Quiz 7′

Student ID Number: Name _____

Math 173A, 3PM

Please justify all your answers November 21, 2019

Please also write your full name on the back

1. Fill in the blank.

   (a) If every prime factor of n is less than B, then n is said to be B-_____.

   (b) True or false? If n is the product of two distinct odd primes, then there exists an integer $a \neq \pm 1 \pmod{n}$ such that $a^2 \equiv 1 \pmod{n}$.

2. Let $N = 61063$. Suppose you know that

$$1882^2 \equiv 270 = 2 \cdot 3^3 \cdot 5 \pmod{61063}$$
$$1898^2 \equiv 60750 = 2 \cdot 3^5 \cdot 5^3 \pmod{61063}.$$

   Describe how you would use this information to factor N (without actually performing the computations).