Regn. No: | | | | | | | | | | |

[F.T]

B.E & B.Tech DEGREE END SEMESTER EXAMINATIONS, APRIL 2019
B.E Computer Science and Engineering & B.Tech Information Technology
Third Semester
MA8351 Algebra and Number Theory
(REGULATION 2012)

Time: 3 Hours | Answer ALL Questions | Maximum Marks:100

Part- A (10x2=20 Marks)

1. Show that the identity element in a group is unique.
2. Examine whether the set $\{-1, 0, 1\}$ forms a group under addition of integers.
3. Does the set $\{0, 1, 2, 3\}$ form a field with respect to addition modulo 4 and multiplication modulo 4 ? Why?
4. What is the remainder when $f(x) = x^{101} + x^{99} + x^{89} + x^{49} + 1 \in \mathbb{Z}_2[x]$ is divided by $g(x) = (x - 1) \in \mathbb{Z}_2[x]$?
5. Find five consecutive composite integers.
6. Find the number of positive integers ≤ 2076, and divisible by neither 4 nor 5.
7. Examine whether the congruence $4x \equiv 8 (\text{mod } 9)$ is solvable. Justify your answer?
8. State Chinese Remainder Theorem
9. State Euler's theorem.
10. Find the remainder when 100! is divided by 101.

Part- B (5x16=80 Marks)

11.a(i) State and prove Euler's Theorem. (8)

(ii) What is the remainder you get when 192^{183} is divided by 19? Justify your answer? (8)

12.a(i) Let $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Show that $\{A, A^2, A^3, A^4\}$ is a group under matrix multiplication and is isomorphic to $\{1, -1, i, -i\}$ under complex multiplication. (8)

a(ii) Let $(G, \circ)$ and $(H, *)$ be two groups with respective identities e_G and e_H. If $f : G \longrightarrow H$ is a homomorphism, then prove that
(1) $f(e_G) = e_H$, (2) $f(a^n) = [f(a)]^n$ for $a \in G$, (3) $f(a^{-1}) = [f(a)]^{-1}$ for $a \in G$,
(4) $f(s)$ is a subgroup of H for each subgroup S of G. (8)

(OR)

12.b(i) Show that $G = \{1, i, -i, -1\}$ is a group under multiplication of complex numbers and is isomorphic to $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ under multiplication modulo 5. Verify that orders of the elements of G divide order of G. (8)

(ii) Show that subgroup of a cyclic group is cyclic (8)

13.a(i) Construct a field consisting of four elements(Hint: use the irreducible binary polynomial $x^2 + x + 1$). (8)

(ii) Show that $\mathbb{Z}_n$ is a field with respect to addition modulo n and multiplication modulo n if and only if n is a prime. (8)

(OR)

13.b(i) Determine whether the following polynomials are irreducible over the given fields
(a) $x^2 + x + 1$ over $\mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$
(b) $x^4 + x^2 + 1$ over $\mathbb{Z}_2$
(c) $x^3 + 3x^2 - x + 1$ over $\mathbb{Z}_5$. (8)

(ii) Prove that every finite field F has exactly p^n elements for some prime number p and positive integer n. (8)

14.a(i) Let a and b be positive integers. Show that there exist integers m and n such that $ma + nb = gcd(a, b)$. (8)

(ii) Let b be an integer ≥ 2. Suppose $b+1$ integers are randomly selected. Prove that the difference of two of them is divisible by b. (8)

(OR)

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

(ii) Find the number of positive integers less than or equal to 3000 and divisible by 2, 5 or 7. Also show that the product of two consecutive integers is even. (8)

15. a(i) Solve the following system of linear congruences: (8)

$$x + 3y \equiv 3 (\text{mod } 11)$$
$$5x + y \equiv 5 (\text{mod } 11).$$

(ii) Show that the linear congruence $ax \equiv b(\text{mod } m)$ is solvable if and only if $gcd(a, m)$ divides b. Also show that if $gcd(a, m)$ divides b, then it has d incongruent solutions, where $d = gcd(a, m)$. (8)

(OR)

15.b(i) Solve the following system of congruences: $x \equiv 2(\text{mod } 3); x \equiv 1(\text{mod } 4); x \equiv 5(\text{mod } 11)$. (8)

(ii) Show that the linear diophantine equation $ax + by = c$ is solvable if and only if gcd(a,b) divides c. (8)