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 — ($10 \times 2 = 20$ 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 $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ 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 $a \equiv \pm 1 \pmod{p}$". (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 $a^{p-1} \equiv 1 \pmod{p}$. (8)

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

Roll No.

QUESTION PAPER CODE: X10666

B.E. / B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2020
Fifth Semester
Computer Science and Engineering
MA8551 –ALGEBRA AND NUMBER THEORY
(Common to Computer and Communication Engineering and Information Technology)
(Regulations 2017)
Answer ALL Questions

Time: 3 Hours **Maximum Marks:100**

PART-A (10×2=20 Marks)

1. Find the inverse of 3 under the binary operation $*$ defined in R by $a * b = \frac{ab}{3}$.
2. How many units and proper zero divisors are there in Z_{17}.
3. Given an example of a polynomial that is irreducible in $Q[x]$ and reducible in $C[x]$.
4. If $f(x) = 2x^4 + 5x^2 + 2$ and $g(x) = 6x^2 + 4$, then determine $f(x) \cdot g(x)$ in $Z_7[x]$.
5. State the pigeonhole principle.
6. Find six consecutive integers that are composite.
7. When does the linear congruence $ax \equiv b \pmod m$ has a unique soloution?
8. Find the remainder when 4^{117} is divided by 15.
9. State Wilson's theorem.
10. Find the value of $\tau(n)$ and $\sigma(n)$ for $n = 29$.

PART-B (5×16=80 Marks)

11. (a) (i) Determine whether $(Z, \oplus, \odot)$ is a ring with the binary operation $x \oplus y = x + y - 7$, $x \odot y = x + y - 3xy$ for all $x, y \in Z$. (8)

(ii) For any group G, prove that G is abelian, if and only if, $(ab)^2 = a^2b^2$ for all $a, b \in G$. (8)

(OR)

(b) (i) Prove that Z_n is field, if and only if, n is a prime. (8)

(ii) Find$[777]^{-1}$ in Z_{1009}. (8)

12. (a) (i) State and prove the factor theorem and remainder theorem. (8)

(ii) Find the remainder, when $f(x) = x^{100} + x^{90} + x^{80} + x^{50} + 1$ is divided by $g(x) = x - 1$ in $Z_2[x]$. (8)

(OR)

(b) (i) If $(F, +, \cdot)$ is a field and $char(F) > 0$, then prove that $char(F)$ must be prime. (8)

(ii) Find the gcd of $x^4 + x^3 + x + 1$ and $x^3 + x^2 + x + 1$ in $Z_2[x]$. (8)

13. (a) (i) Find the number of positive integers ≤ 3000 and divisible by 3, 5 or 7. (8)

(ii) Apply Euclidean algorithm to express the gcd of 2076 and 1776 as a linear combination of themselves. (8)

(OR)

(b) (i) Prove that there are infinitely many primes. (8)

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

14. (a) (i) Find the general solution of the linear Diophantine equation $6x + 8y + 12z = 10$. (8)

(ii) Prove that no prime of the form $4n + 3$ can be expressed as the sum of two squares. (8)

(OR)

(b) (i) Solve $x \equiv 2(\mod 5)$, $x \equiv 3(\mod 7)$ using Chinese remainder theorem. (8)

(ii) Solve the linear system $\begin{array}{l} 3x + 4y \equiv 5(\mod 7) \\ 4x + 5y \equiv 6(\mod 7) \end{array}$. (8)

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

(ii) Let n be a positive integer with canonical decomposition $n = p_1^{\theta_1} p_2^{\theta_2} \ldots p_k^{\theta_k}$. Derive the formula for evaluating Euler's phi function $\phi(n)$ and hence, evaluate the same for $n = 6125$. (8)

(OR)

(b) (i) Solve the linear congruence $25x \equiv 13 (\mod 18)$. (8)

(ii) Prove that tau and sigma functions are multiplicative. (8)

* * * * * * *

Reg. No. :

Question Paper Code : 90348

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2019
Fifth Semester
Information Technology
MA 8551 – ALGEBRA AND NUMBER THEORY
(Common to Computer Science and Engineering/Computer and Communication Engineering)
(Regulations 2017)

Time : Three Hours Maximum : 100 Marks

Answer ALL questions

PART – A **(10×2=20 Marks)**

1. Define a subgroup and give one proper subgroup of $(Z_6, +)$.
2. Give an example for a cyclic group along with its generator.
3. Find all the roots of $f(x) = x^2 + 4x$ in $Z_{12}[x]$.
4. Give an example for an irreducible and reducible polynomial in $Z_2[x]$.
5. Find the number of positive integer's ≤ 3076 and not divisible by 17.
6. Using the canonical decomposition of 1050 and 2574, find their lcm.
7. Determine whether the LDE $2x + 3y + 4z = 5$ is solvable.
8. What is the remainder when 3^{31} is divided by 7 ?
9. State Fermat's little theorem.
10. If $n = 2^k$, then show that the value of Euler's phi function $\phi(n) = n/2$.

PART – B **(5×16=80 Marks)**

11. a) i) Let G be the set of all rigid motions of a equilateral triangle. Identify the elements of G. Show that it is a non-abelian group of order 6.

ii) Let G be a group with subgroups H and K. If $|G| = 660$, $|K| = 66$ and $K \subset H \subset G$, what are the possible values for $|H|$? **(8+8)**

(OR)

b) i) Prove that $(Q, \oplus, \circ)$ is a ring on the set of rational numbers under the binary operations $x \oplus y = x + y + 7$, $x \circ y = x + y + (xy/7)$ for $x, y \in Q$.

ii) Find $[100]^{-1}$ in Z_{1009}. **(8+8)**

12. a) i) If $f(x) \in F[x]$ has degree $n \geq 1$, then prove that $f(x)$ has at most n roots in F.

ii) Find the gcd of $x^{10} - x^7 - x^5 + x^3 + x^2 - 1$ and $x^8 - x^5 - x^3 + 1$ in $Q[x]$. **(8+8)**

(OR)

b) Prove that a finite field F has order p^t, where p is a prime and $t \in Z^+$. **(16)**

13. a) i) Prove that there are infinitely many primes.

ii) Prove that the gcd of the positive integers a and b is a linear combination of a and b. **(8+8)**

(OR)

b) i) Apply Euclidean algorithm to express the gcd of 1976 and 1776 as a linear combination of themselves.

ii) Prove that the product of gcd and lcm of any two positive integers a and b is equal to their products. **(8+8)**

14. a) i) Find the general solution of the LDE $15x + 21y = 39$.

ii) Solve the linear system. **(8+8)**

$5x + 6y \equiv 10 \pmod{13}$

$6x - 7y \equiv 2 \pmod{13}$

(OR)

b) State and prove Chinese Remainder Theorem. Using it find the least positive integer that leaves the remainder 1 when divided by 3, 2 when divided by 4 and 3 when divided by 5. **(16)**

15. a) i) State and prove Wilson's theorem.

ii) Using Euler's theorem find the remainder when 245^{1040} is divided by 18. **(8+8)**

(OR)

b) Let n be a positive integer with canonical decomposition $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Derive the formulae for Tau and Sigma functions. Hence evaluate $\tau(n)$ and $\sigma(n)$ for $n = 1980$. **(16)**