Seat No. : _______________

LH-118

April-2014

B.Sc. : Sem.-VI

Mathematics

MAT-311 : Elective

Convex Analysis & Probability Theory

Time : 3 Hours] **[Max. Marks : 70**

Instructions : (1) All the questions are compulsory. Notations are usual everywhere.

(2) Figures to the right indicate marks of the question.

1. (a) Define convex set and affine set. Also give an example of each of them. **9**

OR

Define convex and concave functions on an interval I.

Also show that the function $f : R \to R$ defined as $f(x) = x^2$ is a convex function on R.

(b) If I is an interval and $f : I \to R$ be a strictly monotonic function such that f (I) is an interval then prove that f is one-one and continuous. **9**

OR

If I is an interval containing more than one point and $f : I \to R$ is a differential function such that f is nonnegative throughout I then prove that f is monotonically increasing on I.

2. (a) Define following terms :

(i) Random experiments (ii) Equiprobable events

(iii) Difference events (iv) Subjective probability

(v) Classical probability **9**

OR

If the probabilities are respectively, 0.86, 0.35 and 0.29 that a family (randomly chosen for a sample survey in a metro city) will own a LED television set, colour television set or both kind of television sets,

(i) what is the probability that such a family will own either kind of set,

(ii) given that he owns a colour television set, what is the probability that he will own LED television set ?

(b) Given a finite sample space S, two mutually exclusive and exhaustive events B_1 and B_2 are defined on S. If P (B_1) and P (B_2) are non negative, then find the probability that any event A on S, occurs with respect to either B_1 or B_2. What is the total probability theorem ? Hence or otherwise, in usual notations, prove it and state the Bayes' rule. **9**

OR

Define conditional probability.

The married couples living in a certain suburb, the probability that the husband will vote in a school board election is 0.21 the probability that his wife will vote in the election is 0.28 and the probability that both will vote is 0.15. What is the probability that at least one will vote ? If it is known that husband will vote in the election, what is the probability that his wife will not vote in the election ?

3. (a) If from six to seven in the evening, one telephone line (X) in every five is engaged in a conversation. 10 telephone lines are selected at random. Do you suggest binomial distribution for X ? Also find

(1) probability that

(i) only two are used,

(ii) at the most three are used.

(2) Mean and Variance of the distribution. **9**

OR

State the probability mass function of Poisson distribution. State its mean and variance. Also, state the situations, where Poisson distribution is applied.

(b) The number of road construction projects that take place at any one time in a certain city follows a Poisson distribution with a mean of 3. Find the probability that

(i) exactly five road construction projects are currently taking place in this city.

(ii) At the most 2 road construction projects are currently taking place in this city,

(iii) At least 1 road construction projects is currently taking place in this city.

$\{e^{-1} = 0.368, e^{-2} = 0.135, e^{-3} = 0.050\}$ **9**

OR

Derive mean and variance of normal distribution. If mean and variance of normal distribution is zero and one, then state the probability function of normal distribution.

4. Attempt any **eight** of the following questions in short : **16**

(a) Define any **two** of the following terms :

(i) Hyper Plane

(ii) Convex combination

(iii) Monotonicity of functions

(b) Explain convex cone with figure.

(c) Give examples of monotonically increasing and decreasing functions on an interval I.

(d) Two coins are tossed, find the probability that two heads are obtained.

(e) A survey found that 21% of Americans watch fireworks on television July 4. Find the mean, variance, and standard deviation of the number of individuals who watch fireworks on television on July 4 if a random sample of 1000 Americans is selected.

(f) State the axiomatic definition of probability.

(g) A random variable X follows Poisson distribution with parameter m, such that $P(X = 2) = P(X = 3)$, then find parameter m and also find $P(X < 2)$.

(h) For two mutually exclusive events A, B on a finite sample space S,

$P(\overline{B} \mid A) = x$ Do you agree that the value of x is 1 ? If yes, justify.

(i) The blood groups of 200 people is distributed as follows : 50 have type A blood, 65 have B blood type, 70 have O blood type and 15 have type AB blood. If a person from this group is selected at random, what is the probability that this person has O blood type ?

(j) A spinner contains eight regions, numbered 1 through 8. The arrow has an equally likely chance of landing on any of the eight regions. If the arrow lands on the line, it is spun again. What is the probability that the arrow lands on an odd number ?

