Math325 Assignment 2: Congruences and Codes

February 3rd, 2009

Answer all questions and give complete reasons and checks for your answers. Hand in ALL of your rough working together with your final answers. The parts of the questions are weighted as shown on the right of the question. Use of Maple to investigate or check answers is encouraged where appropriate but all working must be given by hand. You are reminded that plagiarism is a serious offense and when caught you will suffer the penalties specified by the University.

1. You are given your fragment of a message that you know has been encrypted using the affine method and the 29 letter alphabet "`abcdefghijklmnopqrstuvwxyz␣ , .`")
   (a) Create a frequency table and identify the 5 most common letters in your fragment. [3]
   (b) Assume that the most common letter is not ␣ and guess the most common and hence determine what the other common letters would decode to. Explain why this makes you believe that these are not the correct decoding parameters. [4]
   (c) Use your knowledge of letter frequencies in English to actually decode the fragment. [4]

2. (a) Using a and b from your registration number, solve these congruences for x: [6]

$$7x \equiv a \bmod 30\ , \quad bx \equiv 10 \bmod 17\ , \quad 18x \equiv 42 \bmod 66$$

   (b) Use the Chinese Remainder Theorem to solve all of these three equations at once. [3]

3. (a) Determine algebraically which affine encryption parameters lead to identical decryption parameters (as for `rot13`) for an alphabet with N letters. [2]
   (b) Under what circumstances are affine encryptions of affine encryptions still valid affine encryptions? Is it ever possible when the number of letters in the alphabet of the first affine encryption is different from that in the second? [3]