$

Here $a = 5$, $b = 3$, $m = 6$.

Now, $(a, m) = (5, 6) = 1$.

Therefore $d = 1$.

Since $d = 1$, the linear congruence $5x \equiv 3 \pmod{6}$ has unique solution.

The unique solution is given by $x \equiv a^{-1}b \pmod{m}$.

we see that inverse of 5 is 5 in modulo 6.

$$\Rightarrow x \equiv 5 \times 3 \pmod{6}.$$

$$\Rightarrow x \equiv 15 \pmod{6}.$$

$$\Rightarrow x \equiv 3 \pmod{6}.$$

APPLICATIONS: DIVISIBILITY TESTS

In this section, we establish some simple methods to find the division of numbers. Let n be a positive integer in the decimal system. Let $n = n_k n_{k-1} \dots n_2 n_1 n_0$.

Divisibility Test for 10: An integer is divisible by 10 if and only if its units digit is zero.

Divisibility Test for 5: An integer n is divisible by 5 if and only if its units digit is 0 or 5.

Divisibility Test for 2^i :

Since $10 \equiv 0 \pmod{2}$ and $10^i \equiv 0 \pmod{2^i}$ for all positive integer i .

Thus, n is divisible by 2 if and only if n_0 is divisible by 2.

n is divisible by 2^2 if and only if the last two digits $n_1 n_0$ is divisible by $2^2 = 4$.

In general, an integer n is divisible by 2^i if and only if the number formed by the last i digits in n is divisible by 2^i .

Example 1: Let $n = 343,506,076$. Since $2|6$, $2|n$; $4|76$, so $4|n$. But 8 does not divide 076, so 8 does not divide n .

Divisibility Test for 3 and 9: An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

Example 2: Let $n = 243,506,076$. The sum of its digits is $2+4+3+5+0+6+0+7+6 = 33$. Since $3|33$, $3|n$. But 9 does not divide 33, so 9 does not divide n .

An integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Divisibility Test for 11: An integer n is divisible by 11 if and only if $(n_0 + n_2 + \dots) - (n_1 + n_3 + \dots)$ is divisible by 11. i.e. Sum of digits in the even positions – Sum of digits in the odd positions is divisible by 11.

Example 3: Determine 243,506,076 is divisible by 11.

Solution:

Let $n = 243,506,076$.

Desired difference = $(6+0+0+3+2) - (7+6+5+4) = 11 - 22 = -11$.

Because $11|-11$, $11|n$ also.

Example 4: Determine 4776112 is divisible by 8.

Solution:

Let $n = 4776112$.

The last three-digits of the number is 112 and $8|112$.

Hence, n is divisible by 8.

CHINESE REMAINDER THEOREM

View the lecture on YouTube: <https://youtu.be/A928YhkpeVw>
<https://youtu.be/WHS0eCe-WtE>

SYSTEM OF LINEAR CONGRUENCE

A system of linear congruence is a single variable congruence with more than one congruences. There are two methods to solve system of linear congruence. They are method of iteration and Chinese remainder theorem method.

Method of Iteration

A simplest method for solving a linear congruence system is iteration. In this method, substitute x until the last congruence is used.

The Chinese remainder theorem

Statement: The linear system of congruences

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots \equiv \vdots \vdots \vdots \vdots$$

$$x \equiv a_k \pmod{m_k}$$

where moduli m_1, m_2, \dots, m_k are pairwise relatively prime, has a unique solution modulo M where $M = m_1 \cdot m_2 \dots m_k$.

Proof: The proof consists of two parts. First we will construct a solution and then show that it is a unique modulo M where $M = m_1 \cdot m_2 \dots m_k$.

Let $M_i = \frac{M}{m_i}$, for $1 \leq i \leq k$.

Since the moduli are pairwise relatively prime $(M_i, m_i) = 1$ for every $1 \leq i \leq k$.

Also $M_i \equiv 0 \pmod{m_j}$ for $i \neq j$.------(1)

Part 1. To construct a solution to the linear system.

since $(M_i, m_i) = 1$. The congruence

$$M_i y_j \equiv 1 \pmod{m_j} \text{-----}(2)$$

is solvable and has a unique solution y_j .

Let $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_k M_k y_k$ ------(3)

To show x satisfy the given congruences. Consider

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_k M_k y_k$$

$$\begin{aligned}
&= \sum_{i=1}^n a_i M_i y_i + a_j M_j y_j \\
x(\text{mod } m_j) &= \sum_{i=1}^n a_i M_i y_i (\text{mod } m_j) + a_j M_j y_j (\text{mod } m_j) \\
&= 0 + 1 \cdot a_j (\text{mod } m_j) \\
&= a_j (\text{mod } m_j)
\end{aligned}$$

Therefore, x satisfies $x \equiv a_j (\text{mod } m_j)$ for an arbitrary $j, 1 \leq j \leq k$. So equation (3) is a solution to the linear system to congruences.

Part 2: To show that the solution is unique modulo M .

Let x_0 and x_1 be two solutions of the system.

We shall show that $x_0 \equiv x_1 (\text{mod } M)$, x_0, x_1 being solutions of the given system, we have $x_0 \equiv a_j (\text{mod } m_j)$ and $x_1 \equiv a_j (\text{mod } m_j)$ for $1 \leq j \leq k$

Which implies that, $x_0 - x_1 \equiv 0 (\text{mod } m_j)$

$$\Rightarrow m_j \mid (x_0 - x_1)$$

for each $j, 1 \leq j \leq k$. Thus, $[m_1, m_2, \dots, m_k] \mid (x_0 - x_1)$.

Since m_1, m_2, \dots, m_k are pairwise relatively prime,

$$[m_1, m_2, \dots, m_k] = m_1 \cdot m_2 \dots m_k = M$$

$$\Rightarrow M \mid (x_0 - x_1)$$

$$x_0 - x_1 \equiv 0 (\text{mod } M)$$

$$x_0 \equiv x_1 (\text{mod } M)$$

Example 1. Solve the system using iteration method

$$x \equiv 2 (\text{mod } 5)$$

$$x \equiv 3 (\text{mod } 7)$$

Solution: The given system is

$$x \equiv 2 (\text{mod } 5) \text{-----(1)}$$

$$x \equiv 3 (\text{mod } 7) \text{-----(2)}$$

From (1) we have

$$x = 2 + 5t_1 \text{-----(3)}$$

where t_1 is an arbitrary integer.

Substituting (3) in (2)

$$2 + 5t_1 \equiv 3(\text{mod } 7)$$

$$5t_1 \equiv 1(\text{mod } 7) \text{-----(4)}$$

We know that 3 is the inverse of 5 in modulo 7, so multiply (4) by 3,

$$3 \times 5t_1 \equiv 3(\text{mod } 7)$$

$$t_1 \equiv 3(\text{mod } 7)$$

$$\Rightarrow t_1 = 3 + 7t \text{-----(5)}$$

where t be an arbitrary integer.

Substituting (5) in (3)

$$x = 2 + 5(3 + 7t) = 2 + 15 + 35t$$

$$= 17 + 35t$$

Hence $x = 17 + 35t$ is solution of given congruences.

Example 2. Solve the system using iteration method

$$x \equiv 3(\text{mod } 4)$$

$$x \equiv 5(\text{mod } 9)$$

Solution: The given system is

$$x \equiv 3(\text{mod } 4) \text{-----(1)}$$

$$x \equiv 5(\text{mod } 9) \text{-----(2)}$$

From (1) we have

$$x = 3 + 4t_1 \text{-----(3)}$$

where t_1 is an arbitrary integer.

Substituting (3) in (2)

$$3 + 4t_1 \equiv 5(\text{mod } 9)$$

$$2t_1 \equiv 1(\text{mod } 9) \text{-----(4)}$$

We know that 5 is the inverse of 2 in modulo 9, so multiply (4) by 5,

$$5 \times 2t_1 \equiv 5(\text{mod } 9)$$

$$t_1 \equiv 5(\text{mod } 9)$$

$$\Rightarrow t_1 = 5 + 9t \text{-----(5)}$$

where t be an arbitrary integer.

Substituting (5) in (3)

$$\begin{aligned}
 x &= 3 + 4(5 + 9t) = 3 + 20 + 36t \\
 &= 23 + 36t
 \end{aligned}$$

Hence $x = 19 + 36t$ is solution of given congruences.

Example 3. Solve the system using iteration method

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}.$$

(or)

Consider the puzzle, (due to the Chinese mathematician Sun-Tsu, and appears in Master Sun's Mathematical Manual, written between 287 A.D. and 473 A.D.):

Find a number that leaves a remainder of 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7.

Solution: The given system is

$$x \equiv 1 \pmod{3} \text{-----(1)}$$

$$x \equiv 2 \pmod{5} \text{-----(2)}$$

$$x \equiv 3 \pmod{7} \text{-----(3)}$$

From (1) we have

$$x = 1 + 3t_1 \text{-----(4)}$$

where t_1 is an arbitrary integer.

Substituting (4) in (2)

$$1 + 3t_1 \equiv 2 \pmod{5}$$

$$3t_1 \equiv 1 \pmod{5} \text{-----(5)}$$

We know that 2 is the inverse of 3 in modulo 5, so multiply (5) by 2,

$$2 \times 3t_1 \equiv 2 \pmod{5}$$

$$t_1 \equiv 2 \pmod{5}$$

$$\Rightarrow t_1 = 2 + 5t_2 \text{-----(6)}$$

where t_2 be an arbitrary integer.

Substituting (6) in (4)

$$x = 1 + 3(2 + 5t_2) = 7 + 15t_2 \text{-----(7)}$$

Substituting (7) in (3)

$$\begin{aligned}
7 + 15t_2 &\equiv 3 \pmod{7} \\
15t_2 &\equiv -4 \pmod{7} \\
15t_2 &\equiv 3 \pmod{7} \\
t_2 &\equiv 3 \pmod{7} \\
\Rightarrow t_2 &= 3 + 7t \text{-----(8)}
\end{aligned}$$

where t be an arbitrary integer.

Substituting (8) in (7)

$$\begin{aligned}
x &= 3 + 15(3 + 7t) = 7 + 45 + 105t \\
&= 52 + 105t
\end{aligned}$$

Hence $x = 52 + 105t$ is solution of given congruences.

Example 4. Solve $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$ by Chinese remainder theorem.

Solution: The given system is

$$x \equiv 2 \pmod{5}, x \equiv 3 \pmod{7}$$

Here $M = 5 \times 7 = 35$ and $(5, 7) = 1$

$$a_1 = 2 \quad a_2 = 3$$

$$m_1 = 5 \quad m_2 = 7$$

$$M_1 = \frac{35}{5} = 7 \quad M_2 = \frac{35}{7} = 5$$

$$M_1 y_1 \equiv 1 \pmod{m_1}$$

$$M_2 y_2 \equiv 1 \pmod{m_2}$$

$$7y_1 \equiv 1 \pmod{5}$$

$$5y_2 \equiv 1 \pmod{7}$$

$$y_1 \equiv 3 \pmod{5}$$

$$y_2 \equiv 3 \pmod{7}$$

The least positive solution are $y_1 = 3$, $y_2 = 3$.

$$\begin{aligned}
x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 \pmod{M} \\
&\equiv 2 \times 7 \times 3 + 3 \times 5 \times 3 \pmod{35} \\
&\equiv (42 + 45) \pmod{35} \\
&\equiv 87 \pmod{35} \\
&\equiv 17 \pmod{35}
\end{aligned}$$

The least positive solution is $x = 17$ and general solutions are $x = 17 + 35t$, where t is an arbitrary integer.