Seat No. : _______________

LH-118

April-2014

B.Sc. : Sem.-VI

Mathematics

MAT-311 : Elective

Cryptography

Time : 3 Hours] **[Max. Marks : 70**

Instructions : (1) There are **4** questions. **All** questions are compulsory.

(2) Figures to the right indicate full marks of the question.

1. (a) State and prove the Fermat's Little Theorem. **9**

OR

Explain Euclidean algorithm.

Using Euclidean algorithm explain extended Euclidean algorithm.

(b) Obtain the value of x that satisfies the following four congruence.
$x \equiv 4 \pmod{10}$, $x \equiv 6 \pmod{13}$, $x \equiv 4 \pmod{7}$ and $x \equiv 2 \pmod{11}$. **9**

OR

Using Shank's Algorithm, find the discrete logarithm of 431 (mod 37) with respect to the base 13.

2. (a) (1) Discuss Modern cryptography.

(2) Discuss relation between Hill cipher and Permutation cipher. **9**

OR

Define shift cipher and Affine cipher. A cipher text obtained using the shift cipher is given below. Do the cryptanalysis and obtain the plain text : HAAHJRHAKHDU

(b) Using Vigenere cipher with MATHEMATICS as the key : "Revolutions are not made ; they come." **9**

OR

Encrypt the following text using the permutation cipher scheme of

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$$

"Love which is not always springing is always dying".

3. (a) Alice selects $p = 23$ and $c = 5$ and convey the same to Bob. Alice selects $a = 6$ and Bob selects $b = 15$. What is private key exchange between them using the DH algorithm ? Show how Eve mounts an attack using Shank's algorithm and wrenches the private key shared between Alice and Bob. **9**

OR

Define Trapdoor function. Discuss Birthday Paradox.

(b) Alice and Bob select the prime number $p = 17$ with $g = 6$ as a primitive elements. Alice select a random number $a = 5$ as private key, computes her public key and sends it to Bob ; Bob uses $b = 9$ as the ephemeral key to mail a message $m = 13$ to Alice. Show the full transaction including the recovery of message key using ElGamal Public-Key cryptosystem. **9**

OR

With $p = 17$, $q = 19$, $e = 29$ and $m = 25$. Show that the complete transaction conforming to the RSA cryptosystem.

4. Attempt any **eight** in short : **16**

(a) State Euler's Theorem and give a simple illustrative example.

(b) Obtain the additive and multiplicative inverse of 3 in Z_7.

(c) Give an example of a linear Diophantine equation and give three solutions for it.

(d) What is a 'monoalphabetic cryptosystem' ? What is a 'Polyalphabetic cryptosystem' ?

(e) What is probability that at least two share a birthday form group of n people ?

(f) Which function suggested by Pollard to find discrete logarithm ?

(g) What is the fundamental theorem of arithmetic ? Give an illustrative example.

(h) Define Diagram, Trigram, Plaintext.

(i) Solve $x^2 \equiv 2 \pmod{39}$.

(j) Write two properties of primitive element in Z_p.

Seat No. : _______________

LH-118

April-2014

B.Sc. : Sem.-VI

Mathematics

MAT-311 : Elective

(Operation Research)

Time : 3 Hours] **[Max. Marks : 70**

Instructions : (1) **All** questions are compulsory.
(2) Figures to the right indicate full marks of the question.

1. Attempt any **three** : **18**

(1) Derive the EOQ formula with finite replenishment rate.

(2) Explain the order level, lot size (OLLS) system.

(3) Data relevant to component A used by Eng. India Pvt. Ltd. in 20 different assemblies includes :

Purchase price ₹ 15 per 100, annual usage 1,00,000 units, cost of buying office (fixed) ₹ 15,575 per annum, Set up cost ₹ 12 per order, Rent of component ₹ 3,000 per annum, Interest 25% per annum, insurance 0.05% per annum based on the total purchases, depreciation as 1% per annum of all items purchase.

(i) Calculate EOQ for component A.

(ii) The percentage changes in total annual costs relating to component A if the annual usage was 75,000 units.

