Unit – I (Groups and Rings)

• Part A Questions

1. Find the identity element under * defined by \( a * b = \frac{ab}{2} \), for all \( a, b \in R \).

2. Why is the set of integers not a group under subtraction?

3. Give any two properties of cyclic group.

4. Define a group homomorphism with an example.

5. Obtain the generators of the cyclic group \( (Z_7^*, \cdot) \).

6. Show that the identity element in a group is unique.

7. Prove that a group \( G \) is abelian if and only if \( (ab)^2 = a^2b^2 \) for all \( a, b \) in \( G \).

8. Why is the set of integers not a group under subtraction?

9. Prove that a group is abelian if and only if \( (ab)^{-1} = a^{-1}b^{-1} \).

10. Give any two properties of cyclic group.

11. Define a left coset with an example.

12. What do you mean by a subgroup? Find a subgroup of \( G = (Z_6, +) \).

• Part B Questions

1. 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. (N/D 2019)
2. Let $G = \{ q \in Q \mid q \neq -1 \}$. Define the binary operation $\ast$ by $x \ast y = x + y + xy$. Prove that $(G, \ast)$ is an abelian group.

3. Let $G$ be a group with subgroups $H$ and $K$, if $|G| = 660$, $|K| = 66$ and $K \subset H \subset G$. What are the possible values for $|H|$? (N/D 2019)

4. Prove that every group of prime order is cyclic.

5. Let $f : G \to H$ be a group homomorphism onto $H$. If $G$ is abelian then prove that $H$ is abelian.

6. Show that $(M, \ast)$ is an abelian group where $M = \{ A, A^2, A^3, A^4 \}$ with $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\ast$ is the ordinary matrix multiplication. Further prove that $(M, \ast)$ is isomorphic to the abelian group $(G, \ast)$ where $G = \{ 1, -1, i, -i \}$ and $\ast$ is the ordinary multiplication.

7. Prove that every subgroup of a cyclic group is cyclic.

8. Prove that $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ forms an abelian group under matrix multiplication. (N/D 2015)

Textbook Page No.: 4.2

9. Show that $M_2$, the set of all $2 \times 2$ non-singular matrices over $R$ is a group under usual matrix multiplication. Is it abelian? (A/M 2015)

Textbook Page No.: 4.3

10. If $(G, \ast)$ is an abelian group, show that $(a \ast b)^2 = a^2 \ast b^2$. (N/D 2010)

Textbook Page No.: 4.4

11. In any group $(G, \ast)$, show that $(a \ast b)^{-1} = b^{-1} \ast a^{-1}$, for all $a, b \in G$. (M/J 2016)

Textbook Page No.: 4.5

12. Show that $(Q, \ast)$ is an abelian group, where $\ast$ is defined by $a \ast b = \frac{ab}{2}$, $\forall a, b \in Q^+$. (N/D 2016), (A/M 2018)

Textbook Page No.: 4.6

13. If $\ast$ is a binary operation on the set $R$ of real numbers defined by $a \ast b = a + b + 2ab$,
(1) Find $\langle R, * \rangle$ is a semi group

(2) Find the identity element if it exists

(3) Which elements has inverse and what are they? (A/M 2011)

Textbook Page No.: 4.8

14. If $S = N \times N$, the set of ordered pairs of positive integers with the operation * defined by $(a, b) * (c, d) = (ad + bc, bd)$ and if $f : (S, *) \rightarrow (\mathbb{Q}, +)$ is defined by $f(a, b) = \frac{a}{b}$, show that $f$ is a semigroup homomorphism. (A/M 2015)

Textbook Page No.: 4.11

15. Find the left cosets of the subgroup $H = \{[0], [3]\}$ of the group $\langle \mathbb{Z}_6, +_6 \rangle$.

Textbook Page No.: 4.12 (M/J 2014)


Textbook Page No.: 4.13

17. Prove that the order of a subgroup of a finite group divides the order of the group.

Textbook Page No.: 4.13 (N/D 2011), (M/J 2013), (A/M 2018)