Example 5. Solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$ by Chinese remainder theorem.

Solution: Here $M = 3 \times 4 \times 5 = 60$ and $(3, 4) = (4, 5) = (3, 5) = 1$

$$a_1 = 1 \quad a_2 = 2 \quad a_3 = 5$$

$$m_1 = 3 \quad m_2 = 4 \quad m_3 = 5$$

$$M_1 = 20 \quad M_2 = 15 \quad M_3 = 12$$

$$M_1 y_1 \equiv 1(\text{mod } m_1) \quad M_2 y_2 \equiv 1(\text{mod } m_2) \quad M_3 y_3 \equiv 1(\text{mod } m_3)$$

$$20y_1 \equiv 1(\text{mod } 3) \quad 15y_2 \equiv 1(\text{mod } 4) \quad 12y_3 \equiv 1(\text{mod } 5)$$

$$2y_1 \equiv 1(\text{mod } 3) \quad y_2 \equiv 3(\text{mod } 4) \quad 2y_3 \equiv 1(\text{mod } 5)$$

$$y_1 \equiv 2(\text{mod } 3) \quad y_3 \equiv 3(\text{mod } 5)$$

The least positive solution are $y_1 = 2$, $y_2 = 3$ and $y_3 = 3$

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 (\text{mod } M) \\ &\equiv 1 \times 20 \times 2 + 2 \times 15 \times 3 + 3 \times 12 \times 3 (\text{mod } 35) \\ &\equiv 238 (\text{mod } 35) \\ &\equiv 58 (\text{mod } 35) \end{aligned}$$

The least positive solution is $x = 58$ and general solutions are $x = 58 + 105t$, where t is an arbitrary integer.

Example 6. Solve $x \equiv 1(\text{mod } 3)$, $x \equiv 2(\text{mod } 5)$, $x \equiv 3(\text{mod } 7)$.

Solution: The given system is

$$x \equiv 1(\text{mod } 3), x \equiv 2(\text{mod } 5), x \equiv 3(\text{mod } 7).$$

$$\text{Here } M = 3 \times 5 \times 7 = 105 \text{ and } (3, 5) = (5, 7) = (3, 7) = 1$$

$$a_1 = 1 \quad a_2 = 2 \quad a_3 = 3$$

$$m_1 = 3 \quad m_2 = 5 \quad m_3 = 7$$

$$M_1 = 35 \quad M_2 = 21 \quad M_3 = 15$$

$$M_1 y_1 \equiv 1(\text{mod } m_1) \quad M_2 y_2 \equiv 1(\text{mod } m_2) \quad M_3 y_3 \equiv 1(\text{mod } m_3)$$

$$35y_1 \equiv 1(\text{mod } 3) \quad 21y_2 \equiv 1(\text{mod } 5) \quad 15y_3 \equiv 1(\text{mod } 7)$$

$$2y_1 \equiv 1(\text{mod } 3) \quad y_2 \equiv 1(\text{mod } 5) \quad y_3 \equiv 1(\text{mod } 7)$$

$$y_1 \equiv 2(\text{mod } 3)$$

The least positive solution are $y_1 = 2$, $y_2 = 1$ and $y_3 = 1$

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 (\text{mod } M) \\ &\equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 (\text{mod } 105) \\ &\equiv 157 (\text{mod } 105) \\ &\equiv 52 (\text{mod } 105) \end{aligned}$$

The least positive solution is $x = 52$ and general solutions are $x = 52 + 105t$, where t is an arbitrary integer.

2 × 2 LINEAR SYSTEMS

Definition: A 2×2 linear system is a system of linear congruences of the form $ax + by \equiv e(mod\ m)$
 $cx + dy \equiv f(mod\ m)$

where a, b, c, d, e, f are integers and m is a positive integer.

Note:

A solution of the system is a pair $x \equiv x_0(mod\ m), y \equiv y_0(mod\ m)$ that satisfies both the congruences.

The linear system of congruences are solved by the elementary – elimination method and also by the well-known Cramer’s rule.

The following theorem provides a necessary and sufficient condition for a 2×2 linear system to have a unique solution.

Theorem 1: The linear system
 $ax + by \equiv e(mod\ m)$
 $cx + dy \equiv f(mod\ m)$
has a unique solution if and only if $(\Delta, m) = 1$, where $\Delta \equiv (ad - bc)(mod\ m)$.

Proof:

Suppose the system has a solution $x \equiv x_0(mod\ m), y \equiv y_0(mod\ m)$:

$ax_0 + by_0 \equiv e(mod\ m)$ -----(1)

$cx_0 + dy_0 \equiv f(mod\ m)$ -----(2)

(1) x d and (2) x b, we get

$adx_0 + bdy_0 \equiv ed(mod\ m)$

$bcx_0 + bdy_0 \equiv bf(mod\ m)$

Subtracting we get, $(ad - bc)x_0 \equiv (ed - bf)(mod\ m)$

We know that, The linear congruence $ax \equiv b(\text{mod } m)$ has a unique solution iff $(a, m) = 1$.

$\therefore x_0$ has a unique value modulo m iff $(\Delta, m) = 1$.

Similarly, y_0 has a unique value modulo m iff $(\Delta, m) = 1$.

Thus, the system has a unique solution modulo m iff $(\Delta, m) = 1$.

Although Theorem 1 can be used to determine whether a system has a unique solution, it does not furnish us with the solution when it is solvable. However, the following theorem does.

Theorem 2: When the linear system

$$ax + by \equiv e(\text{mod } m)$$

$$cx + dy \equiv f(\text{mod } m)$$

has a unique solution modulo m , it is given by $x_0 \equiv \Delta^{-1}(ed - bf)(\text{mod } m)$ and $y_0 \equiv \Delta^{-1}(af - ce)(\text{mod } m)$, where $\Delta \equiv (ad - bc)(\text{mod } m)$ and Δ^{-1} is the inverse of Δ modulo m .

Proof:

By Theorem 1, since the system has a unique solution modulo m , $(\Delta, m) = 1$; So, Δ is invertible.

Because the linear system has a unique solution, it suffices to show that x_0, y_0 satisfies the system:

$$ax_0 + by_0 \equiv a\Delta^{-1}(ed - bf) + b\Delta^{-1}(af - ce)(\text{mod } m)$$

$$\equiv (ad - bc)\Delta^{-1}e + \Delta^{-1}(abf - abf)(\text{mod } m)$$

$$\equiv \Delta\Delta^{-1}e + 0(\text{mod } m)$$

$$\equiv e(\text{mod } m). \quad \text{Since, } \Delta\Delta^{-1} \equiv 1(\text{mod } m)$$

Also,

$$\begin{aligned} cx_0 + dy_0 &\equiv c\Delta^{-1}(de - bf) + d\Delta^{-1}(af - ce)(\text{mod } m) \\ &\equiv (ad - bc)\Delta^{-1}f + \Delta^{-1}(cde - cde)(\text{mod } m) \\ &\equiv \Delta\Delta^{-1}f + 0(\text{mod } m) \\ &\equiv f(\text{mod } m). \end{aligned}$$

Since, $\Delta\Delta^{-1} \equiv 1(\text{mod } m)$.

Thus, $x \equiv x_0 (\text{mod } m)$, $y \equiv y_0 (\text{mod } m)$ is the unique solution of the linear system.

Remark:

The formulas for $x_0 (\text{mod } m)$ and $y_0 (\text{mod } m)$ closely resemble those for x and y in Cramer’s rule of a linear system of equations. To see this, we can rewrite the values of Δ , x_0 and y_0 in terms of determinants:

$$\begin{aligned} \Delta &\equiv ad - bc \equiv \begin{vmatrix} a & b \\ c & d \end{vmatrix} (\text{mod } m) \\ x_0 &\equiv \Delta^{-1}(de - bf) \equiv \Delta^{-1} \begin{vmatrix} e & b \\ f & d \end{vmatrix} (\text{mod } m) \\ y_0 &\equiv \Delta^{-1}(af - ce) \equiv \Delta^{-1} \begin{vmatrix} a & e \\ c & f \end{vmatrix} (\text{mod } m). \end{aligned}$$

Example 1:

Solve the linear system
 $x + 3y \equiv 3 (\text{mod } 11)$
 $5x + y \equiv 5 (\text{mod } 11)$ by the method of elimination.

Solution:

$$\begin{aligned} x + 3y &\equiv 3 (\text{mod } 11) && \text{-----(1)} \\ 5x + y &\equiv 5 (\text{mod } 11) && \text{-----(2)} \end{aligned}$$

$$\Rightarrow x + 3y \equiv 3 \pmod{11}$$

$$\Rightarrow 15x + 3y \equiv 15 \pmod{11}$$

Multiplying both sides of equation (2) by 3.

Subtracting, we get

$$-14x \equiv -12 \pmod{11}$$

$$-3x \equiv -12 \pmod{11} \quad [\text{since } 14 \equiv 3 \pmod{11}]$$

$$3x \equiv 12 \pmod{11}$$

$$x \equiv 4 \pmod{11} \quad [\text{since } (3, 11) = 1]$$

Substituting in (2), we get

$$20 + y \equiv 5 \pmod{11}$$

$$\Rightarrow y \equiv -15 \pmod{11}$$

$$\Rightarrow y \equiv -4 \pmod{11} \quad [\text{since } 15 \equiv 4 \pmod{11}]$$

$$\Rightarrow y \equiv 7 \pmod{11}. \quad [\text{since } 7 \equiv -4 \pmod{11}]$$

\therefore The solution is $x \equiv 4 \pmod{11}$, $y \equiv 7 \pmod{11}$ (or) $x = 4 + 11t$, $y = 7 + 11t$,
 $t \in \mathbb{Z}$.

Example 2. Solve the system

$$3x + 13y \equiv 8 \pmod{55}$$

$$5x + 21y \equiv 34 \pmod{55} \text{ by using Cramer's rule.}$$

Solution:

We shall solve by Cramer's method.

$$\Delta \equiv 3 \times 21 - 13 \times 5 \equiv 53 \pmod{55}.$$

Here $\Delta = 53$, $m = 55$.

Also, $(\Delta, m) = (53, 55) = 1$

\therefore The system has unique solution modulo 55.

The general solution is

$$x_0 \equiv \Delta^{-1}(de - bf) \equiv \Delta^{-1} \begin{vmatrix} e & b \\ f & d \end{vmatrix} (\text{mod } m)$$

$$y_0 \equiv \Delta^{-1}(af - ce) \equiv \Delta^{-1} \begin{vmatrix} a & e \\ c & f \end{vmatrix} (\text{mod } m)$$

To find Δ^{-1} :

$$\Delta \Delta^{-1} \equiv 1 (\text{mod } 55)$$

$$\Rightarrow 53 \Delta^{-1} \equiv 1 (\text{mod } 55)$$

$$\Rightarrow -2 \Delta^{-1} \equiv 1 (\text{mod } 55)$$

$$\text{If } \Delta^{-1} = -28, \text{ then } (-2)(-28) = 56 \equiv 1 (\text{mod } 55)$$

$$\therefore \Delta^{-1} = -28 (\text{mod } 55)$$

$$\Rightarrow \Delta^{-1} \equiv 27 (\text{mod } 55).$$

$$\therefore \Delta^{-1} = 27$$

$$\therefore x_0 \equiv \Delta^{-1}(de - bf) \equiv 27(21 \times 8 - 13 \times 34) \equiv 27 (\text{mod } 55)$$

$$y_0 \equiv \Delta^{-1}(af - ce) \equiv 27(3 \times 34 - 5 \times 8) \equiv 24 (\text{mod } 55).$$

Thus, $x \equiv 27 (\text{mod } 55)$ and $y \equiv 24 (\text{mod } 55)$ is the unique solution to the given system.

