Reg. No. :

Question Paper Code : 80874

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 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 × 2 = 20 marks)

1. Let $G = \langle Z_6, +_6 \rangle$ Suppose $H = \{0, 2, 4\}$, can $\langle H, +_6 \rangle$ be a group under the binary operation $+_6$ modular addition 6? If so, what is the relation between H and G? If not, give the reason.

2. Let a, b be any two elements in a ring R. Prove or disprove : $a(-b) = (-a)b = -(ab)$.

3. Consider the polynomials $p(x) = 4x^2 + 1$ and $q(x) = 2x + 3$ in the ring $Z_8[x]$. The degree of the polynomial $p(x)q(x)$ is 3 in $Z_8[x]$. Comment on this statement.

4. The polynomial $x^2 + 1$ is a reducible polynomial over z_5. Comment on this statement.

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(120, 28) using Euclidean algorithm.

7. Is it possible to find the remainder when 1! + 2! + 3! + ...+ 50! is divided by 12? Justify your answer.

8. Compute the value of m such that $2^{161} \equiv m \pmod 5$.

9. If ϕ denotes Euler's totient function, then compute value of $\phi(240)$.

10. Compute the value of $\tau(23)$ and $\sigma(12)$.

PART B — ($5 \times 16 = 80$ marks)

11. (a) Prove that, If G is a finite group and H is a subgroup of G then $O(H)$ divides $O(G)$. (16)

Or

(b) (i) Prove that every finite integral domain is a field. (8)

(ii) Let $\varphi : Z_4 \to Z_6$ defined as $\varphi(x) = 5x$. Prove that φ is a ring homomorphism under the usual operations defined on Z_4 and Z_6. (8)

12. (a) (i) Find the quotient and remainder when $f(x) = 3x^4 + x^3 + 2x^2 + 1$ is divided by $g(x) = x^2 + 4x + 2$, it is given that $f(x)$ and $g(x)$ are two polynomials in $Z_5[x]$. (8)

(ii) Determine whether the polynomials given below are irreducible? If so, give the reason, if not, provide their factors. $f(x) = x^4 + 2x^2 + 1$ over Q and $g(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$ over Q. (8)

Or

(b) (i) Prove that, the product of two primitive polynomials is primitive. (8)

(ii) Let $f(x) \in Z[x]$. If $f(x)$ is reducible over Q, then it is reducible over Z. (8)

13. (a) (i) Express 3014 in base eight. (8)

(ii) Study the following number pattern and add two more lines. In addition, establish the validity of the number pattern. (8)

$1.9 + 2 = 11$

$12.9 + 3 = 111$

$123.9 + 4 = 1111$

$1234.9 + 5 = 11111$

$12345.9 + 6 = 111111$

$123456.9 + 7 = 1111111$

$\vdots$

Or

(b) (i) Every composite number n has a prime factor less than or equal to $\lfloor \sqrt{n} \rfloor$. (8)

(ii) State and prove fundamental theorem of arithmetic. (8)

14. (a) (i) Twenty-three weary travelers entered the outskirts of a lush and beautiful forest. They found 63 equal heaps of plantains and seven single fruits, and divided them equally. Find the number of fruits in each heap. (8)

(ii) Find all the solutions of $12x \equiv 48 \pmod{18}$. (8)

Or

(b) (i) When 3^{247} is divided by 17, determine the remainder. (8)

(ii) Solve the following linear system.

$2x + 3y \equiv 4 \pmod{13}$ and $3x + 4y \equiv 5 \pmod{13}$ (8)

15. (a) (i) State and prove Fermat's little theorem. (8)

(ii) Let p be a prime. Then prove that $(p-1)! \equiv -1 \pmod{p}$. (8)

Or

(b) Let m be a positive integer and a be any integer with $(a, m) = 1$. Then prove that $a^{\phi(m)} \equiv 1 \pmod{m}$. Use this result and evaluate the remainder when 245^{1040} is divided by 18. (16)

———————