QUESTION BANK

Name of the Department : Science & Humanities

Subject Code & Name : MA8551 & Algebra and Number Theory

Year & Semester : III&V

UNIT I GROUPS AND RINGS

PART-A

1. In an abelian group (G,*), prove that $(a*b)^2 = a^2 * b^2 \forall a,b \in G$.
2. Show that the inverse of an element in a group (G,*) is unique.
3. State Lagrange's theorem for finite groups.
4. If H is a subgroup of G, among the right cosetsof H inG then prove that there is only one subgroupH.
5. Give an example of a ring which is not a field
6. Define a group and give an example.
7. Prove that any group of prime order is cyclic.
8. Find all the subgroups of $(Z_{12,} +_{12})$
9. Define a commutative ring
10. Prove that every subgroup of an abelian group is normal
11. Determine U_{14}.
12. Find the order of -1 and 3 in $(R^*\ .)$
13. Find the order of 2 in $(Z_8,+)$
14. Verify $(Z_7^*,\ .)$ is cyclic.
15. Find all the subgroups of $(Z_{12}\ ,\ +)$
16. Given example of a ring with 8 elements.
17. Does there exist a finite field with 16 elements.
18. Does there exist a finite field with 15 elements
19. Prove that G=(-1,1) is not a group under + .
20. State any two properties of a group.
21. Define homomorphism and isomorphism between two algebraic systems.
22. Give an example of a group.
23. State the minimum order of a non-abelian group.
24. Find a subgroup of order two of the group $(Z_8,+_8)$.

PART-B

1. Verify that set S= $\{10n|\ n\ \epsilon Z\}$ under addition is a group or not
2. If $H_1 and\ H_2$ are subgroups of (G,*), then prove that $H_1 \cup H_2$ is a subgroup of H iff $H_1 \subseteq H_2$ or$H_2 \subseteq H_1$.
3. Every subgroup of a cyclic group is cyclic

4. State and prove Lagranges's theorem
5. Fundamental theorem of group homomorphism.
6. For the group G=$(Z_{12},+)$, $H = \{[0],[4],[8]\}$ is asubgroup .Find the cosets H in G.
7. Prove that any finite integral domain is a field
8. Find $[25]^{-1}$ in the ring Z_{72}
9. Find the dihedral group D_3.
10. Find total order of element in S_5
11. If $H_1 and\ H_2$ are subgroups of a group (G,*) prove that $H_1 \cap H_2$ is a subgroup of (G,*).
12. Is f(x) = $x^3 + x + 1\ in\ Z_2(x) is\ irreducible$?.
13. .In Z_n $[a]$ is a unit iff a and n are relatively prime.
14. Whether the non-zero element s of Z_6 form a group under multiplication or not?
15. If f is a homomorphism from a group (G,*) into $(G^{'},.) then\ prove\ that$
    $(i) f(e) = e^{'}$,where e,e' are the identities of G and G' respectively.
    (ii) f(a^{-1})=$[f(a)]^{-1}$ for all a$\in G$. (iii) f(a^n) = $[f(a)]^n$.
16. Let H be a subgroup of G.Then H≠$\emptyset$,since H contains at least e$\in G$ and so,f(H)≠ $\emptyset$.
17. In Z_n $[a]$ is a unit iff a and n are relatively prime.
18. Prove that the intersection of two normal subgroup of (G,*) is a normal subgroup of (G,*)
19. Let G be the set of all(symmetric) rigid motions of a equilateral triangle. Identify the elements of G
    Determine the value of the integer n>1 for which the give congruence is true.

