Math373 **Quiz 9** **Fri. Apr 1, 2022**

Name: ____

Directions: Show all work. No credit for answers without work.

1. [**3 points**] Solve for x in $x^{19} \equiv 21 \pmod{79}$.

2. [**2 points**] Suppose that $N = pq$ for distinct primes p and q. Given $N = 167653$ and $N' = (p-1)(q-1) = 166828$, find p and q using the efficient method from class.

3. Alice generates an RSA key with $p = 13$, $q = 19$, and she picks public exponent $e = 5$.

   (a) [**2 points**] What is Alice's public key? What is her private key?

   (b) [**2 points**] Bob wishes to encrypt and send the message $m = 189$ to Alice. What should he send?

   (c) [**1 point**] After many years of using $e = 5$, Alice wishes to change her public exponent. What would you recommend to Alice?