MATH247 September 2002 Solutions.

Section A.

1. $a \in R$ is a *unit* if there exists $b \in R$ with $ab = ba = 1$.
[2 marks]
b is then the *multiplicative inverse* of a. (It is unique.)
[2 marks]
a) $\mathbf{Z}_3 = \{0, 1, 2\}$. $1 \times 1 = 2 \times 2 = 1$ (and $0 \times a = 0$ for all $a \in \mathbf{Z}_3$). So 1 and 2 are the units in $\mathbf{Z}_3$.
[2 marks.]
b) $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ $1 \times 1 = 3 \times 3 = 1$ and $2 \times 2 = 0$. No element can be both a unit and a zero divisor. So 1 and 3 are the units in $\mathbf{Z}_4$.
c)
$$(a_n x^n + \cdots)(b_m x^m + \cdots) = a_n b_m x^{n+m} + \cdots$$
So the only way in which to get product 1 is if both polynomials are constant. So the units are all the constant polynomials a_0 with $a_0 \neq 0$, with inverse $1/a_0$.
[3 marks.]
[$10 = 2 + 1 + 2 + 2 + 3$ marks.]
The first part is standard theory, the rest standard homework problems.

2. $a(x) = x^4 + x^2 + 1$, $b(x) = x^3 + 1 \in \mathbf{Z}_2[x]$. We have
$$x^4 + x^2 + 1 = x(x^3 + 1) + x^2 + x + 1 \tag{1}$$
by inspection or long division
[2 marks] and
$$x^3 + 1 = (x + 1)(x^2 + x + 1) \tag{2}$$
again by inspection or long division
[2 marks]
So $c(x) = x^2 + x + 1$ is the g.c.d. of $a(x)$ and $b(x)$
[1 mark] and $d(x) = x + 1$ from (2), while from (1) and (2) (or alternatively by long division)
$$x^4 + x^2 + 1 = x(x + 1)(x^2 + x + 1) + x^2 + x + 1 = (x^2 + x + 1)(x^2 + x + 1)$$
and $e(x) = x^2 + x + 1$.
[2 marks]
From (1),
$$x^2 + x + 1 = x^4 + x^2 + 1 + x(x^3 + 1).$$
So $m(x) = 1$ and $n(x) = x$.
[1 mark]
[$8 = 2 + 2 + 1 + 2 + 1$ marks]
Standard homework exercise.

3. $x^4 + 1$ has no zeros in $\mathbf{Z}$ (or $\mathbf{R}$).

[1 mark.]
So if it factorizes in $\mathbf{R}[x]$ or $\mathbf{Z}[x]$, it must have a factorization as a product of two degree two polynomials, and we are allowed to assume this is of the form

$$(x^2+ax+b)(x^2-ax+b).$$

(This actually follows from considering the coefficients of the x^3 term and then the x term, since we must have $a\neq 0$.) Then $b^2=1$, giving $b=\pm 1$. Then $a^2=2b=\pm 2$, giving no real a unless $b=1$, in which case $a=\sqrt{2}$. Both factors have no real zeros because $(\sqrt{2})^2-4<0$, and hence they are irreducible in $\mathbf{R}[x]$.
[5 marks]
So there is a factorization in $\mathbf{R}[x]$

$$x^4+1=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$$

but x^4+1 is irreducible in $\mathbf{Z}[x]$ because $\sqrt{2}\notin\mathbf{Z}$.
[2 marks]
In $\mathbf{Z}_2[x]$ we have

$$x^4+1=(x+1)^4,$$

which is the factorization into irreducibles in $\mathbf{Z}_2[x]$.
[3 marks]
[$11=1+5+2+3$ marks]
Standard homework exercise.