PRACTICE QUIZ: DIOPHANTINE EQUATIONS AND CONGRUENCES

Diophantine Equations and Congruences

Practice Quiz – 15 questions

<https://quizizz.com/print/quiz/5f48a21d6bafd3001bb11603>

STUCOR APP

ASSIGNMENTS: UNIT IV

1. Prove that the LDE $ax + by = c$ is solvable if and only if $d|c$, where $d = \gcd(a, b)$. Further obtain the general solution of $15x + 21y = 39$.
2. Find the general solution of the LDE $6x + 8y + 12z = 10$.
3. Show that the linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $\gcd(a, m)$ divides b . Also, show that if $\gcd(a, m)$ divides b , then it has d incongruent solutions, where $d = \gcd(a, m)$.
4. If $a|b$ and $c|d$ then prove that $\gcd(a, c)|\gcd(b, d)$.
5. Determine whether the congruence $12x \equiv 48 \pmod{18}$ is solvable and also find all the solutions if solvable.
6. Twenty-three weary travelers entered the outskirts of a lush and beautiful forest. They found 63 equal heaps of plantains and seven single fruits, and divide them equally. Find the number of fruits in each heap. (This problem is taken from Mahavira's book.)
7. Solve the following system of congruences: $x \equiv 2 \pmod{3}$, $x \equiv 4 \pmod{5}$, $x \equiv 5 \pmod{7}$.
8. Solve the linear system $x \equiv 3 \pmod{7}$, $x \equiv 4 \pmod{9}$, $x \equiv 8 \pmod{11}$.
9. Show that $n^2 + n \equiv 0 \pmod{2}$ for any positive integer n .
10. Find the remainder when $(n^2 + n + 41)^2$ is divided by 12.
11. Compute the remainder when 3^{181} is divided by 17.
12. State and prove Chinese remainder theorem.
13. Solve Sun-Tsu's puzzle by CRT.
14. Solve the following system of linear congruences: $x + 3y \equiv 3 \pmod{11}$ and $5x + y \equiv 5 \pmod{11}$.

PART A QUESTIONS AND ANSWERS: UNIT IV**1. Define the Linear Diophantine Equation.** (K1, CO5)

Solution: A Linear Diophantine equation (in 2 variables) is an equation of the form $ax + by = c$ where a, b, c are integers and x, y are unknowns.

2. Examine the linear Diophantine equation $12x + 16y = 18$ is solvable. Write the general solution if solvable. (K2, CO5)

Solution: Given LDE is $12x + 16y = 18$ (1)

Here $a = 12, b = 16, c = 18$. (2)

$$\therefore (a, b) = (12, 16) = 4$$

$$\text{so, } d = (a, b) = 4$$

since 4 is doesn't a factor of 18, (i.e) $4 \nmid 18$

We have $d \nmid c$.

So, the LDE is not solvable.

3. Check whether the LDE $6x + 8y = 25$ is solvable. (K2, CO5)

Solution: We have $d = (6, 8) = 2$ and $2 \nmid 25$.

\Rightarrow the equation is not solvable.

4. Check whether the LDE $8x + 10y + 16z = 25$ is solvable.

(K2, CO5)

Solution: We have $d = (8, 10, 16) = 2$ and $2 \nmid 25$.

\Rightarrow the equation is not solvable.

5. Check whether the LDE $6x + 18y + 12z = 10$ is solvable.

(K2, CO5)

Solution: We have $d = (6, 18, 12) = 6$ and $6 \mid 10$.

\Rightarrow the equation is solvable.

6. If today is Wednesday, what will it be in 129 days?

(K2, CO5)

Solution:

To find day of a week we use $\text{mod } 7$.

$$129 \equiv 3 \pmod{7}.$$

So, if today is Wednesday then after 3 days it will be Saturday.

7. If it is 11:30 AM now what time will it be in 1769 hours?

(K2, CO5)

Solution:

To find the time we consider $\text{mod } 12$.

$$1769 \equiv 5 \pmod{12}.$$

So, if now the time is 11:30 AM, then after 5 hours it will be 4:30 PM.

8. Is $2x \equiv 7 \pmod{4}$ solvable?

(K2, CO5)

Solution:

Given the linear congruence,

$$2x \equiv 7 \pmod{4}.$$

$$\text{Here } a = 2, \quad b = 7, \quad m = 4.$$

$$\text{Now, } (a, m) = (2, 4) = 2.$$

$$\text{Therefore } d = 2.$$

Since $2 \nmid 7$, we have $d \nmid b$ and hence the linear congruence is insolvable.

9. Determine the number of incongruent solutions of $48x \equiv 144 \pmod{84}$.

(K2, CO5)

Solution:

Given the linear congruence,

$$48x \equiv 144 \pmod{84}.$$

$$\text{Here } a = 48, \quad b = 144, \quad m = 84$$

$$\text{Now, } (a, m) = (48, 84) = 12.$$

$$\text{Therefore } d = 12.$$

Since $12 \mid 144$, we have $d \mid b$ and so the linear congruence is solvable.

Hence it has 12 incongruent solutions.

10. Using inverse find the incongruent solutions of the linear congruence $5x \equiv 3 \pmod{6}$. (K2, CO5)

Solution:

Given the linear congruence,

$$5x \equiv 3 \pmod{6}.$$

$$\text{Here } a = 5, \quad b = 3, \quad m = 6.$$

$$\text{Now, } (a, m) = (5, 6) = 1.$$

$$\text{Therefore } d = 1.$$

Since $d = 1$, the linear congruence $5x \equiv 3 \pmod{6}$ has unique solution.

The unique solution is given by $x \equiv a^{-1}b \pmod{m}$.

we see that inverse of 5 is 5 in modulo 6.

$$\Rightarrow x \equiv 5 \times 3 \pmod{6}.$$

$$\Rightarrow x \equiv 15 \pmod{6}.$$

$$\Rightarrow x \equiv 3 \pmod{6}.$$

11. Find the unit digit in 3^{55} .

(K3, CO5)

Solution:

The unit digit of 3^{55} is the remainder when it is divided by 10.

So, we use modulo 10.

$$\text{Now, } 3^2 \equiv 9 \pmod{10}.$$

$$\Rightarrow 3^4 \equiv 9^2 \pmod{10}.$$

$$\equiv 81 \pmod{10}.$$

$$\Rightarrow 3^4 \equiv 1 \pmod{10}.$$

$$\Rightarrow (3^4)^{13} \equiv 1^{13} \pmod{10}.$$

$$\Rightarrow 3^{52} \equiv 1 \pmod{10}.$$

$$\text{Also } 3^3 \equiv 7 \pmod{10}.$$

$$\text{So, } 3^{55} = 3^{52+3} = 3^{52} \cdot 3^3 \equiv 1 \cdot 7 \pmod{10}.$$

$$\Rightarrow 3^{55} \equiv 7 \pmod{10}.$$

Hence the unit digit in 3^{55} is 7.

12. Define 2X2 linear system.

(K1, CO5)

Solution:

A system of linear congruence of the form

$$ax + by \equiv e \pmod{m}$$

$$cx + dy \equiv f \pmod{m}$$

is called a 2X2 linear system, where $a, b, c, d, e, & f$ are the integers and m is a positive integer.

A solution of the linear system is a pair $x \equiv x_0 \pmod{m}, y \equiv y_0 \pmod{m}$ that satisfies both the congruences.

13. Determine whether the linear system $6x + 8y \equiv 10 \pmod{13}$ and $8x + 10y \equiv 12 \pmod{13}$ is solvable.

(K2, CO5)

Solution:

Given linear system is

$$6x + 8y \equiv 10 \pmod{13}$$

$$8x + 10y \equiv 12 \pmod{13}$$

$$\Delta \equiv \begin{vmatrix} 6 & 8 \\ 8 & 10 \end{vmatrix}$$

$$\equiv 60 - 64$$

$$\equiv -4$$

$$\equiv 9 \pmod{13}$$

Here, $m = 13$.

So, $(\Delta, m) = (9, 13) = 1$.

Hence the system is solvable and it has unique solution.

14. Determine 243,506,076 is divisible by 11.

(K2, CO5)

Solution:

Let $n = 243,506,076$.

Desired difference = $(6+0+0+3+2) - (7+6+5+4) = 11 - 22 = -11$.

Because $11 \mid -11$, $11 \mid n$ also.

15. Determine 4776112 is divisible by 8.

(K2, CO5)

Solution:

Let $n = 4776112$.

The last three-digits of the number is 112 and $8|112$.

Hence, n is divisible by 8.

16. State Chinese remainder theorem.

(K2, CO5)

Solution:

The linear system of congruences

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots \equiv \vdots \vdots \vdots \vdots$$

$$x \equiv a_k \pmod{m_k}$$

where moduli m_1, m_2, \dots, m_k are pairwise relatively prime, has a unique solution modulo M , where $M = m_1 \cdot m_2 \dots m_k$.

17. Write the system of equations for the following puzzle "Find a number that leaves a remainder of 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7".

(K2, CO5)

Solution:

The required system is

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

18. Prove that $a \equiv b \pmod{m}$ if and only if $a = b + mk$ for some integer k .

(K2, CO5)

Solution:

Let $a \equiv b \pmod{m}$.

Then $m|(a - b)$

$$\Rightarrow a - b = mk \text{ for some integer } k.$$

$$\Rightarrow a = b + mk.$$

Conversely, let $a = b + mk$.

$$\text{Then, } a - b = mk.$$

$$\Rightarrow m|(a - b).$$

$$\Rightarrow a \equiv b \pmod{m}.$$

PART B QUESTIONS: UNIT IV

1. Prove that the LDE $ax + by = c$ is solvable if and only if $d|c$, where $d = \gcd(a, b)$. Further obtain the general solution of $15x + 21y = 39$. (K2, CO5)
2. Find the general solution of the LDE $6x + 8y + 12z = 10$. (K2, CO5)
3. Show that the linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $\gcd(a, m)$ divides b . Also, show that if $\gcd(a, m)$ divides b , then it has d incongruent solutions, where $d = \gcd(a, m)$. (K2, CO5)
4. If $a|b$ and $c|d$ then prove that $\gcd(a, c)|\gcd(b, d)$. (K2, CO5)
5. Twenty-three weary travelers entered the outskirts of a lush and beautiful forest. They found 63 equal heaps of plantains and seven single fruits, and divide them equally. Find the number of fruits in each heap. (This problem is taken from Mahavira's book.) (K3, CO5)
6. Determine whether the congruence $12x \equiv 48 \pmod{18}$ is solvable and also find all the solutions if solvable. (K2, CO5)
7. Show that $n^2 + n \equiv 0 \pmod{2}$ for any positive integer n . (K3, CO5)
8. Prove that $4^{2n} + 10n \equiv 0 \pmod{25}$. (K3, CO5)
9. Find the remainder when $(n^2 + n + 41)^2$ is divided by 12. (K3, CO5)
10. Compute the remainder when 3^{181} is divided by 17. (K3, CO5)
11. Compute the remainder when 3^{247} is divided by 25. (K3, CO5)
12. State and prove Chinese remainder theorem. (K3, CO5)
13. Solve Sun-Tsu's puzzle by CRT. (K3, CO5)
14. Find the least positive integer that leaves the remainder 1 when divided by 3, 2 when divided by 5 and 3 when divided by 7. (K3, CO5)
15. Solve the following system of congruences: $x \equiv 2 \pmod{3}$, $x \equiv 4 \pmod{5}$, $x \equiv 5 \pmod{7}$. (K3, CO5)
16. Solve the linear system $x \equiv 3 \pmod{7}$, $x \equiv 4 \pmod{9}$, $x \equiv 8 \pmod{11}$. (K3, CO5)
17. Solve the linear system $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$. (K3, CO5)
18. Solve the following system of linear congruences: $x + 3y \equiv 3 \pmod{11}$ and $5x + y \equiv 5 \pmod{11}$. (K3, CO5)
19. Solve the following system of linear congruences: $2x + 3y \equiv 4 \pmod{13}$ and $3x + 4y \equiv 5 \pmod{13}$. (K3, CO5)
20. Solve the following system of linear congruences: $5x + 6y \equiv 10 \pmod{13}$ and $6x - 7y \equiv 2 \pmod{13}$. (K3, CO5)

SUPPORTIVE ONLINE CERTIFICATION COURSES

The following NPTEL and Coursera courses are the supportive online certification courses for the subject Algebra and Number theory.

