SECTION A

1. Define a *zero divisor* and a *unit* in a commutative ring R with identity. Find all units and zero divisors in the ring $\mathbf{Z}_{10}$, and find the multiplicative inverse of each element, where it exists.

[9 marks]

2. Find the g.c.d. c of elements a and b in the ring R, in each of the following examples. Also, find m and $n \in R$ such that $c = ma + nb$.

a) $R = \mathbf{Z}_2[x]$, $a = x^4 + 1$, $b = x^3 + 1$.

b) $R = \mathbf{Z}[i]$, $a = 9 - 2i$, $b = 7 - i$.

[9 marks]

3. In the projective plane $P^2(\mathbf{Z}_3)$:

a) find all points in the projective line $2X + Y + Z = 0$,

b) and hence, or otherwise, find all projective lines through the point $[2 : 1 : 1]$.

[7 marks]

4. Let J be the ideal $\mathbf{Z}_2[x].(1 + x + x^3)$ in $\mathbf{Z}_2[x]$. For each n, $1 \leq n \leq 7$, write each of the elements $(J + x)^n$ in the form $J + f$ for $f \in \mathbf{Z}_2[x]$ of degree ≤ 2. Hence, or otherwise, write $(J + x)^{-1}$ in the form $J + f$ for $f \in \mathbf{Z}_2[x]$ of degree ≤ 2.

[10 marks]

5. State, with brief reasons, which of the following exist.

a) A 1-design with parameters $(15, 4, 3)$.

b) A 1-design with parameters $(15, 3, 2)$.

c) A 2-design with parameters $(12, 3, 1)$.

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

[10 marks]

6. Consider the Hamming code with check matrix

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

Give a lower bound on the minimum distance between any two codewords, with a brief reason. Determine which of the following are codewords, and correct those which are not, assuming that just one error has been made.

a) 1001011, b) 1010100.

[10 marks]

SECTION B

7. a) Give the definition of a homomorphism between rings R_1 and R_2.

b) Let R_1 and R_2 be rings with identity, let R_2 have no zero divisors and let $\varphi : R_1 \to R_2$ be a homomorphism with $\varphi(x) \neq 0$ for at least one $x \in R_1$. By considering the equation $x \times 1 = x$ or otherwise, show that $\varphi(1) = 1$.

c) Determine which of the following are homomorphisms:

(i) $\varphi_1 : \mathbf{Z} \to \mathbf{Z}$ given by $\varphi_1(n) = -n$ for all n,

(ii) $\varphi_2 : \mathbf{Z}[i] \to \mathbf{Z}[i]$ given by $\varphi_2(z) = \bar{z}$.

d) Now let $\varphi : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}$ be a homomorphism with $\varphi(x) \neq 0$ for at least one x. Show that $\varphi(2) = 2$. By considering $\varphi(\sqrt{2})$ (or otherwise) show that such a homomorphism φ does not exist.

[15 marks]

8. a) Find all irreducible factors of $x^{10} + 1$ in $\mathbf{Z}_2[x]$, possibly showing first that, in $\mathbf{Z}_2[x]$,

$$x^{10} + 1 = (x^5 + 1)^2.$$

b) Write down the check matrices for the cyclic codes over $\mathbf{Z}_2$ of length 10, corresponding to those [reducible] factors of $x^{10} + 1$ which have degrees 4, 5 and 6. [There is one for each degree.] Find one of these codes which has weight at least 3, explaining why this is so.

[15 marks]

9. a) List the elements of the group Q of quadratic residues in $\mathbf{Z}_{31}$.

b) Show that any irreducible polynomials of degree 5 in $\mathbf{Z}_2[x]$ must be of the form

$$1 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + x^5,$$

where either exactly one or exactly three of the a_i are equal to one. Assuming that the irreducible polynomials in $\mathbf{Z}_2[x]$ of degrees two and three are

$$1 + x + x^2,\ 1 + x + x^3,\ 1 + x^2 + x^3,$$

find the two degree 5 polynomials in $\mathbf{Z}_2[x]$ of the above form which are *reducible* in $\mathbf{Z}_2[x]$.

c) Write $x^{31} + 1 = f(x)$ as a product of irreducible factors in $\mathbf{Z}_2[x]$, explaining what theory you are using.

d) Let $x^{31} + 1 = f(x)$ as in part c). Let $g_0(x)$ be a factor of $f(x)$, and let g_0 be a generator of a quadratic residue code of length 31. Let α be a zero of g_0 in some extension field of $\mathbf{Z}_2$. Describe the other zeros of g_0, in terms of α and Q, where Q is as in part a).

[15 marks]

10. a) State Kirkman's Schoolgirls problem (in any guise you like).

b) Let A and the vectors z, $y_i \in \mathbf{Z}_2^4$ be given by

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \; z = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; y_0 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \; y_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; y_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Show that

$$Az = z, \; Ay_0 = y_1, \; Ay_1 = y_2, \; Ay_2 = y_0 + y_1.$$

Hence or otherwise compute $y_i = A^i y_0 \in \mathbf{Z}_2^4$ for $0 \leq i \leq 7$, show that $\{y_i : 0 \leq i \leq 6\}$ are all distinct, and that $y_7 = y_0$. Show also that if $x_i = y_i + z$ then $A^i x_0 = x_i$ for $0 \leq i \leq 7$.

c) Show that if x, y, $w \in \mathbf{Z}_2^4$ with $w = x + y$, then

$$x = y + w, \; y = x + w.$$

Show that if x_i, y_i are as above and $y_\ell = y_j + y_k$ then $y_\ell = x_j + x_k$. Verify that each of the following triples $\{x, y, w\}$ satisfies $w = x + y$:

$$\{z, y_0, x_0\}, \; \{y_1, y_2, y_4\}, \; \{x_1, x_5, y_6\}, \; \{x_2, x_3, y_5\}, \; \{x_4, x_6, y_3\}.$$

d) Hence, or otherwise, describe a solution to the Kirkman's Schoolgirls problem. You need not justify your answer.

[15 marks]

11. a) Give a definition of a 2-design with parameters (v, k, r). Explain why the set of lines in $\mathbf{Z}_3^2$ is a 2-design with parameters $(9, 3, 1)$. Show that each point lies on 4 lines.

[It is possible to do this without writing the lines down.]

b) Let A be the incidence matrix for the 2-design of lines in $\mathbf{Z}_3^2$, with columns indexed by points in $\mathbf{Z}_3^2$, and rows by lines. Show that any column of A has 1's in exactly 4 rows. Show that, for any two columns of A, there is exactly one row in which *both* columns have a 1. Let C be the code whose words are the columns of A. Show that the distance between any 2 words of C is 6.

c) Now let F be a field with q elements. State, without proof, the number of lines through any point of F^2.

[15 marks]