4a) $x+y+2=0\ \Leftrightarrow y=1+2x$ (in $\mathbf{Z}_3$).
So taking $x=0,\ 1,\ 2$ gives the points $(0,1)$, $(1,0)$, $(2,2)$.
b)

$$x+y+2=0,\ 2x+y+1=0.$$

Subtracting the first equation from the second gives $x-1=0$, that is, $x=1$, so that from the first equation $y=1+2x=0$. So (1,0) is the point of intersection.
[2 marks.]
c) The lines through $(1,0)$ are of the form

$$a(x-1)+by=0$$

for $(a,b)\neq(0,0)$. To avoid duplication of lines, we take $b=1$ or $b=0$ and $a=1$.
$b=1$ gives $y=0$, $x+y+2=0$, $2x+y+1=0$.
$b=0$ and $a=1$ gives $x+2=0$.
[3 marks]
[$7=2+2+3$ marks.]
[Standard homework exercise.]

5a) 6 does not divide 11×3. So there is no 1-design with these parameters.
[1 mark]
b) $6\mid 10\times 3$ and $3<\binom{9}{5}$. So there is a 1-design with these parameters.
[2 marks]

c) The set of lines in $P^2(\mathbf{Z}_2)$ is such a 2-design: $P^2(\mathbf{Z}_2)$ has 7 points, each line has 3 points and any two lines intersect in 1 point.

[3 marks]

d) There is no 2design with these parameters (v, k, r) because $2 = k - 1$ does not divide $(v-1)r = 7$.

[3 marks]

[$9 = 1 + 2 + 3 + 3$ marks]

Standard homework exercises.

6. All the columns of H are distinct and not identically 0. So H corrects one error

[2 marks]

The weight has to be 3

[1 mark.]

a)

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

This is not a code word. Since the third column of the check matrix is obtained, the third letter must be wrong and the corrected word is 1100110.

[4 marks]

b)

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

So this is a codeword

[3 marks.]

$10 = 2 + 1 + 4 + 3$ marks.]

Standard homework exercise, with a bit of standard theory at the start.

Section B.

7(i) $S \subset R$ is a *subring* of R if $S \neq \phi$ and x, $y \in S \Rightarrow x - y \in S$, $xy \in S$.

[2 marks]

$S \subset R$ is an *ideal* of R if $S \neq \phi$ and x, $y \in S \Rightarrow x - y \in S$, $x \in S$, $y \in R \Rightarrow xy \in S$.

(i)a) $(2+i) = -1 + 2i \notin S$, although $2 + i$, $i \in S$. So S is not a subring, and hence not an ideal

[2 marks]

$(i)b)$ $$(m_1+2n_1i)-(m_2+2n_2i)=(m_1-m_2)+2(n_1-n_2)i.$$
$$(m_1+2n_1i)(m_2+2n_2i)=(m_1m_2-4n_1n_2)+2(n_1m_2+n_2m_1)i$$

for all integers m_i, n_i, $i=1, 2$. So S is a subring.

[3 marks]

But S is not an ideal because $1 \in J$ but $i.1 = i \notin J$.

[1 mark]

(ii) Let $b \neq 0$, $b \in J$ with $v(b)$ minimal. Take any $a \in J$. Then $a = qb + r$ for some a, $r \in R$ with $r = 0$ or $v(r) < v(b)$. We have $r = a - qb \in J$ Since $v(b)$ is minimal for $b \neq 0$, we must have $r = 0$, and hence $a = qb$. So $J \subset bR$. But $bR \subset J$. So $J = bR$.

[5 marks.]

[$15 = 2+2+2+3+1+5$ marks]

(i) is standard theory for the definitions and similar to homework exercises for a) and b), while (ii) is standard theory, with hints provided.

8(i). For $f(x) = x^3 + 2x + 1$, we have $f(0) = 1$, $f(1) = 1$, $f(2) = 13 = 1$. So f has no zeros in $\mathbf{Z}_3$, hence no degree one factors, and is irreducible

[2 marks]

$$f(x+1) = (x+1)^3 + 2(x+1) + 1 = x^3 + 2x + (3x^2 + 3x) + 1 + 2 + 1 = f(x).$$

[2 marks]

$$f(x+2) = (x+2)^3 + 2(x+2) + 1 = x^3 + 6x^2 + 12x + 8 + 2x + 4 + 1 = f(x).$$

[1 mark]

(ii)

$$f(J+x) = J + x^3 + 2(J+x) + 1 = J + x^3 + 2x + 1 = J = 0.$$

[1 mark]

a is a zero $\Leftrightarrow$ $a+1$ and $a+2$ are zeros by a) (since $a = (a+1)+2 = (a+2)+1$). So $J+x+1$ and $J+x+2$ are the other zeros.