    (a) 401≡ $323(mod n)$ (b) 57≡ $1(mod n)$ (c) 68≡ $37(mod n)$ (d) 49≡ $1(mod n)$
20. Show that the set of all non-zero real numbers is an abelian group under the operation * defined by
    a*b=ab/2

UNIT II FINITE FIELDS AND POLYNOMIALS

PART-A

1. Define Equal polynomials.
2. Define Divisor of a polynomial
3. Determine all the roots of f(x) = x^2+3x+2 ϵ Z_6 $[X]$.
4. Define Irreducible polynomials
5. Define Characteristic of a ring
6. Find the number of polynomials of degeree n in $Z_{12}[X]$.
7. Test whether 2x+1$\in$ $Z_{12}[X]$.
8. Definition Greatest common divisor.
9. If f(x) =x^2 +1 in Z$[X]$ is irreducible over Z.
10. If f(x) =x^3+x +1 in Z$[X]$ is irreducible over Z.
11. .Find the roots of the polynomial x^2 -2 over the real numbers R.
12. Define Root of a polynomial

PART-B

1. Find $[25]^{-1}$ in the ring Z_{72}
2. Let k, m be fixed integers. Find all values of k, m for which (Z ,⊕,⊙)is a ring under the binary operations
   a. x ⊕ y = x+ y –k and x⊙y =x+y- mxy ∀ x,y ϵ z.
3. In Z_n $[a]$ is a unit iff a and n are relatively prime
4. Prove that R$[x]$ is an integral domain iff R is an integral domain.
5. If R is an integral domain, then deg (f(x). g(x)) = deg f(x) + deg g(x)
6. State and prove Division algorithm
7. If f(x) ϵ $F[X]$ is of degree n ≥ 1, $then\ f(x)\ Has\ at\ most\ n\ roots\ if\ F$
8. The number of elements of a finite field is p^n, Where p is a prime number and n is a positive integer.
9. Fined the g.c.d of x^4+ x^3+ $2x^2$ +x+1 and x^3-1 over Q
10. Determine the value of the integer n>1 for which the give congruence is true.
    (a) 401≡ $323(mod n)$ (b) 57≡ $1(mod n)$ (c) 68≡ $37(mod n)$ (d) 49≡ $1(mod n)$
11. Is f(x) = $x^3 + x + 1\ in\ Z_2(x) is\ irreducible$?.
12. Define the binary operations ⊕ and ⊙ in Z by x ⊕ y = x+y-7 and x⊙ y = x+ y-3xy, for $\forall x, y\ \epsilon\ Z$. Explain
13. Why (Z, ⊕ ,⊙) is not a ring?
14. Let R be a ring, The (R$[x]$,+ , .) is a ring.
15. Find all the roots of f(x) = x2=4x in Z_{12} $[X]$
16. If f(x)= 2 x^4 +$5x^2$+2,g(x) =$6x^4$+4 , then determine g(x) and r(x) in Z_7 $[X]$,when f(x) is divided by g(x).
17. Find two non-zero polynomials f(x),g(x) in Z_7 $[X]$ such that f(x) g(x) ≠ 0 .
18. The number of elements of a finite field is p^n, Where p is a prime number and n is a positive integer.
19. The characteristic of a field (F,+ ,°) is either 0 or a prime number.

UNIT III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS

PART-A

1. State the pigeon hole principle.
2. Express $(1776)_8$ as a decimal number.
3. Find the g.c.d of a+ b, a^2- $b^{2.}$
4. Find the value of the base b if 54_b = 64 .
5. The sum of any two oId integers is even.
6. Express 10110 $_{two}$
7. Find the number of ones in the binary representations of 2^4 -1
8. Every integer n≥ 2 has a prime factor
9. Defintion Least common multiple
10. Find the lcm of each pair of integers 110,210
11. Find the number of ones in the binary representations of 2^9 -1
12. Find the number of ones in the binary representations of 2^{13} -1
13. Express 10110 $_{two}$ in base 10.

