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)
