Week 2 Quiz

Student ID Number: Name ____________________

Math 173A, 11AM

Please justify all your answers July 1, 2022

Please also write your full name on the back

1. Fill in the blank or answer with "True" or "False".

   (a) Fix a prime p and suppose that a is coprime to p. The smallest positive integer k such that $a^k \equiv 1 \pmod{p}$ is called the ____________ of $a \pmod{p}$.

   (b) True or false? If p is prime and a is any integer then $a^{p-1} \equiv 1 \pmod{p}$.

   (c) Fix a prime p. An element $g \in \mathbb{F}_p^\times$ whose powers give every element of $\mathbb{F}_p^\times$ is called a ____________ of $\mathbb{F}_p^\times$.

2. (a) Solve $7d \equiv 1 \pmod{30}$.

   (b) Suppose you write a message as a number $m \pmod{31}$. Encrypt m as $m^7 \pmod{31}$. How would you decrypt? *Hint: Decryption can be done by raising the ciphertext to a power mod 31. Fermat's little theorem will be useful.*

3. (a) What is one topic or example from the course so far that you find confusing? What do you find confusing about it?

   (b) What would you like to see more of in the discussion sections? What would you like to see less of?