UNIT-1

① Find the inverse of 3 under the binary operation $*$ defined in R by $a * b = \frac{ab}{3}$

Soln Given $a * b = \frac{ab}{3}$

Let 'e' be the identity element in $(R, *)$

Then $a * e = a$

$\Rightarrow \frac{ae}{3} = a$

$\Rightarrow \boxed{e = 3}$

To find a^{-1}: $a * a^{-1} = e$

$\frac{a \cdot a^{-1}}{3} = 3$

$\boxed{a^{-1} = \frac{9}{a}}$

Checking: $a * a^{-1} = a * \frac{9}{a} = \frac{a\frac{9}{a}}{3} = 3$ (identity in $(R, *)$)

Also $a^{-1} * a = 3$ (identity in $(R, *)$)

② How many proper zero divisors are there in Z_{17}.

Soln The number of zero divisors in $Z_n = n - [1 + \phi(n)]$

$\phi(17) = 16$.

∴ The number of zero divisors in Z_{17} $= 17 - [1 + 16]$

$= 0$.

Alter: $(Z_{17}, \oplus, \odot)$ is a field.

By dfn a field has no zero divisors.

∴ No. of zero divisors in $Z_{17} = 0$.

(5) Prove or disprove : Every field is an Integral domain.

Proof Every field is an Integral domain.

Let $(F, +, \cdot)$ be a field.

To prove : $(F, +, \cdot)$ is an Integral domain.

Let $a, b \in F$ with $a \cdot b = 0 \longrightarrow (1)$

Since F is a field, $a^{-1} \in F$.

Operating a^{-1} both sides on (1)

$$a^{-1} a b = a^{-1} 0$$

$$b = 0$$

$\Rightarrow$ F is an Integral domain.

(4) Consider a Set G together with a well defined binary operation $*$ on it. Let $e_1, e_2 \in (G, *)$ such that $e_1 * a = a * e_1 = a$ and $e_2 * a = a * e_2 = a \quad \forall a \in G$.

What is the relation between e_1 and e_2? Justify your answer.

Soln

$$e_1 * a = a * e_1 = a$$

$$e_2 * a = a * e_2 = a$$

$\Rightarrow e_1 = e_2$ (∵ Identities element is unique)

(5) Define Integral domain : A commutative ring with identity having no zero divisor is called an Integral domain.

(6) Define Field : A commutative ring with identity and every non zero element has a multiplicative inverse is a field.

(7) Define Zero divisor : Let $(R, +, \cdot)$ be a commutative ring.

Let $a, b \in R$ with $a \cdot b = 0$

Then if either $a = 0$ or $b = 0$ then a and b are not zero divisors. Otherwise they are zero divisors.

i) If $a \neq 0$ and $b \neq 0$ but $a \cdot b = 0$.

(8) Define Isomorphism and homomorphism between Rings.

Let $(R_1, +, \cdot)$ and $(R_2, +, \cdot)$ be two rings.

Define a function $f : R_1 \to R_2$ by $f(x) = y$.

Then f is a homomorphism if

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

(ii) $f(xy) = f(x) \cdot f(y)$

A 1–1 homomorphism onto R_2 is an isomorphism.

(9) State Lagrange's Theorem: Let $(G, *)$ be any finite group of order n and $(H, *)$ be a subgroup of order m of $(G, *)$. Then m divides n.

(10) Is converse of Lagranges theorem TRUE?

Converse of Lagrange's theorem may not be TRUE.

Example Let G be a group of permutation with 3 symbols.

Then $G = S_3$ constains 6 elements.

3 divides 6

But S_3 cannot have a subgroup of order 3.

(11) Is $(N, +)$ is a group.

Soln $(N, +)$ is not a group.

Since any element does not have an inverse in N.

12) Show that $\mathbb{Z}$ is not a group under '.'

Soln The elements other than 1 and -1 do not have inverse in $\mathbb{Z}$. $\therefore (\mathbb{Z}, \cdot)$ is not a group.