18. Find all the subgroups of $\langle \mathbb{Z}_9, +_9 \rangle$. (M/J 2014)

Textbook Page No.: 4.15

19. Prove the theorem: Let $\langle G, * \rangle$ be a finite cyclic group generated by an element $a \in G$. If $G$ is of order $n$, that is, $|G| = n$, then $a^n = e$, so that $G = \{a, a^2, a^3, ..., a^n = e\}$. Further more $n$ is a least positive integer for which $a^n = e$. (N/D 2011)

Textbook Page No.: 4.16

20. Prove that the intersection of two subgroups of a group $G$ is again a subgroup of $G$. (N/D 2015)
21. Prove that intersection of any two subgroups of a group \((G, \ast)\) is again a subgroup of \((G, \ast)\).  
   (N/D 2013)

   Textbook Page No.: 4.16

22. Prove that intersection of two normal subgroups of a group \((G, \ast)\) is a normal subgroup of a group \((G, \ast)\).  
   (M/J 2013), (N/D 2016), (A/M 2018)

   Textbook Page No.: 4.18

23. Show that the union of two subgroups of a group \(G\) is a subgroup of \(G\) if and only if one is contained in the other.  
   (A/M 2015)

24. Prove that every cyclic group is an abelian group.  
   (N/D 2013)

   Textbook Page No.: 4.18

25. Prove that every subgroup of a cyclic group is cyclic.  
   (M/J 2016), (A/M 2017)

   Textbook Page No.: 4.19

26. Find \([100]^{-1}\) in \(\mathbb{Z}_{1000}\).  
   (N/D 2019)

27. Prove that the necessary and sufficient condition for a non empty subset \(H\) of a group \(\{G, \ast\}\) to be a subgroup is \(a, b \in H \Rightarrow a \ast b^{-1} \in H\).  
   (N/D 2012)

   Textbook Page No.: 4.20

28. If \(\ast\) is the operation defined on \(S = \mathbb{Q} \times \mathbb{Q}\), the set of ordered pairs of rational numbers and given by \((a, b) \ast (x, y) = (ax, ay + b)\), show that \((S, \ast)\) is a semi group. Is it commutative? Also find the identity element of \(S\).  
   (N/D 2012)

   Textbook Page No.: 4.9

29. Define the Dihedral group \(\langle D_4, \ast\rangle\) and give its composition table. Hence find the identify element and inverse of each element.  
   (A/M 2011)

   Textbook Page No.: 4.22

- **Homomorphism and Isomorphism**

1. Prove that the group homomorphism preserves the identity element.  
   (N/D 2015)
2. Prove that every finite group of order \( n \) is isomorphic to a permutation group of order \( n \).  
(N/D 2011), (M/J 2013)

3. State and prove the fundamental theorem of group homomorphism.  
(N/D 2013)

4. Let \( f : G \rightarrow G' \) be a homomorphism of groups with Kernel \( K \). Then prove that \( K \) is a normal subgroup of \( G \) and \( G / K \) is isomorphic to the image of \( f \).  
(M/J 2012)

5. Let \( (G,\ast) \) and \( (H,\Delta) \) be two groups and \( g : (G,\ast) \rightarrow (H,\Delta) \) be group homomorphism. Prove that the Kernel of \( g \) is normal subgroup of \( (G,\ast) \).  
(M/J 2013), (M/J 2016), (A/M 2017)

6. Show that the Kernel of a homomorphism of a group \( (G,\ast) \) into another group \( (H,\Delta) \) is a subgroup of \( G \).  
(A/M 2011), (A/M 2018)

7. If \( f : G \rightarrow G' \) is a group homomorphism from \( (G,\ast) \) to \( (G',\Delta) \) then prove that for any \( a \in G \), \( f(a^{-1}) = [f(a)]^{-1} \).  
(N/D 2012)

8. If \( (Z,+) \) and \( (E,+) \) where \( Z \) is the set all integers and \( E \) is the set all even integers, show that the two semi groups \( (Z,+) \) and \( (E,+) \) are isomorphic.  
(N/D 2010)

9. Let \( (S,\ast) \) be a semi group. Then prove that there exists a homomorphism \( g : S \rightarrow S^S \), where \( (S^S,\circ) \) is a semi group of functions from \( S \) to \( S \) under the operation of (left) composition.  
(N/D 2011)
• **Rings and Fields**

1. Prove that \((Q, \oplus, \circ)\) is a ring on the set of rational numbers under the binary operations
\[
x \oplus y = x + y + 7, \quad x \circ y = x + y + \frac{xy}{7}
\] for \(x, y \in Q\).

