Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 40793

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2021.

Fifth Semester

Computer Science and Engineering

MA 8551 — ALGEBRA AND NUMBER THEORY

(Common to Computer and Communication Engineering/Information Technology)

(Regulations 2017)

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Consider a set G together with a well defined binary operation * on it. Let $e_1, e_2 \in G, * >$ such that $e_1 = a = a * e_1 = a$ and $e_2 = a = a * e_2 = a$ for all $a \in G$. What is the relation between e_1 and e_2? Justify your answer.

2. Prove or disprove: Every Field is an Integral domain.

3. Suppose $p(x)$ and $q(x)$ are two polynomials each of degree m and n respectively, over the ring of integer moduto 8. The degree of the polynomial $p(x)q(x)$ is $m + n$. Comment on this statement.

4. Consider the polynomial $p(x) = x^2 + 2x + 6$ in the field $Z_7[x]$. What are the factors of $p(x)$?

5. Let a, b and c be any integers. If $a \mid b$ and $b \mid c$, then prove that $a \mid c$.

6. Find the $GCD(161, 28)$ using Euclidean algorithm.

7. Is it possible to find the remainder when 1! + 2! + 3! + + 100! is divided by 15? Justify your answer.

8. Compute the value of x such that $2^8 \equiv x(\text{mod } 7)$.

9. Compute the value of $\tau(18)$ and $\sigma(28)$.

10. If ϕ denotes Euler's totient function, then compute value of $\phi(\phi(38))$.

PART B — ($5 \times 16 = 80$ marks)

11. (a) State and prove Lagrange's theorem. (16)

Or

(b) If $f : (R, +, \cdot) \to (S, \oplus, \odot)$ is a ring homomorphism from R to S then prove the following:

(i) If R is a commutative ring then S is a commutative ring. (8)

(ii) If I is an ideal of R then $f(I)$ is an ideal of S. (8)

12. (a) Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ be a polynomial of *degree n* with integer coefficients, and let p be a prime number. Suppose that p does not divide a_n, p divides $a_0, a_1, a_2 \ldots a_{n-1}$, and p^2 does not divide a_0. Then prove that the polynomial f is irreducible over the field Q of rational numbers. Also verify whether or not the polynomial $3x^5 + 15x^4 - 20x^3 + 10x + 20$ is reducible over Q. (16)

Or

(b) Suppose $f(x) = x^2 + 1$ and $g(x) = x^4 + x^3 + x^2 + x + 1$ are the two polynomials over the field $Z_2[x]$ then

(i) Find $q(x)$ and $r(x)$ such than $g(x) = q(x)f(x) + r(x)$ where $r(x) = 0$ or degree of $r(x) <$ degree of $f(x)$. (12)

(ii) Compute $f(x)g(x)$. (4)

13. (a) Let a be any integer and b a positive integer. Then prove that there exist unique integers q and r such that $a = bq + r$ where $0 \le r \le b$. (16)

Or

(b) State and prove fundamental theorem of arithmetic. (16)

14. (a) (i) Solve the linear Diophantine equation $1076x + 2076y = 3076$. (8)

(ii) Find all the solutions of $2076x = 3076 \pmod{1076}$. (8)

Or

(b) (i) Compute the remainder when 3^{247} is divided by 17 (8)

(ii) Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12. (8)

15. (a) (i) Prove that "A positive integer a is self invertible modulo p if and only if $a \equiv \pm 1 (\mathrm{mod}\ p)$". (8)

(ii) State and prove Wilson's Theorem. (8)

Or

(b) (i) If p is a prime number and a is any integer such that $p \nmid a$ then prove that $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. (8)

(ii) State and prove Euler's Theorem. (8)