13) Define Subgroup Test

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

14) Define cyclic group with example

Let G be a group and $a \in G$. Then G is cyclic if $\langle a \rangle = G$.

Example: $\{1, -1, i, -i\}$ is a cyclic group under the multiplication.

Since i and $-i$ are generators of G.

15) What is the condition that a element 'r' $\in (Z_n, \oplus, \odot)$ is a unit ?

If $\gcd(r, n) = 1$ then r is a unit in $(Z_n, \oplus, \odot)$

Example: In $(Z_3, \oplus, \odot)$, 2 is a unit

($\because \gcd(2, 3) = 1$)

UNIT-2

① Suppose $p(x)$ and $q(x)$ are two polynomials each of degree m and n respectively over the ring of integers modulo 8. The degree of the polynomial $p(x).q(x)$ is $m+n$. Comment On this statement.

Soln Take $p(x) = 2x \rightarrow$ degree 1

$q(x) = 4x^2 \rightarrow$ degree 2

Then $p(x).q(x) = 2x.4x^2$

$= 0$ zero polynomial.

$\therefore \deg(p(x).q(x))$ need not be equal to $m+n$

② What are the factors of x^2+2x+6 in $\frac{Z}{7}[x]$.

Soln 2 and 3 are roots of x^2+2x+6 in $Z_7[x]$.

$\therefore x^2+2x+6 = (x-2)(x-3)$

③ Give an example of a polynomial that is irreducible in $Q[x]$ and reducible in $C[x]$.

Soln x^2+1 is irreducible in $Q[x]$ but reducible in $C[x]$

④ If $f(x) = 2x^4+5x^2+2$, $g(x) = 6x^2+4$ then determine $f(x).g(x)$ in $\frac{Z}{7}[x]$..

Soln $f(x).g(x) = (2x^4+5x^2+2).(6x^2+4)$

$= 5x^6+3x^4+4x^2+1$

(5) Define Divisor: Let F be a field. The non-zero polynomial $f(x) \in F[x]$ is called a divisor of $g(x)$ if $\exists\ q(x) \in F[x]$ such that $f(x) \cdot q(x) = g(x)$.

(6) State Division algorithm: Let $f(x), g(x) \in F[x]$ with $f(x)$ is a non zero polynomial. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x) \cdot f(x) + r(x) \quad \text{where } r(x) = 0 \text{ or } \deg r(x) < \deg f(x).$$

(7) State Remainder thm: For $f(x) \in F[x]$ and $a \in F$ the remainder is $f(a)$ when $f(x)$ is divided by $(x-a)$

(8) State Factor theorem: If $f(x) \in F[x]$ and $a \in F$ then $(x-a)$ is a factor of $f(x)$ iff a is a root of $f(x)$.

(9) Define monic polynomial: A polynomial $f(x) \in F[x]$ is called monic if its leading coefficient is 1.

Example: $x^4 + 3x^2 + 2x + 100$ is monic polynomial.

(10) Define Characteristic of ring:

Let $(R, +, \cdot)$ be a ring. If there is a least positive integer n such that $nr = 0\ \forall r \in R$ then we say that $(R, +, \cdot)$ has characteristic n and we write $\text{char}(R) = n$.

When no such integer exists, R is said to have characteristic zero.

(11) What is the characteristic of $(Z_3, \oplus, \odot)$

Soln

$\text{Char}(Z_3) = 3$

Since, $Z_3 = \{0, 1, 2\}$.

$3.(0) = 0 \oplus 0 \oplus 0 = 0$

$3(1) = 1 \oplus 1 \oplus 1 = 0$

$3(2) = 2 \oplus 2 \oplus 2 = 0$.

(12) What is the $\text{char}(F)$ where F is a field.

Soln

$\text{Char}(F)$ is a prime number when F is a field.

(13) What is the order of a ring ?

The order of a ring = number of elements in that ring.