   (N/D 2019)

2. Show that \((Z, +, \times)\) is an integral domain where \(Z\) is the set of all integers.

   Textbook Page No.: 4.34 (N/D 2010)

3. Prove that the set \(\mathbb{Z}_4 = \{[0],[1],[2],[3]\}\) is a commutative ring with respect to the binary operation addition modulo and multiplication modulo \(+4\) and \(\times4\).

   Textbook Page No.: 4.35 (N/D 2012),(N/D 2015)

**Unit – II (Finite Fields and Polynomials)**

• **Part A Questions**

1. What is the remainder when \(f(x) = x^5 + 2x^3 + x^2 + 2x + 3 \in \mathbb{Z}_5[x]\) is divided by \((x - 1)\)?

2. What is the remainder when \(f(x) = 2x^3 + x^2 + 2x + 3 \in \mathbb{Z}_5[x]\) is divided by \((x - 2)\)?

3. Every field is an integral domain. Justify.

4. Give any example of an irreducible polynomial of degree 2 in \(\mathbb{Z}_5[x]\).

5. Define a field with an example.

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

7. If \(f(x) = 2x^4 + 5x^2 + 2\) and \(g(x) = 6x^2 + 4\) then determine \(f(x) \cdot g(x)\) in \(\mathbb{Z}_3[x]\).

8. Find all subgroups of \(G = (Z_{12}, +)\).

• **Part B Questions**

1. 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 divide by \(g(x)\).
2. If $R$ is a ring under usual addition and multiplication, show that $(R[x], +, \cdot)$ is a ring of polynomials over $R$.

3. If $f(x) \in F(x)$ has degree $n \geq 1$, then prove that $f(x)$ has at most $n$ roots in $F$.

(N/D 2019)

4. If $(F, +, \cdot)$ is a field and $\text{char}(F) > 0$, then prove that $\text{char}(F)$ must be prime.

5. Define the inverse of 25 in $Z_{72}$.


7. Find $[100]^{-1}$ in $Z_{1009}$.

(N/D 2019)

8. State and prove remainder theorem.

9. Prove that every finite field has $p^n$ elements for some prime number $p$ and some positive integer $n$.

10. Prove that a finite field has order $p^t$, where $p$ is prime and $t \in Z^+$. (N/D 2019)

11. Prove that $Z_n$ is a field if and only if $n$ is a prime.

12. Prove that in $Z_n$, $[a]$ is a unit if and only if $\gcd(a, n) = 1$.

13. Let $k, m$ be fixed integers. Find all values of $k, m$ for which $(Z, \oplus, \circ)$ is a ring under the binary operations $x \oplus y = x + y - k$, $x \circ y = x + y - mxy$, where $x, y \in Z$.

14. Define a ring with an example. Determine whether $(Z, \oplus, \circ)$ is a ring with the binary operations $x \oplus y = x + y - 7$, $x \circ y = x + y - 3xy$, where $x, y \in Z$. (N/D 2019)

Unit – III (Divisibility Theory and Canonicals Decompositions)

