Exam. Code : 211003
Subject Code : 3856

M.Sc. (Mathematics) 3rd Semester

MATH–586 : NUMBER THEORY

Time Allowed—3 Hours] [Maximum Marks—100

Note :— Attempt any **TWO** questions from each unit. All questions carry equal marks.

UNIT—I

1. (a) Solve $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$. 5

   (b) Prove that the Fermat number F_5 is divisible by 641. 5

2. State and prove Wolsten-Holme's Theorem. 10

3. (a) If the integer a has order k modulo n, then prove that for h > 0, the order of a^h is $k/\gcd(h, k)$ modulo n. 5

   (b) If r is a primitive root of odd prime p, then prove that $r^{\frac{(p-1)}{2}} \equiv -1 \pmod p$. 5

4. Prove that an integer n > 1 has a primitive root if and only if $n = 2, 4, p^k$ or $2p^k$, p odd prime. 10

UNIT—II

5. (a) Let n be an integer possessing a primitive root and let gcd (a, n) = 1. Prove that the congruence $x^k \equiv a \pmod{n}$ has a solution if and only if $a^{\phi(n)/d} \equiv 1 \pmod{n}$. 5

(b) If r is a primitive root of the odd prime p, then prove that $\text{ind}_r(-1) = \text{ind}_r(p-1) = \frac{p-1}{2}$. 5

6. (a) Let r be a quadratic residue of odd prime p and $ab \equiv r \pmod{p}$. Prove that a and b both are quadratic residues of p or both are quadratic non-residues of p. 5

(b) For a primitive root r of odd prime p, prove that the product of quadratic residues of p is congruent to $r^{(p^2-1)/4}$ modulo p. 5

7. State and prove Gauss Lemma. 10

8. (a) Prove that there are infinitely many primes of the form 5k – 1. 5

(b) For an odd prime p, show that $\sum_{a=1}^{p-2} \left(\frac{a(a+1)}{p}\right) = -1$. 5

UNIT—III

9. (a) Find the form of all positive integers n such that $\tau(n) = 10$. What is the smallest positive integer n for which $\tau(n) = 10$? 5

(b) Find $\sum_{d/n} \mu(d)$ for each positive integer $n \geq 1$. 5

10. (a) Let $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ be the prime factorization of n. Prove that $\sum_{d/n} \mu(d)\,\sigma(d) = (-1)^r p_1 p_2 \ldots p_r$. 5

(b) For a perfect number n, prove that $\sum_{d/n} \frac{1}{d} = 2$. 5

11. Prove that if for $k > 1$, $2^k - 1$ is prime, then $2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form. 10

12. Prove that an odd prime p is expressible as sum of two squares if and only if $p \equiv 1 \pmod{u}$. 10

UNIT—IV

13. Prove that a positive integer n is expressible as sum of two squares if and only if each of its prime factors of the form $4k + 3$ occurs to an even power. 10

14. Prove that any prime can be written as sum of four squares. 10

15. State and prove Hurwitz Theorem. 10

16. (a) For two successive terms $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ of F_n, prove that $b_1 + b_2 > n$. 5

(b) If n is a positive integer and x is a real number, then prove that there is a fraction $\frac{a}{b}$ such that

$$\left| x - \frac{a}{b} \right| \leq \frac{1}{b(n+1)}.$$ 5

UNIT—V

17. (a) If $\frac{p_n}{q_n}$ is the n^{th} convergent of the continued fraction $<a_0, a_1, ..., a_n>$, show that $<a_n, a_{n-1}, ..., a_1> = \frac{q_n}{q_{n-1}}$. 5

(b) Evaluate $<-3, 2, 4, 5, 2>$. 5

18. (a) Expand $\frac{5+\sqrt{37}}{4}$ as continued fraction. 5

(b) Prove that the even convergents of infinite continued fraction forms a strictly increasing sequence. 5

19. (a) Prove that if p and q are positive integers such that $p^2 - dq^2 = 1$, then $\frac{p}{q}$ is a convergent of the continued fraction expansion of $\sqrt{d}$. 5

(b) Show that $x^2 - dy^2 = -1$ has no solution if $d \equiv 3 \pmod 4$. 5

20. Prove that if (x_1, y_1) is the fundamental solution of $x^2 - dy^2 = 1$, then all positive solutions are given by (x_n, y_n), where x_n, y_n are the integers such that :

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n, n = 1, 2, 3, ...$$

Further find the fundamental solution of $x^2 - 48y^2 = 1$. 10