CS 70 Discrete Mathematics and Probability Theory
Fall 2016 by Sinho Chewi, Jin Park, Alvin Wan, Davis Yang **Review**

1. **Divisible or Not**

   (a) Prove that for any number n, the number formed by the last two digits of n are divisible by 4 if and only if n is divisible by 4. (For example, '23xx' is divisible by 4 if and only if the number 'xx' is divisible by 4.)

   (b) Prove that for any number n, the sum of the digits of n are divisible by 3 if and only if n is divisible by 3.

2. **Squared RSA**

   (a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is relatively prime to p and p is prime.

   (b) Use the identity above to construct a RSA scheme. In other words, what is the public key and private key?

   (c) Prove that your scheme is correct, i.e. $x^{ed} \equiv x \pmod{N}$.

   (d) Prove that your scheme is unbreakable, i.e. your scheme is at least as difficult as ordinary RSA.

3. **Safety of Secret Sharing**

   In class we derived the secret sharing scheme to protect a secret s among n people such that any group of $\geq k$ people could recover the secret, and any group of $< k$ people cannot. In this problem let's explore the safety of secret sharing from a probability point of view. Suppose that we are working in the finite field GF(p). Alice, Bob and Cathy share a secret s that can be recovered if and only if all of them come together. Now, suppose that only Alice and Bob come together. Show that the probability of them recovering the secret is as low as the probability of a random guess.

4. **Berlekamp-Welch Algorithm with Fewer Errors**

   In class we derived how Berlekamp-Welch algorithm can be used to correct k general errors, given $n+2k$ points transmitted. In real life, it is usually difficult to determine the number of errors that will occur. What if we have less than k errors?

   Suppose Alice wants to send 1 message to Bob and wants to guard against 1 general error. She decides to encode the message with $P(x) = 4$ (on GF(7)) such that $P(0) = 4$ is the message she want to send. She then sends $P(0), P(1), P(2) = (4,4,4)$ to Bob.

   (a) Suppose Bob receives the message $(4,5,4)$. Without performing Gaussian elimination explicitly, find $E(x)$ and $Q(x)$.

(b) Now, suppose there were no general errors and Bob receives the original message $(4,4,4)$. Show that the $Q(x), E(x)$ that you found in part (a) still satisfies $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

(c) Show that $E(x) = x$, $Q(x) = 4x$ is another possible set of polynomials that satisfies $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

(d) Suppose you're actually trying to decode the received message $(4,4,4)$. Based on what you showed in the previous two parts, can you predict what will happen during row reduction when you try to solve for the unknowns?

(e) As you showed in the previous part, when there are less than k errors and Bob actually receives $n+2k$ packets, there will be multiple possible $Q(x)$ and $E(x)$ polynomials. Prove that no matter what the solution of $Q(x)$ and $E(x)$ are, the recovered $P(x)$ will always be the same.

5. **Hotel Bert**

Hillbilly Bert has a hotel H that has infinite rooms R_i where $i \in \mathbb{N}$. Due to the popularity of the hotel, each room is filled with one person P_i. However, infinite rooms allows him to accomodate more guests. Prove, with bijection, that he can accomodate the following:

(a) One new guest G_1.

(b) Infinitely new guests G_j where $j \in \mathbb{N}$.

(c) Consider a car with infinite guests, $C_j = (G_{j1}, G_{j2}, ...)$ where $j \in \mathbb{N}$. How can he accommodate all guests in the infinite cars?

6. **Hello World!**

Determine the computability of the following tasks. If it's not computable, write a reduction or self-reference proof. If it is, write the program.

(a) You want to determine whether a program P on input x outputs "Hello World!". Is there a computer program that can perform this task? Justify your answer.

(b) You want to determine whether a program P prints "Hello World!" by a specific line k. Is there a computer program that can perform this task? Justify your answer.

(c) You want to determine whether a program P prints "Hello World!" in the first k lines of code run. Is there a computer program that can perform this task? Justify your answer.

7. **Montagues and Countulets!**

Two families, Montagues and Capulets, each have n men and n women. However, due to family rivalry, the Montagues and Capulets do not marry each other. Answer the following questions about marriage arrangements.

(a) How many ways marriage arrangements are there for just the Montague family?

(b) How many marriage arrangments are there for both the Montagues and Capulets?

(c) Now, say Romeo Montague and Juliet Capulet **can** (but not necessarily) get married. How many marriage arrangements are there for both families?

8. **Presidential Election**

We want to determine which presidential candidate will win this coming election. There are two candidates, Clinton and Trump.

(a) For each state, Clinton has p chance of winning. What is the probability that Clinton will win exactly half the states (there are 50 states)?

(b) What is the probability that she will win at least one state?

(c) Say that $p = 0.25$ or $p = 0.75$ with equal chance. If Clinton wins every single state, what is the probability that $p = 0.75$? (Hint: Use Bayes Rule)