- **Part A Questions**

1. State the pigeonhole principle.

2. Find the GCD of 168 and 180 using the canonical decomposition.

3. Find the positive integer $a$ if $[a, a + 1] = 132$.

4. Find the canonical decomposition of $2^9 - 1$. 
5. Find GCD of \( a + b, a^2 - b^2 \).

6. Obtain the Greatest Common Divisor of \( a^2 - b^2, a^4 - b^4 \).

7. Prove that \( n^2 + n \) is an even integer, where \( n \) is an arbitrary integer.

8. Using the canonical decomposition of 1050 and 2574, find their lcm.

9. Compute the remainder when \( 2^{35} \) is divided by 7.

10. State Euler’s theorem.

11. Find the number of positive integers \( \leq 3000 \) and divisible by 3, 5 or 7.

12. Find the number of positive integers \( \leq 2076 \) and divisible by neither 4 nor 5.

**Part B Questions**

1. Find the gcd of \( x^{10} - x^7 - x^5 + x^2 - 1 \) and \( x^5 - x^3 + x^2 + 1 \) in \( \mathbb{Q}[x] \).

2. Prove that there are infinitely many primes of the form \( 4n + 3 \). \hfill (N/D 2019)

3. Find the number of positive integers \( \leq 3000 \) and divisible by 3, 5 or 7.

4. Prove that every integer \( n \geq 2 \) has a prime factor.

5. Apply the Euclidean algorithm to find \( (3076,1976) \) and hence express \( (3076,1976) \) as a linear combination of \( 3076 \) and \( 1976 \).

6. If \( a' \) and \( b' \) are relatively prime and if \( a / bc \), then prove that \( a / c \). \hfill (4)

7. Show that if \( m = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdots p_k^{n_k} \), where \( p_1, p_2, p_3, \ldots, p_k \) are distinct primes and each \( n_i \geq 1 \), then \( \varphi(m) = m \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_k} \right) \).

8. Let \( a \) and \( b \) be positive integers. Then prove that \( [a,b] = ab / (a,b) \).

9. Evaluate \( \sigma(17640) \) and \( \tau(17640) \). \hfill (5)

10. Find the number of positive integers in the range 1976 through 3776 that are not divisible by 17.

11. Find the number of positive integers in the range 1976 through 3776 that are divisible by 13.
12. Find eight consecutive integers that are composite. (4)

13. Obtain the six consecutive integers that are composite. (8)

14. State and prove Euclid’s theorem. (6)

15. Prove that the product of gcd and lcm of any two positive integers \(a\) and \(b\) is equal to their products. (N/D 2019)

16. Prove that the gcd of the positive integers \(a\) and \(b\) is a linear combination of \(a\) and \(b\). (N/D 2019)

17. Apply Euclidean algorithm to compute \((2076, 1776)\).

18. Apply Euclidean algorithm and express \((4076, 1024)\) as a linear combination of 4076 and 1024.

19. Apply Euclidean algorithm to express the gcd of 1976 and 1776 as a linear combination of themselves. (N/D 2019)

20. Using induction prove that \(n^4 + 2n^3 + n^2\) is divisible by 4. (4)

21. Using recursion evaluate \((18, 30, 60, 75, 132)\). (4)

22. Prove that \((a, a-b) = 1\) if and only if \((a, b) = 1\). (8)


**Unit – IV (Diophantine Equations and Congruences)**

- **Part A Questions**

1. Determine whether the LDE \(6x + 8y = 25\) is solvable.

2. Find the remainder when \(2^{97}\) is divided by 13.

3. Compute the remainder when \(2^{35}\) is divided by 7.


5. Find the remainder when \(1! + 2! + 3! + \ldots + 1000!\) is divided by 12.

6. Find the remainder when \(1! + 2! + 3! + \ldots + 1000!\) is divided by 6.
7. Verify that the linear system \(2x + 3y \equiv 4 \pmod{13}; 3x + 4y \equiv 5 \pmod{13}\) has a unique solution modulo 13.

8. Determine the number of incongruent solutions of \(48x \equiv 144 \pmod{84}\).

9. Give an example of an linear congruence equation that has an unique solution.

**Part B Questions**

1. Find the remainder when \((n^2 + n + 41)^2\) is divided by 12.

2. Prove that the LDE \(ax + by = c\) is solvable if and only if \(d \mid c\) where \(d = (a, b)\). Further obtain the general solution of \(15x + 21y = 39\).

