

Reg. No. :

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code : 40878

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2025.

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. Define the group and given an example.
2. Define homomorphism.
3. What is meant by a root of the polynomial?
4. Define reducible polynomial.
5. Check whether the given $s(x) = x^2 + x + 2$ in $z_3[x]$ polynomial is irreducible or not.
6. Prove that 15,036 in the hexadecimal system, that is, in base sixteen.
7. Find the number of positive integer's ≤ 2076 and divisible by neither 4 nor 5.
8. Solve, if possible, Mahavira's puzzle if there were 24 travelers.
9. Let $p=11$. Then $(p-1)! = 10! = 1.2.3.4.5.6.7.8.9.10$. Prove that the least residues modulo 11 that are self-invertible are 1 and 10.
10. Let p be a prime and a any integer such that $p \nmid a$. Then prove that the solution of the linear congruence $ax \equiv b \pmod{p}$ is given by $x \equiv a^{p-2}b \pmod{p}$.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Let $(G, \circ), (H, *)$ be groups with respective identities e_G, e_H . If $f: G \rightarrow H$ is a homomorphism, then prove that $f(e_G) = e_H$, $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$ and $f(a^n) = [f(a)]^n$ for all $a \in G$ and $n \in \mathbb{Z}$, also prove that $f(S)$ is a subgroup of H for each subgroup S of G .

- (ii) Let G be a cyclic group. Then prove that, if $|G|$ is infinite, then G is isomorphic to $(\mathbb{Z}, +)$. And if $|G| = n$, where $n > 1$, then G is isomorphic to $(\mathbb{Z}_n, +)$.

Or

- (b) (i) State and prove Lagrange's theorem.
(ii) Let any ring $(R, +, \cdot)$ is a subring, if $\emptyset \neq S \subseteq R$, then show that $(S, +, \cdot)$ is a subring of R if and only if for all $a, b \in S$, we have $a - b \in S$ and $ab \in S$ and give the example.

12. (a) (i) Using long division and solve the given polynomial $f(x) = 3x^2 + 4x + 2$ and $g(x) = 6x^4 + 4x^3 + 5x^2 + 3x + 1$.
(ii) If $f(x) \in F[x]$ has degree $n \geq 1$, then $f(x)$ has at most n roots in F .

Or

- (b) State and prove Division Algorithm.

13. (a) Add two more rows to the following pattern, conjecture a formula for the n^{th} row and prove it:

$$9.9 + 7 = 88$$

$$98.9 + 6 = 888$$

$$987.9 + 5 = 8888$$

$$9876.9 + 4 = 88888$$

$$98765.9 + 3 = 888888$$

....

Or

- (b) State and prove Lamé's theorem.

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

Or

- (b) State and prove Chinese Remainder Theorem.

15. (a) Find the primes p for which $\frac{2^{p-1}-1}{p}$ is a square.

Or

- (b) (i) Let p be a prime. Then show that $(p-1)! \equiv -1 \pmod{p}$.

- (ii) Find the remainder when 24^{1947} is divided by 17.
-

