Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. [JJJ 1.36] Compute the value of $2^{(p-1)/2} \pmod{p}$ for every prime $3 \leq p < 20$. (You do not need to show the details of your computation.) Make a conjecture as to the possible values of $2^{(p-1)/2} \pmod{p}$ and prove that your conjecture is correct.

2. [JJJ 1.41] Consider the affine cipher with key $k = (\alpha, \beta)$ whose encryption and decryption functions are given by

$$e_k(m) \equiv \alpha m + \beta \pmod{p}$$
$$d_k(c) \equiv \alpha^{-1}(c - \beta) \pmod{p}$$

   (a) Let $p = 541$ and let $k = (34, 71)$. Encrypt the message $m = 204$. Decrypt the ciphertext $c = 431$.

   (b) Assuming that p is public knowledge, explain why the affine cipher is vulnerable to a chosen plaintext attack. How many plaintext/ciphertext pairs are likely to be needed to recover the private key?

   (c) Alice and Bob decide to use the prime $p = 601$ for their affine cipher. The value of p is public knowledge. Eve intercepts the ciphertexts $c_1 = 324$ and $c_2 = 381$, and she also manages to find the corresponding plaintexts are $m_1 = 387$ and $m_2 = 491$. Determine the private key (α, β) and then use it to encrypt the message $m_3 = 173$.

   (d) **[Challenge]** Suppose now that p is not public knowledge. Is the affine cipher still vulnerable to a chosen plaintext attack? Explain.

3. [JJJ 1.43] Let n be a large integer and let $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{Z}_n$. For each of the functions below, answer the following questions.

   - Is e an encryption function? In other words, is e an injective function?
   - If e is an encryption function, what is the associated decryption function d?
   - If e is not an encryption function, can you make it into an encryption function by restricting the set of keys $\mathcal{K}$ to a smaller, but still reasonably large subset?

   (a) $e_k(m) \equiv k - m \pmod{n}$

   (b) $e_k(m) \equiv k \cdot m \pmod{n}$

   (c) $e_k(m) \equiv (k + m)^2 \pmod{n}$