1. Introduction to Abstract Group Theory (NPTEL course)

<https://nptel.ac.in/courses/111/106/111106113/>

2. Introduction to Rings and Fields (NPTEL course)

<https://nptel.ac.in/courses/111/106/111106131/#>

3. Mathematical Foundations for Cryptography (Coursera online course)

<https://www.coursera.org/learn/mathematical-foundations-cryptography>

4. Number Theory (NPTEL course)

<https://nptel.ac.in/courses/111/103/111103020/>

5. Computational Number Theory & Cryptography (NPTEL course)

<https://nptel.ac.in/courses/106/103/106103015/>

6. A Basic course in Number Theory (NPTEL course)

<https://nptel.ac.in/courses/111/101/111101137/>

REAL TIME APPLICATIONS

View the lecture on YouTube: <https://youtu.be/c9dG59sEoHI>

The best known application of number theory is public key cryptography, such as the RSA algorithm. Public key cryptography in turn enables many technologies for granted such as the ability to make secure online transactions. In addition to cryptography, number theory has been applied to other areas, such as:

- Military information transmission
- Error correcting codes
- Numerical integration
- Computer Arithmetic
- Random and quasi-random number generation.

STUCOR APP

DOWNLOADED FROM STUCOR APP

CONTENT BEYOND THE SYLLABUS

The topic **Introduction to Vector space** is the content beyond the syllabus for the course Algebra and Number Theory.

View the lecture on YouTube:

<https://youtu.be/YshfZm99wjk>

Value Added Courses:

1. Mathematics for Machine Learning: Linear Algebra (Coursera online course)
<https://www.coursera.org/learn/linear-algebra-machine-learning>

2. Mathematical Foundations for Cryptography (Coursera online course)
<https://www.coursera.org/learn/mathematical-foundations-cryptography>

3. Cryptography and Network Security (NPTEL course)
<https://nptel.ac.in/courses/106/105/106105162/>

PRESCRIBED TEXT BOOKS & REFERENCE BOOKS

TEXTBOOKS:

1. Grimaldi, R.P and Ramana, B.V., "Discrete and Combinatorial Mathematics", Pearson Education, 5th Edition, New Delhi, 2007.
2. Koshy, T,—“Elementary Number Theory with Applications”, Elsevier Publications, New Delhi, 2002.

REFERENCES:

1. Lidl, R. and Pitz, G, "Applied Abstract Algebra", Springer Verlag, New Delhi, 2nd Edition, 2006.
2. Niven, I., Zuckerman.H.S., and Montgomery, H.L., —“An Introduction to Theory of Numbers”, John Wiley and Sons , Singapore, 2004.
3. San Ling and Chaoping Xing, —“Coding Theory – A first Course”, Cambridge Publications, Cambridge, 2004.

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

STUCOR APP

STUCOR APP

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

MA8551 - Algebra and Number Theory

Department: Mathematics

Batch/Year: CSE/ III

Created by: J.LEO AMALRAJ

Date: 24.09.2020

Table of Contents

Contents

1	Course Objectives	6
2	Pre-requisites	7
3	Syllabus	8
4	Course Outcomes	9
5	CO – PO/PSO Mapping	10
6	Lecture Plan	11
7	Activity Based Learning	12
8	Lecture Notes: Unit V Classical Theorems and Multiplicative Functions	13
9	Wilson’s Theorem	14
10	Fermat’s Little Theorem	17
11	Euler’s Theorem	20
12	Multiplicative Functions	23
13	Tau and Sigma Functions	28
14	Practice Quiz: Classical Theorems and Multiplicative Functions	34
15	Assignments: Unit V	35
16	Part A Questions and Answers: Unit V	36
17	Part B Questions: Unit V	39
18	Supportive online Certification courses	40
19	Real time Applications	41
20	Content beyond the Syllabus	42
21	Prescribed Text Books & Reference Books	43

COURSE OBJECTIVES

To introduce the basic notions of groups, rings, fields which will then be used to solve related problems.

To introduce and apply the concepts of rings, finite fields and polynomials.

To understand the basic concepts in number theory.

To examine the key questions in the Theory of Numbers.

To give an integrated approach to number theory and abstract algebra, and provide a firm basis for further reading and study in the subject.

PRE-REQUISITES

Pre-requisites for the subject Algebra and Number Theory is
MA8351 - Discrete Mathematics.

STUCOR APP

SYLLABUS**MA8551****ALGEBRA AND NUMBER THEORY****L T P C****4 0 0 4****UNIT I GROUPS AND RINGS****12**

Groups : Definition - Properties - Homomorphism - Isomorphism - Cyclic groups - Cosets - Lagrange's theorem. Rings: Definition - Sub rings - Integral domain - Field - Integer modulo n - Ring homomorphism.

UNIT II FINITE FIELDS AND POLYNOMIALS**12**

Rings - Polynomial rings - Irreducible polynomials over finite fields - Factorization of polynomials over finite fields.

UNIT III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS**12**

Division algorithm – Base - b representations – Number patterns – Prime and composite numbers – GCD – Euclidean algorithm – Fundamental theorem of arithmetic – LCM.

UNIT IV DIOPHANTINE EQUATIONS AND CONGRUENCES**12**

Linear Diophantine equations – Congruence's – Linear Congruence's - Applications: Divisibility tests - Modular exponentiation-Chinese remainder theorem – 2×2 linear systems.

UNIT V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS**12**

Wilson's theorem – Fermat's little theorem – Euler's theorem – Euler's Phi functions – Tau and Sigma functions.

TOTAL: 60 PERIODS

COURSE OUTCOMES

CO 1: Apply the basic notions of groups which will be used to solve group theory related problems.

CO 2: Apply the basic notions of rings, fields which will then be used to solve related problems.

CO 3: Demonstrate accurate and efficient use of advanced algebraic techniques such as finite fields and polynomials.

CO 4: Explain the fundamental concepts of number theory, advanced algebra and their role in modern mathematics.

CO 5: Demonstrate the number theory concepts by solving non - trivial related problems.

CO 6: Apply integrated approach to number theory and abstract algebra and prove simple theorems.

Course Out Comes	Program Outcomes												Program Specific Outcomes		
	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6	PO-7	PO-8	PO-9	PO-10	PO-11	PO-12	PSO-1	PSO-2	PSO-3
C01	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C02	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C03	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C04	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
C05	3	2	-	-	-	-	-	-	-	-	-	-	-	-	-
C06	3	2	1	-	-	-	-	-	-	-	-	-	1	-	-

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High)

UNIT V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS							
S. No	Topic	No. of Periods	Proposed date	Actual date	Pertaining CO(s)	Taxonomy level	Mode of Delivery
1	Wilson's theorem	2			CO6	K2	PPT
2	Fermat's little theorem	2			CO6	K2	PPT
3	Euler's theorem	2			CO6	K3	PPT
4	Euler's Phi functions	2			CO6	K2	PPT
5	Multiplicative function	2			CO6	K2	PPT
6	Tau and Sigma functions	2			CO6	K3	PPT

ACTIVITY BASED LEARNING

Activity based learning helps students express and embrace their curiosity. Once the students become curious, they tend to explore and learn by themselves. To evoke curiosity in students, Practice quiz is designed for all the five units.

Quiz – Unit V Classical Theorems And Multiplicative Functions

<https://quizizz.com/print/quiz/5f5337558eafbf001b0141a1>

Play game Quiz: Classical Theorems And Multiplicative Functions

<https://quizizz.com/join/quiz/5f5337558eafbf001b0141a1/start>

STUCOR APP

LECTURE NOTES**UNIT V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS**

In this chapter, we will discuss three important classical theorems 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.

Wilson's theorem – Fermat's little theorem – Euler's theorem – Euler's Phi functions – Tau and Sigma functions.

E- Book Reference:

<https://drive.google.com/file/d/1frQQxDZ4wWsS78NHZK6xQAZqfXofcIGQ/view?usp=drivesdk>

WILSON'S THEOREM

View this lecture on YouTube:

https://youtu.be/7Wn_C8iAEG0

Theorem: (Wilson's Theorem)

Statement: If p is a prime, then $(p - 1)! \equiv -1 \pmod{p}$.

Proof: We have to prove that $(p - 1)! \equiv -1 \pmod{p}$.

when $p = 2$, $(p - 1)! = (2 - 1)! = 1 \equiv -1 \pmod{2}$.

So, the theorem is true for when $p = 2$.

Now let $p > 2$ and let a be the positive integer such that $1 \leq a \leq p - 1$.

Since p is prime, and $a < p$, $(a, p) = 1$.

Then the congruence $ax \equiv 1 \pmod{p}$ has a solution a' congruence modulo p .

$\therefore aa' \equiv 1 \pmod{p}$, where $1 \leq a' \leq p - 1$.

a and a' are the inverses of each other modulo p .

If $a' = a$ then $a \cdot a \equiv 1 \pmod{p} \Rightarrow a^2 - 1 \equiv 0 \pmod{p}$

$\therefore p \mid (a^2 - 1) \Rightarrow p \mid (a + 1)(a - 1) \Rightarrow p \mid (a + 1)$ or $p \mid (a - 1)$.

Since $a < p$, if $p \mid (a + 1)$ then $a = p - 1$.

if $p \mid (a - 1)$ then $(a - 1) = 0 \Rightarrow a = 1$

$\therefore a = 1$ or $a = p - 1$ if $a' = a$

(i.e) 1 and $p - 1$ are their own inverses.

If $a' \neq a$, excluding 1 and $p - 1$ the remaining $p - 3$ residues.

$2, 3, 4, \dots, (p - 3), (p - 2)$ can be grouped into $\frac{p-3}{2}$ pairs of the type a, a' such that $aa' \equiv 1 \pmod{p}$.