14. Find the number of positive integers ≤ 2076 and divisible by 4 nor 5
15. Find the value of the base b if $64_b = 54$.
16. If (a,b)=d ,then prove that(a/d , b/d) =1
17. If n is a positive integer, then prove that g.c.d (n,n+2)=1 or 2.
18. Find the positive integer a if (a, a+1) = 132.
19. If a and b are positive integers with $a.b = 2^4 . 3^4 . 5^3 .7.11^3.13$

PART-B

1. Let a be any integer and b be a positive integer. Then there exist unique integers q and r such that a= qb+r, where $0 \leq r < b$.
2. State and prove Fundamental theorem of arithmetic.
3. Find the number of integers 1 to 250 that are divisible by any of the integers 2 ,3,5,or7.
4. Find the number of primes≤ 100 using the formula for (n).
5. Apply Euelidean algorithm to compute (2076,1776)
6. Use recursion to evaluate (18, 30, 60, 75,132)
7. Apply Euelidean algorithm to express the gcd of 1976 and 1776 as a linear combination of them
8. Find the largest power of 2 that divides 97!
9. Obtain five consecutive integers that are composite numbers
10. Prove that (a, a-b) =1.if and only if (a, b) =1
11. Find the number of positive integers ≤ 3000 and divisible by 3,5,or7
12. Prove that there are infinitely many primes of the form 4n+3.
13. There are infinitely many primes.
14. Find the number of primes≤ 47 using the formula for $\pi(n)$.
15. Obtain six consecutive integers that are composite numbers
16. Find the positive integer a if $(a, \quad a+1) = 32$
17. Find the gcd and lcm of 504 and 540
18. Find the canonical decomposition of 23!
19. Use recursion to evaluate (24,28,36,40).
20. The g.c.d of two positive integers a and b is a linear combination of a and b.

UNIT IV LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES

PART-A

1. If a.b$\equiv o$ (mod m), then a$\equiv 0$ (mod m) and b$\equiv 0$ (mod m) .
2. Is it true that 9^{100} -1 is divisible by 10
3. If today is Wednesday, what day will it be in 129 days?
4. If today is Monday, what day will it be in 999 days?
5. If it is 11.30 AM now what time will it be in 1769 hours?
6. Is 2x$\equiv 7(mod4)$ solvable?
7. Solve the linear congruence 3x$\equiv 1(mod)$.

8. Determine the number of incongruent solutions of the congruence $48x \equiv 144 (mod 84)$
9. Given an example of a linear congruence that has an unique solution.
10. Find the remainder when 2^{97} is divided by 13.
11. Find the inverse of 7 modulo 26.
12. Determine the number of incongruent solutions of $4x \equiv 5 (mod 9)$
13. Find the last digit in 3^{55}
14. State Chinese remainder theorem
15. Determine whether the LDE 6x+8y=25 is solvable .
16. Determine whether the linear system $x \equiv 5$(mod 9) and $x \equiv 7$ (mod 12) is solvable.
17. 2 x 2 linear systems definition.
18. Is the linear Diophantine equation 6x+8y=25 solvable?

PART-B

1. Determine if the LDE 12x+18y=30 is solvable. If so, find the solutions.
2. Examine whether the LDE 12x+16y=18 is solvable. Write the general solution if solvable.
3. Prove that LDE ax + by=c is solvable if and only if d / c, where d = (a, b). Further obtain the general Solution of 15x+21y=39.
4. Find the general solution of the LDE 6x+8y+12z=10
5. Find the general solution of the LDE 2x+4y-5z=11.
6. $a \equiv b$ (mod m) if and only if a=b+km for some integer k..
7. Find the remainder when 1! +2! +3! +4! +………+100! Is divided by 15
8. Find the remainder when 1! +2! +3! +4! +………+300! Is divided by 13
9. Find the ones digit in the sum 1! +2! +3! +4! +………+100! , when expressed in decimal notation.
10. Compute the remainder when 3^{247} is divided by 25.
11. Compute the remainder when 3^{181} is divided by 17
12. Find the remainder when13^{218} is divided by 17
13. Determine whether the congruence $12x \equiv 48 (mod 18)$ is solvable and also find all the solutions .
14. Determine the number of incongruent solutions of $48x \equiv 144 (mod 84)$.
15. 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 divided them equally, Find the number of fruits in each heap.

