# CS 13: Mathematics for Computer Scientists — Spring 2023

## Written Homework 03 (due June 2nd, 2023)

**Directions**: *Write up carefully argued solutions to the following problems. Your solution should be clear enough that it should explain to someone who does not already understand the answer why it works. You may use results from lecture and previous homeworks without proof.*

## 0. Hashing (0 points)

Suppose $n$ names are chosen (with replacement) independently at random from a universe of $N \gg n$ possible names, then hashed into a hash table with $b$ buckets. Suppose that $N$ is a multiple of $b$, and that the hash function maps exactly $N/b$ of the possible names into each of the $b$ buckets. What is the probability that this results in *no collisions*, i.e., no two picks hash to the *same* bucket? For $b = 10000$, write a short program in Python or Java to *simulate* this process for *1000* trials when $n = 115, \ldots, 125$. Upload your code as well. What is the largest value of $n$ such that this probability is greater than 0.5? Check that your theoretical answers match your empirical ones. Include a graph of your theoretical results.

## 1. $\phi$ not? (0 points)

The *Euler Totient Function*, $\phi(n)$, has applications in cryptography. In particular, it is used to show the RSA cryptosystem works correctly. $\phi(n)$ is the number of numbers less than $n$ that are relatively prime to $n$. For example, if $n = 5$, $1, 2, 3$, and $4$ are all relatively prime to $n$ and less than $n$.

(a) [0 Points] If $n$ is prime, find and explain a closed form for $\phi(n)$.

(b) [0 Points] If $n = pq$, where $p$ and $q$ are distinct primes, find and explain a closed form for $\phi(n)$.

(c) [0 Points] If $n = p^k$, where $p$ is prime and $k \geq 0$, find and explain a closed form for $\phi(n)$.

(d) [0 Points] Find a product for $\phi(n)$, in general in terms of the primes that make up the prime factorization of $n$.

*Hint 1*: You will want to use inclusion-exclusion.
*Hint 2*: You will want to use the concept of a powerset somewhere in this question.

## 2. Andrew and Andrew (0 points)

Andrew Wei and Andrew Li have decided that their names are too similar. To settle the dispute (and claim the new awesome name "Andy"), they have decided to get violent. They will battle in the best way they know how: by shooting each other with guns! Since they're gentlemen, their fight follows the following procedure:

(Step 1) Andrew Wei shoots Andrew Li with his gun and hits with probability $p$.

(Step 2) If Andrew Li is not shot, he shoots Andrew Wei and hits with probability $q$.

(Step 3) If Andrew Wei is not shot, then they start over again.

What is the probability that Andrew Wei wins the title of "Andy"?

(a) [0 Points] Write out code for this situation using the random primitives from lecture.
*Hint:* You might want to make your function *recursive*!

(b) [0 Points] Define any events you need for the rest of the problem.

(c) [0 Points] Write a recurrence for the probability that Andrew Wei wins the title of "Andy". Explain why it is correct.

(d) [0 Points] Solve your recurrence to find the actual probability in terms of $p$ and $q$.

## 3. Graph Theory 3 (0 points)

Let $G$ be a graph with $v$ vertices and $v - 1$ edges. Show that the following are equivalent:

(a) $G$ is connected

(b) $G$ is acyclic

(c) Every two vertices of $G$ are joined by a unique path.