CS 355, Fall, 2019, Homework 4

1. Suppose $M = 10001010$ and $C = 11110011$ are corresponding bit streams in a known plaintext attack on a four-bit LFSR. M was enciphered from left to right, that is, the bit at the left end (1 for M) was enciphered first. Each bit of M was XORed with the next bit output by the LFSR to produce the next bit of C. Find the matrix H, the tap sequence T, and the initial contents of the register. Show all of your work.

2. Evaluate the Euler phi function $\phi(n)$ for all integers $40 \le n \le 49$.

3. Use congruences to find the last two (the low-order two) decimal digits of 37^{543}. Do not use any integers larger than 9999 in your solution. Do not use any computer. Show all of your work. Hint: You may use the Chinese Remainder Theorem in your solution.