Quiz 3

Student ID Number: Name _____

Math 173A, 3PM

Please justify all your answers July 5, 2019

Please also write your full name on the back

1. Fill in the blank.

   (a) Given a prime p, g, $g^a \pmod p$ and $g^b \pmod p$ for some $g \in \mathbb{F}_p^\times$ and integers a and b, the task of finding $g^{ab} \pmod p$ is called the _____ problem.

   (b) Given a prime p, g, and $g^a \pmod p$ for some $g \in \mathbb{F}_p^\times$ and integer a, the task of finding $a \pmod{p-1}$ is called the _____ problem.

   (c) True or false? If $g^a \equiv g^b \pmod p$ for some prime p, $g \in \mathbb{F}_p^\times$ and integers a and b, then $a = b$.

   (d) In the ElGamal cryptosystem, Alice chooses a prime p and an element $g \in \mathbb{F}_p^\times$. She then secretly chooses an element $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ and publishes $g^a \pmod p$, called her _____.

2. Suppose you know that

$$3^5 \equiv 44 \pmod{137}, \quad 3^{10} \equiv 2 \pmod{137}.$$

   Find a value of x with $0 \leq x \leq 135$ such that $3^x \equiv 11 \pmod{137}$. *Hint: this can be done quickly without a calculator.*