Math 4981 Spring 2021
Cryptography HW 8
Due Thursday, March 11

1. Use the Euclidean Algorithm to compute $\gcd(5320, 2156)$.

2. If n is a positive integer, use the Euclidean algorithm to find $\gcd(2n^2 + 6n - 4, 2n^2 + 4n - 3)$.

3. Use Pollard's $p - 1$ method to factor 1517. Show all your steps.

4. Use the Discrete Logarithm factoring algorithm to factor 3403, using the fact that $\log_2(1) = 820$ modulo 3403. (I know you could factor this directly, but use the discrete logarithm algorithm and explain the steps you're using.)

5. The group S_3 is the set $\{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, where e is the identity and multiplication obeys the following rules: $\sigma^3 = e = \tau^2, \tau\sigma = \sigma^2\tau$.

   (a) What are σ^{-1} and τ^{-1}? That is, tell me which of the six elements in the set I gave you is σ^{-1} and which is τ^{-1}.

   (b) Compute $\tau\sigma^2, \tau(\sigma\tau), (\sigma\tau)(\sigma\tau)$, an $(\sigma\tau)(\sigma^2\tau)$. (Again, your answer for each part should be one of the six elements I gave you.)

6. Let $m > 2$ be a positive integer. Prove that $\mathbb{Z}/m\mathbb{Z}^\times$ with the operation of multiplication is an abelian group. (Non-obvious thing to check: is multiplication a binary operation? That is, if you multiply two elements together, do you get another?)