THE UNIVERSITY
of LIVERPOOL

1. Show that $x^3 + 2x + 2$ is an irreducible polynomial in $(\mathbf{Z}/3\mathbf{Z})[x]$.
Let $\mathbf{F} = (\mathbf{Z}/3\mathbf{Z})[x]/\langle x^3 + 2x + 2\rangle$.

(i) Find the number of elements in $\mathbf{F}$ and $\mathbf{F}^*$. List the possible orders of elements of $\mathbf{F}^*$.

(ii) Show that 2 is not a square in $\mathbf{F}$. (Hint: what would the order of its square root be, if it were?)

(iii) Show that $2x^2$ is not a square in $\mathbf{F}$.

(iv) Show that $(x+2)^2 = x^2 + x + 1$. Hence, or otherwise, show that $x^2 + x + 1$ has order 13 in $\mathbf{F}^*$. (Hint: It is not necessary to compute $(x^2 + x + 1)^{13}$ to obtain this result.)

[20 marks]

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

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

Write down the units in $\mathbf{Z}[i]$ and prove that if $N(a+bi)$ is a prime in $\mathbf{N}$ then $a+bi$ is irreducible in $\mathbf{Z}[i]$. Factorise the following elements of $\mathbf{Z}[i]$ into irreducibles.

(i) 3,

(ii) 5,

(iii) $1 + 4i$,

(iv) $3 + 5i$,

(v) $7 - i$.

Give an example of an irreducible element $a + bi$ of $\mathbf{Z}[i]$ for which $N(a + bi)$ is NOT a prime in $\mathbf{Z}$.

[20 marks]

3. a) Find the minimal polynomials of $\sqrt{2}$ in $\mathbf{Q}[x]$ and of $\sqrt{2}+\sqrt{7}$ in $\mathbf{Q}[x]$. This means showing that the polynomials you find are irreducible.

b) Let $\alpha = \sqrt{2}+\sqrt{7}$. By computing $\alpha(\alpha^2-9)$, or otherwise, show that $\sqrt{2} \in \mathbf{Q}[\alpha]$. Find the degrees of the following field extensions.

(i) $\mathbf{Q} \subseteq \mathbf{Q}[\sqrt{2}]$,

(ii) $\mathbf{Q} \subseteq \mathbf{Q}[\alpha]$,

(iii) $\mathbf{Q}[\sqrt{2}] \subseteq \mathbf{Q}[\alpha]$.

Prove that $\sqrt{7} \notin \mathbf{Q}[\sqrt{2}]$. [20 marks]

4. Suppose $f(x)$ is irreducible in $\mathbf{Q}[x]$. Explain why, given a polynomial $g(x) \in \mathbf{Q}[x]$ of degree strictly less than the degree of $f(x)$, we can find polynomials $a(x), b(x) \in \mathbf{Q}[x]$ with

$$a(x)f(x) + b(x)g(x) = 1.$$

Explain how to find a multiplicative inverse for (the class of) $g(x)$ in $\mathbf{Q}[x]/\langle f(x)\rangle$. Find multiplicative inverses for

(i) $g(x) = x+1$ in $\mathbf{Q}[x]/\langle x^3+x+1\rangle$ and,

(ii) $g(x) = x^2+1$ in $\mathbf{Q}[x]/\langle x^3+4x^2+2\rangle$.

[20 marks]

5. Write down the number p of points in $(\mathbf{Z}/5\mathbf{Z})^2$ and the number of points on any line in $(\mathbf{Z}/5\mathbf{Z})^2$.

(i) Find the number l of lines in $(\mathbf{Z}/5\mathbf{Z})^2$ and the number of lines through a given point in $(\mathbf{Z}/5\mathbf{Z})^2$. (Hint: you may assume that there is a unique line through any two distinct points.)

(ii) Construct a 1-$(p,5,6)$-design and a 2-$(p,5,1)$-design with underlying set the set of points in $(\mathbf{Z}/5\mathbf{Z})^2$.

(iii) Construct a 1-$(l,6,5)$-design and a 1-$(l,5,1)$-design with underlying set the set of lines in $(\mathbf{Z}/5\mathbf{Z})^2$. (Hint: for the second design it may help to consider parallel lines.)

[20 marks]

6. a) A gardener is testing out seven varieties of flowers. He plants three different varieties in each of seven locations, in such a way that each pair of varieties is grown together in at least one location. By using points and lines in $\mathbf{P}^2(\mathbf{Z}/2\mathbf{Z})$ draw up a schedule to show that this is possible. Make clear what the points and lines represent and which properties of points and lines in $\mathbf{P}^2(\mathbf{Z}/2\mathbf{Z})$ you use.

b) Give the formal definition of a 2-(v, k, r)-design. Let $\mathbf{B}$ be a 2-(v, k, r)-design. Write down two restrictions on the parameters (v, k, r) of the design. Show that if $r = 1$ and $k = 3$ then v is of the form $6n + 1$ or $6n + 3$ for some integer n.

[20 marks]

7. a) Find the irreducible degree 2 polynomial in $(\mathbf{Z}/2\mathbf{Z})[x]$, and the three irreducible degree 4 polynomials in $(\mathbf{Z}/2\mathbf{Z})[x]$. You should prove that the polynomials you find are irreducible. Hence factorize $x^{15} + 1$ into irreducibles in $(\mathbf{Z}/2\mathbf{Z})[x]$, explaining what theory you are using.

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

c) Give a complete list of generators for the cyclic codes of length 15 and give the corresponding dimensions of the codes. (You may write the generators in any form you wish, in particular, if you find them as products of polynomials you need not work these products out.)

[20 marks]

8. a) Define the *minimum distance* and *weight* of a linear code in $(\mathbf{Z}/2\mathbf{Z})^n$, and show that they coincide.

b) Let M be the check matrix of a linear code C in $(\mathbf{Z}/2\mathbf{Z})^n$.

(i) Show that if no column of M is identically zero, then C has weight > 1.

(i) Show that if, in addition, no two columns of M are the same, then C has weight > 2.

(i) Show that if, in addition, the sum of any three columns is not identically zero, then C has weight > 3.

(iv) Now consider the check matrix

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

Show that the corresponding code C has weight 4. In particular this means that you should find a word in C of weight 4. State the number of errors *detected* and the number of errors *corrected* by this code.

[20 marks]