NUMBER THEORY I
SPRING 2018

ASSIGNMENT 12.2
DUE APRIL 18

Exercise 1. If

$$p = 4093082899,$$
$$q = 4093982899,$$

and $n = pq$, what is the maximum number of steps it will take to factor n using the Fermat Factorization Method? (Determine this without actually implementing the method.)

Exercise 2. Eliza and Zoey decide to use the Diffie-Hellman key exchange with modulus $p = 127$ and generator $g = 92$. Eliza sends Zoey the "partial key" 42 and Zoey sends Eliza 70. Use this information (and brute force) to determine their shared secret key.

Exercise 3.

a. Find every solution to the congruence $x^2 \equiv 16 \pmod{63}$. [*Suggestion:* The given congruence is equivalent to the pair of simultaneous congruences $x^2 \equiv 16 \pmod{7}$ and $x^2 \equiv 16 \pmod{9}$. Solve these individually and then "glue" the results together using the CRT.]

b. Find every solution to the quadratic congruence

$$5x^2 + 14x + 9 \equiv 0 \pmod{63}.$$

[*Suggestion:* Consider the congruence as an *equation* in the ring $\mathbb{Z}/63\mathbb{Z}$ and apply the quadratic formula. Use part **a**.]