Version JS/3

EGT3
ENGINEERING TRIPOS PART IIB

---

25 April 2017 9.30 to 11.10

Module 4F5

ADVANCED COMMUNICATIONS AND CODING

*Answer not more than **three** questions.*

All questions carry the same number of marks.

*The **approximate** percentage of marks allocated to each part of a question is indicated in the right margin.*

*Write your candidate number **not** your name on the cover sheet.*

STATIONERY REQUIREMENTS
Single-sided script paper

SPECIAL REQUIREMENTS TO BE SUPPLIED FOR THIS EXAM
CUED approved calculator allowed
Engineering Data Book

10 minutes reading time is allowed for this paper at the start of the exam.

You may not start to read the questions printed on the subsequent pages of this question paper until instructed to do so.

1 (a) Calculate the remainder $R_9(17^{17}+17)$. [10%]

(b) Prove that, for any odd number n, 10^n+1 is divisible by 11. [10%]

(c) Show that $n = 554433221122334455$ is divisible by 11.
Hint: write n as a sum of powers of 10. [10%]

(d) Calculate $\gcd(138600, 305760)$. [10%]

(e) Let a, b, c be integers. If c divides both a and b, express $\gcd\left(\frac{a}{c}, \frac{b}{c}\right)$ as a function of $\gcd(a,b)$. [10%]

(f) 7561 is a prime number and $7560 = 2^3 \times 3^3 \times 5 \times 7$. Consider the algebraic system consisting of the set of integers $\{0, 1, \ldots, 7560\}$ and multiplication modulo 7561.

(i) Is this algebraic system a monoid or a group? [5%]

(ii) Now omit the zero and consider the set of integers $\{1, 2, \ldots, 7560\}$ and multiplication modulo 7561. For each of the following values of k, explain why it is possible or not to find an α in the set such that $\alpha^k = 1$:

$$k = 2, 6, 11, 16.$$

[15%]

(iii) How many possible values can the orders of elements in the multiplicative group of integers modulo 7561 have? [10%]

(g) Let

$$\mathbf{C} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

be the companion matrix of X in GF(16).

(i) What is $X(1+X^2)$ in GF(16)? [10%]

(ii) What is $X^3(1+X^2)$ in GF(16)? [10%]

2 $\alpha = 2$ has multiplicative order 12 in GF(13). We wish to construct and operate a Reed-Solomon code of rate $R = 1/2$ and of length $N = 4$ over GF(13).

(a) Find an element β of multiplicative order 4. [10%]

(b) Write out the Discrete Fourier Transform (DFT) matrix and its inverse. Note that $1/N = 1/4 = 10$ in GF(13). [20%]

(c) Specify a parity-check matrix for the Reed-Solomon code. [10%]

(d) Give an encoding matix for the Reed-Solomon code. [10%]

(e) How many codewords does the Reed-Solomon code have? [10%]

(f) How many errors can the Reed-Solomon code detect and how many can it correct? [10%]

(g) A codeword from this Reed-Solomon code was transmitted and the symbols $[11, 12, 3, 4]$ were received. Show that there was at least one transmission error. [10%]

(h) Assuming a single error in the received symbols specified in part (g), decode the information sequence if the encoder matrix you computed previously was used to generate the codeword. [20%]

3 (a) (i) The Rivest-Shamir-Adelmann (RSA) cryptosystem is a public key scheme that operates by publishing a pair of integers (m,e) that can be used to encode messages only decryptable by a party who knows the factorisation of m into two large primes p_1 and p_2. Here, we will consider the operation of RSA using *small* primes $p_1 = 11$ and $p_2 = 13$.

A. Encrypt the secret message $X = 42$ using the public key $(m,7)$. [15%]

B. Decrypt the public message using the secret key.
It may be helpful for you to note that $\gcd(120,7) = 1 = 120 - 17 \times 7$. [15%]

(ii) The Diffie-Hellman key agreement protocol relies on the difficulty of taking logarithms in a multiplicative group, and operates by taking exponents modulo a large prime. One may consider, as an alternative, operating a Diffie-Hellman protocol on an additive group, i.e., addition modulo a large integer m.

A. Explain how this would work and what would be the corresponding operations to generate a public key and agree on a joint key. [20%]

B. Explain why this is not secure. [10%]

(b) Consider a dispersive fading channel, where the discrete-time output of the demodulator at time k is

$$Y_k = \sum_{\ell=0}^{L-1} h_\ell X_{k-\ell} + N_k,$$

where the noise N_k is complex Gaussian random with i.i.d. real and imaginary parts.

(i) Draw a block diagram describing the main components of the OFDM scheme to communicate over this channel. [20%]

(ii) What is the minimum length of the cyclic prefix required for the scheme? [5%]

(iii) Briefly explain the role of the cyclic prefix in the OFDM scheme. [15%]

4 (a) Consider the 4-point constellation shown in Fig. 1 below. The constellation is used for signalling over the discrete-time AWGN channel $Y = X + N$, where the noise N is a complex Gaussian random variable whose real and imaginary parts are each i.i.d. $\sim \mathcal{N}(0, \frac{N_0}{2})$. Assume that each of the constellation symbols is equally likely to be transmitted.

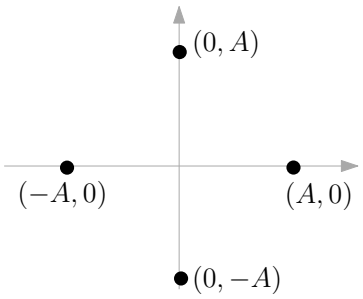

Fig. 1

(i) Specify the average energy per bit E_b of the constellation, in terms of A. [10%]

(ii) Sketch the decision regions for the optimal detector. [10%]

(iii) Compute an upper bound on the probability of detection error. Your upper bound should be expressed in terms of the ratio $\frac{E_b}{N_0}$ and the Q-function. [25%]

(iv) If the constellation were used for signalling over a fading channel $Y = hX + N$, how would the probability of error decay with increasing E_b/N_0? You do not need to explicitly compute the probability of error, but briefly explain the reason for the difference from the behaviour in part (a)(iii). You may assume coherent detection, and a Rayleigh fading assumption for the fading coefficient h. [15%]

(b) Consider a binary random variable X, which takes value $+1$ and -1 with equal probability. Suppose that we observe the pair of random variables (Y_1, Y_2), where

$$Y_1 = X + N_1,$$
$$Y_2 = N_1 + N_2.$$

Here N_1, N_2 are i.i.d. Gaussian $\sim \mathcal{N}(0, \sigma^2)$. Show that the optimal decision rule to detect X from (Y_1, Y_2) can be expressed as

$$\hat{X} = \begin{cases} 1, & Y_1 + \alpha Y_2 \geq T, \\ -1 & \text{otherwise}, \end{cases}$$

and specify the constants α and T.

Hint: In the calculations, you will need to express N_1 and N_2 in terms of Y_1, Y_2, and X. [40%]

END OF PAPER

Numerical Answers

I don’t believe in numerical answers as they train the wrong skills. Students who use numerical answers tend to fiddle around until they can get the right answer. If you are not getting the right answer on the first attempt, it is often indicative of the fact that you have misunderstood something fundamental and you should not just move on and find a way to get those numbers. Hence, I am not providing numerical answers for this exam. Full answers are in the crib, as usual.