(14) What is the order of a field ?

The order of a field is p^t where p is a prime number and $t \in Z^+$.

(15) What are the roots of $x^2 + 3x + 2$ in $Z_6[x]$.

Soln 1, 2, 5 are roots.

$\because \quad 1^2 + 3(1) + 2 \equiv 0$

$2^2 + 3(2) + 2 \equiv 0$

$5^2 + 3(5) + 2 \equiv 0$.

UNIT-3

① Determine whether 1601 is a prime.

Soln $\sqrt{1601} = 40.012.$

Prime numbers which are $\leq \sqrt{1601}$ listed by

2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

None of the above listed primes divides 1601.

∴ 1601 is a prime number.

② Find the six consecutive integers that are composites.

Soln $n = 6.$

∴ $(6+1)! + 2$, $(6+1)! + 3$, $(6+1)! + 4$, $(6+1)! + 5$, $(6+1)! + 6$, $(6+1)! + 7$ are required number.

v) 5042, 5043, 5044, 5045, 5046, 5047 are consecutive integers which are composites.

③ Find gcd of 161 and 28.

Soln

Divide 161 by 28

$$28 \overline{)\,161\,(5} \quad 140 \quad 21$$

Divide 28 by 21

$$21 \overline{)\,28\,(1} \quad 21 \quad 7$$

Divide 21 by 7

$$7 \overline{)\,21\,(3} \quad 21 \quad 0$$

∴ Last non zero remainder $= 7 = \gcd(161, 28)$

④ State pigeonhole principle: If m pigeons are placed into n pigeonhole where $m > n$ then atleast two pigeons must occupy the same pigeonhole.

⑤ Write the general formula for finding n consecutive integers where n is any +ve integer.

Soln

$(n+1)! + 2,\ (n+1)! + 3,\ (n+1)! + 4,\ \ldots,\ (n+1)! + (n+1)$

⑥ State division algorithm: Let a be any integer and 'b' a +ve integer. Then ∃ unique integers q and r such that

$a = bq + r$ where $0 \leq r < b$

Here b → divisor
q → quotient
r → remainder

⑦ Find the quotient 'q' and the remainder 'r' when 907 is divided by 15.

Soln

$$\begin{array}{r|l} & 13 \\ \hline 15 & 907 \\ & 195 \\ \hline & 12 \end{array}$$

∴ Quotient $= q = 13$

Remainder $= r = 12$

⑧ Prove if a/b and a/c then $a/(\alpha b + \beta c)$.

Soln

$a/b \Rightarrow b = aq_1$

$a/c \Rightarrow c = aq_2$

$\alpha b + \beta c = \alpha \cdot aq_1 + \beta aq_2 = a(\alpha q_1 + \beta q_2)$

$\Rightarrow a/(\alpha b + \beta c)$.

(9) Prove the Transitive property of divisibility.

Soln

Transitive property: If a/b and b/c then a/c.

$a/b \Rightarrow b = aq_1 \longrightarrow (1)$

$b/c \Rightarrow c = bq_2 \longrightarrow (2)$.

Sub (1) in (2)

$c = aq_1q_2$

$\Rightarrow a/c$.

(10) Express 3014 in base eight.

Soln

8	3014
8	376 — 6
8	47 — 0
	5 — 7.

$\therefore 3014 = (5706)_8$.

(11) Define Greatest common Divisor

Let a and b be integers not both zero.

A positive d is called the gcd of (a, b) if it satisfies the following.

(i) d/a and d/b

(ii) Suppose another m/a and m/b then $m \leq d$.

(12) Define Relatively prime: Two positive integers a and b are relatively prime if their gcd is 1.

(13) State Euler theorem: The gcd of the positive integers a and b is a linear combination of a and b

(14) State Euclids theorem: If a and b are relatively prime and if $a|bc$ then $a|c$.

(15) State Fundamental theorem of Arithmetic:

Every integer $n \geq 2$ is either a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of factors.

