Quiz 2

Student ID Number: Name _____

Math 173A, 3PM

Please justify all your answers July 1, 2019

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 $\mathbb{F}_p^\times$.

   (d) True or false? $(\mathbb{Z}/n\mathbb{Z})^\times$ contains $\phi(n)$ elements, where ϕ is the Euler totient function.

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 is done by raising the ciphertext to a power mod 31. Fermat's little theorem will be useful.*