Problem 0:

(a) Show that, if E1, E2 , ••• , En are mutually independent, then so are $\overline{E_1}, \overline{E_2}, \dots, \overline{E_n}$.

(b) Give an example of three random events X, Y, Z for which any pair are independent but all three are not mutually independent.

(c) I choose a number uniformly at random from the range [1,1,000,000]. Using the inclusion-exclusion principle, determine the probability that the number chosen is divisible by one or more of 4 and 9.

(d) Determine the probability that the number chosen is divisible by one or more of 4, 6 and 9.

Problem 1:

Alice is trying to send Bob a love letter, saying "I love you" through a chain of friends; the letter goes through a series of n friends before it arrives to Bob. Each friend flips the word 'love' to 'hate' (both directions) independently with probability p.

(a) Compute the probability that Bob receives the original letter.

(b) We consider an alternative way to calculate this probability. Let us introduce the definition of bias; a friend has bias q if the probability she changes the word is (1 - q)/2. The bias q is therefore a real number in the range [-1, 1]. Prove that sending a bit through two friends with bias q1 and q2 is equivalent to sending a bit through one friend with bias q1*q2.

(c) Recomputation of (a). Prove that the probability that Bob receives the original letter when the letter passes through n friends is (1 + (2p - 1)^n)/ 2.

Problem 2:

I am playing in a racquetball tournament, and I am up against a player I have watched but never played before. I consider three possibilities for my prior model: we are equally talented, and each of us is equally likely to win each game; I am slightly better, and therefore I win each game independently with probability 0.6; or he is slightly better, and thus he wins each game independently with probability 0.6. Before we play, I think that each of these three possibilities is equally likely. In our match we play until one player wins three games. I win the second game, but he wins the first, third, and fourth. After this match, in my posterior mode, with what probability should I believe that my opponent is slightly better than I am?

Problem 3:

A medical company touts its new test for a certain genetic disorder. The false negative rate is small: if you have the disorder, the probability that the test returns a positive result is 0.999. The false positive rate is also small: if you do not have the disorder, the probability that the test returns a positive result is only 0.005. Assume that 2% of the population has the disorder. If a person chosen uniformly from the population is tested and the result comes back positive, what is the probability that the person has the disorder?

Problem 4:

We have a function $F: \{O, \dots, n - 1\} \rightarrow \{O, \dots, m - 1\}$. We know that, for $0 <= x, y <= n - 1$, $F((x + y) \bmod n) = (F(x) + F(y)) \bmod m$. The only way we have for evaluating F is to use a lookup table that stores the values of F. Unfortunately, a baby girl has changed the value of 1/5 of the table entries when her parents were not looking. Describe a simple randomized algorithm that, given an input z, outputs a value that equals F(z) with probability at least 1/2. Your algorithm should work for every value of z, regardless of what values the baby changed. Your algorithm should use as few lookups and as little computation as possible. Suppose I allow you to repeat your initial algorithm three times. What should you do in this case, and what is the probability that your enhanced algorithm returns the correct answer?

Problem 5:

Hashing is frequently used in password checking to protect against hacking. Instead of storing passwords as ciphertext or even as plaintext, a system stores them offline and store the hash map of passwords. Given a password, the system hashes the password and check if the hash index is not empty. Assume that there are m unique passwords, and the size of the hash map is n >> m, compute the probability of making wrong decision. Discuss the mechanism to reduce the probability.