

## Problem Set 2

**INSTRUCTIONS:** These are additional problems for you to practice and improve your skill in this area. DO NOT turn in your solution for these problems for grading. These problems are only to test yourself and solutions for these problems will not be posted.

1. The ciphertext AEVJVJCTAPXEPUUFCNFKSTGUFL was encrypted by using the Affine Cipher mod 26. The plaintext begins with **th**. Find the key by using the method discussed in class and decrypt the message.
2. Calculate the value of Euler phi function  $\phi(100)$ . Use it to determine the number of keys in an Affine Cipher over  $\mathbb{Z}_{100}$ .
3. Recall the definition of involutory key from Homework 1.
  - (a) Show that a key  $k = (a, b)$  in the Affine Cipher over  $\mathbb{Z}_{26}$  is an involutory key if and only if  $a^2 \equiv 1 \pmod{26}$  and  $b(a + 1) \equiv 0 \pmod{26}$ .
  - (b) Find all involutory keys in the Affine Cipher over  $\mathbb{Z}_{26}$ . (Hint: There are 28 of them!)
4. The following cipher text was encrypted by using the Affine Cipher mod 26. Determine the key and decrypt.  
  
GHHFYDYLKXYGWHYOYWFESXNHLKHEQTCLYGWYHFYWKWHYIWMYKWPGCYWQVY
5. List all the numbers in  $\mathbb{Z}_{15}$  which have multiplicative inverse and find the inverse for each of them.