[1 mark]

(iii)

$$J+g_1(x) = J+g_2(x) \;\Leftrightarrow\; f(x) \mid (g_1(x)-g_2(x)) \;\Leftrightarrow\; f(x) = f(x+1) \mid (g_1(x+1)-g_2(x+1))$$
$$\Leftrightarrow\; J + g_1(x+1) = J + g_2(x+1).$$

[3 marks]

This shows that $\varphi(J+g(x)) = J + g(x+1)$ is well-defined and one-to-one.

[1 mark]

To show that it is onto and compute the inverse: $\psi(J+h(x)) = J + h(x+2)$ is also well-defined for similar reasons (or alternatively, $\psi = \varphi \circ \varphi$) and

$$\psi \circ \varphi(J+g(x)) = J + g(x+3) = J + g(x) = \varphi \circ \psi(J+g(x)).$$

[2 marks.]

(iv) Any isomorphism Φ has to map $J+x$ to a zero of f, that is, to $J+x$ or $J+x+1$ or $J+x+2$, and then $\Phi(J+g(x)) = g(\Phi(J+x))$.

[2 marks]

[$15 = 2+2+1+1+1+3+1+2+2$ marks.

Standard exercises on quotient rings, parts of (iii) and (iv) are basically unseen, but also similar in part to standard homework exercises on computing inverse homomorphisms.

9a) Use the 2-design of lines in $\mathbf{Z}_3^2$. The 9 points in $\mathbf{Z}_3^2$ correspond to the cars. The sessions correspond to the sets of parallel lines. Each set of parallel lines is of the form $\{ax+by+c=0 : c \in \mathbf{Z}_3\}$ for fixed $(a,b) \neq (0,0)$ (where $(\lambda a, \lambda b)$ gives the same line as (a,b) for $\lambda \neq 0$). The test-drivers correspond to the values of $c \in \mathbf{Z}_3$. In the incidence matrix below, 1 indicated that a car is tested by that driver in that session.

[4 marks for explanation]

*	$(0,0)$	$(1,0)$	$(2,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(0,2)$	$(1,2)$	$(2,2)$
Session 1	*	*	*	*	*	*	*	*	*
$x=0$	1	0	0	1	0	0	1	0	0
$x+1=0$	0	0	1	0	0	1	0	0	1
$x+2=0$	1	0	0	1	0	0	1	0	
Session 2	*	*	*	*	*	*	*	*	*
$y=0$	1	1	1	0	0	0	0	0	0
$y+1=0$	0	0	0	0	0	0	1	1	1
$y+2=0$	0	0	0	1	1	1	0	0	0 .
Session 3	*	*	*	*	*	*	*	*	*
$x+y=0$	1	0	0	0	0	1	0	1	0
$x+y+1=0$	0	0	1	0	1	0	1	0	0
$x+y+2=0$	0	1	0	1	0	0	0	1	
Session 4	*	*	*	*	*	*	*	*	*
$x+2y=0$	1	0	0	0	1	0	0	0	1
$x+2y+1=0$	0	0	1	1	0	0	0	1	0
$x+2y+2=0$	0	1	0	0	0	1	1	0	0

[7 marks]

b) The 2-design corresponding to Kirkman's Schoolgirls problem will do. The 7 days in Kirkman's problem correspond to the 7 testdriving session. The 15 girls correspond to the 15 cars. The 5 groups of girls (on each day) correspond to the 5 groups of cars driven by the 5 testdrivers.

