Midterm – Math 173A

Instructor: Liam Hardiman

July 11, 2022

Instructions:

- You must show your work and clearly explain your line of reasoning.
- You may use a calculator, but only for basic arithmetic. If you didn't bring a calculator, you may use your phone, but it must be set to airplane/flight mode and you must clear all notifications before you start.
- You have one hour to complete the exam.

GOOD LUCK!

1. (10 points)

   (a) (2 points) Define *primitive roots* of $\mathbb{F}_p$.

   (b) (4 points) If g is a primitive root of $\mathbb{F}_p$, prove that g^k is a primitive root of $\mathbb{F}_p$ if and only if $\gcd(k, p-1) = 1$.

   (c) (4 points) Find all primitive roots of $\mathbb{F}_{13}$. (Part (b) might be helpful.)

2. (10 points)

   (a) (6 points) Carefully, but briefly describe each step in the Diffie-Hellman key exchange protocol.

   (b) (4 points) If Eve has an oracle that solves the discrete logarithm problem, can she compromise a Diffie-Hellman key exchange? Why or why not?

3. (10 points) Use the baby step giant step algorithm to find $\log_3(7)$ in $\mathbb{F}_{19}$.

4. (10 points)

   (a) (6 points) Carefully, but briefly describe each step in the ElGamal encryption scheme.

   (b) (4 points) Show that the ElGamal scheme is multiplicatively homomorphic. That is, show that if you know the encryptions of two messages m_1 and m_2, then you can construct the encryption of their product $m_1 m_2$ *without knowing the key.* Be sure to prove that your answer really decrypts to the right message.

5. (10 points) Given two functions $f, g : \mathbb{N} \to \mathbb{R}$, we say that $f(n) = o(g(n))$ if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

(a) (4 points) Show that if $f(n) = o(g(n))$, then $f(n) = O(g(n))$ as well.

(b) (4 points) Give an example of functions f and g where $f(n) = O(g(n))$, but $f(n) \neq o(g(n))$.

(c) (2 points) Suppose you have two algorithms that solve the same problem where one runs in $f(n)$ steps and the other runs in $g(n)$ steps. If $f(n) = o(g(n))$, which algorithm would you prefer to use for large values of n? Explain your choice.