Algebra and Number Theory

UNIT - I - Groups

2mark

1. Define abelian group and give an example of an infinite non abelian group.
2. Prove that intersection of two subgroups is a subgroup. Justify that union of two subgroups need not be a subgroup.
3. Define normal subgroups and give an example.
4. Give an example of a finite abelian group which is not cyclic.
5. Prove that a group homomorphism maps an identity element to an identity element.
6. Define cyclic groups and give an example.
7. What is the order of the permutation (1, 2, 4, 6)(4, 7, 8, 9)(2, 3, 5) in S_9?
8. Find the number of distinct cycles of length 1988 in S_{2511}?
9. Define group homomorphism and give an example.
10. Define quotient group and give an example.
11. Prove that the centre of a group is a normal subgroup.

6 mark

1. State and prove the fundamental theorem of cyclic groups.
2. State and prove the necessary and sufficient condition for a nonempty set to be a subspace.
3. Prove that the quotient group $\mathbb{Z}/5\mathbb{Z}$ is isomorphic to $(\mathbb{Z}_5, \oplus_5)$.
4. Prove that every cyclic group is abelian but not conversely justify.
5. What are the possible orders for the elements of S_6 and A_6?

10 mark

1. State and prove the fundamental theorem of group homomorphism.
2. State and prove Lagrange's theorem
3. State and prove Cayley's theorem

UNIT - II - Rings and Fields

2mark

1. Define division ring and give an example of a division ring which is not a field
2. Give an example of a subring which is not an ideal.
3. Prove that intersection of two ideals of a ring is also an ideal. Also, justify that union of two ideals of a ring is need not be an ideal.
4. Give an example of a finite field which has 125 elements.
5. Find the number of subfields of a field having 2401 elements.
6. Define irreducible polynomial with an example.
7. Define primitive polynomial with an example
8. State structure theorem for finite fields.

6 mark

1. State and prove Eisenstein criterion.

2. Prove that a finite integral domain is a field. Also give an example of an infinite integral domain which is not a field.
3. Prove that ring of real quaternions is a division ring.
4. State whether the following polynomials are reducible or irreducible?
    a) $x^2 + 2$ over the field of rationals
    b) $x^4 + x^2 + 1$ over $\mathbb{Z}_2$
    c) $x^{2311} + 2311$ over the field of rationals
    d) $x^3 + 1$ over $\mathbb{Z}_3$

10 mark

1. State and prove Gauss lemma.
2. State and prove fundamental theorem of ring homomorphism. Also give an example of a ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_{25}$ whose kernel is $25\mathbb{Z}$.

UNIT - III - Number Theory

2mark

1. Define greatest common divisor and give an example.
2. Express $(12,15,21)$ as a linear combination on $12, 15$ and 21
3. Define pairwise relatively prime integers and give an example.
4. Prove that $d|(a,b)$ where d is a common divisor of a and b.
5. If $a|bc$ and $(a,b) = 1$, then prove that $a|c$
6. Let $(a,b) = d$. Prove that the integers $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.

6 mark

1. State and prove division algorithm
2. Prove that the gcd of the positive integers a and b is a linear combination of a and b.
3. Prove that if the positive integers $a_1, a_2, a_3, \cdots, a_n$ are pairwise relatively prime, then $(a_1, a_2, a_3, \cdots, a_n) = 1$.
4. Prove that $(a,b) = (a, a-b)$.

10 mark

1. State and prove fundamental theorem of arithmetic
2. Prove that $(\mathrm{a}, \mathrm{b}) = (\mathrm{b}, \mathrm{r})$ where $a \geq b \geq 0$ and r is the reminder when a is divided by b. Write Euclidean algorithm also find gcd of 45 and 250 using Euclidean algorithm.
3. Write extended Euclidean algorithm. Also find (13,166) and write (13,166) as a linear combination of 13 and 166 using extended Euclidean algorithm.

UNIT - IV - Modular Arithmetic and congruence

2mark

1. Prove that $\equiv$ is an equivalence relation.
2. Suppose $a \equiv b (mod\ n)$ and $c \equiv d (mod\ n)$. Prove that $a - c \equiv b - d (mod\ n)$
3. Suppose $a \equiv b (mod\ n)$ and $c \equiv d (mod\ n)$. Prove that $ac \equiv bd (mod\ n)$
4. Compute 3^8 modulo 13.

5. What is $45^{-1}\ mod(49)$ and $-5\ mod(45)$
6. State Chinese remainder theorem.
7. How many solutions the congruence $14\ x \equiv 12\ mod(18)$ have? Jusitify

<u>6 mark</u>

1. Suppose $ab \equiv ac(mod\ n)$ and $(a, n) = 1$, then prove that $b \equiv c(mod\ n)$
2. Prove that $f(x) = x^5 - x^2 + x - 3$ has no integer roots.
3. Prove that $6|a(a + 1)(2a + 1)$ for every $a \in \mathbb{N}$.
4. Prove that the linear congruence $ax \equiv b(mod\ n)$ has a solution if and only if $d = (a, n)$ divides b.

<u>10 mark</u>

1. Write fast exponentiation algorithm. Also compute 240^{262} modulo 14.
2. Write an algorithm for solving linear congruence and find all the solutions of $18\ x\ \equiv 42(mod\ 50)$ using algorithm.
3. State and Prove Chinese reminder theorem.
4. Solve the system of linear congruence

$$x\ \equiv 2(mod\ 7)$$
$$x\ \equiv 7(mod\ 9)$$
$$x\ \equiv 3(mod\ 4)$$

using Chinese reminder theorem

<u>UNIT - V - Primality and Factorization</u>

<u>2mark</u>

1. State Euler's theorem.
2. Define Euler phi function with an example.
3. Define quadratic residue with an example.
4. Define Legendre and Jacobi symbol.
5. What is discrete logarithm.

<u>6 mark</u>

1. Prove that $\phi(nm) = \phi(n)\phi(m)$ where m and n are positive integers and $(n, m) = 1$
2. Find the discrete logarithm of each unit modulo 11 to the base 2
3. List all the properties of Legendre and Jacobi symbol.
4. Factorize 809009 using Fermat factorization method.

<u>10 mark</u>

1. State and prove Fermat's little theorem.
2. Write Miller-Rabin algorithm for primality test. Using it check whether 561 is a prime or not.
3. Write Pollard Rho algorithm for factorize 10403 using that algorithm.