4 marks]

[$15 = 4+7+4$ marks]

Part a) is similar to standard homework exercise, b) tests knowledge of Kirkman's schoolgirls problem (and would be similar to a standard homework problem, but harder, if it were developed).

10(i) We have $1+x^3 = (1+x)(1+x+x^2)$ in $\mathbf{Z}_2[x]$. Hence, since $(1+y)^2 = 1+y^2$, we have

$$1+x^{12} = (1+x^3)^4 = (1+x)^4(1+x+x^2)^4.$$

$1+x+x^2$ is irreducible in $\mathbf{Z}_2[x$ since it has no zero in $\mathbf{Z}_2$ - and of course $1+x$ is irreducible as well

[3 marks]

(ii) A general factor of $1+x^{12}$ is of the form $(1+x)^r(1+x+x^2)^s$ where $0 \le r$, $s \le 4$. To get a factor $g(x)$ of degree 5 we need $r+2s=5$, and the only possibilities are $r=3$, $s=1$ or $r=1$, $s=2$. To get a factor $h(x)$ of degree 7 we must have $r=3$, $s=2$ or $r=1$, $s=3$.

[2 marks]

a) With canonical generator $g(x)=(1+x)^3(1+x+x^2)$, the check matrix is computed from

$$h(x)=(1+x)(1+x+x^2)^3=(1+x^3)(1+x^2+x^4)=x^7+x^5+x^4+x^3+x^2+1$$

from which the check matrix is

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

All columns are distinct and nonzero. So this code corrects one error.

[5 marks.]

b) With canonical generator $g(x)=(1+x)(1+x+x^2)^2$, the check matrix is computed from

$$h(x)=(1+x)^3(1+x+x^2)^2=(1+x)(1+x^6)=x^7+x^6+x+1,$$

from which the check matrix is

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

The first and seventh columns are the same. So the code has weight two and does not correct one error.

5 marks

[$15=3+2+5+5$ marks.]

Standard homework exercise.

11(i) Every row of A has exactly three 1's (because there are three points on every line in $P^2(\mathbf{Z}_2)$). For any two rows of A, there is exactly one column where both have a 1, because any two lines intersect in exactly one point. So the distance between any two rows of A is 4.

[4 marks.]

Write $\mathbf{1}$, $\mathbf{0}$ for the vectors of all 1's and all 0's. If $\mathbf{c}$ and $\mathbf{c}'$ are rows of A with $\mathbf{c} \ne \mathbf{c}'$, then $\mathbf{c}$ and $\mathbf{1}-\mathbf{c}'$ agree in the entries where $\mathbf{c}$ and $\mathbf{c}'$ differ. They agree in exactly four entries, and hence differ in three.

[3 marks.]

Let E be the matrix of all 1's. Since any row of A or $E-A$ has either 3 or 4 1's, these all differ from $\mathbf{0}$ and $\mathbf{1}$ in at least three entries. So the minimum distance of C is 3.

[2 marks.]

(ii) There are $\binom{v}{i}$ words which differ from $\mathbf{c}$ in exactly i entries (this being the number of i-element subsets of a v-element set). So the number of words differing from $\mathbf{c}$ in $\leq e$ entries is

$$1+\binom{v}{1}+\cdots+\binom{v}{e}.$$

[3 marks.]

Write $B(\mathbf{c})$ for this set. For minimum distance $2e+1$, the sets $B(\mathbf{c})$ must all be disjoint. Since C' has m words and $\mathbf{Z}_2^v$ has 2^v words, this gives

$$2^v \geq m\left(1+v+\cdots\binom{v}{e}\right).$$

[2 marks.]

To get equality, take C' to be the code C of part a), which has $m=16$ words in $\mathbf{Z}_2^7$ and has minimum distance $2e+1=3$ with $e=1$. The equality then says $2^7=16\times(7+1)=2^4\times 2^3$ - which is true.

1 mark.

[$15=4+3+2+3+2+1$ marks.]

(i) is similar to a homework exercise. Most of (ii) is basic theory. The last bit is unseen.