Multiplying all these pairs together we get,

$$2 \cdot 3 \cdot 4 \cdots (p - 3)(p - 2) \equiv 1 \pmod{p}.$$

$$\Rightarrow 1 \cdot 2 \cdot 3 \cdots (p - 2)(p - 1) \equiv p - 1 \pmod{p}$$

$$(p - 1)! \equiv -1 \pmod{p}.$$

Hence the theorem.

Example 1: Find the remainder when $63!$ is divided by 71.

Solution: Given $p = 71$ is a prime, therefore by Wilson's theorem, we have

$$(p - 1)! \equiv -1 \pmod{p}.$$

$$\begin{aligned}(p-1)! &\equiv -1 \pmod{p} \\ (71-1)! &\equiv -1 \pmod{71} \\ 70! &\equiv -1 \pmod{71} \\ 70 \times 69 \times 68 \times 67 \times 66 \times 65 \times 64 \times 63! &\equiv -1 \pmod{71} \\ (-1)(-2)(-3)(-4)(-5)(-6)(-7)(63!) &\equiv -1 \pmod{71} \\ -5040 \times 63! &\equiv (-1) \pmod{71} \\ -70 \times 63! &\equiv -1 \pmod{71} \\ 63! &\equiv 70 \pmod{71} \\ \therefore \text{Remainder} &= 70.\end{aligned}$$

Example 2: Find the remainder when $14!$ is divided by 17 .

Solution: Given $p = 17$ is a prime, therefore by Wilson's theorem, we have $(p-1)! \equiv -1 \pmod{p}$

$$\begin{aligned}(17-1)! &\equiv -1 \pmod{17} \\ 16! &\equiv -1 \pmod{17} \\ 16 \times 15 \times 14! &\equiv -1 \pmod{17} \\ (-1)(-2)(14!) &\equiv -1 \pmod{17} \\ 2 \times 14! &\equiv (-1) \pmod{17} \\ 2 \times 14! &\equiv 16 \pmod{17} \\ 14! &\equiv 8 \pmod{17} \\ \Rightarrow \text{Remainder} &= 8.\end{aligned}$$

Example 3: Show that $18!+1$ is divisible by 437 .

Solution: Here $437 = 19 \times 23$, where 19 and 23 are primes. By Wilson's theorem, $(p-1)! + 1$ is divisible by a prime p .

19 is a prime number.

$$\therefore (19-1)! + 1 \text{ is divisible by } 19. \text{-----(1)}$$

i.e., $18! + 1$ is divisible by 19

23 is a prime number.

$$\therefore 22! + 1 \text{ is divisible by } 23. \text{-----(2)}$$

i.e., $22! + 1 \equiv 0 \pmod{23}$

$$\text{i.e., } 22 \times 21 \times 20 \times 19 \times 18! + 1 \equiv 0 \pmod{23} \text{-----(2)}$$

But, $22 \equiv -1(\text{mod } 23)$, $21 \equiv -2(\text{mod } 23)$, $20 \equiv -3(\text{mod } 23)$, and $19 \equiv -4(\text{mod } 23)$.

$$22 \times 21 \times 20 \times 19 \equiv -1 \times -2 \times -3 \times -4(\text{mod } 23)$$

$$22 \times 21 \times 20 \times 19 \equiv 24(\text{mod } 23)$$

$$22 \times 21 \times 20 \times 19 \equiv 1(\text{mod } 23), \text{ since } 24 \equiv 1(\text{mod } 23).$$

From equation (2), $22 \times 21 \times 20 \times 19 \times 18! + 1 \equiv 0(\text{mod } 23)$

$$1 \times 18! + 1 \equiv 0(\text{mod } 23)$$

Hence, $18! + 1 \equiv 0(\text{mod } 23)$.

i.e., $18! + 1$ is divisible by 23.

From equation (1), $18! + 1$ is divisible by 19.

$\therefore 18! + 1$ is divisible by 19 and 23.

$\therefore 18! + 1$ is divisible by 19×23 .

i.e., $18! + 1$ is divisible by 437.

Example 4: If p is a prime number and $p = 4m + 1$, where m is a positive integer, prove that $((2m)!)^2 + 1$ is divisible by p .

Solution: Since p is a prime number $(p - 1)! + 1 \equiv 0(\text{mod } p)$.

$$(4m + 1 - 1)! + 1 \equiv 0(\text{mod } p).$$

$$\Rightarrow (4m)! + 1 \equiv 0(\text{mod } p).$$

$$(4m)(4m - 1) \dots (2m + 1)(2m)! + 1 \equiv 0(\text{mod } p).$$

$$(4m)(4m - 1) \dots (4m - (2m - 1))(2m)! + 1 \equiv 0(\text{mod } p)$$

But $p = 4m + 1$, then $4m = p - 1$.

$$(p - 1)(p - 2) \dots [p - 1 - 2m + 1](2m)! + 1 \equiv 0(\text{mod } p) \text{-----(1)}$$

Since, $p - 1 \equiv -1(\text{mod } p)$

$$p - 2 \equiv -2(\text{mod } p)$$

$$\dots\dots\dots p - 2m \equiv (-2m)(\text{mod } p)$$

From (1), $(-1)(-2) \dots (-2m)(2m)! + 1 \equiv 0(\text{mod } p)$

$$(2m)!(2m)! + 1 \equiv 0(\text{mod } p)$$

$$\Rightarrow ((2m)!)^2 + 1 \equiv 0(\text{mod } p).$$

Hence, $((2m)!)^2 + 1$ is divisible by p .

FERMAT'S LITTLE THEOREM

View this lecture on YouTube:

<https://youtu.be/zHHpgyzFULE>

<https://youtu.be/tTuWmcikE0Q>

Theorem: (Fermat's Little Theorem)

Statement: If p is a prime and a is any integer not divisible by p , then $a^{p-1} \equiv 1 \pmod{p}$.

Proof : Given that, p is a prime and a is any integer not divisible by p . (i.e) $p \nmid a$.

When an integer divided by p the set of possible remainders are $0, 1, 2, 3, \dots, p-1$.

Consider the set of integers $1 \cdot a, 2 \cdot a, 3 \cdot a, \dots, (p-1)a$. ----- (1)

Suppose $ia \equiv 0 \pmod{p}$, then $p \mid ia$.

But $p \nmid a \therefore p \mid i$ which is impossible, since $i < p$.

$\therefore ia \not\equiv 0 \pmod{p}$ for $i = 1, 2, 3, \dots, p-1$.

So, no term of (1) is zero.

Next, we shall prove that all are distinct.

Suppose, $ia \equiv ja \pmod{p}$, where $1 \leq i, j \leq p-1$.

Then $(i-j)a \equiv 0 \pmod{p} \Rightarrow p \mid (i-j)a$.

Since $p \nmid a$, $p \mid (i-j)$ and $i, j < p \Rightarrow |i-j| < p$.

$\therefore i-j = 0 \Rightarrow i \equiv j \pmod{p}$.

$\therefore i \neq j \Rightarrow ia \neq ja$.

This means, no two of the integers in (1) are congruent modulo p .

Therefore, the least residues 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 .

$\therefore a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$

$\Rightarrow 1 \cdot 2 \cdot 3 \cdots (p-1) \cdot a^{p-1} \equiv (p-1)! \pmod{p}$

$\Rightarrow (p-1)! a^{p-1} \equiv (p-1)! \pmod{p}$.

$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$.

Hence the theorem.

Example 1: Find the remainder when 24^{1947} is divided by 17.

Solution: We know that $24 \equiv 7 \pmod{17}$.

By Fermat's theorem $a=7, p=17$ and $p \nmid a$. Therefore, $a^{p-1} \equiv 1 \pmod{p}$.

$$7^{17-1} \equiv 1 \pmod{17}$$

$$7^{16} \equiv 1 \pmod{17}$$

$$24^{1947} \equiv 7^{1947} \pmod{17}$$

$$24^{1947} \equiv (7^{16})^{121} \times (7^{11}) \pmod{17}$$

$$24^{1947} \equiv (1)^{121} \times (7^{11}) \pmod{17}$$

$$24^{1947} \equiv (7^{11}) \pmod{17}$$

$$24^{1947} \equiv 7^8 \times 7^3 \pmod{17}$$

$$24^{1947} \equiv (-1)(343) \pmod{17}$$

$$24^{1947} \equiv (-3) \pmod{17}$$

$$24^{1947} \equiv 14 \pmod{17}$$

The remainder is 14.

Example 2: Find the remainder when 30^{2020} is divided by 19.

Solution: We know that $30 \equiv 11 \pmod{19}$.

By Fermat's theorem, $a=11, p=19$ and $p \nmid a$. Therefore, $a^{p-1} \equiv 1 \pmod{p}$.

$$11^{18} \equiv 1 \pmod{19}.$$

$$30^{2020} \equiv 11^{2020} \pmod{19}.$$

$$30^{2020} \equiv (11^{18})^{112} 11^4 \pmod{19}$$

$$30^{2020} \equiv (1)^{112} 11^4 \pmod{19}.$$

$$30^{2020} \equiv 11^4 \pmod{19}.$$

$$\text{Consider } 11^2 = 121 \equiv 7 \pmod{19}.$$

$$11^2 \equiv 7 \pmod{19}.$$

$$11^4 \equiv (7)^2 \pmod{19}.$$

$$11^4 \equiv 49 \pmod{19}.$$

$$11^4 \equiv 11 \pmod{19}.$$

$$\text{But, } 30^{2020} \equiv 11^4 \pmod{19}.$$

$$30^{2020} \equiv 11 \pmod{19}.$$

Therefore, the remainder is 11.

Example 3:

If m and n are distinct primes then show that $m^{n-1} + n^{m-1} \equiv 1 \pmod{mn}$.

Solution: Since m and n are distinct primes, we have $n \nmid m$ and $m \nmid n$.

By Fermat's little theorem, we have

$$m^{n-1} \equiv 1 \pmod{n} \dots\dots\dots(1)$$

and $n^{m-1} \equiv 1 \pmod{m} \dots\dots\dots(2)$

Clearly $n^{m-1} \equiv 0 \pmod{n} \dots\dots\dots(3)$

and $m^{n-1} \equiv 0 \pmod{m} \dots\dots\dots(4)$

Adding equations (1) and (3) we have $m^{n-1} + n^{m-1} \equiv 1 \pmod{n} \dots\dots\dots(5)$

Adding equations (4) and (2) we have $m^{n-1} + n^{m-1} \equiv 1 \pmod{m} \dots\dots\dots(6)$

By known theorem namely,

If $a \equiv b \pmod{p}$ and $a \equiv b \pmod{q}$, where a, b are the integers and p, q are the distinct primes, then $a \equiv b \pmod{pq}$.

So, from the equations (5) and (6), we must have $m^{n-1} + n^{m-1} \equiv 1 \pmod{mn}$.

Example 4: Find the remainder when $13^{18} + 19^{12}$ is divided by 247.

Solution: We have $247 = 13 \times 19$.

Both 13 and 19 are primes.

By Fermat's little theorem, $13^{19-1} \equiv 1 \pmod{19}$.

$$\Rightarrow 13^{18} \equiv 1 \pmod{19} \dots\dots\dots(1)$$

Since $19 \equiv 0 \pmod{19}$, we have $19^{12} \equiv 0 \pmod{19} \dots\dots\dots(2)$

Adding equations (1) and (2), $13^{18} + 19^{12} \equiv 1 \pmod{19} \dots\dots\dots(A)$

Further, $13 \equiv 0 \pmod{13} \Rightarrow 13^{18} \equiv 0 \pmod{13} \dots\dots\dots(3)$

By Fermat's little theorem, $19^{13-1} \equiv 1 \pmod{13}$

$$\Rightarrow 19^{12} \equiv 1 \pmod{13} \dots\dots\dots(4)$$

Adding equations (3) and (4), $13^{18} + 19^{12} \equiv 1 \pmod{13} \dots\dots\dots(B)$

From equations (A) and (B), we must have $13^{18} + 19^{12} \equiv 1 \pmod{13 \times 19}$.

