SECTION A

1. Define a *unit* in a ring R with identity, and the *multiplicative inverse* of a unit $a \in R$. Find all units in R, in each of the following cases. Justify your answers.

a) $R = \mathbf{Z}$, b) $R = \mathbf{R}$,

c) $R = \mathbf{Z}[i] = \{m + ni : m,\ n \in \mathbf{Z}\}$.

[10 marks]

2. Show that the g.c.d. of $a(x) = x^4 + x + 1$ and $b(x) = x^3 + x + 1$ in $\mathbf{Z}_2[x]$ is 1. Find $m(x)$ and $n(x) \in \mathbf{Z}_2[x]$ such that

$$1 = m(x)a(x) + n(x)b(x).$$

[8 marks]

3. Show that

$$f(x) = x^3 + 2x^2 - x + 1$$

is irreducible in $\mathbf{Z}[x]$. Decide whether or not it is irreducible in $\mathbf{Q}[x]$. Show that it is reducible in $\mathbf{Z}_3[x]$. Factorise it as a product of irreducibles in $\mathbf{Z}_3[x]$.

[7 marks]

4. a) Write down all points on the line $x + 2y + 1 = 0$ in $\mathbf{Z}_3^2$.

b) Write down all points in $P^2(\mathbf{Z}_3)$ on the line $X + 2Y + Z = 0$.

c) Write down all lines in $\mathbf{Z}_3^2$ that are parallel to the line in a).

d) Find the point of intersection in $P^2(\mathbf{Z}_3)$ between the line of b) and the line $X + 2Y + 2Z = 0$.

[9 marks]

5. Give an example of each of the following, or explain why it does not exist.

a) A 1-design with parameters $(11, 5, 3)$.

b) A 1-design with parameters $\left(10, 5, \binom{9}{4}\right)$.

c) A 2-design with parameters $(9, 3, 1)$.

d) A 3-design with parameters $(9, 3, 2)$.

[10 marks]

6. Determine the dimension of the code $C \subset \mathbf{Z}_2^7$ with the following check matrix H. (You may be able to find a simpler check matrix.)

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

Define the *weight* of a linear code. Give a useful lower bound of weight of the linear code C. Determine which of the following are codewords of the code C, and, assuming at most one error, correct those which are not codewords.

a) 1000011 b) 1100110 [11 marks]

SECTION B

7. a) Let R be a commutative ring. Give the definition of a *subring* of R and of an *ideal* in R. Determine which of the following subsets J are subrings of the given ring R, and which are ideals. You need not give full explanations.

(i) $R = \mathbf{Z}[x]$, and $J = 2\mathbf{Z}[x] = \{2f(x) : f(x) \in \mathbf{Z}[x]\}$.

(ii) $R = \mathbf{R}[x]$, and J is as in (i).

b) Now let $R = \mathbf{Q}[x]$, and let J be an ideal in $\mathbf{Q}[x]$. Let $f(x) \in J$ be of minimal degree among polynomials in J that are not identically zero. By using the fact that $\mathbf{Q}[x]$ is a Euclidean domain with degree as the Euclidean valuation, show that $J = f(x)\mathbf{Q}[x]$. [15 marks]

8.

Show that $f_1(x)$ and $f_2(x)$ are irreducible in $\mathbf{Z}_3[x]$, where

$$f_1(x) = x^3 + 2x + 1 , \; f_2(x) = x^3 + 2x + 2.$$

Let $y = 2x + 1$, where addition and multiplication are in $\mathbf{Z}_3$. Express x in terms of y. Show that

$$2f_1(y) = f_2(x).$$

Let $J_i = f_i(x)\mathbf{Z}_3[x]$ for $i = 1, \; 2$. Show that $X = J_1 + x$ is a solution of $f_1(X) = 0$, where the 0 on the righthand side of this equation is the zero element J_1 in the ring $\mathbf{Z}_3[x]/J_1$. Show that for any $g_1(x), \; g_2(x) \in \mathbf{Z}_3[x]$,

$$J_1 + g_1(x) = J_1 + g_2(x) \Leftrightarrow J_2 + g_1(2x + 1) = J_2 + g_2(2x + 1).$$

Hence, or otherwise, find an isomorphism from $\mathbf{Z}_3[x]/J_1$ to $\mathbf{Z}_3[x]/J_2$, and write down the inverse of this isomorphism.

[15 marks]

9. a) A panel of three winetasters has nine wines to test. Testing takes place in four sessions. In each session, each winetaster takes three of the bottles of wine to compare. Each pair of bottles is tested by the same winetaster in exactly one session. By considering lines in $\mathbf{Z}_3^2$ or otherwise, draw up a schedule to show that this is possible.

b) Now suppose that there are sixteen wines, four winetasters, and five sessions. Explain why a schedule is still possible, but do *not* write it down in detail. [15 marks]

10. a) Let n be an integer greater than 1 and let

$$1 + x^n = g(x)h(x)$$

where $g(x)$, $h(x) \in \mathbf{Z}_2[x]$, multiplication is in $\mathbf{Z}_2(x)$, and

$$h(x) = \sum_{i=0}^{n-k} h_i x^i$$

with $0 < k < n$. Using the coefficients h_i, describe a *check matrix* for the cyclic code C with generator $g(x)$. Now describe what codes you get when $k = 0$ or n, that is, $g(x) = 1$ or $g(x) = 1 + x^n$.

b) Now let $n = 20$. Find all possible generators $g(x) \in \mathbf{Z}_2[x]$ of cyclic codes of length 20. You may write $g(x)$ in any form you like. If, for example, you find $g(x)$ as a product of polynomials, you need not work the product out.

c) Consider the unique choice of $h(x)$ as in a) which is of degree 9. Show, if possible without writing down the check matrix completely, that the corresponding cyclic code has weight at least 3. Also, give the number of columns and rows in this check matrix. [15 marks]

11. Let $\mathbf{B}$ be a 2-design with parameters $(v, k, 1)$. Let the sets in the collection $\mathbf{B}$ be subsets of the v-element set V.

a) Show that the number of sets in $\mathbf{B}$ is

$$\frac{v(v-1)}{k(k-1)}.$$

[*Hint*: You might find it useful to state the number of 2-element sets in V, and the number of 2-element sets in any set in the collection $\mathbf{B}$. You will obtain some credit if you state these correctly.]

b) Let C be the code whose words are the rows of the incidence matrix of $\mathbf{B}$, where the incidence matrix has columns indexed by the elements of V, and rows indexed by the sets in $\mathbf{B}$. Show that the distance between any two codewords is at least $2k-2$.

c) Now let C' be any code in $\mathbf{Z}_2^v$ with m words and with minimum distance at most $2k-3$. Show that the number of words of $\mathbf{Z}_2^v$ with distance at most $k-2$ from any fixed word in C' is

$$1 + v + \binom{v}{2} + \cdots + \binom{v}{k-2}.$$

Hence, or otherwise, show that

$$2^v \geq m\left(1 + v + \binom{v}{2} + \cdots + \binom{v}{k-2}\right).$$

Deduce that if there exists a 2-design with parameters $(v, k, 1)$ then

$$k(k-1)2^v \geq v(v-1)\left(1 + v + \binom{v}{2} + \cdots + \binom{v}{k-2}\right).$$

[15 marks]