THE UNIVERSITY *of* LIVERPOOL

SECTION A

1. Give a criterion for a non-zero $a \in \mathbf{Z}/n\mathbf{Z}$ to be

i) a zero-divisor;

ii) a unit.

Identify the zero-divisors and units in the ring $\mathbf{Z}/14\mathbf{Z}$ and find the multiplicative inverse of each unit.

[9 marks]

2. In each of the following cases factorise the polynomial $f(x)$ into irreducibles in the ring R.

(i) $R = (\mathbf{Z}/5\mathbf{Z})[x]$, $f(x) = x^3 + 2x + 2$;

(ii) $R = \mathbf{Z}[x]$, $f(x) = x^4 + 3x^3 + 6x + 15$;

(ii) $R = \mathbf{C}[x]$, $f(x) = x^4 - 1$.

(Hint: you may find Eisenstein's criterion helpful in (ii).) [9 marks]

3. Let $p \in \mathbf{Z}$ be prime and $f \in (\mathbf{Z}/p\mathbf{Z})[x]$ be a monic polynomial. Give a necessary and sufficient condition, in terms of the polynomial f, for the quotient ring $(\mathbf{Z}/p\mathbf{Z})[x]/\langle f \rangle$ to be a finite field.

Find a degree 2 polynomial $f \in (\mathbf{Z}/3\mathbf{Z})[x]$ satisfying your condition. Deduce that there is a finite field with 9 elements.

[9 marks]

4. a) Write down all the points on the line $x + 2y + 2 = 0$ in $(\mathbf{Z}/3\mathbf{Z})^2$.

b) Write down all the points on the line $2x + 2y + z = 0$ in $\mathbf{P}^2(\mathbf{Z}/3\mathbf{Z})$.

c) Write down all the lines in $(\mathbf{Z}/3\mathbf{Z})^2$ which are parallel to $x+2y+2 = 0$.

d) Find the point of intersection of the lines $2x+2y+z = 0$ and $x+y+z = 0$ in $\mathbf{P}^2(\mathbf{Z}/3\mathbf{Z})$.

[9 marks]

5. Let C be the code in $(\mathbf{Z}/2\mathbf{Z})^7$ with check matrix

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

Give the property of this matrix which ensures that the code corrects *exactly* one error. Determine which of the following words are in C, and, assuming at most one error, correct those which are not.

(i) 1111000,

(ii) 1000011.

[9 marks]

6. Find the greatest common divisor $\gcd(\alpha, \beta)$ in $\mathbf{Z}[i]$ of $\alpha = 5 + 2i$ and $\beta = 3 + 4i$. Also find Gaussian integers $\gamma, \delta \in \mathbf{Z}[i]$ with

$$\gcd(\alpha, \beta) = \alpha\gamma + \beta\delta.$$

[10 marks]

SECTION B

7. Let $N : \mathbf{Z}[\sqrt{-3}] \to \mathbf{N}$ be given by $N(a + b\sqrt{-3}) = a^2 + 3b^2$. Show that N is multiplicative i.e. for any two elements $r, s \in \mathbf{Z}[\sqrt{-3}]$ we have

$$N(rs) = N(r)N(s).$$

Show that

1. r is a unit in $\mathbf{Z}[\sqrt{-3}]$ if and only if $N(r) = 1$;
2. there are no elements r with $N(r) = 2$ in $\mathbf{Z}[\sqrt{-3}]$.

Using these results, or otherwise, show that the elements 2 and $1 \pm \sqrt{-3}$ are irreducible in $\mathbf{Z}[\sqrt{-3}]$. By factorising 4 into irreducibles in $\mathbf{Z}[\sqrt{-3}]$ in two different ways show that 2 is not a prime in $\mathbf{Z}[\sqrt{-3}]$.

[15 marks]

8. a) Show that neither a 2-$(11, 6, 2)$-design, nor a 2-$(10, 5, 1)$-design, exists.

b) Explain carefully why the lines in the projective plane $\mathbf{P}^2(\mathbf{Z}/5\mathbf{Z})$ form a 2-design in which a block is given by the set of lines passing through a given point. Find the parameters of this design.

[15 marks]

9. Say what is meant by an *ideal* of a ring R. Decide whether or not each subset S listed below is an ideal in the given ring R. You should give a careful justification of each answer.

(i) $S = \mathbf{Z}$, $R = \mathbf{Q}$;

(ii) $S = \{5a + 17b : a, b \in \mathbf{Z}\}$, $R = \mathbf{Z}$;

(iii) $S = \{\alpha \in \mathbf{Z}[i] : (3 + 4i) \text{ divides } \alpha\}$, $R = \mathbf{Z}[i]$;

(iv) $S = \{f(x) \in (\mathbf{Z}/7\mathbf{Z})[x] : f(4) = 0\}$, $R = (\mathbf{Z}/7\mathbf{Z})[x]$.

[15 marks]

10. Let $R = (\mathbf{Z}/5\mathbf{Z})[x]$ and let $I \subset R$ be the ideal generated by

$$f(x) = x^2 + x + 1.$$

Show that f is irreducible.

Write down the number of elements in the quotient ring R/I and the number of elements in $(R/I)^*$. State the possible orders of elements in $(R/I)^*$. Find the orders of the elements

(i) x,

(ii) $3x + 4$.

Compute the product $x(3x + 4)$ and deduce that $x + 2$ has order 24. (Hint: no further computation is necessary.)

[15 marks]

11. a) State a result which describes the factorisation of $x^{32} + x$ into irreducibles in $(\mathbf{Z}/2\mathbf{Z})[x]$. Noting that there are precisely 2 irreducible polynomials of degree 1, namely x and $x + 1$, deduce that there are precisely 6 irreducible polynomials of degree 5 in $(\mathbf{Z}/2\mathbf{Z})[x]$. Now

(i) explain why $f(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + 1 \in (\mathbf{Z}/2\mathbf{Z})[x]$ is not irreducible if $a + b + c + d$ is even;

(ii) compute the products $(x^2 + x + 1)(x^3 + x + 1)$ and $(x^2 + x + 1)(x^3 + x^2 + 1)$ in $(\mathbf{Z}/2\mathbf{Z})[x]$.

Finally, write down a list of the irreducible degree 5 polynomials in $(\mathbf{Z}/2\mathbf{Z})[x]$. (Hint: start by writing down a list of degree 5 polynomials in $(\mathbf{Z}/2\mathbf{Z})[x]$ which have neither x nor $x + 1$ as a factor. Then use (ii) above to eliminate two polynomials which factorise from this list so that there are only 6 remaining.)

[15 marks]