N20P 1186

Reg. No. : .....

Name : .....

III Semester M.Sc. Degree (CBSS – Reg./Suppl./Imp.)
Examination, October 2020
(2017 Admission Onwards)
MATHEMATICS
MAT3C11 : Number Theory

Time : 3 Hours

Max. Marks : 80

PART – A

Answer **any four** questions from Part – A. **Each** question carries 4 marks.

1. If (a, b) = 1, then prove that (a + b, a – b) is either 1 or 2.
2. Find all integers n such that $\varphi(n) = \varphi(2n)$.
3. Assume $a \equiv b \pmod{m}$. If d|m and d|a, then prove that d|b.
4. Determine those odd primes p for which (2|p) = 1 and for which (2|p) = –1.
5. Explain Knapsack problem.
6. Express the polynomial $t_1^2t_2 + t_1^2t_3 + t_1t_2^2 + t_1t_3^2 + t_2^2t_3 + t_2t_3^2$ in terms of elementary symmetric polynomials. **(4×4=16)**

PART – B

Answer **any four** questions from Part – **B** not omitting any Unit. **Each** question carries **16** marks.

UNIT – 1

7. a) State and prove the fundamental theorem of arithmetic.

   b) Show that the infinite series $\sum_{n=1}^{\infty} \frac{1}{P_n}$ diverges.

8. a) Show that if $n \geq 1$, then $\sum_{d/n} \varphi(d) = n$.

   b) Assume f is multiplicative, prove that $f^{-1}(n) = \mu(n)f(n)$ for every square free n.

P.T.O.

9. a) State and prove Lagrange theorem for polynomial congruence modulo prime p.
   b) State and prove Wilson's theorem.

UNIT – 2

10. a) State Gauss Lemma and prove the quadratic reciprocity law for Legendre symbol.
    b) Find the quadratic residues and non-residues modulo 13.

11. a) Let (a, m) = 1, prove that a is a primitive root mod m if and only if, the numbers $a, a^2, a^3, \ldots, a^{\varphi(m)}$ form a reduced system mod m.
    b) Let x be an odd integer. Prove that, if $\alpha \geq 3$ we have $x^{\frac{\varphi(2^\alpha)}{2}} \equiv 1 \pmod{2^\alpha}$, so there are no primitive roots mod $2^\alpha$.

12. a) Explain public key cryptosystem and explain the RSA public key algorithm.
    b) Solve the super increasing Knapsack problem
    $28 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$.

UNIT – 3

13. a) Prove that every symmetric polynomial in $R[t_1, t_2, \ldots, t_n]$ is expressible as a polynomial with coefficients in R in the elementary symmetric polynomials $s_1, s_2, \ldots, s_n$.
    b) Suppose that L is an extension of the field K, $p \in K[t]$, degree of polynomial p is n and the zeros of p are $\theta_1, \theta_2, \ldots, \theta_n \in L$. If $h(t_1, t_2, \ldots, t_n) \in K[t_1, t_2, \ldots, t_n]$ is symmetric, then prove that $h(\theta_1, \theta_2, \ldots, \theta_n) \in K$.

14. a) Prove that the set A of algebraic numbers is a subfield of the complex field $\mathbb{C}$.
    b) If $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$ is a basis of K consisting of integers then prove that the discriminant $\Delta[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is a rational integer, not equal to zero.

15. a) Let d be a squarefree rational integer. Then prove that the integers of $\mathbb{Q}(\sqrt{d})$ are :
    i) $Z[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$  ii) $Z\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right]$ if $d \equiv 1 \pmod 4$
    b) Find the integral basis and discriminant for $\mathbb{Q}(\sqrt{-7})$. (4×16=64)