F10PC1

HERIOT WATT UNIVERSITY

Department of Mathematics

F10PC1

Pure Mathematics C

Duration: 2 Hours

Semester 1 Exam Diet 2010

Attempt three questions

A University approved calculator may be used
for basic computations, but
appropriate working must be shown to obtain full credit.

1. In parts (a) and (b) of this question, please use the following numerical correspondences

$$A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25.$$

(a) The following ciphertext was enciphered using a Caesar cipher. The division into blocks is just for ease of reading — all spaces in the cleartext were omitted.

PXPX KXEN **VDRU** XVTN LXHY MXGM AXYK
XJNX GVRF XMAH WGXX WLEH GZXK VBIA XKMX QM

Find the cleartext corresponding to the ciphertext in bold, and explain your reasoning. [6 marks]

(b) Show that the matrix

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$$

is an enciphering matrix for a Hill 2-cipher. Decipher the ciphertext FWMDIQ. [7 marks]

(c) This question concerns an RSA code having the following parameters

- $p = 47$.
- $q = 59$.
- Encryption key $e = 17$.
- Decryption key $d = 157$.

The ciphertext received was 1973. What was the cleartext? [7 marks]

2. (a) Define what is meant by a *code* C in $\mathbb{Z}_2^n$. Define the *Hamming metric* on $\mathbb{Z}_2^n$, and the *minimum distance* of the code C. [3 marks]

Prove that if a code has minimum distance d then it can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors. [5 marks]

What does it mean to say that such a code C is *linear*? [1 mark]

Prove that the minimum distance of a linear code is equal to the minimum non-zero weight. [3 marks]

(b) The following is a generator matrix of a linear code.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Find the associated parity check matrix H and show all your calculations. [6 marks]

The vector 101111 is received. What was the most likely codeword sent? [2 marks]

Questions continue

3. (a) Define the 'big-oh' notation for comparing the rate of growth of functions, and use it to define what is meant by a problem being *solvable in polynomial time.* [2 marks]

   A problem can be solved by means of four different algorithms A,B,C and D which have, respectively, the following time complexities: $n^2, 2^n, \log\log n, \log n$. Arrange the four algorithms in order from fastest to slowest. [1 mark]

   The usual algorithm for deciding whether a number n is prime or not involves trial divisions by all numbers less than or equal to $\sqrt{n}$. Show that this algorithm runs in exponential time in the length of n as a decimal number. [4 marks]

   Does this result mean that the problem of determining whether a number is prime or not is intractable? Explain. [1 mark]

   (b) Let n be an odd number. Show that there is a bijective correspondence between factorizations $n = ab$ where $a \geq b$ and representations of n as a difference of two squares $n = u^2 - v^2$. [3 marks]

   Use this result to factorize the number 5959. [2 marks]

   Under what circumstances is this technique most effective? [1 mark]

   (c) State, without proof, the Prime Number Theorem. [1 mark]

   Use it to estimate the number of primes with exactly 200 decimal digits. [2 marks]

   A computation shows that 2^n is not congruent to 2 modulo n. Explain what this tells you about n, and justify your answer by appealing to standard theorems. [3 marks]

4. Assuming the result

$$\sum_{d|n} \phi(d) = n$$

   prove that the group $\mathbb{U}_p$ of invertible integers under multiplication modulo the prime p is cyclic. Any standard results from group theory should be clearly stated. [14 marks]

   From your proof state how many generators the group $\mathbb{U}_p$ has. [1 mark]

   Find all generators of the group $\mathbb{U}_{11}$. [5 marks]

End of exam paper