SECTION A

1. Give the definition of a *zero-divisor* in a ring.

For each of the following, state, with justification, whether it is a zero-divisor in the stated ring.

(a) 6 in $\mathbf{Z}/8$;

(b) 4 in $\mathbf{Z}/11$;

(c) $3x^2 + 5x + 7/3$ in $\mathbf{Q}[x]$;

(d) $x - 1$ in $\mathbf{Z}/2[x]/(x^5 - 1)$. [9 marks]

2. For each of the following pairs r, s in the given ring R, find the GCD. In each case also find $a, b \in R$ such that $ar + bs = \gcd(r, s)$.

(a) $r = -3 + 6i$, $s = 7 + i$, $R = \mathbf{Z}[i]$;

(b) $r = x^3 + 2x^2 + 3x + 1$, $s = 2x^3 + 3x^2 + 2x + 1$, $R = \mathbf{Z}/5[x]$. [9 marks]

3. Let $f = 2x^3 - 2x^2 + 2x + 4$. Factor f into a product of irreducibles in:

(a) $\mathbf{Z}/3[x]$;

(b) $\mathbf{Z}/5[x]$;

(c) $\mathbf{Z}[x]$. [9 marks]

4. Let R be the ring $\mathbf{Z}[i]$ and I the principal ideal generated by 2.

(i) Write the multiplication table of the quotient ring R/I.

(ii) State the definition of *field* (in terms of the definition of "ring"). Is R/I a field? If not, say why not. [9 marks]

5. Define *t-(v, k, r)-design*. Prove that if there is a 1-(v, k, r)-design, then $k|vr$ and $r \le \binom{v-1}{k-1}$. [9 marks]

6. Let C be a linear code in $(\mathbf{Z}/2)^5$ whose check matrix is

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

(i) What are the dimension and information rate of this code?

(ii) List all words in this code. Using this list, determine the minimum distance of the code and the number of errors it corrects. [10 marks]

SECTION B

7. Define *ideal* and *principal ideal* of a ring. For each of the following subsets I of rings R, state with justification whether I is an ideal.

(a) $R = \mathbf{Z}[x]$, I is the set of polynomials whose constant term is a multiple of 3.

(b) $R = \mathbf{Z}[i]$, I is the set of nonnegative integers;

(c) $R = \mathbf{Z}$, I is the set of all composite numbers together with 0;

(d) $R = \mathbf{Z}[i]$, $I = \{a + bi : a, b \in \mathbf{Z},\ a + b \in 2\mathbf{Z}\}$. [15 marks]

8. Define *prime ideal.* Prove that an ideal I of a ring R is prime if and only if R/I is an integral domain. [15 marks]

9. Let $R = \mathbf{Z}/3\,[x]$, let $f(x) = x^3 + 2x + 2 \in R$ (you may assume that this f is irreducible in R), and let $I = (f(x)) \subset R$.

(i) Give the number of elements of R/I and the number of elements of $(R/I)^*$. State the possible orders of elements of $(R/I)^*$.

(ii) Verify that $(x^2 + 1)^2 = x + 1$ in R/I.

(iii) Using your results from (i) and (ii), or otherwise, determine the order of $x + 1$ in $(R/I)^*$. [15 marks]

10. (i) Explain (by considering lines on a plane over a finite field, or otherwise) why a 2-$(7, 3, 1)$-design exists, and write down the sets in it.

(ii) Explain why a 2-$(64, 8, 1)$-design exists. It should not be necessary to list all the sets that constitute the design. [15 marks]

11. (i) Verify that $f(x) = x^5 + 2x^3 + 2x^2 + x + 2$ divides $x^8 - 1$ in $\mathbf{Z}/3\,[x]$.

(ii) Let C be the cyclic code over $\mathbf{Z}/3$ generated by $f(x)$. Write a check matrix for C.

(iii) State a theorem about check matrices that ensures that C corrects one error.

(iv) Assuming at most one error, decode these words: 21021202, 10200121, 10221011. [15 marks]