PART (I) DISCRETE MATH.

1. Suppose X is a random variable which takes two values x_1 and x_2 with probability 0.3 and 0.7 respectively. Suppose that the value of X is to be revealed to us by some one who cannot communicate except by means of the words 'yes' and 'no'. What is the average number of questions required tq specify the outcome of a joint experiment involving two independent observations of X? (13%)

2. Consider the following relations on the set A={a,b,c}:
   f={(a,c), (b,c), (c,a)}
   g={(a,b), (c,a)}
   h={(a,c), (b,a), (a,b), (c,a)}
   l={(a,b), (b,c), (c,a)}
   Determine which relation(s) is a function? Which relation(s) is a 1−1 and onto function? (10%)

3. Let N be the set of all positive integers.
   Let
   $a*b=\gcd(a,b)$
   $a\circ b=a^b$,
   where gcd(a,b) denotes the greatest common divisor of a and b. Is (N,*) a semigroup? How about (N,$\circ$)? (10%)
   [Hint: A set S together with an associative operation is called a semigroup.]

4. Consider a context−free grammar G with the following productions:
   S −−> aAB
   A −−> Bba
   B −−> bB
   B −−> c.
   Can the word W='abcbabbc' be derived from S? Draw the derivation tree of W. (10%)

5. What is the coefficient of x^8y^9 in the expression $(2x-y)^{12}$? (7%)

PART (II) LINEAR ALGEBRA.

1. To prevent important information from being disclosed or eavesdropped by unauthorized users, it is required to transform the important information (M) into unintelligible information (C). The unintelligible information (C) should be able to be recovered to M by the authorized user.
If this transformation is specified by a set of matrices, what condition(s) should be put on these matrices? (10%)

2. A transformation is called cryptographically secure if it cannot be figured out (broken) knowing both M and C (see problem 1.) in polynomial time. Do you think the matrix transformation in problem 1 is cryptographically secure? Why? (10%)

3. Use Lagrange interpolation formula to find a polynomial f over GF(7) such that f has degree $=<2$ and

$$\begin{cases} f(1) = 2 \\ f(2) = 2 \\ f(3) = 1 \\ f(0) = 1 \end{cases} \pmod 7.$$

(10%)

4. Given the vectors

$$\beta_1 = (3,0,4)$$
$$\beta_2 = (-1,0,7)$$
$$\beta_3 = (2,9,11)$$

in R^3. Apply the Gram–Schmidt process to construct an orthogonal basis for R^3. (10%)

5. Define the following terms:
   (a) a monic polynomial, (5%)
   (b) the dimension of a vector space. (5%)