CSci 4554 Assignment 5

Due Monday, March 8th in class

Problem 1 (5 points). Consider a multiplicative group $\mathbb{Z}_{55}^*$. List all possible orders of elements in this group and give an example of one element fro each of the orders (Hint: see Section 5.2.4).

Problem 2 (10 points). For each of the following equations find all solutions. If there are no solutions, please explain why. You may use a Extended Euclidean algorithm program (the applet on the course web page or your own program) to find λ. Show all the steps in computing the solutions.

1. $13x \equiv 5 (\text{mod } 27)$
2. $13x \equiv 5 (\text{mod } 26)$
3. $13x \equiv 0 (\text{mod } 26)$
4. $2x \equiv 10 (\text{mod } 26)$

Problem 3 (10 points). Russian alphabet has 33 letters.
Question 1. Which of the following are possible coefficients for an affine cipher for Russian?

1. $a = 4, b = 11$
2. $a = 9, b = 7$
3. $a = 1, b = 3$
4. $a = 22, b = 15$
5. $a = 10, b = 0$

Please show all your computations and briefly explain your answers.
Question 2. For those values that are possible, what is the encryption of the letter я - the last letter of the Russian alphabet? What is its decryption when it appears in ciphertext? Just give the letter numbers as the result, although if you are really interested, you can look up the letters at

http://en.wikipedia.org/wiki/Russian_language#Writing_system

Question 3. One of the possible affine ciphers above is equivalent to a simpler cipher. Which one and to what cipher?

Problem 4 (10 points). Solve the following system of linear equations using the Chinese Remainder Theorem:

$$x \equiv 1 (\text{mod } 3)$$
$$x \equiv 2 (\text{mod } 4)$$
$$x \equiv 5 (\text{mod } 7)$$