(4) A dealer supplies you the following information with regard to a product deal in by him : Annual demand 5000 units, ordering cost ₹ 25 per order, inventory carrying cost is 30% per unit per year of purchase cost ₹ 100 per unit. The dealer is considering the possibility of allowing some back-orders to occur for the product. He is estimated that the annual cost of back ordering the product will be ₹ 10 per unit.

(i) What should be the optimum number of units of the product he should buy in one lot ?

(ii) What quantity of the product should he allow to be back – ordered ?

(iii) How much additional cost will he have to incur on inventory if he does not permit back – ordering ?

(5) The demand for an item in a company is 18,000 units per year and the company can produce the item at a rate of 3,000 units per month. The cost of one set-up is ₹ 500, the holding cost of one unit per month is ₹ 0.15 and the shortage cost of one unit is ₹ 20 per month.

Determine the optimum manufacturing quantity and the number of shortages. Also determine the manufacturing time and the time between two set-up ?

2. Attempt any **three** : **18**

(1) Explain the basic difference between PERT and CPM.

(2) Draw a network based on the given following information for a project.

Activity	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Immediate Predecessor	-	-	-	A,B	B,C	A,B	C	D,E,F	D	G	G	H,J	K	I,L

(3) Consider the following data regarding the project.

Activity	A	B	C	D	E	F	G	H	I
Immediate Predecessor	–	A	B	B	C	D	C	E,F	G,H
Duration	5	7	2	3	1	2	1	3	10

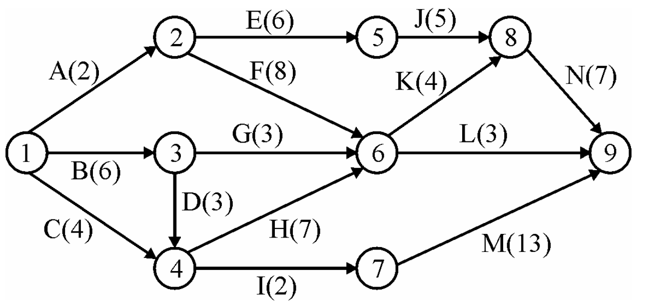
Construct the project network. Find total float and free float for each non-critical activities.

(4) A small project consists of 13 activities which take place and time for completion according as follows :

Activity	A	B	C	D	E	F	G	H	I	J	K	L	M
Immediate Predecessor	–	A	B	A	D	E	–	G	H,J	–	A	C,K	I,L
Duration	6	4	7	2	4	10	2	10	6	13	9	3	5

Draw the project network. Determine the critical path.

(5) For the given network project :



Indicate the critical path. Find the total float and free float for all activities. Also verify that the total float of all activities in the critical path are zero.

3. Attempt any **three** : **18**

(1) Explain the principle of dominance in Game theory.

(2) Explain the following terms :

(a) Pure strategy

(b) Mixed strategy

(c) Pay – off matrix

(3) Solve the game whose pay-off matrix is given below.

Player B

		B_1	B_2	B_3
Player A	A_1	-2	4	-1
	A_2	3	-1	4
	A_3	2	-2	3

Is this game fair ?

(4) Solve the following game by matrix method after reducing it to 2×2 matrix.

		Player B		
		B_1	B_2	B_3
Player A	A_1	1	7	2
	A_2	6	2	7
	A_3	5	1	6

(5) Using the method of oddments solve the following game whose pay-off matrix is given below.

		Player B		
		B_1	B_2	B_3
Player A	A_1	3	1	1
	A_2	1	1	5
	A_3	1	4	1

4. Attempt any **eight** : **16**

(1) List the costs which involved in inventory problem.

(2) Write down the EOQ formula for EOQ model with constant demand rate.

(3) In the EOQ model with constant demand, if the order quantity increased by 20% then how much total cost increase ?

(4) Draw the network for the following information :

Activity	A	B	C	D	E
Immediate predecessor	–	–	A	A,B	C,D

(5) What is the float ? List the types of float.

(6) Define : Critical activities. How to identify them ?

(7) Define : A zero-sum game.

(8) Give an example of pay-off matrix for game without saddle point.

(9) Determine the value of the game with the pay-off matrix.

		Player B		
		B_1	B_2	B_3
Player A	A_1	2	0	2
	A_2	1	-3	2

(10) List any two methods which are used to solve the games without saddle point.