Math325 Number Theory: Assignment 2 (October 2010)

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.

Let the last four digits of your registration number be a, b, c and d and the four digit number be n.

1. (a) Find 13^{-1} and 169^{-1} modulo n. [3]

   (b) Explain why $(y^k)^{-1} \equiv (y^{-1})^k \pmod{m}$ for any $k \in \mathbb{Z}$ and $\gcd(y, m) = 1$. [3]

2. A group of people tries to arrange itself into a number of rows which each have the same number of people in. If there are 23 to a row there are a people left over and when 20 to a row the last row is b people short. What is the smallest number of people that is in such a group? [5]

3. (a) Under an affine encoding

$$\mathbb{C} \equiv e\mathbb{P} + f \pmod{N}$$

   explain, in general, how many letters will map to themselves for any given e and f. Is there guaranteed to be at least one letter fixed if $e \neq 1$? [6]

   (b) Decode the phrase on your slip of paper given that it was encoded using an affine encoding with the 29 letter alphabet with $A = 0, \ldots, Z = 25$, space as 26, the comma as 27 and the exclamation mark as 28. The letter indicated is one which maps to itself. Are there any other letters fixed? Check your answer against your prediction in the first part of the question. [8]