Math 373-578 **Name** _____

Homework Assignment 3
March 1, 2019

1. Let p be an odd prime. Compute $1^p + 2^p + \cdots + (p-2) + (p-1)^p$ modulo p.

2. Consider the (symmetric) affine cipher with encryption function defined by

$$e_k(m) \equiv k_1 \cdot m + k_2 \pmod{p}.$$

   Recall that $\mathcal{M} = \mathcal{C} = (\mathbb{Z}/p\mathbb{Z})^*$, for a prime p, and $\mathcal{K}$ consists of pair of elements (k_1, k_2) of $(\mathbb{Z}/p\mathbb{Z})^*$.

   (a) Compute the decryption function d_k.

   (b) Suppose that $p = 19$ and that your key is $(k_1, k_2) = (5, 7)$. Decrypt the ciphertext 17.

3. Consider the Diffie-Hellman key exchange with public parameters $p = 71$ and $g = 11$.

   (a) Compute the order of g modulo p.

   (b) Suppose Bob chooses $b = 18$. Compute the value he sends to Alice.

   (c) Suppose Alice sends to Bob the value 14. Compute the secret key generated by the Diffie-Hellman algorithm.

4. Alice and Bob use the ElGamal public key cryptosystem with parameters $p = 8237$ and $g = 3$. Suppose that Alice sends to Bob the value $A = 5616$. Bob did not attend last class and so he uses the same key k for all his plaintexts $m_1, m_2, \ldots$. You happen to know that he is extremely predictable and always sends "Hi" as a first message, encoded as $m_1 = 190$. The first and second ciphertexts he sends are $(c_1, c_2) = (7830, 4537)$ and $(c_1', c_2') = (7830, 1647)$, respectively. Compute the second plaintext m_2.

5. (Challenge) Show that there is no positive integer n such that $\phi(n) = 14$.