Recitation - Final Review

Date: May 4 and May 6, 2015

Problem - Final Review.1

Let A and B be finite sets such that $|A| = |B|$. Prove by contradiction that a function $f : A \to B$ is injective if and only if it is surjective.

Problem - Final Review.2

In public key cryptography, each individual has a public key and a secret key. The public key is used to encrypt messages, and the secret key is used to decrypt messages. The public key is known by everyone, so that anyone can encrypt a message and send it to the individual. The secret key is known only by the individual, so that only they can decrypt the messages sent to them.

A common example of public key cryptography uses the product of two large distinct primes $n = pq$ as a public key and the factorization (p, q) as a secret key. In this problem, we will explore one tactic for discovering someone's secret key.

Let $n = pq$ be a public key. Suppose you have found two integers x and y such that $x^2 \equiv y^2 \mod n$, but $x \not\equiv \pm y \mod n$. Explain how you can find (p, q).

Problem - Final Review.3

The old jazz standard "Everybody Loves My Baby" includes the line "Everybody loves my baby, but my baby loves nobody but me."

Define the following predicates and variables over the set of all people D:

- $L(x, y)$ = "x loves y."
- $E(x, y)$ = "x equals y."
- b = "my baby."
- m = "me."

You may assume that the singer is a person.

a) Translate the line of the song into logical notation, using the predicates and variables defined above.

b) Prove that the singer of this song is his or her own baby.

Problem - Final Review.4

Alice finds herself on trial in the Queen of Hearts's court, and the only way to get home safely is to guess a secret password that the Queen of Hearts has decided upon ahead of time. She is given as many guesses as she needs, but she is not permitted to go free until she guesses correctly. Fortunately for Alice, the Mad Hatter happens to be in attendance at court, and discreetly informs her that the Queen's secret password is an anagram of "THEMARCHHARE".

a. If Alice knows nothing else about the password, how many possibilities must she try to guarantee that she guesses the password correctly? Your answer can be left as an expression containing factorials.

b. While attempting to guess the password so she can escape the Queen's court, Alice realizes that every member of the court in attendance is an avid tea-drinker. How many possible passwords contain the word "TEA" in them?

c. Alice guesses all of the anagrams of "THEMARCHHARE" but the Queen still won't let her leave! The Hatter accidentally lets slip that the password is actually three words, separated by spaces. Each word in the password must consist of at least 1 character, and the non-space characters still form an anagram of "THEMARCHHARE". How many possible passwords are there for Alice to try now?

Problem - Final Review.5

A standard deck of cards contains 52 distinct cards, each of which is marked with one of 13 possible rank $(2, 3, ..., K, A)$. Two cards are chosen at random from a standard deck without replacement.

a. What is the probability that both cards have the same rank?

b. What is the probability that the first card drawn has a higher rank than the second card drawn?

c. Now suppose the deck is shuffled to generate a random sequence of cards from the top to the bottom of the deck. What is the expected number of consecutive pairs of cards that have the same rank? (for example, the abbreviated sequence $3\clubsuit, J\heartsuit, J\spadesuit, J\clubsuit, 5\heartsuit, 10\diamondsuit, 10\spadesuit$ has 3 such pairs)

Problem - Final Review.6

Let $V = \{0,1\}^n$, i.e. the set of 0/1 strings of length n. Let $G = (V, E)$ be a graph such that for any $u, v \in V$, $\{u, v\} \in E$ if and only if u and v differ in exactly one bit. We call G an n-dimensional hypercube.

a. Count the number of edges in G for each n.

b. For which n is G Eulerian? Prove your answer.

c. Prove that for all $n \geq 2$, G has a Hamiltonian cycle.

d. Deterimine the chromatic number of G and prove your answer. The chromatic number of a graph is the minimum number of colors needed to assign colors to its vertices such that no two adjacent vertices have the same color.

Problem - Final Review.7

For a graph G, the complement of G (written $\overline{G}$) is the graph $(V, \overline{E})$ where $\overline{E} = \{(x, y) : x, y \in V, (x, y) \notin E\}$.

Let T be a tree which contains at least two vertices v such that $deg(v) \geq 2$. Prove that $\overline{T}$ is connected.