Therefore $13^{18} + 19^{12} \equiv 1 \pmod{247}$.

Hence the remainder is 1.

View this lecture on YouTube:

<https://youtu.be/nXL-PZmTPWw>

Euler's Phi Function

Definition: Let m be a positive integer. Then Euler's phi function $\varphi(m)$ denotes the number of positive integers $\leq m$ and relatively prime to m .

For example, Since $1 \leq 1$ and relatively prime to 1, $\therefore \varphi(1) = 1$.

$\varphi(2) = 1$, since 1 is the only integer ≤ 2 and relatively prime to 2.

Similarly, $\varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6$.

Lemma 1: A positive integer p is a prime if and only if $\varphi(p) = p - 1$.

Proof: Let p be a prime. Then there are $p - 1$ positive integers $\leq p$ and relatively prime to p ,

So, $\varphi(p) = p - 1$.

Conversely, let p be a positive integer such that $\varphi(p) = p - 1$.

Let $d|p$, where $1 < d < p$. Since there are exactly $p - 1$ positive integers $< p$, d is one of them, and $(d, p) \neq 1$, so $\varphi(p) < p - 1$, a contradiction.

Thus, p must be a prime.

Theorem 1: (Euler's Theorem)

Let m be a positive integer and a any integer with $(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof: Given m is a positive integer and a is any integer with $(a, m) = 1$.

Let $r_1, r_2, \dots, r_{\varphi(m)}$ be the least residues modulo m that are relatively prime to m .

Consider the products $ar_1, ar_2, \dots, ar_{\varphi(m)}$.

Since $(a, m) = 1$, $ar_i \not\equiv ar_j \pmod{m}$, if $i \neq j$.

We find, $ar_1, ar_2, \dots, ar_{\varphi(m)} \pmod{m}$ are distinct.

We now, prove $(ar_i, m) = 1$

Suppose $(ar_i, m) > 1$. Let p be a prime factor of (ar_i, m) .

Then $p \mid ar_i$ and $p \mid m$.

$\Rightarrow p \mid a$ or $p \mid r_i$ and $p \mid m$

If $p \mid r_i$ and $p \mid m$ then $(r_i, m) \neq 1$ which is a contradiction.

If $p \mid a$ and $p \mid m$ then $p \mid (a, m) \Rightarrow (a, m) \neq 1$ which is again a contradiction.

$\therefore (ar_i, m) = 1; i = 1, 2, \dots, \varphi(m)$.

\therefore The least residues $ar_1, ar_2, \dots, ar_{\varphi(m)} \pmod{m}$ are distinct and relatively prime to m .

$$\therefore ar_1 \cdot ar_2 \cdot \dots \cdot ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \pmod{m}.$$

$$\Rightarrow a^{\varphi(m)} r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \pmod{m}$$

Since $(r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}, m) = 1$,

we get $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Hence the proof.

Note: We can deduce Fermat's Theorem from Euler's Theorem. If p is prime then $\varphi(p) = p - 1$. $\therefore a^{p-1} \equiv 1 \pmod{p}$

Example 1: Find the remainder when 245^{1040} is divided by 18, using Euler's theorem.

Solution: By Euler's theorem, If $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Here, $a = 245$, $m = 18$ and $(245, 18) = 1$.

$$\therefore 245^{\varphi(18)} \equiv 1 \pmod{18}.$$

$$\Rightarrow 245^6 \equiv 1 \pmod{18}, \text{ since } \varphi(18) = 6.$$

$$\therefore (245^6)^{173} \equiv 1^{173} \pmod{18}$$

$$\Rightarrow 245^{1038} \equiv 1 \pmod{18}$$

$$\text{But, } 245^{1040} = 245^{1038} 245^2.$$

$$\text{Since } 245 \equiv 11 \pmod{18}.$$

$$\Rightarrow 245^2 \equiv 11^2 \pmod{18}$$

$$\Rightarrow 245^2 \equiv 121 \pmod{18} \equiv 13 \pmod{18}$$

$$\therefore 245^{1040} \equiv 1 \times 13 \pmod{18}$$

$$\therefore 245^{1040} \equiv 13 \pmod{18}.$$

$$\therefore 13 \text{ is the remainder when } 245^{1040} \text{ is divided by } 18.$$

Example 2: Using Euler's Theorem, find the remainder when 7^{1020} is divided by 15.

Solution: By Euler's theorem, if $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Here $a = 7, m = 15$ and $(7, 15) = 1$.

$$\therefore 7^{\phi(15)} \equiv 1 \pmod{15}$$

$$\Rightarrow 7^8 \equiv 1 \pmod{15}, \text{ since } \phi(15) = 8.$$

$$\therefore 7^{1020} \equiv 7^{(8 \times 127) + 4} \pmod{15}$$

$$\equiv (7^8)^{127} 7^4 \pmod{15}$$

$$\equiv (1)^{127} 7^4 \pmod{15}$$

$$\equiv 7^2 7^2 \pmod{15}$$

$$\equiv 49 \times 49 \pmod{15}$$

$$\equiv 4 \times 4 \pmod{15}$$

$$\equiv 16 \pmod{15}$$

$$\equiv 1 \pmod{15}.$$

$$\therefore 1 \text{ is the remainder when } 7^{1020} \text{ is divided by } 15.$$

View this lecture on YouTube:

<https://youtu.be/vz7ExhgMFy4>

Definition: A number-theoretic function f is multiplicative if $f(mn) = f(m)f(n)$, whenever m and n are relatively prime.

Theorem 1: Let f be a multiplicative function and n be a positive integer with canonical decomposition $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Then $f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_k^{e_k})$.

Proof: (by induction on the number of distinct primes in n)

If $k = 1$, i.e., $n = p_1^{e_1}$, then $f(n) = f(p_1^{e_1})$, so the theorem is trivially true.

Assume it is true for any integer with canonical decomposition consisting of k distinct primes: $f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_k^{e_k})$.

Let n be any integer with $k + 1$ distinct primes in its canonical decomposition, say, $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} p_{k+1}^{e_{k+1}}$.

Since $(p_1^{e_1}, p_2^{e_2}, \dots, p_k^{e_k}, p_{k+1}^{e_{k+1}}) = 1$ and f is multiplicative,

$$f(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} p_{k+1}^{e_{k+1}}) = f(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}) f(p_{k+1}^{e_{k+1}}) = f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_k^{e_k}) f(p_{k+1}^{e_{k+1}}).$$

(By inductive hypothesis)

Therefore, by induction, the result is true for any positive integer n .

Theorem 2: Let p be a prime and e any positive integer. Then $\varphi(p^e) = p^e - p^{e-1}$.

Proof: $\varphi(p^e)$ = number of positive integers $\leq p^e$ and relatively prime to it.

$\varphi(p^e) = (\text{number of positive integers } \leq p^e) - (\text{number of positive integers } \leq p^e \text{ and not relatively prime to it}).$

The number of positive integers $\leq p^e$ and not relatively prime to it, are the various multiples of p , namely $p, 2p, 3p, \dots (p^{e-1})p$ and they are p^{e-1} in number.

Thus, $\varphi(p^e) = p^e - p^{e-1}$.

Example 1: Compute $\varphi(8), \varphi(81)$ and $\varphi(15625)$.

Solution: $\varphi(8) = \varphi(2^3) = 2^3 - 2^{3-1} = 8 - 4 = 4$.

$\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$.

$\varphi(15625) = \varphi(5^6) = 5^6 - 5^5 = 12500$.

Theorem 3: The function φ is multiplicative.

Proof: Let m and n be positive integers such that $(m, n) = 1$.

To prove that $\varphi(mn) = \varphi(m)\varphi(n)$.

Arrange the integers through mn in m rows of n each:

1 $m+1$ $2m+1$... $(n-1)m+1$

2 $m+2$ $2m+2$... $(n-1)m+2$

3 $m+3$ $2m+3$... $(n-1)m+3$

· · · ·

· · · ·

r $m+r$ $2m+r$... $(n-1)m+r$

· · · ·

· · · ·

m $2m$ $3m$... nm

Let r be a positive integer $\leq m$ such that $(r, m) > 1$.

Now, we will show that no element of the r^{th} row in the array is relatively prime to mn .

Let $d = (r, m)$. Then $d|r$ and $d|m \Rightarrow d|km+r$, for $k \in \mathbb{Z}$.

i.e., d is a factor of every element in the r^{th} row is relatively prime to m and hence mn if $(m, n) > 1$.

In other words, the element in the array relatively prime to mn come from the r^{th} row only if $(r, m) = 1$.

Since $r < m$ and relatively prime to m , we find there are $\varphi(m)$ such integers r and hence $\varphi(m)$ such row.

Now, Let us consider the r^{th} row where $(r, m) = 1$.

The element in the r^{th} row are $r, m + r, 2m + r, \dots, (n - 1)m + r$.

When they are divided by n , the remainders are $0, 1, 2, \dots, n - 1$ in some order of which $\varphi(n)$ are relatively prime to n .

\therefore Exactly $\varphi(n)$ elements in the r^{th} row are relatively prime to n and hence to mn .

Thus there are $\varphi(m)$ rows containing positive integers relatively prime to mn and each row contain $\varphi(n)$ elements relatively prime to it.

Hence the array contains $\varphi(m)\varphi(n)$ positive integers $\leq mn$ and relatively prime to mn .

i.e., $\varphi(mn) = \varphi(m)\varphi(n)$.

Hence φ is multiplicative.

Example 2: Evaluate $\varphi(221)$ and $\varphi(1105)$.

Solution: $\varphi(221) = \varphi(13 \times 17) = \varphi(13)\varphi(17) = 12 \times 16 = 192$.

$\varphi(1105) = \varphi(5 \times 13 \times 17) = \varphi(5)\varphi(13)\varphi(17) = 4 \times 12 \times 16 = 728$.

Theorem 4: Let $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ be canonical decomposition of a positive integer n . Then $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$.

Proof: Given $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

Since φ is multiplicative.

$$\therefore \varphi(n) = \varphi(p_1^{e_1}) \varphi(p_2^{e_2}) \dots \varphi(p_k^{e_k})$$

$$= p_1^{e_1} \left(1 - \frac{1}{p_1}\right) p_2^{e_2} \left(1 - \frac{1}{p_2}\right) \dots p_k^{e_k} \left(1 - \frac{1}{p_k}\right), \text{ (since } \varphi(p^e) = p^e - p^{e-1} \text{)}$$

$$= p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Hence the proof.

Example 3: Compute $\varphi(666)$ and $\varphi(1976)$.

Solution: $666 = 2 \times 3^2 \times 37$.

$$\varphi(666) = 666 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{37}\right).$$

$$1976 = 2^3 \times 13 \times 19.$$

$$\varphi(1976) = 1976 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{13}\right) \left(1 - \frac{1}{19}\right).$$

Example 4: Compute $\varphi(600)$ and $\varphi(7!)$.