(16) Write the canonical decomposition of 2520.

Soln

	2520
2	1260
2	630
2	315
3	105
3	35
5	7

$\therefore 2520 = 2^3 \times 3^2 \times 5^1 \times 7^1$ is required canonical decomposition

UNIT – 4

① When does the linear congruence $ax \equiv b \pmod{m}$ has a unique soln.

Soln If $\gcd(a, m) = 1$ then $ax \equiv b \pmod{m}$ has a unique soln.

② Find the remainder when 4^{117} is divided by 15

Soln

$$4^2 \equiv 1 \pmod{15}$$

$$\Rightarrow (4^2)^{58} \equiv (1)^{58} \pmod{15}$$

$$\Rightarrow 4^{116} \equiv 1 \pmod{15}$$

$$\Rightarrow 4^{116} \cdot 4 \equiv 1(4) \pmod{15}$$

$$\Rightarrow 4^{117} \equiv 4 \pmod{15}.$$

$\therefore$ Required remainder is '4'

③ Find the value of x such that $2^8 \equiv x \pmod{7}$.

Soln We have to find the remainder when 2^8 is divided by 7.

$2^8 = 256$.

Divide 256 by 7.

$$\begin{array}{r} 36 \\ 7\overline{)256} \\ 21 \\ \hline 46 \\ 42 \\ \hline 4 \end{array}$$

$\therefore 2^8 \equiv 4 \pmod{7}$.

$\therefore \boxed{x = 4}$

④ Is it possible to find the remainder when $1! + 2! + 3! + \cdots + 100!$ is divided by 15.

Soln

$1! \equiv 1 \pmod{15}$

$2! \equiv 2 \pmod{15}$

$3! \equiv 6 \pmod{15}$

$4! \equiv 9 \pmod{15}$

$5! \equiv 0 \pmod{15}$

$6! \equiv 0 \pmod{15}$

$\vdots$

$(100)! \equiv 0 \pmod{15}$

Adding, $1! + 2! + 3! + \cdots + 100! \equiv 18 \pmod{15}$

$18 \equiv 3 \pmod{15}$.

$\therefore$ By Transitive property $1! + 2! + \cdots + 100! \equiv 3 \pmod{15}$.

$\therefore$ Required remainder is 3.

⑤ What is the remainder when 3^{31} is divided by 7.

Soln

$3^6 \equiv 1 \pmod{7}$

$\Rightarrow (3^6)^5 \equiv 1^5 \pmod{7}$

$\Rightarrow 3^{30} \equiv 1 \pmod{7}$

$\Rightarrow 3^{30} \cdot 3 = 1 \cdot 3 \pmod{7}$

$\Rightarrow 3^{31} \equiv 3 \pmod{7}$

$\therefore$ 3 is the required remainder.

⑥ Define Linear diophantine eqn: A linear diophantine eqn in two variables x and y is an eqn of the form

$ax + by = c$

Here a, b, c are integers with a & b are not both zero.

⑦ When does a linear diophantine eqn has a soln?

The linear diophantine eqn $ax+by=c$ has a soln iff d/c where $d=\gcd(a,b)$.

⑧ Determine the LDE $24x+52y=102$ is solvable?

Soln $\gcd(24,52)=4$

$4 \nmid 102$

∴ The given LDE is not solvable.

⑨ Define congruence modulo m.

Let m be a +ve integer.

An integer 'a' is congruent to an integer b modulo m if $m/(a-b)$

In symbol $a \equiv b \pmod m$

Example $23 \equiv 3 \pmod 4$

⑩ State Transitive property of congruence

Soln If $a \equiv b \pmod m$ and

$b \equiv c \pmod m$

then $a \equiv c \pmod m$

UNIT-5

① State Wilson's theorem: If p is a prime number then $(p-1)! \equiv -1 \pmod{p}$

② Find the remainder when $15!$ is divided by 17.

Soln 17 is a prime.

