Math 1350 Quiz 1 - July 7, 2010

(3 points) Name: Solutions

1. (7 points) Describe the meaning of $a \equiv b \pmod{m}$.

   Possible answers:

   a is congruent to b when $a - b$ is divisible by m. a is congruent to b when $a - b = m \cdot k$ where k is an integer. a is congruent to b when a and b leave the same remainder when divided by m.

2. Suppose there were a new language called Cornellish, where there are 12 different letters in the alphabet.

   (a) (5 points) Fill in the following table to give an example of a shift (a.k.a. Caesar) cipher in this language. The letters on the top row are written in "alphabetical" order in Cornellish.

   One possibility:

plain	C	O	R	N	E	L	U	I	V	S	T	Y
cipher	N	E	L	U	I	V	S	T	Y	C	O	R

   (b) (2 points) Use your answer to part (a) to encrypt `VISITOR`.

   Based on (a), encryption: `YTCTOEL`.

   (c) (8 points) Could the equation $y \equiv 3x + 5 \pmod{12}$ describe an affine cipher for this alphabet? Why or why not? (*HINT:* Your answer should be more than 1 sentence.)

   No, the given equation could not be an affine cipher. A cipher must be a one-to-one function because we must have an inverse function to decipher. The function $3x + 5$ is not one-to-one mod 12, because 3 and 12 are not relatively prime, so 3 does not have a multiplicative inverse mod 12.

   (d) (Bonus - 5 points) How many different affine ciphers would there be for this alphabet? Explain. There are 4 numbers that have inverses mod 12 (1, 5, 7, 11), so 4 possible keys for the decimation part. There are 12 letters, so 12 possible shifts. However, the affine cipher with decimation key 1 and shift 0 does not change the letters at all. Thus, there are $4 \cdot 12 - 1 = 47$ possible affine ciphers.