MA20013

Indian Institute of Technology, Kharagpur

Date...................... FN/AN   Time: 3 Hrs   Full Marks: 50   No. of Students: 77
End (Spring) Semester 2017-18   Subject Name: Discrete Mathematics
Deptt: MA/CE/MF/HS/EX/AE/EE

Instruction: Answer **all** questions. Notations used are as explained in the class.

Question 1 $[6 \times 2 = 12$ marks$]$

a) Let the positive integer n be written in terms of powers of the prime p so that we have $n = a_k p^k + \cdots + a_2 p^2 + a_1 p + a_0$, where a_i is integer with $0 \leq a_i < p$ for $i = 0, 1, \ldots, k$. Show that the exponent of the highest power of p appearing in the prime factorization of $n!$ is $\frac{n-(a_k+\cdots+a_2+a_1+a_0)}{p-1}$.

b) Find the inverse of ~~98~~ 89 mod 1972.

c) If an abelian group G of order 10 contains an element of order 5, prove that G must be a cyclic group.

d) Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 7 & 5 & 2 & 3 & 1 \end{pmatrix}$. Is α^{-1} an even permutation? Justify your answer.

e) Let $U_n = \{i : 1 \leq i < n, \mathsf{gcd}(i, n) = 1\}$. Show that U_8 is not a cyclic group.

f) i) Is the ring $Z_3[X]$ (mod $X^3 + X + 1$) a field? Explain your answer.

ii) Compute $(2X^2+X+2)+(2X+1)$ and $(2X^2+X+2).(2X+1)$ in $Z_3[X]$ (mod $X^3 + X + 1$).

Question 2 $[2 \times 4 = 8$ marks$]$

a) Express the following argument as a propositional formulae and establish its validity by the tableau method:
"*If it has snowed, it will be poor driving. If it is poor driving, I will be late unless I start early. Indeed, it has snowed. Therefore, I must start early to avoid being late.*"

b) Write the following statement in predicate logic and then negate it. Clearly mention what is your domain and predicates.
"*Let x and y be real numbers. If x is rational and y is irrational, then $x + y$ is irrational.*"

c) Three boxes are presented to you. One contains gold, the other two are empty. Each box has imprinted on it a clue as to its contents; the clues are:

Box 1: "*The gold is not here*"
Box 2: "*The gold is not here*"
Box 3: "*The gold is in* Box 2"

Only one message is true; the other two are false. Which box has the gold?
Formalize the puzzle in propositional logic and find the solution using a truth table.

d) Consider the following list of statements about a book:

i) There are three statements in this list.

ii) Two of them are not true.

iii) The average increase in IQ scores of those who read this book is more than 20 points.

Is statement (*iii*) true? Justify your answer.

Question 3 [$3 \times 3 = 9$ marks]

a) Given the Boolean function $F(x, y, z) = \overline{x}y + xy\overline{z}$, derive an algebraic expression for the complement of F. Express in sum-of-products form.

b) Use the Quine-McCluskey method to simplify the *sum-of-products* expression for

$$f(x, y, z) = xyz + xy\overline{z} + x\overline{y}z + x\overline{y}\,\overline{z} + \overline{x}yz + \overline{x}\,\overline{y}z + \overline{x}\,\overline{y}\,\overline{z}$$

c) Implement the following function with two-input NOR gates. Assume that both the normal and complement inputs are available.

$$A\overline{B}C\overline{D} + \overline{A}BC\overline{D} + A\overline{B}\,\overline{C}D + \overline{A}B\overline{C}D$$

Question 4 [$7 \times 3 = 21$ marks]

a) Let G be the set of four functions f_1, f_2, f_3, f_4 on $R - \{0\}$ defined by:

$$f_1(x) = x,\ f_2(x) = \frac{1}{x},\ f_3(x) = -x,\ f_4(x) = -\frac{1}{x},\ x \in R\{0\}.$$

Prove that $(G, \circ)$ is a commutative group where $\circ$ is the functional composition.

b) In a group G, for all $a, b \in G, (ab)^n = a^n b^n$ holds for three consecutive integers n. Prove that the group is abelian.

c) Suppose that a and $n > 1$ are relatively prime positive integers. Then prove that $a^i \equiv a^j \pmod{n}$ if, and only if, $i \equiv j \pmod{\mathrm{ord}_n(a)}$ for nonnegative integers i, j, where $\mathrm{ord}_n(a)$ denotes the order of a modulo n.

d) Let S_3 be the group of all permutations of the set $\{a, b, c\}$. In S_3, show that there are two elements f and g such that $(f \cdot g)^2 \neq f^2 \cdot g^2$.

e) Let $(G, \circ)$ be a finite cyclic group generated by a. Prove that $o(G) = n$ if and only if $o(a) = n$.

f) i) Determine whether there are any primitive roots mod 98; if so, how many will there be?

ii) If there are primitive roots mod 98, find one.

iii) If there are primitive roots, use the one you found in part (b) to construct another.

g) Let E be the modular elliptic curve defined by $y^2 = x^3 + 6x \pmod{13}$.

i) Find all points of E (including the point at infinity).

ii) Find $(4, 7) + (0, 0)$.