Note: Please cite any resources used, and mention any classmates that you worked with on this assignment. If you worked alone, please also say so. We will start taking points off if this is missing.

Problem 1.

Which of the numbers (mod 15) are relatively prime to 15? List them in CRT (Chinese Remainder Theorem) notation, as you did in your answer to Homework 2 Problem 4a. What is the pattern or identifier for those numbers which are NOT relatively prime to 15?

Problem 2.

(a) Consider all the possible sets of two square roots s, t of 1 (mod 15) where s t (mod 15) Note: since there are 4 different roots, there are 6 combinations of distinct roots.

For all possible combinations of distinct roots s t, compute gcd(s + t, 15). Which combinations give you a single prime factor of 15?

(b) Using CRT notation, show what is going on for all the combinations you considered in the previous part. Explain why sometimes the gcd(s + t, 15) yields a factor of 15, and why sometimes it does not.

Problem 3.

Use the method described in section 2.8.1 to find square roots modulo the following composite moduli:

(a) Find a square root of 340 modulo 437. (Note that $437 = 19 \cdot 23$.)

(b) Find a square root of 253 modulo 3143.

(c) Find four square roots of 2833 modulo 4189. (The modulus factors as $4189 = 59 \cdot 71$. Note that your four square roots should be distinct modulo 4189.)

(d) Find eight square roots of 813 modulo 868.
Note: that method is Proposition 2.26. Let p be a prime satisfying $p == 3(mod4)$. Let a be an integer such that the congruence $x**2 == a(modp)$ has a solution, ie, such that a has a $squareroot(modp)$. Then $b == a^{(p+1)/4}(modp)$ is a solution. That is, it satisfies $b**2 == a(modp)$.

Taken from Hoffstein 2.23

Problem 4.

(a) Explain why a successful attack on second pre-image resistance implies a successful attack on collision resistance.

(b) Explain why a successful attack on collision resistance does not imply an attack on second pre-image resistance (under the assumption that second pre-image hash functions exist).
Note: A good place to start is to write in your own words what an attack on second pre-image resistance means, and also what an attack on collision resistance means. Stallings 11.3 “Security Requirements for Cryptographic Hash Functions” has a good description of how these properties are subtly different.