INDIAN STATISTICAL INSTITUTE

Semestral Examination: (2025-2026)

Subject Name : **Algebra and Number Theory**

Course Name : M.Tech. (CrS) I yr. Year: 2025

Max Score: 100 Date: 19.11.25 Duration: 180 Mins

Question 1 is compulsory.
You can attempt all the rest. with total marks $(\mathbf{32 + 88 =}) \mathbf{120}$. but the maximum score is **100**. Marks are given on the margin.
Notation: R is a commutative ring; $\mathbb{Z}_p^*$ is the group of units in $\mathbb{Z}_p$, the integers modulo p: K is a field and $\mathbb{F}_q$, a finite field of size q.
Calculators are not allowed.

---

1. (a) Prove that, for an odd integer n, if x is a quadratic residue modulo n, then the Jacobi symbol $\left(\frac{x}{n}\right) = 1$.

   Compute $\left(\frac{109}{385}\right)$.

   (b) Prove that if $x \in R$ is nilpotent and $\mathbf{p}$ be any prime ideal in R. then $x \in \mathbf{p}$.
   Show that, for any unit $u \in R$, $x + u$ is also a unit.

   (c) Prove that $a \in K$ is a root of a polynomial $f \in K[X]$ if and only if $(X - a)$ divides f.
   Use the above result to find *all* irreducible polynomials over $\mathbb{F}_2$ of degree 2. Establish which one of these is primitive.

(6+4) + (5+5) + (5+7) = 32

2. Let p be an odd prime and k be a positive integer.

   (a) Establish that, for $b \in \mathbb{Z}_{p^k}$, $b^2 = 1$ if and only if $b = \pm 1$.

   (b) Assuming the relevant Euler's theorem, prove that if $a \in \mathbb{Z}_p^*$ is a quadratic non-residue modulo p, then

$$a^{\frac{p-1}{2}} = -1$$

$4 + 8 = 12$

3. Let $p > 1$ be an odd, prime integer, and let a be an integer which is not divisible by p. Show that there exists a set $\mathcal{S} \subset \{1, 2, \ldots, p-1\}$, where any $s \in \mathcal{S}$ satisfies $s > p/2$, related to the Legendre symbol defined by a as follows:

$$\left(\frac{a}{p}\right) = (-1)^{|\mathcal{S}|}.$$

where $|\mathcal{S}|$ denotes the size of $\mathcal{S}$.
Demonstrate your result for $p = 11$ and $a = 15$.

$(8 + 4 =)$ 12

4. (a) Describe the basic Solovay-Strassen primality test algorithm.

   (b) Prove that for an odd, composite integer $n > 0$, there exists an Euler witness (Solovay-Strassen) which is a non-witness for the greatest common divisor test.

$4 + 8 = 12$

5. (a) Let $\phi : R \to S$ be a ring homomorphism and $\mathbf{a} \subset S$ be an ideal. Prove that the set $\phi^{-1}(\mathbf{a})$ is an ideal in R.
   Illustrate the above result using the following canonical homomorphism:

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_{15}: \quad z \longmapsto z \mod 15.$$

   (b) Prove that if R is a field, then the only ideals in R are (0) and the unit ideal.

$(5 + 4) + 5 = 14$

6. (a) Let $f \in K[X]$ be an irreducible polynomial of degree n and α be a root of f. Prove that there exists a simple, algebraic extension of K defined by α.

   (b) Stating the relevant result, construct the subfield lattice of $\mathbb{F}_{2^{45}}$ with proper justification.

$7 + 5 = 12$

7. Prove that a polynomial $f \in \mathbb{F}_{p^n}[X]$, where n is a positive integer, has its formal derivative $f' = 0$ if and only if $f = g(X^p)$ for some $g \in \mathbb{F}_{p^n}[X]$.

10

8. (a) Let $S \subseteq V$ be a subspace of the vector space V over K. Show that the set given by $\{\mathbf{x}_1 + S, \ldots, \mathbf{x}_k + S\}$ is a basis of the quotient space V/S if and only if the set $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ is a basis of a complementary subspace of S in V.

   (b) Let V, W be two vector spaces over $\mathbb{F}_2$ of dimensions 5 and 3, respectively. Further, let X be a 2-dimensional subspace of V. Prove that the number of 1-dimensional subspaces of W and the number of 3-dimensional subspaces of V, which pairwise intersect precisely in X, are given by the same Gaussian coefficient. Compute the Gaussian coefficient.

$7 + 9 = 16$