CS 355, Fall, 2019, Homework 6

1. Show all of your work as you use the Chinese Remainder Theorem to find the complete solution to the two simultaneous congruences

$$x \equiv 2 \pmod{15}$$

$$x \equiv 4 \pmod{7}.$$

2. Find all the square roots of 60 modulo 77. Show all your work. Use an algorithm which would work for 200-digit numbers in place of 2-digit numbers, assuming the factorization of the modulus is given.

3. Use Euler's Criterion to show that if both a and b are quadratic non-residues modulo an odd prime p, then ab is a quadratic residue modulo p.

4. Is there a way that either Alice and Bob could deliberately lose the coin-tossing protocol when the other player follows the protocol? Explain your answer.