

Reg. No. :

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

Question Paper Code : 90822

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2022.

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

PART A — (10 × 2 = 20 marks)

1. (a) Choose the correct option:

Which of the following set is/are group under (+, .)

- (i) Set of all real numbers (\mathbb{R})
- (ii) \mathbb{N} - set of natural number
- (iii) Set of all integer (\mathbb{Z})
- (iv) All of the above

- (b) True (or) False: Every subgroup of a cyclic group is cyclic.

2. If \mathbb{R} has no proper divisors of zero. Then \mathbb{R} is called _____

- (a) Field
- (b) integral domain
- (c) group
- (d) none of these

3. Define Root of polynomial.

4. Define relatively prime.

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

6. Express 10110_{two} in base ten.
7. Prove that no prime of the form $4n + 3$ can be expressed as the sum of two squares.
8. Solve the linear system $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$.
9. Statement only: Fermat's little theorem.
10. Define Euler phi function.

PART B — ($5 \times 16 = 80$ marks)

11. (a) For every group G , prove that the following statements.
 - (i) the identity of G is unique.
 - (ii) the inverse of each element of G is unique.
 - (iii) if $a, b, c \in G$ and $ab = ac$ then $b = c$. (Left cancellation property)
 - (iv) if $a, b, c \in G$ and $ba = ca$, then $b = c$. (Right cancellation property)

(16)

Or

- (b) (i) State and prove the Lagrange's theorem. (8)
 - (ii) Given a ring $(R, +, \cdot)$ for all $a, b \in R$, prove that the following statements
 - (1) $-(-a) = a$,
 - (2) $a(-b) = (-a)b = -(ab)$, and
 - (3) $(-a)(-b) = ab$ (8)
12. (a) (i) If $f(x) = 3x^2 + 4x + 2$ and $g(x) = 6x^4 + 4x^3 + 5x^2 + 3x + 1$ are polynomial in $Z_7[x]$, Find finite field. (8)
 - (ii) If $f(x) \in F[x]$ has degree $n \geq 1$, then prove that $f(x)$ has at most n roots in F . (8)

Or

- (b) (i) Prove that a finite field F has order p^t , where p is prime and $t \in \mathbb{Z}^+$. (8)
- (ii) Let $(F, +, \cdot)$ Be a field. If $\text{char}(F) > 0$, then prove that the $\text{char}(F)$ must be prime. (8)

13. (a) (i) Let $(a, b) = d$, then prove the following statements : (8)

$$(1) \quad \left(\frac{a}{d}, \frac{b}{d} \right) = 1$$

$$(2) \quad (a, a - b) = d$$

- (ii) If $d = (a, b)$ and d' is any common divisor of a and b , then prove that $d' \mid d$. (8)

Or

- (b) (i) Let a and b be any positive integers, and r the remainder, when a is divisible by b , then prove $(a, b) = (b, r)$. (8)

- (ii) Let f_i denote the i^{th} Fermat number then, prove that $f_0 f_1 \dots f_{n-1} = f_n - 2$, where $n \geq 1$. (8)

14. (a) (i) If a cock is worth five coins, a hen three coins, and three chicks together one coin, how many cocks, hens, and chicks, totaling 100, can be bought for 100 coins? (8)

- (ii) State and prove Chinese Remainder theorem. (8)

Or

- (b) (i) Prove : $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m . (8)

- (ii) Find the positive integers n for which $\sum_{k=1}^n k!$ is a square. (8)

15. (a) (i) Find the primes p for which $\frac{2^{p-1} - 1}{p}$ is a square. (8)

- (ii) Solve the congruence $24x \equiv 11 \pmod{17}$. (8)

Or

- (b) (i) State and prove: Euler's Theorem and find the remainder 245^{1040} is divided by 18. (8)

- (ii) State and prove: Fermat's Little theorem and solve the linear congruence $35x \equiv 47 \pmod{24}$. (8)