3. Find the general solution of the LDE, \(6x + 8y = 10\).

4. Find the general solution of the LDE, \(15x + 21y = 39\). (N/D 2019)

5. Solve the congruence \(91y \equiv 119 \pmod{28}\).

6. State and prove Chinese Remainder Theorem. Use it to find the least positive integer that leaves the remainder 2 when divided by 3, remainder 4 when divided by 5 and 5 when divided by 7. (N/D 2019)

7. Use the Chinese remainder theorem to solve \(x \equiv 1 \pmod{3}; x \equiv 2 \pmod{5}; x \equiv 3 \pmod{7}\).

8. Solve \(x \equiv 1 \pmod{3}; x \equiv 2 \pmod{4}; x \equiv 3 \pmod{5}\).

9. Solve the linear system \(x \equiv 3 \pmod{7}; x \equiv 4 \pmod{9}; x \equiv 8 \pmod{11}\).

10. The linear Diophantine equation \(ax + by = c\) is solvable iff \(d \mid c\), where \(d = (a, b)\). If \(x_0, y_0\) is a particular solution of the linear Diophantine equation, then prove that all its solution given by \(x = x_0 + (b/d)t\) and \(y = y_0 + (a/d)t\), where \(t\) is an arbitrary integer.

11. Solve the linear system \(5x + 6y \equiv 10 \pmod{13}\) and \(6x - 7y \equiv 2 \pmod{13}\). (N/D 2019)

12. Compute the remainder when \(13^{213}\) is divided by 17.

13. Compute the remainder when \(13^{181}\) is divided by 17.

14. Compute the remainder when \(3^{247}\) is divided by 25.

15. If \(a \mid b\) and \(c \mid d\) then prove that \((a, c) \mid (b, d)\).
16. Prove that $4^{2n} + 10n \equiv (\text{mod } 25)$.

17. Prove that $n^2 + n \equiv 0 \pmod{2}$ for any positive integer $n$.

**Unit – V (Classical Theorems and Multiplicative Functions)**

- **Part A Questions**

1. Find the remainder when $18!$ is divided by $19$.

2. Find the remainder when $100!$ is divided by $101$.

3. Compute the value of sigma functions for $n = 28$.

4. Compute the value of sigma functions for $n = 36$.

5. State and prove Wilson's theorem.

6. Find all the positive integers $n$ that satisfy, $\phi(n) = 6$.

7. Define a multiplicative function with an example.

- **Part B Questions**

1. Find the remainder when $24^{1947}$ is divided by $17$.

2. Define Euler's Phi function and prove that it is multiplicative.

3. Using Euler’s theorem find the remainder when $245^{1040}$ is divided by $18$. (N/D 2019)

4. State and prove Fermat’s Little Theorem.

5. State and prove Wilson’s theorem. (N/D 2019)

6. Prove that $\phi(2^{24+1})$ is a square.

7. Let $n$ be a positive integer with canonical decomposition $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Derive the formulae for Tau and Sigma functions. Hence evaluate $\tau(n)$ and $\sigma(n)$ for $n = 1980$. (N/D 2019)

8. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the canonical decomposition of a positive integer $n$, then derive a formula to calculate the Euler's phi function $\phi(n)$ and compute $\phi(6860)$.
9. If \( p \) is a prime and \( e \) be any positive integer then prove that \( \phi(p^e) = p^e - p^{e-1} \). Hence compute \( \phi(81) \).

10. If \( p \) is a prime and \( e \) be any positive integer then prove that \( \phi(p^e) = p^e - p^{e-1} \). Also show that \( \phi(n) = n / 2 \), when \( n = 2^k \).

11. Let \( p_1, p_2, p_3 \) be distinct primes and \( n = p_1 p_2 p_3 \). Evaluate \( \tau(n) \) and show that \( \sigma(n) = (p_1 + 1)(p_2 + 1)(p_3 + 1) \).

**Book for Reference:**

“Discrete Mathematics (Solved University Questions)”

Edition: 1st Edition

Publication: Sri Hariganesh Publications

Author: C. Ganesan

Mobile: 9841168917, 8939331876

To buy the book visit www.hariganesh.com/textbook

----All the Best----