K21P 1068

Reg. No. : ....

Name : ....

III Semester M.Sc. Degree (CBSS – Reg./Suppl./Imp.) Examination, October 2021
(2018 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, if(a,b) = 1 and (a,c) =1, then (a,bc) = 1.

2. Prove that $\varphi(n) > \frac{n}{6}$ for all n with at most 8 distinct prime factors.

3. If n>1 and $(n-1)!+1 \equiv 0 \pmod n$, then prove that n is a prime.

4. Determine those odd primes p for which $(-1/p) = 1$ and for which $(-1/p) = -1$.

5. Explain the factorization problem with an example.

6. Express the polynomial $t_1^2 + t_2^2 + t_3^2$ in terms of elementary symmetric polynomials.

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) If $n \geq 1$, prove that $\varphi(n) = n\prod_{p/n} (1-\frac{1}{p})$.

   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 Chinese remainder theorem.

   b) Show that the of lattice points in the plane visible from the origin contains arbitrarily large gaps.

UNIT – 2

10. a) State and prove Gauss' lemma.

    b) Prove that Legendre's symbol is a completely multiplicative function.

11. a) If p is an odd prime and $\alpha \geq 1$,then prove that there exist odd primitive roots g modulo p^{α} and each such g is also a primitive root modulo $2p^{\alpha}$

    b) Given $m \geq 1$, where m is not of the form m = 1, 2, 4, p^{α} or $2p^{\alpha}$, where p is an odd prime. Then prove that for any a with (a, m) = 1 we have $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$.

12. a) Explain the RSA public key algorithm with an example.

    b) Compare Private Key and Public Key Cryptosystems.

UNIT – 3

13. a) 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.

    b) Let G be a free abelian group of rank r and H a subgroup of G. Then prove that $\frac{G}{H}$ is finite if and only if the ranks of G and H are equal.

14. a) Prove that the set A of algebraic numbers is a subfield of the complex field $\mathbb{C}$.

    b) Prove that the algebraic integers form a subring of the field of algebraic numbers.

15. a) Prove that the minimal polynomial of $\zeta = e^{\frac{2\pi i}{p}}$ p an odd prime, over $\mathbb{Q}$ is $f(t) = t^{p-1} + t^{p-2} + \ldots + t + 1$ and the degree of $\mathbb{Q}(\zeta)$ is $p-1$.

    b) Find integral basis and discriminant for $\mathbb{Q}(\sqrt{3})$.
