MACM 442/CMPT 881/MATH 800
Assignment 1, Fall 2006

Michael Monagan

Due Thursday September 21st, 9:30am, BEFORE class starts.
Late penalty: -10% for each day late.

Chapter 1

Exercises 1.7, 1.9, 1.13, 1.16, and 1.21.

Notes on exercises.
For 1.9 and 1.13 you may simply use Maple to compute the answers.
You will probably find that you will spend more time on problem 1.21 than all the other problems on this assignment and so it will be worth more marks. It is also the question which is the most fun. Note that the plaintext for one of the problems is not English.

Additional questions for all students:

1: Oscar knows that the plaintext "SELLIT" when encrypted with the Hill Cipher that Alice is using yields the ciphertext "GCGJFA" (using the encoding A=0, B=1, C=2, ..., Z=25). If Oscar also knows that $m = 2$, does he have enough information to determine the key uniquely? If so, what is it? If not, what keys, if any, are possible?

2: Table 1.4 lists values for M_g for the ciphertext in Example 1.12 on page 34 which begins CHREEVO.... Write a program that reproduces the the numbers in row 2 of the table, i.e. the numbers 0.069, 0.044, 0.032, ...

Additional problem for MATH 800 and CMPT 881 students.

3: Do exercise 1.12(a) and the following. Let p and q be primes. Find a formula for the number of invertible 2×2 matrices over (i) $\mathbf{Z}_{p^2}$ and (ii) $\mathbf{Z}_{pq}$? You have some data from exercise 1.13 to check your answers but you will want more data to check your answer for (i). I did 1.12(a) by counting the number of ways the determinant of a 2×2 matrix over $\mathbf{Z}_p$ could be 0. By modifying this argument one can derive a formula for (i).
Alternatively, assume the formulae are polynomials in p (and q), compute some more data and interpolate the data using Maple.