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) $R = \mathbf{Z}_3$, b) $R = \mathbf{Z}_4$,

c) $R = \mathbf{R}[x]$.

[10 marks]

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

$$a(x) = d(x)c(x),\ b(x) = e(x)c(x),$$
$$c(x) = m(x)a(x) + n(x)b(x).$$

[8 marks]

3. Factorize $x^4 + 1$ as a product of irreducibles in each of the rings $\mathbf{Z}[x]$, $\mathbf{R}[x]$, $\mathbf{Z}_2[x]$. You may assume that if $x^4 + 1$ factorizes in $\mathbf{Z}[x]$, $\mathbf{R}[x]$ as a product of two degree two factors, then the factorization must be of the form

$$(x^2 + ax + b)(x^2 - ax + b).$$

[11 marks]

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

b) Find the point of intersection in $\mathbf{Z}_3^2$ of the lines $x + y + 2 = 0$ and $2x + y + 1 = 0$.

c) Find all lines in $\mathbf{Z}_3^2$ through the point $(1, 0)$.

[7 marks]

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

a) A 1-design with parameters $(11, 6, 3)$.

b) A 1-design with parameters $(10, 6, 3)$.

c) A 2-design with parameters $(7, 3, 1)$.

d) A 2-design with parameters $(8, 3, 1)$.

[9 marks]

6. Let C be the linear code with check matrix

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

Give a condition on H which implies that C corrects one error. Write down what the weight of a linear code C has to be for it to correct one error. Determine which of the following are codewords of the code C, and, assuming at most one error, correct those which are not codewords.

a) 1110110 b) 1001011 [10 marks]

SECTION B

7. (i) 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 ring $R = \mathbf{Z}[i]$, and which are ideals.

a) $J = \{2m + ni : m,\ n \in \mathbf{Z}\}$.

b) $J = \{m + 2ni : m,\ n \in \mathbf{Z}\}$.

(ii) Now let R be any Euclidean domain with valuation v, and let J be any ideal in R apart from the trivial ideal $\{0\}$. Let b be any element of J such that $b \neq 0$ and such that $v(b) \leq v(r)$ for all $r \in J$, $r \neq 0$. By considering the equation $a = qb + r$ or otherwise, show that $J = \{qb : q \in R\} = bR$.

[15 marks]

8. (i) Show that $f(x) = x^3 + 2x + 1$ is irreducible in $\mathbf{Z}_3[x]$. Show also that $f(x) = f(x+1) = f(x+2)$ in $\mathbf{Z}_3[x]$.

(ii) Let $J = f(x)\mathbf{Z}_3[x]$. Show that $\alpha = J + x$ is a solution of $f(X) = 0$, where the 0 on the righthand side of this equation is the zero element J in the ring $\mathbf{Z}_3[x]/J$. Give two other solutions.

(iii) Show that for any $g_1(x)$, $g_2(x) \in \mathbf{Z}_3[x]$,

$$J + g_1(x) = J + g_2(x) \Leftrightarrow J + g_1(x+1) = J + g_2(x+1).$$

Hence, or otherwise, find an isomorphism φ from $\mathbf{Z}_3[x]/J$ to itself which is not the identity isomorphism, and write down the inverse of φ.

(iv) Explain why the identity isomorphism, φ and φ^{-1} are the only isomorphisms of $\mathbf{Z}_3[x]/J$ to itself.

Hint: the fact that f has precisely three zeros in $\mathbf{Z}_3[x]/J$ is relevant.

[15 marks]

9. a) Three people are testdriving nine cars for a consumer guide. Testdriving takes place in four sessions. In each session, each testdrives three of the cars. Each pair of cars is driven by the same person 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 fifteen cars, five people, and seven sessions. Explain why a schedule is still possible, but do *not* write it down in detail. [15 marks]

10. (i) Factorize $x^{12} + 1$ in $\mathbf{Z}_2[x]$ as a product of irreducibles.

Hint: You may find it useful to factorize $x^3 + 1$ in $\mathbf{Z}_2[x]$ first, and to use the fact that $(1+y)^2 = 1 + y^2$.

(ii) Find all degree five factors $g(x)$ of $1+x^{12}$ in $\mathbf{Z}_2[x]$, and all degree seven factors $h(x)$. Hence or otherwise, write down the check matrices H of all the cyclic codes of length 12 with canonical generators $g(x) \in \mathbf{Z}_2[x]$ of degree five. Determine which of these codes correct one error.

[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.

(i) Let A be the incidence matrix with rows and columns indexed by lines and points of $P^2(\mathbf{Z}_2)$ respectively. Let $\mathbf{1}$ be the 7-letter word with 1 in every entry, and let $\mathbf{0}$ be similarly defined. Let C be the code in $\mathbf{Z}_2^7$ whose words are $\mathbf{1}$, $\mathbf{0}$, and all words $\mathbf{a}$, $\mathbf{1}-\mathbf{a}$ where $\mathbf{a}$ is any word (in the letters 0 and 1) made from a row of A. Show that C has minimum distance 3. It is not necessary to write down A explicitly. It is enough to state clearly any property about points and lines in $P^2(\mathbf{Z}_2)$ that you use.

(ii) Now let C' be any code in $\mathbf{Z}_2^v$ with m words and with minimum distance at most $2e+1$. Show that the number of words of $\mathbf{Z}_2^v$ distance at most e from any fixed word in C' is

$$1 + v + \binom{v}{2} + \cdots + \binom{v}{e}.$$

Hence, or otherwise, show that

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

Give an example of a code for which equality is obtained with $v = 7$ and $m = 16$ and $e = 1$.

[15 marks]