Reg. No. : ....

Name : ....

III Semester M.Sc. Degree (CBSS – Reg./Sup./Imp.)
Examination, October 2022
(2019 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. Prove that the infinite series $\sum_{n=1}^{\infty} 1/P_n$ diverges.
2. State and prove Euclid's lemma.
3. If f is multiplicative then prove that f(1) = 1.
4. Assume that (a, m) = d. Then prove that the linear congruence $ax \equiv b \pmod m$ has solutions if and only if d|b.
5. Determine whether 219 is a quadratic residue or non residue mod 383.
6. Prove that an algebraic number α is an algebraic integer if and only if its minimum polynomial over Q has coefficients in Z.

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 division algorithm.
   b) Prove that every integer n > 1 is either a prime number or a product of prime numbers.

P.T.O.

8. a) If $n \geq 1$, then Prove that $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.
   b) Assume f is multiplicative. Prove that $f^{-1}(n) = \mu(n)\, f(n)$ for every square free n.
9. a) State and prove Lagrange's theorem.
   b) Solve the congruence $5x \equiv 3 \pmod{24}$.

Unit – 2

10. a) Prove that the Legendre' symbol (n|p) is a completely multiplicative function of n.
    b) State and prove quadratic reciprocity law.
11. a) Let (a, m) = 1. Then prove that if a is a primitive root mod m if and only if the numbers $a, a^2, \ldots, a^{\phi(m)}$ form a reduced residue system mod m.
    b) If p is an odd prime and $\alpha \geq 1$ then prove that there exist an odd primitive roots g modulo p^α and each such g is also a primitive root modulo $2p^\alpha$.
12. a) Write in detail any one application of primitive roots in cryptography.
    b) Solve the superincreasing knapsack problem.
    $28 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$

Unit – 3

13. a) Prove that every subgroup H of a free abelian group G of rank n is free of rank $s \leq n$. Moreover there exist a basis $u_1, u_2, \ldots, u_n$ of G and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$ such that, $\alpha_1 u_1, \alpha_2 u_2, \ldots, \alpha_s u_s$ is a basis for H.
    b) Let G be a free abelian group of rank n with basis $\{x_1, x_2, \ldots, x_n\}$. Suppose (a_{ij}) is an $n \times n$ matrix with integer entries. Then prove that the elements $y_i = \sum_j a_{ij} x_j$ form a basis of G if and only if (a_{ij}) is unimodular.

14. a) Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \in D$ form a Q-basis for K. Then prove that if $\Delta[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is square free then $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is an integral basis.
    b) Prove that every number field K possess an integral basis and the additive group of D is free abelian group of rank n equal to the degree of K.
15. a) Let d be a square free rational integer. Then prove that the integers of $Q(\sqrt{d})$ are
       a) $Z|\sqrt{d}|$ if $d \not\equiv 1 \pmod 4$
       b) $Z|\frac{1}{2} + \frac{1}{2}\sqrt{d}|$ if $d \not\equiv 1 \pmod 4$.
    b) Prove that the minimum polynomial of $\xi = e^{\frac{2\pi i}{p}}$, p an odd prime, over Q is $f(t) = t^{p-1} + t^{p-2} + \ldots + t + 1$ and the degree of $Q(\xi)$ is $p - 1$.

____