CS 170 - Fall 2003 - Midterm 2

Associate Professor Satish Rao

Problem 1: Number Theory and Cryptography (25 points)

1. Given a pair of numbers, x,y, where $GCD(x, y) = 1$, argue that x has an inverse mod y. You must start with the output of Euclid's extended algorithm.
2. Given a number $n = pq$ where p and q are prime integers, how many numbers in $Z_{\mathrm{n}} = \{0,...,n - 1\}$ do not have multiplicative inverses mod n?
3. Give a decryption key for the RSA public key (39, 7).
4. For a RSA public key (N, e), given that the RSA signature of a is x and the RSA signature of b is y give the signature of ab. (Recall that a signature is the encoding of a by the secret key.)

Problem 2: Coding (25 points)

1. Give the Huffman code for the character set { (a, 1/8), (b, 1/8), (c, 1/4), (d, 1/2) }.
2. What is the expected number of bits/character for a file with the frequencies as specified above?
3. What is the entropy of files generated from the distribution on part (a)? Does the Huffman coding achieve the entropy in terms of expected costs?
4. Give the Lempel-Ziv encoding of 001011010101, with dictionary size 4. (The empty string is A(0), so you get three more.)

Problem 3 (20 points)

Say a pony express rider wishes to minimize the number of horses that she uses along a M mile route, with n hitching posts at miles m_1, m_2,..., m_n, each of which contains k horses where the jth horse at the ith changing post can travel $t_{i,\,j}$ distance? (Assume she can only take one horse at a time.)

1. Does she ever need to use a horse that does not have the longest range among the k horses at any hitching post?
2. Give a dynamic programming algorithm to find the smallest number of horses she can use along the route.
3. Say the jth horse at the hitching post i costs $c_{i,\,j}$, give a dynamic programming algorithm to find the minimum cost set of horses she can use. (The number of horses she uses is not relevant.)

Problem 4 (20 points)

1. Give an $O(n^2)$ time algorithm to check if there is an interval (i.e., an interval is defined by an $i \leq j$ which specifies the numbers a_{i}, $a_{\mathrm{i+1}}$,..., a_{j}) that adds up to the number k.
2. Give an $O(nk)$ time algorithm to check if there is an interval that adds up to k.

3. Give an $O(nkt)$ time algorithm to check if there is a set of t nonoverlapping nonempty intervals that add up to k.

Problem 5: Linear Programming (10 points)

1. We presume you need at least 10 grams of fat and 6 grams of sugar in your diet. Say that a slice of pie contains 5 grams of fat per unit and 2 grams of sugar and costs 4 dollars per slice. Say that a piece of carrot cake contains 2 grams of fat and 2 grams of sugar and costs 3 dollars per slice.

   Write a linear program for this problem that minimizes the cost so that you get the required amount of fat and sugar. (You can buy fractions of pieces of cake or pie.)

   Write your linear program so that it has only two variables.