$\therefore (17-1)! \equiv -1 \pmod{17}$ (By Wilson's thm)

$16! \equiv -1 \pmod{17}$.

$16 \times 15! \equiv -1 \pmod{17}$. $\longrightarrow$ ①

$-1 \equiv 16 \pmod{17}$ $\longrightarrow$ ②

$\Rightarrow 16 \times 15! \equiv 16 \pmod{17}$

$\Rightarrow 15! \equiv 1 \pmod{17}$.

$\therefore$ Required remainder $= 1$

③ Define multiplicative function:

A number – theoritic function f is multiplicative if $f(mn) = f(m) \cdot f(n)$ whenever m and n are relatively prime.

④ Define Euler phi function:

Let m be a +ve integer. Then euler phi function denotes the number of positive integers $\leq m$ and relatively prime to m. It is denoted by $\phi(m)$.

(5) Define Tau function: Let m be a +ve integer. Then $\tau(m)$ denote the number of positive divisors of m.

(6) Define Sigma Function: Let m be a +ve integer. Then $\sigma(m)$ denote the sum of positive divisors of m

$$\sigma(m) = \sum_{d/m} d$$

(7) Write the Formula for $\phi(m)$, $\tau(m)$ and $\sigma(m)$ where $m = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$ is the canonical decomposition of m. $(m>0)$

Soln

$$\phi(m) = m\left(1-\tfrac{1}{p_1}\right) \times \left(1-\tfrac{1}{p_2}\right) \times \cdots \times \left(1-\tfrac{1}{p_k}\right)$$

$$\tau(m) = (a_1+1) \times (a_2+1) \times \cdots \times (a_k+1)$$

$$\sigma(m) = \left(\frac{p_1^{a_1+1}-1}{p_1-1}\right) \times \left(\frac{p_2^{a_2+1}-1}{p_2-1}\right) \times \cdots \times \left(\frac{p_k^{a_k+1}-1}{p_k-1}\right)$$

(8) If $n = 2^k$ then prove that Euler phi function of n is $\frac{n}{2}$.

Soln Given $n = 2^k$.

$$\phi(n) = n\left(1-\tfrac{1}{2}\right)$$
$$= 2^k\left(1-\tfrac{1}{2}\right) = \frac{2^k}{2}$$
$$= \frac{n}{2} \quad (\because 2^k = n)$$

(9) Find $\sigma(28)$ and $\tau(18)$

Soln $18 = 2^1 \times 3^2$

$\Rightarrow \tau(18) = (1+1) \times (2+1)$
$= 2 \times 3$
$= 6.$

$28 = 2^2 \times 7^1$

$$\sigma(28) = \left(\frac{2^3-1}{2-1}\right) \times \left(\frac{7^2-1}{7-1}\right)$$
$$= \tfrac{7}{1} \times \tfrac{48}{6}$$
$$= 56$$

(10) State Euler Theorem: Let m be a +ve integer, and 'a' be any integer with gcd (a,m) = 1 then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

(11) Fermat's Little Theorem: Let p be a prime number and a be any integer such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$

(12) If gcd (a,35) = 1 then show that $a^{24} \equiv 1 \pmod{35}$

Soln

$$35 = 5 \times 7.$$

$$\therefore \phi(35) = 35\left(1-\tfrac{1}{5}\right) \times \left(1-\tfrac{1}{7}\right) = 35 \times \tfrac{4}{5} \times \tfrac{6}{7}$$

$$\phi(35) = 24$$

$\therefore$ By Euler's thm $a^{24} \equiv 1 \pmod{35}$.

(13) Find $\tau(6120)$

Soln

2	6120
2	3060
2	1530
3	765
3	255
5	85
	17

$$\therefore 6120 = 2^3 \times 3^2 \times 5^1 \times 17^1$$

$$\tau(6120) = (3+1)(2+1)(1+1)(1+1)$$

$$= 4 \times 3 \times 2 \times 2$$

$$= 48$$