Solution: $600 = 2^3 \times 3 \times 5^2$.

$$\therefore \varphi(600) = \varphi(2^3) \varphi(3) \varphi(5^2)$$

$$= 2^3 \left(1 - \frac{1}{2}\right) \times 2 \times 5^2 \left(1 - \frac{1}{5}\right)$$

$$= 4 \times 2 \times 5 \times 4.$$

$$\varphi(600) = 160.$$

$$7! = 5040 = 2^4 \times 3^2 \times 5 \times 7.$$

$$\therefore \varphi(7!) = \varphi(2^4) \varphi(3^2) \varphi(5) \varphi(7)$$

$$= 2^4 \left(1 - \frac{1}{2}\right) 3^2 \left(1 - \frac{1}{3}\right) 4 \times 6$$

$$\varphi(7!) = 1152.$$

Theorem 5: Let n be a positive integer. Then $\sum_{d|n} \varphi(d) = n$.

Proof: We partition the set of positive integers 1 through n into various classes C_d as follows, where $d|n$.

Let m be a positive integer $\leq n$. Then m belongs to class C_d if and only if $(m, n) = d$.

i.e., if and only if $(m|d, n|d) = 1$.

The number of elements in C_d equals the number of positive integers $\leq n|d$ and relatively prime to it, namely, $\varphi(n|d)$; thus, each class C_d contains $\varphi(n|d)$ elements.

Since there is a class corresponding to every factor of d of n and every integer m belongs to exactly one class, the sum of the elements in the various classes must yield the total number of elements. i.e., $\sum_{d|n} \varphi(d) = n$.

But as d runs over the divisors of n , so does $n|d$.

Consequently, $\sum_{d|n} \varphi(n|d) = \sum_{d|n} \varphi(d)$, thus $\sum_{d|n} \varphi(d) = n$.

Example 5: For $n = 11^3 \times 5$, verify that $\sum_{d|n} \varphi(d) = n$.

Solution: Given $n = 11^3 \times 5 = 6655$.

The divisors of n are 1, 5, 11, 5×11 , 11^2 , 5×11^2 , 11^3 , 5×11^3 . Thus there are 8 divisors.

$$\sum_{d|n} \varphi(d) = \varphi(1) + \varphi(5) + \varphi(11) + \varphi(5 \times 11) + \varphi(11^2) + \varphi(5 \times 11^2) + \varphi(11^3) + \varphi(5 \times 11^3)$$

$$= 1 + 4 + 10 + 40 + 110 + 440 + 1210 + 4840$$

$$= 6655 = n.$$

Hence, $\sum_{d|n} \varphi(d) = n$.

TAU AND SIGMA FUNCTIONS

Definition: Let n be a positive integer. Then $\tau(n)$ denotes the number of positive divisors of n .

$$\tau(n) = \sum_{d|n} 1$$

Definition: Let n be a positive integer. Then $\sigma(n)$ denotes the sum of positive divisors of n .

$$\sigma(n) = \sum_{d|n} d$$

Theorem 1: If f is a number theoretic function which is multiplicative and for any positive integer n the function F given by

$$F(n) = \sum_{d|n} f(d)$$

is also multiplicative.

Proof: Given f is a multiplicative function.

\therefore for any two positive integer m and n which are relatively prime.

$$f(m.n) = f(m).f(n) \text{-----(1)}$$

Given

$$F(n) = \sum_{d|n} f(d)$$

\therefore

$$F(mn) = \sum_{d|mn} f(d)$$

Since $(m,n) = 1$, every positive divisor d of mn is the product of a unique pair of positive divisors d_1 of m and d_2 of n , where $(d_1, d_2) = 1$.

\therefore

$$\begin{aligned} F(mn) &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) && \text{[using (1)]} \\ &= \sum_{d_2|n} \left[\sum_{d_1|m} f(d_1) \right] f(d_2) && \text{[Being finite sum]} \\ &= \sum_{d_2|n} [F(m)] f(d_2) \end{aligned}$$

$$= F(m) \sum_{d_2|n} f(d_2)$$

$$\Rightarrow F(mn) = F(m) \cdot F(n)$$

Hence F is multiplicative.

As a particular case of this theorem we will prove that τ and σ are multiplicative.

Theorem 2: The tau and sigma functions are multiplicative.

Proof: The constant function $f(n) = 1$ is multiplicative, we have

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} 1 = \tau(n)$$

is multiplicative.

The function $g(n) = n$ is multiplicative. Therefore,

$$F(n) = \sum_{d|n} g(d) = \sum_{d|n} d = \sigma(n)$$

is multiplicative.

If $(m, n) = 1$, then

$$\tau(mn) = \tau(m)\tau(n)$$

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Theorem 3: Let p be any prime and k any positive integer. Then

$$\tau(p^k) = k + 1.$$

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

Proof: If p is prime then the divisor are 1 and p , so $\tau(p) = 2$.

Now the divisors of p^k are $1, p, p^2, \dots, p^k$ and there are $k + 1$ terms.

$$\tau(p^k) = k + 1$$

$$\sigma(p^k) = \text{sum of divisors of } p^k$$

$$= 1 + p + p^2 + \dots + p^k$$

$$= \frac{p^{k+1} - 1}{p - 1}$$

Since $p > 1$.

Theorem 4: Let $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$. Then

$$\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_r + 1).$$

$$\sigma(n) = \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \dots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1} \right)$$

Proof: Here the composite number n is given in the canonical decomposition form, that is, $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$. Hence the corresponding τ and σ functions are

$$\begin{aligned}\tau(n) &= \tau(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) \\ &= \tau(p_1^{k_1}) \tau(p_2^{k_2}) \dots \tau(p_r^{k_r}) \\ &= (k_1 + 1)(k_2 + 1) \dots (k_r + 1) \\ \sigma(n) &= \sigma(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) \\ &= \sigma(p_1^{k_1}) \sigma(p_2^{k_2}) \dots \sigma(p_r^{k_r}) \\ &= \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \dots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1} \right)\end{aligned}$$

Hence the proof.

Note : The tau and sigma functions are summarized as follows.

$$\begin{aligned}\tau(n) &= \begin{cases} 2 & n = p \text{ prime} \\ k + 1 & n = p^k \\ (k_1 + 1)(k_2 + 1) \dots (k_r + 1) & n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \end{cases} \\ \sigma(n) &= \begin{cases} p + 1 & n = p \text{ prime} \\ \frac{p^{k+1} - 1}{p - 1} & n = p^k \\ \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \dots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1} \right) & n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \end{cases}\end{aligned}$$

Example 1: Compute $\tau(23)$, $\tau(857)$ and $\tau(6491)$.

Solution: Here $n = 23, 857, 6491$. These are prime numbers.

If p is prime then $\tau(p) = 2$. Hence

$$\tau(23) = 2$$

$$\tau(857) = 2$$

$$\tau(6491) = 2.$$

Example 2: Compute $\tau(81)$, $\tau(2187)$ and $\tau(1024)$.

Solution: The τ function is defined as

$$\tau(n) = \begin{cases} 2 & n = p \text{ prime} \\ k + 1 & n = p^k \\ (k_1 + 1)(k_2 + 1) \dots (k_r + 1) & n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \end{cases}$$

Here $n = 81, 2187, 1024$ are of the form p^k . Hence

$$\tau(81) = \tau(3^4) = 4 + 1 = 5$$

$$\tau(2187) = \tau(3^7) = 7 + 1 = 8$$

$$\tau(1024) = \tau(2^{10}) = 10 + 1 = 11.$$

Example 3: Compute $\tau(36)$, $\tau(1560)$, $\tau(6120)$ and $\tau(44982)$.

Solution: The τ function is defined as

$$\tau(n) = \begin{cases} 2 & n = p \text{ prime} \\ k + 1 & n = p^k \\ (k_1 + 1)(k_2 + 1) \dots (k_r + 1) & n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \end{cases}$$

$$\begin{aligned} \tau(36) &= \tau(4 \times 9) = \tau(4)\tau(9) = \tau(2^2)\tau(3^2) \\ &= (2 + 1)(2 + 1) = 3 \times 3 \\ &= 9. \end{aligned}$$

$$\begin{aligned} \tau(1560) &= \tau(2^3 \times 3 \times 5 \times 13) \\ &= (3 + 1)(1 + 1)(1 + 1)(1 + 1) \\ &= 32. \end{aligned}$$

$$\begin{aligned} \tau(6120) &= \tau(2^3 \times 3^2 \times 5 \times 17) \\ &= (3 + 1)(2 + 1)(1 + 1)(1 + 1) \\ &= 48. \end{aligned}$$

$$\begin{aligned} \tau(44982) &= \tau(2 \times 3^3 \times 7^2 \times 17) \\ &= (1 + 1)(3 + 1)(2 + 1)(1 + 1) \\ &= 48. \end{aligned}$$

Example 4: Compute $\sigma(97)$, $\sigma(331)$ and $\sigma(4027)$.

Solution: If p is prime then $\sigma(p) = p + 1$.

Here $n = 97, 331, 4027$ are prime numbers.

$$\sigma(97) = 97 + 1 = 98$$

$$\sigma(331) = 331 + 1 = 332.$$

$$\sigma(4027) = 4027 + 1 = 4028.$$

Example 5: Compute $\sigma(81)$, $\sigma(2187)$ and $\sigma(1024)$.

Solution: The σ function is defined as

$$\sigma(n) = \begin{cases} p + 1 & n = p \text{ prime} \\ \frac{p^{k+1} - 1}{p - 1} & n = p^k \\ \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \dots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1} \right) & n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \end{cases}$$

Here, $n = 81, 2187, 1024$ are of the form p^k . Hence

$$\begin{aligned}\sigma(81) &= \sigma(3^4) = \frac{3^{4+1} - 1}{3 - 1} = \frac{3^5 - 1}{2} \\ &= \frac{243 - 1}{2} = 121\end{aligned}$$

$$\begin{aligned}\sigma(2187) &= \sigma(3^7) = \frac{3^{7+1} - 1}{3 - 1} = \frac{3^8 - 1}{2} \\ &= \frac{6561 - 1}{2} = 3280\end{aligned}$$

$$\begin{aligned}\sigma(1024) &= \sigma(2^{10}) = \frac{2^{10+1} - 1}{2 - 1} = 2^{11} - 1 \\ &= 2048 - 1 = 2047.\end{aligned}$$

Example 6: Compute $\sigma(36)$, $\sigma(1560)$, $\sigma(6120)$ and $\sigma(2187)$.