    Using inverse find the incongruent solutions of the linear congruence $5x \equiv 3 (mod 6)$.
16. Solve the system of congruence's $x \equiv 1 (mod 3)$. $X \equiv 2 (mod 5)$. $X \equiv 3 (mod 7)$.
17. State and prove Chinese remainder theorem
18. Solve the system $x \equiv 1 (mod 3)$. $x \equiv 2 (mod 4)$. $x \equiv 3 (mod 5)$.
19. Solve the linear system $x \equiv 3 (mod 7)$. $x \equiv 4 (mod 9)$. $x \equiv 8 (mod 11)$.
20. Solve the system of linear congruence's 5x+6y≡10 (mod13), 6x-7y≡2 (mod13)
21. Solve the system of linear congruence's 3x+13y≡8 (mod55), 5x+21y≡34(mod55)

UNIT V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

PART-A

1. Compute the remainder when 3^{302} is divided by 5.
2. Find the remainder when 100! Is divided by 101.
3. Find the remainder when 18! Is divided by 19.
4. State Euler's theorem.
5. Define a multiplicative function with an example.
6. Compute the value of sigma function if n=28.
7. Verify Wilson's theorem (p-1)! $\equiv -1$ (Mod p) if p=7.
8. Compute the value of sigma function for n=36.
9. When $n=2^k$ prove that $\emptyset(n) = n ∴ 2$.
10. If p is a prime and a is any integer such that p $\aleph\, a$. then prove that a^{p-2} is an inverse of a mod p.
11. Given two different numbers m and n for which $\tau(m) = \tau(n)$.
12. If p is a prime such that $\sigma(p)$ is odd, then find p.
13. Prove that for a prime p , $\varphi(p) + \sigma(p)$ is always even.
14. If n is a power of 2, then prove that $\tau(n)$ is always odd.
15. Find the self invertible least residue modulo 7.
16. Prove that $\varphi(n)$ is even if n$\leq$ 3.
17. Find the incongruent solutions of 12x≡8 (mod14)
18. Show that $n^2+n \equiv 0$ (mod2)for any positive integer n.
19. State Wilson's theorem

PART-B

1. Find the remainder when 24^{1947} is divided by 7.
2. Define Euler's phi function and prove that it is multiplicative.
3. If p is a prime and e any positive integer then prove that f (p^e) = $p^e - p^{e-1}$ .Also show that f(n) = n/2 n= 2^k
4. State and prove Wilson's theorem
5. Show that 18! +1 is divisible by 437
6. Prove that 63! ≡-1(mod71)
7. If p is a prime, prove that (p-1)(p-2)(p-3)…….(p-k) ≡ $(-1)^k$ k! (Mode), where $1 \leq k < p$.
8. If x=1.3.5…….(p-2),where p is an odd prime, show that $x^2 \equiv (-1)^{p+1/2}$ (modp).
9. Find the remainder when 2^{1000} is divided by 17.
10. Find the remainder when 193^{183} is divided by 19
11. Find the remainder when 24^{1947} is divided by 17
12. Compute the remainder when 7^{1001} is divided by 17
13. Find $\varphi(1105)$ and $\varphi(7!)$
14. Compute $\varphi(6860)$.
15. Find the positive integers n such that $\varphi(p) = 6$.
16. Prove that φ (2^{2k+1}) is a square.

17. Using Euler's theorem find the remainder when 245^{1040} is divided by 18.
18. For any prime p, prove that (i) $\varphi(p+2) = \varphi(p)$ +2 (ii) $\varphi(p)$ is odd.
19. Prove that the cube of an integer has one of the forms 9m,9m+1,9m+8.
20. Show that for any integer n, $n^5 - n$ is divisible by 30.
21. State and prove Fermat's Theorem.