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

Question Paper Code : 30879

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2024.

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 — ($10 \times 2 = 20$ marks)

1. List all the generators of $(\mathbb{Z}_{12}, \oplus)$.

2. Determine all the units of $(\mathbb{Z}_9, \oplus, \circ)$.

3. Define irreducible polynomial with example.

4. Check whether the polynomial $x^4 + 2x + 2$ is irreducible or not over the field of rational.

5. Find the number of positive integers ≤ 2076 and divisible by neither 4 nor 5.

6. Express 3014 in base eight.

7. Find the remainder when 16^{53} is divided by 7.

8. Determine whether the LDEs $12x + 18y = 30$, $2x + 3y = 4$ and $6x + 8y = 25$ are solvable.

9. Compute: $\phi(16)$ and $\phi(28)$.

10. Solve the linear congruence $35x \equiv 47 \pmod{24}$.

PART B — (5 × 16 = 80 marks)

11. (a) (i) State and prove Lagrange's theorem. (8)

(ii) If H and K are two subgroups of a group G then HK is a subgroup of G if and only if HK = KH. (8)

Or

(b) (i) Find the units of the Gaussian integer $\mathbb{Z}[i]$. (6)

(ii) Let $f: R \to R'$ be an onto ring homomorphism and $I = Ker(f) = \{x \in R \mid f(x) = 0\}$. Then show that $\frac{R}{I}$ is isomorphic to R'. (10)

12. (a) (i) Let R be a commutative ring with unity whose only ideals are $\{0\}$ and R itself, then show that R is a field. (10)

(ii) Show that if a polynomial $f(x)$ is divided by $(x - a)$, then $f(a)$ is the remainder. (6)

Or

(b) (i) Prove that every Euclidean ring is a Principal Ideal Domain. (8)

(ii) Let $f(x) = 2x^2 + 3x^3 - 5x^2 - 3x + 1$ and $g(x) = 7x^4 - 5x^3 + 2x^2 - x + 11$. Compute $f(x).g(x)$ in the following ring

(I) $\mathbb{Q}[x]$, (2)

(II) $\mathbb{Z}_7[x]$, (2)

(III) $\mathbb{Z}_2[x]$, and (2)

(IV) $\mathbb{Z}_{11}[x]$ (2)

13. (a) (i) State and prove division algorithm. (8)

(ii) Prove that the product of any two integers of the form $4n + 1$ is also of the same form. (8)

Or

(b) (i) State and prove fundamental theorem of arithmetic. Using this to find the canonical decomposition of 2520. (10)

(ii) Explain Euclidean algorithm and using it. Express GCD (4076, 1024) as a linear combination of 4076 and 1024. (6)

14. (a) (i) Solve the LDE $1076x + 2076y = 3076$ by Euler's method. (8)

(ii) Find the general solution of the LDE $6x + 8y + 12z = 10$. (8)

Or

(b) (i) Find the remainder when $(n^2 + n + 41)^2$ is divided by 12. (8)

(ii) State the Chinese Remainder Theorem (CRT) and Using CRT to solve the system $x \equiv 1 (\text{mod}\, 3)$, $x \equiv 2 (\text{mod}\, 4)$, $x \equiv 3 (\text{mod}\, 5)$. (8)

15. (a) (i) State and Wilson theorem. Using this theorem to show that $\frac{(np)!}{n!\, p^n} \equiv (-1)^n (\text{mod}\, p)$, where p is prime and n is any positive integer. (10)

(ii) State the Fermat's theorem and using this theorem to find the remainder when 24^{1947} divided by 17. (6)

Or

(b) (i) State and Prove Euler's theorem. Using this theorem find the remainder when 245^{1040} is divided by 18. (8)

(ii) Prove that, if a and b are relatively prime, then $a^{\varphi(b)} + b^{\phi(a)} \equiv 1 (\text{mod}\, ab)$. (8)