Solution: The σ function is defined as

$$\sigma(n) = \begin{cases} p+1 & n = p \text{ prime} \\ \frac{p^{k+1} - 1}{p - 1} & n = p^k \\ \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1}\right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1}\right) \dots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1}\right) & n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \end{cases}$$

Here, $n = 36, 1560, 6120, 2187$. Hence

$$\begin{aligned}\sigma(36) &= \sigma(4 \times 9) = \sigma(4)\sigma(9) = \sigma(2^2)\sigma(3^2) \\ &= \frac{2^{2+1} - 1}{2 - 1} \times \frac{3^{2+1} - 1}{3 - 1} \\ &= 7 \times 13 = 91\end{aligned}$$

$$\begin{aligned}\sigma(1560) &= \sigma(2^3 \times 3 \times 5 \times 13) \\ &= \frac{2^{3+1} - 1}{2 - 1} \times \frac{3^{1+1} - 1}{3 - 1} \times \frac{5^{1+1} - 1}{5 - 1} \times \frac{13^{1+1} - 1}{13 - 1} \\ &= 15 \times \frac{8}{2} \times \frac{24}{4} \times \frac{168}{12} \\ &= 15 \times 4 \times 6 \times 14 \\ &= 5040\end{aligned}$$

$$\begin{aligned}\sigma(6120) &= \sigma(2^3 \times 3^2 \times 5 \times 17) \\ &= \frac{2^{3+1} - 1}{2 - 1} \times \frac{3^{2+1} - 1}{3 - 1} \times \frac{5^{1+1} - 1}{5 - 1} \times \frac{17^{1+1} - 1}{17 - 1} \\ &= 15 \times 13 \times 6 \times 18 \\ &= 21060\end{aligned}$$

$$\sigma(2187) = \sigma(2 \times 3^3 \times 7^2 \times 17)$$

$$\begin{aligned}
&= \frac{2^{1+1} - 1}{2 - 1} \times \frac{3^{3+1} - 1}{3 - 1} \times \frac{7^{2+1} - 1}{7 - 1} \times \frac{17^{1+1} - 1}{17 - 1} \\
&= 3 \times \frac{80}{2} \times \frac{342}{6} \times \frac{288}{16} \\
&= 3 \times 40 \times 57 \times 18 \\
&= 123120.
\end{aligned}$$

Example 7: Let n be the product of a pair of twin prime p being the smallest of the two then show that $\sigma(n) = (p + 1)(p + 3)$.

Proof: Given that n is the product of a pair of twin prime, then

$$\begin{aligned}
n &= p(p + 2) \\
\sigma(n) &= \sigma[p(p + 2)] \\
&= \sigma(p)\sigma(p + 2) \\
&= (p + 1)(p + 2 + 1) \\
&= (p + 1)(p + 3).
\end{aligned}$$

Example 8: If p and q are twin primes with $p < q$ then show that

$$\sigma(q) = \sigma(p) + 2 \text{ or } \sigma(p + 2) = \sigma(p) + 2.$$

Proof: If p and q are twin primes with $p < q$ then $q = p + 2$.

If p is prime then $\sigma(p) = p + 1$. q is also prime then

$$\begin{aligned}
\sigma(q) &= \sigma(p + 2) \\
&= p + 2 + 1 = (p + 1) + 2 \\
&= \sigma(p) + 2.
\end{aligned}$$

ASSIGNMENTS: UNIT V

1. State and prove Fermat's little theorem.
2. State and prove Euler's theorem.
3. State and prove Wilson's theorem.
4. Show that Euler's phi function φ is multiplicative.
5. Find the remainder (a) when 13^{1302} is divided by 121. (b) when 193^{183} is divided by 19.
6. Using Euler's theorem find the remainder when 245^{100} is divided by 18.
7. Find the remainder when 24^{1947} is divided by 17.
8. If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is the canonical decomposition of a positive integer n , then derive a formula to calculate the Euler's phi function $\varphi(n)$ and compute $\varphi(6860)$.
9. Find the value of $\varphi(81)$ and $\varphi(303)$, where phi is the Euler phi function. What is the remainder you get when 192^{183} is divided by 19? Justify your answer.
10. Prove that $\varphi(2^{2k+1})$ is a square.
11. For $n = 11^3 \times 5$, verify that $\sum_{d|n} \varphi(d) = n$.
12. Let p_1, p_2, p_3 be distinct primes and $n = p_1 \cdot p_2 \cdot p_3$. Evaluate $\tau(n)$ and show that $\sigma(n) = (p_1 + 1)(p_2 + 1)(p_3 + 1)$.

PART A QUESTIONS AND ANSWERS: UNIT V

1. State Wilson's Theorem.

(K1, CO6)

Solution: If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.**2. State Fermat's Little Theorem.**

(K1, CO6)

Solution: If p is a prime and a is any integer not divisible by p , then $a^{p-1} \equiv 1 \pmod{p}$.**3. Find the remainder when 15^{1976} is divided by 23.**

(K2, CO6)

Solution: We know that $15 \equiv 15 \pmod{23}$.By Fermat's theorem $a=15, p=23$ and $p \nmid a$. Therefore, $a^{p-1} \equiv 1 \pmod{p}$.

$$15^{22} \equiv 1 \pmod{23}.$$

$$15^{1976} \equiv 15^{1975} \pmod{23}$$

$$15^{1976} \equiv (15^{22})^{89} \times 15^{18} \pmod{23}$$

$$15^{1976} \equiv 1^{89} \times 15^{18} \pmod{23}$$

$$15^{1976} \equiv 15^{18} \pmod{23}$$

$$15^{1976} \equiv (-5)^9 \pmod{23}$$

$$15^{1976} \equiv (-11) \pmod{23}$$

$$15^{1976} \equiv 12 \pmod{23}$$

$$\Rightarrow \text{Remainder} = 12.$$

4. State Euler's theorem.

(K1, CO6)

Solution: Let m be a positive integer and a any integer with $(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.**5. Define a multiplicative function and give an example.**

(K1, CO6)

Solution: A number-theoretic function f is multiplicative if $f(mn) = f(m) \cdot f(n)$, whenever m and n are relatively prime.

Example: Euler's Phi function

6. When $n = 2^k$, prove that $\phi(n) = \frac{n}{2}$.

(K2, CO6)

Solution: $\phi(n) = \phi(2^k) = 2^k \left(1 - \frac{1}{2}\right) = 2^k \frac{1}{2} = \frac{n}{2}$.

7. Prove that $\varphi(2^{2k+1})$ is a square.

(K2, CO6)

Solution: $\varphi(2^{2k+1}) = 2^{2k+1} \left(1 - \frac{1}{2}\right) = 2^{2k+1} \frac{1}{2} = 2^{2k} = (2^k)^2$.

8. Define Tau function.

(K1, CO6)

Solution: Let n be a positive integer. Then $\tau(n)$ denotes the number of positive divisors of n .

$$\tau(n) = \sum_{d|n} 1.$$

9. Define Sigma function.

(K1, CO6)

Solution: Let n be a positive integer. Then $\sigma(n)$ denotes the sum of positive divisors of n . $\sigma(n) = \sum_{d|n} d$.

10. Compute $\tau(23)$.

(K2, CO6)

Solution: Here $n = 23$ is a prime number.

If p is prime then $\tau(p) = 2$.

Hence $\tau(23) = 2$.

11. Compute $\tau(81)$.

(K2, CO6)

Solution: The τ function is defined as $\tau(n) =$

$$\begin{cases} 2 & n = p \text{ prime} \\ k + 1 & n = p^k \\ (k_1 + 1)(k_2 + 1) \dots (k_r + 1), & n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \end{cases}$$

Here $n = 81$ is of the form p^k .

Hence $\tau(81) = \tau(3^4) = 4 + 1 = 5$.

12. Compute $\sigma(36)$.

(K2, CO6)

Solution: The σ function is defined as

$$\sigma(n) = \begin{cases} p + 1 & n = p \text{ prime} \\ \frac{p^{k+1} - 1}{p - 1} & n = p^k \\ \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1}\right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1}\right) \dots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1}\right) & n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \end{cases}$$

Here, $n = 36, 1560, 6120, 2187$.

Hence $\sigma(36) = \sigma(4 \times 9) = \sigma(4)\sigma(9) = \sigma(2^2)\sigma(3^2)$

$$\begin{aligned} &= \frac{2^{2+1}-1}{2-1} \times \frac{3^{2+1}-1}{3-1} \\ &= 7 \times 9 = 91. \end{aligned}$$

13. Compute $\sigma(97)$.

(K2, CO6)

Solution: If p is prime then $\sigma(p) = p + 1$.

Here $n = 97$ is a prime numbers.

$$\sigma(97) = 97 + 1 = 98.$$

14. Evaluate $\varphi(221)$.

(K2, CO6)

Solution: $\varphi(221) = \varphi(13 \times 17) = \varphi(13)\varphi(17) = 12 \times 16 = 192$.

15. Compute $\varphi(81)$.

(K2, CO6)

Solution: $\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$.

16. Define Euler's Phi Function.

(K1, CO6)

Solution: Let m be a positive integer. Then Euler's phi function $\varphi(m)$ denotes the number of positive integers $\leq m$ and relatively prime to m .

17. If $\varphi(n) = n - 1$, then prove that the positive n is a prime. (K2, CO6)

Solution: Let n be a positive integer such that $\varphi(n) = n - 1$.

Let $d|n$, where $1 < d < n$. Since there are exactly $n - 1$ positive integers $< n$, d is one of them, and $(d, n) \neq 1$, so $\varphi(n) < n - 1$, a contradiction.

Thus, n must be a prime.

18. Let p be a prime and e any positive integer. Then prove that $\varphi(p^e) = p^e - p^{e-1}$. (K2, CO6)

Solution: $\varphi(p^e)$ = number of positive integers $\leq p^e$ and relatively prime to it.

$\varphi(p^e) = (\text{number of positive integers } \leq p^e) - (\text{number of positive integers } \leq p^e \text{ and not relatively prime to it}).$

The number of positive integers $\leq p^e$ and not relatively prime to it are the various multiples of p , namely $p, 2p, 3p, \dots, (p^{e-1})p$ and they are p^{e-1} in number.

Thus, $\varphi(p^e) = p^e - p^{e-1}$.

PART B QUESTIONS: UNIT V

1. State and prove Fermat's little theorem. (K2, CO6)
2. State and prove Euler's theorem. (K2, CO6)
3. State and prove Wilson's theorem. (K2, CO6)
4. State Wilson's theorem and verify the theorem for $p = 7$. (K2, CO6)
5. Show that Euler's phi function φ is multiplicative. (K2, CO6)
6. Find the remainder (a) when 13^{1302} is divided by 121. (b) when 193^{183} is divided by 19. (K2, CO6)
7. Using Euler's theorem find the remainder when 245^{100} is divided by 18. (K2, CO6)
8. Find the remainder when 24^{1947} is divided by 17. (K2, CO6)
9. If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is the canonical decomposition of a positive integer n , then derive a formula to calculate the Euler's phi function $\varphi(n)$ and compute $\varphi(6860)$. (K2, CO6)
10. Find the value of $\varphi(81)$ and $\varphi(303)$, where phi is the Euler phi function. What is the remainder you get when 192^{183} is divided by 19? Justify your answer. (K2, CO6)
11. Prove that $\varphi(2^{2k+1})$ is a square. (K2, CO6)
12. If p is a prime and e any positive integer then prove that $\varphi(p^e) = p^e - p^{e-1}$. Hence compute $\varphi(81)$. (K2, CO6)
13. If p is a prime and e any positive integer then prove that $\varphi(p^e) = p^e - p^{e-1}$. Also show that $\varphi(n) = n/2$, when $n = 2^k$. (K2, CO6)
14. For $n = 11^3 \times 5$, verify that $\sum_{d|n} \varphi(d) = n$. (K2, CO6)
15. Using Euler's theorem, find the value of $100^{422} \pmod{49}$. Also for $n = 7^2 \times 3$, find the value of $\sum_{d|n} \varphi(d)$. (K2, CO6)
16. Let p_1, p_2, p_3 be distinct primes and $n = p_1 \cdot p_2 \cdot p_3$. Evaluate $\tau(n)$ and show that $\sigma(n) = (p_1 + 1)(p_2 + 1)(p_3 + 1)$. (K2, CO6)