CSCI2300 – Introduction to Algorithms
Spring 2021, Exam I (100 Points + 10 Bonus)

Academic Integrity

This is an open book exam. You are only allowed to use a calculator for the computations. You must show all work for full credit.

Q0. (0 points) Read the following statements on academic integrity.

- I will not use any unauthorized materials (e.g., from the web, or other students).
- I will not use any unauthorized communication (e.g., messaging or other apps).
- I will not use any unauthorized means (e.g., any program/tool other than calculator).

Write the following statement at top of your answer sheet, followed by name and signature:

I certify that all work is my own; I have not sought or offered any unauthorized aid.

Name: ________________________ **Signature:** ________________________

Q1. (10 points) Let $f(n) = 3^{\log(n)+\frac{n}{2}}$ and $g(n) = 2^n$. Find whether f is O, Ω or Θ of g, and why.

Q2. (25 points) Consider a divide-and-conquer algorithm to multiply two n-bit numbers x and y, such that we divide each number into three parts with $n/3$ bits for each part. Answer the following questions:

(a) (10 points) Give a recursive algorithm to correctly compute the product $x \cdot y$ using this three part approach, and analyze its running time by solving a recursive equation based on $T(n)$, the time to solve a problem of size n.

(b) (15 points) Improve the algorithm above by eliminating multiplications to yield fewest number of sub-problems. Analyze the running time of your improved algorithm in terms of $T(n)$.

Q3. (10 points) Prove or Disprove: If $x \cdot y \equiv 0 \mod N$, then either $x \equiv 0 \mod N$ or $y \equiv 0 \mod N$, where N is a Carmichael number.

Q4. (30 points) Consider the RSA encryption scheme. Let $N = 899$ and Alice's public key $e = 407$.

(a) (15 points) What is the value of Alice's private key, d?

(b) (15 points) What is the encryption of the message $m = 11$? Use the modular exponentiation method and show all steps.

Q5. (10 points) Consider the following hashing scheme from $\mathbb{Z}_m \to \mathbb{Z}_n$:

$$h_{ab}(x) = (ax + b \mod m) \mod n$$

where $a \neq 0$ and $a, b \in \mathbb{Z}_m$. Also, assume that n is prime, but m is not, and $m > n$. Give an example that shows that the family of functions h_{ab} is not universal.

Q6. (15 points) Given an unsorted array A of integers (with possible duplicate values) of length n, give an $O(n)$ time (expected) algorithm to find the k-th most frequent element. Give the pseudo-code for your algorithm, reason about its correctness, and then show that its expected running time is $O(n)$.

Q7. **Bonus:** (10 points) The Fibonacci series can be generated by taking powers of the matrix $M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, whose eigenvalues are given as

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \qquad \lambda_2 = \frac{1-\sqrt{5}}{2}$$

The n-th element of the Fibonacci series is given as:

$$F_n = \frac{\lambda_1^{n+1}}{1+\lambda_1^2} + \frac{\lambda_2^{n+1}}{1+\lambda_2^2}$$

Prove that the above expression is equivalent to:

$$F_n = \frac{1}{\sqrt{5}} \left(\lambda_1^n - \lambda_2^n\right)$$

Hint: use the fact that $\lambda_i^2 - \lambda_i - 1 = 0$ for $i = 1, 2$.