INDIAN STATISTICAL INSTITUTE

SEMESTRAL EXAMINATION

B. STAT III YEAR

NUMBER THEORY

Date: 02.05.2025 Maximum marks: 100 Duration: 3 hours

There are 12 questions each worth 10 marks; for questions which have two parts, each part is worth 5 marks. Answer as much as you can, the maximum you can score is 100.

Note. For a positive integer n, $\mathbb{Z}_n$ denotes the set $\{0, \ldots, n-1\}$ and U_n denotes the set of numbers in $\{1, \ldots, n-1\}$ which are co-prime to n; $\phi()$ denotes the Euler's totient function; $\mu()$ denotes the Möbius function; $\left(\frac{\cdot}{\cdot}\right)$ denotes the Jacobi symbol; and $\mathbb{Z}[i]$ denotes the set of Gaussian integers.

1. Let p be an odd prime. Show that for any $a \in U_p$,

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p.$$

2. (a) Let n be a positive integer. Let e be the maximum of the orders of all elements in U_n. Show that for any $a \in U_n$, the order of a divides e.

   (b) Give an example of a positive integer n, and two distinct integers $a, b \in \mathbb{Z}_n$, such that $a + b \not\equiv 0 \bmod n$, and the order of $a + b$ is not equal to the least common multiple of the order of a and the order of b.

3. If p is an odd prime and b is an integer such that p does not divide b, show that for all positive integers n and s,

$$a^{p^s} \equiv b^{p^s} \bmod p^{n+s} \quad \text{implies} \quad a \equiv b \bmod p^n.$$

4. Let p be an odd prime and $m = 2p^3$. Let $n \geq 2$ be an integer and let $d = \gcd(\phi(m), n)$. Show that the equation $x^n \equiv c \bmod m$ has a solution in x if and only if c is a solution of the equation $y^{\phi(m)/d} \equiv 1 \bmod m$.

5. (a) Let n be a positive integer. Show that any integer solution in x to the equation

$$\phi(x) = 4n + 2$$

   is either of the form $x = p^\alpha$, or of the form $x = 2p^\alpha$, where p is a prime congruent to 3 modulo 4, and α is a positive integer.

   (b) Show that the product of all the primitive roots of 98 in U_{98} is congruent to 1 modulo 98.

6. Show that there are integers x, y and z which are not all 0, such that $121x^2 - 25y^2 - 169z^2$ is either equal to 0 or equal to $-121 \cdot 25 \cdot 169$. Provide all details.

7. (a) Show that the only rational solution to the equation $y^2 = x^3 + x$ is $(0, 0)$.

   (b) Let p be a prime. Show that the congruence $x^2 + y^2 + 1 \equiv 0 \bmod p$ has at least one solution.

8. (a) Show that for an integer $n \geq 1$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

   (b) Suppose f is a function from the positive integers to positive integers. Let F be a function defined on the positive integers as follows:

$$F(n) = \sum_{d|n} f(d).$$

   Show that if F is multiplicative, then f is also multiplicative.

9. Show that there is a positive constant c such that for all $n > 3$,

$$\phi(n) > \frac{cn}{\log \log n},$$

   where $\log x$ denotes the natural logarithm of x.

10. Show that for all sufficiently large primes p, there is a quadratic non-residue modulo p between 1 and $\sqrt{p}$.

11. (a) Find a subset S of $\mathbb{Z}[i]$ satisfying the following two properties.

   - For $\alpha, \beta \in S$, $\alpha \not\equiv \beta \bmod (-3 + 2i)$.
   - For every $\gamma \in \mathbb{Z}[i]$, there is some $\alpha \in S$ such that $\gamma \equiv \alpha \bmod (-3 + 2i)$.

   (b) For $\alpha, \beta \in \mathbb{Z}[i]$, with α, β co-prime show that $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$.

12. Show that if p is a prime congruent to 1 modulo 4, then p can be written as a sum of two squares in essentially one way. Provide all details.