Math 3207 Assignment 2, October 2018

Please show all working and reasoning to get full marks for any question. Hand in your rough working as well so I can see how you investigated and reached your final results. You can use Maple at any point and can email me any worksheets you created.

You are reminded that plagiarism is a serious offense and when it is detected you will be punished. Feel free to discuss the questions in general with myself and your colleagues but the work attempted must be yours alone. A maximum of $20 - \frac{p_y}{2}$ marks can be received for this assignment if you hand your work in y days after the deadline, where p_y is the y^{th} prime number; $p_1 := 2$, $p_2 := 3$, $p_3 := 5$, $p_4 := 7$, $p_5 := 11$, etc.

1. You have randomly picked one of the slips of paper with the information required for this question. The encoding system used is the single letter affine one in the 29 character alphabet.

   (a) Given that the most common character in your plaintext is space, suppose that the second most common is E and use that information to find what the next two most common characters in the plaintext would be. Do these two letters indicate you might have the correct decoding formula? [4]

   (b) Now using the actual second most common letter, find the encoding parametesr used and decode the message to get a mathematical question. [4]

   (c) Encode the correct answer to the decoded question using digraph encoding; use the parameters a and b which will allow me to decode using the values $e = 273$ and $f = 84$. [3]

2. (a) Let the last 3 digits of your registration number be r, s and t. Use the Chinese Remainder Theorem to find the solution to this system of equations with the smallest modulus: [4]

   $$x \equiv s + 2 \pmod{17}\ , \quad 3x \equiv r - t - 3 \pmod{18}\ , \quad 8x \equiv r + t + 2 \pmod{19}$$

   (b) How would the proof of Theorem 3.5 change if we have $k = 2$ but $\gcd(m_1, m_2) = n > 1$? In particular, under what circumstances would there be no solution and how many solutions would we have otherwise? [2]

3. What is the criteria for whether or not a particular number y is divisible by your number z when y is written in dozenal? Use modular arithmetic to prove the relation and verify it for some numbers that are multiples of z, and some that aren't. [3]

“`.sicmhnmlhjwmvhkunm,kw`”
“I” is second most common
$z := 4 \times 4 = 14$ is your dozenal number

“`,xfmwndywyufwmxlxmumwzgwytn`”
“D” is second most common
$z := 3 \times 6 = 16$ is your dozenal number