SECTION A

1.

a) Let $a \in R$, where R is a ring with identity. Define what is meant by the *multiplicative inverse* of a in R (if it exists).

b) In each of the following, either find the multiplicative inverse of $a \in R$, or explain why it does not exist.

(i) $R = \mathbf{Z}_5$, $a = 3$.

(ii) $R = \mathbf{Z}[\sqrt{2}]$, $a = 7 + 5\sqrt{2}$.

(iii) $R = \mathbf{R}[x]$, $a = x + 1$.

(iv) R is any ring with identity, and $a = u_1 u_2$, where u_1, u_2 are units in R.

[8 marks]

2. Find the g.c.d. c of a, $b \in \mathbf{Z}[i]$, where

$$a = 1 - 7i,\ b = 2 + 4i.$$

Also find d, e, m, $n \in \mathbf{Z}[i]$ such that $a = dc$, $b = ec$, $c = ma + nb$.

[9 marks]

3. Find the minimum polynomial in $\mathbf{Q}[x]$ of

(i) $(-1 + \sqrt{5})/2$, (ii) $\frac{1}{2}(\sqrt{7} - \sqrt{3})$.

In the second case, check that the polynomial that you find (which should be of degree four) is irreducible.

[12 marks]

4. Write down the 7×7 incidence matrix of lines and points in $P^2(\mathbf{Z}_2)$. You should write down all the points and lines in $P^2(\mathbf{Z}_2)$ explicitly when indexing the points and lines.

[8 marks]

5. Write down the multiplication table of the ring $\mathbf{Z}_2[x]/J$ where

(i) $J = x^2\mathbf{Z}_2[x]$, (ii) $J = (x^2 + x + 1)\mathbf{Z}_2[x]$.

[8 marks]

6. Let C be the code with check matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

a) Give the *length*, *dimension* and a lower bound on the *weight* of this code. Also, give the number of words in the code and a lower bound on the number of errors that can be corrected.

b) Determine which of the following are words of C, and correct any which are not words of C, assuming only one error:

(i) 1101011, (ii) 1100110.

[10 marks]

SECTION B

7.

a) Let R be a commutative ring. Give the definition of a *subring* and of an *ideal* of R.

b) Determine which of the following subsets J of the given ring R are subrings and which are ideals, giving brief reasons.

(i) $R = \mathbf{Q}[x]$, $J = \mathbf{Z}[x]$.

(ii) $R = \mathbf{Q}[x]$, $J = x^3\mathbf{Q}[x]$

c) Now let R be a commutative ring with identity. Let $J_1 \subset J_2$, $J_1 \neq J_2$, be ideals in R such that R/J_1 is a field. Show that $1 \in J_2$. Hence, or otherwise, show that $J_2 = R$.

[15 marks]

8.

a) Let $\mathbf{Z}_7^*$ denote the multiplicative group of $\mathbf{Z}_7$. Give the orders of all 6 elements of $\mathbf{Z}_7^*$.

b) Show that $x^2 + 1$ is irreducible in $\mathbf{Z}_7[x]$.

Now write $J = (x^2 + 1)\mathbf{Z}_7[x]$. Let $F = \mathbf{Z}_7[x]/J$ (which is a field) and let F^* be the multiplicative group of F.

c) Give the number of elements in F^* and the possible orders of elements of F^*.

d) Find the orders in F^* of

(i) $J + x$ (ii) $J + 5x$ (iii) $J + (x - 1)$.

[15 marks]

9.

a) A team of 3 people is visiting a city's supermarkets for a consumer guide. There are 9 supermarkets. Each supermarket is visited by some team member on each of 4 successive days (but not necessarily always by the same team member). Each pair of supermarkets is visited by the same team member on one of these four days. By using lines in $\mathbf{Z}_3^2$, explain how it is possible to draw up a schedule of visits, but do NOT write down a schedule in detail. However, your explanation should describe explicitly the objects related to $\mathbf{Z}_3^2$ which correspond to: the supermarkets, the team-members, the days.

b) The team next moves on to two larger cities, one with 12 supermarkets, and the other with 15. For exactly one of these it is possible to draw up a schedule satisfying the rules above, but with an increased number of days. Write down which one is possible, identifying the well-known 2-design which can be used, and giving the number of days the schedule will take. Give also a brief reason why such a schedule is not possible for the other city.

[15 marks]

10.

a) Write down the irreducible degree 2 polynomial in $\mathbf{Z}_2[x]$, and the three irreducible degree 4 polynomials in $\mathbf{Z}_2[x]$. You need not justify your answer. Hence factorize $x^{15}+1$ into irreducibles in $\mathbf{Z}_2[x]$, explaining what theory you are using.

b) Now take the factor $f(x)=(x+1)(x^4+x^3+1)$ of $x^{15}+1$, and find g such that $f(x)g(x)=x^{15}+1$. Hence, find the check matrix of the cyclic code with *generator* f, and show that it has weight ≥ 3.

c) Give the number of cyclic codes of length 15 with dimension 10, and the number with dimension 11, giving a brief explanation.

[15 marks]

11.

a) Let A be the (13×13) incidence matrix of points and lines in the projective plane $P^2(\mathbf{Z}_3)$, with rows indexed by points and columns by lines. State how many 1's there are in each column of A. Explain why, for any two columns of A, there is exactly one row such that 1 occurs in this row for both columns.

[*Hint:* what do you know about a given point and pairs of lines in a projective plane?]

Show that any two columns of A differ in exactly 6 entries.

b) Let E be the 13×13 matrix with 1 in every entry, let A be the matrix in part a), and let $A'=E-A$, taking subtraction in $\mathbf{Z}_2$. Show that any column of A' differs from any column of A in at least 7 entries.

c) Now let C be the code whose words are the columns of A and the columns of A'. Suppose that a word (not necessarily in C, but of length 13) differs in ≤ 2 entries from a column of A. Give an upper bound on the number of 1's it can have.

Now let a word have six 1's. Give the best possible lower bound on the number of corresponding points which must lie on the same line..

[*Hint*: remember that entries are indexed by points in $P^2(\mathbf{Z}_3)$.]

Do the same if the word has four 1's.

[15 marks]