12\11\13

Roll No.										

B.E. (Full Time) DEGREE END SEMESTER EXAMINATIONS, NOV / DEC 2013

Computer Science and Engineering

Third Semester

MA 8351 – ALGEBRA AND NUMBER THEORY

(Regulation 2012)

Time : 3 Hours — Answer ALL Questions — Max. Marks 100

PART-A (10 x 2 = 20 Marks)

1. Does the set $\{5n : n \in \mathbb{Z}\}$ form a group under addition? Justify your answer?
2. Examine whether $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ is a cyclic group under multiplication modulo 5.
3. Does the set $\{0, 1, 2, 3\}$ form a field with respect to addition modulo 4 and multiplication modulo 4 ? Why?
4. Let F be a field. Can F[x](set of all polynomials over F)be a field? Why?
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 linear Diophantine equation $12x + 16y = 18$ is solvable.Write the general solution if solvable.
8. Solve the linear congruence $3x \equiv 1 (\text{mod } 5)$.
9. State Euler's theorem.
10. Find the remainder when 100! is divided by 101.

Part- B(5x16=80 Marks)

11a. 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. (10)

ii. 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. (6)

12.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

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)

13.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. Show that every composite integer n has a prime factor $\leq \lfloor\sqrt{n}\rfloor$. (8)

OR

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

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

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

$$\begin{aligned} 5x + 6y &\equiv 10(\text{mod } 13) \\ 6x - 7y &\equiv 2(\text{mod } 13). \end{aligned}$$

ii. State and prove Chinese Remainder Theorem. (8)

OR

b. i. Find the least positive integer that leaves the remainder 1 when divided by 3, 2 when divided by 5 and 3 when divided by 7. (8)

ii. Determine whether the congruence $12x \equiv 48(\text{mod } 18)$ is solvable and also find all the solutions if solvable. (8)

15.a. i. State and prove Fermat's Little Theorem. (8)

ii. Find the remainder (a) when 13^{1102} is divided by 121. (4)
(b) When 193^{183} is divided by 19. (4)

OR

b. i. Show that Euler's phi function ϕ is multiplicative. (10)

ii. For $n = 11^3 \times 5$, verify that $\sum_{d/n} \phi(d) = n$. (6)