MATH247 January 2002. Solutions.

SECTION A

1. The table is as shown.

.	.	0	1	2	3	4	5	6
.	.	.	.	.	.	.	.	.
0	.	0	0	0	0	0	0	0
1	.	0	1	2	3	4	5	6
2	.	0	2	4	6	1	3	5
3	.	0	3	6	2	5	1	4
4	.	0	4	1	5	2	6	3
5	.	0	5	3	1	6	4	2
6	.	0	6	5	4	3	2	1

[5 marks.]

There are no zero divisors

[1 mark.]

The units are 1, 2, 3, 4, 5, 6 with multiplicative inverses 1, 4, 5, 2, 3, 6.

[3 marks.]

[$9 = 5 + 1 + 3$ marks.]

Standard homework exercise.

2a) $a = x^3 + 1$, $b = x^2 + x - 1$.

$$x^3 + 1 = (x-1)(x^2 + x - 1) + 2x \ \ (a = q_1 b + r). \tag{1}$$

[2 marks.]

$$x^2 + x - 1 = (\tfrac{1}{2}x + \tfrac{1}{2})2x - 1 \ \ (b = q_2 r_1 + r_2). \tag{2}$$

[2 marks.]

Clearly $-1 \mid r_2$ in $\mathbf{R}[x]$. So -1 is the g.c.d. of a and b.

[1 mark]

Equivalently 1 is the g.c.d. of a and b. To write $1 = ma + nb$:

$$-1 = x^2 + x - 1 - (\tfrac{1}{2}x + \tfrac{1}{2})2x (\text{ from } (2))$$

$$= x^2 + x - 1 - (\tfrac{1}{2}x + \tfrac{1}{2})(x^3 + 1 - (x-1)(x^2 + x - 1)) \ (\text{from } (1))$$

$$= x^2 + x - 1 - (\tfrac{1}{2}x + \tfrac{1}{2})(x^3 + 1) + \tfrac{1}{2}(x^2 - 1)(x^2 + x - 1)$$

$$= (\tfrac{1}{2}x^2 + \tfrac{1}{2})(x^2 + x - 1) - (\tfrac{1}{2}x + \tfrac{1}{2})(x^3 + 1).$$

So, multiplying by -1, $m = \frac{1}{2}(x+1)$, $n = -\frac{1}{2}(x^2+1)$.

[3 marks].

2b) $53 = |7 + 2i|^2 > 25 = |4 - 3i|^2$. So

$$\frac{7+2i}{4-3i} = \frac{(7+2i)(4+3i)}{25} = \frac{22}{25} + \frac{29}{25}i$$

$$= 1 + i + \frac{-3+4i}{25} \ \ (= q_1 + r_1/b).$$

[2 marks.]

So in $a = q_1 b + r_1$, $q_1 = 1 + i$ and

$$7 + 2i = (1 + i)(4 - 3i) + i.$$

[1 mark.]

Now i is a unit in $\mathbf{Z}[i]$, so $i \mid 4 - 3i$ and i is the g.c.d. of $7 + 2i$ and $4 - 3i$. Equivalently, 1 is the g.c.d. of $7 + 2i$ and $4 - 3i$. We have

$$i = 7 + 2i - (1 + i)(4 - 3i),$$

and hence

$$1 = -i(7 + 2i) + (i - 1)(4 - 3i).$$

So writing $1 = ma + nb$, we have $m = -i$, $n = 1 + i$.

[2 marks]

[$13 = 2 + 2 + 1 + 3 + 2 + 1 + 2$ marks.]

Standard homework exercises.

3a) $x^2 + 1 = (x - i)(x + i)$ is reducible in $\mathbf{C}[x]$.

[1 mark.]

b) $x^2 + 1$ is irreducible in $\mathbf{R}[x]$, because there are no real zeros.

[1 mark.]

c) $x^3 + 2$ is irreducible in $\mathbf{Q}[x]$ because there are no rational zeros: $-\sqrt[3]{2} = -2^{\frac{1}{3}}$ is not rational.

[2 marks.]

d) $x^3 + 2$ is reducible in $\mathbf{R}[x]$:

$$x^3 + 2 = (x + 2^{\frac{1}{3}})(x^2 - 2^{\frac{1}{3}}x + 2^{\frac{2}{3}}).$$

[2 marks.]

[$6 = 1 + 1 + 2 + 2$ marks.]

Standard homework exercises.

4a) The general equation of a line in F^2 is

$$ax + by + c = 0$$

for a, b, $c \in F$ with $(a, b) \neq (0, 0)$. [Not required, but useful knowledge for part b): (a_1, b_1, c_1) and (a_2, b_2, c_2) give the same line $\Leftrightarrow$ $(a_2, b_2, c_2) = \lambda(a_1, b_1, c_1)$ for some $\lambda \neq 0$.]

[2 marks.] The general equation of a line through (x_0, y_0) is

$$a(x - x_0) + b(y - y_0) = 0$$

for $(a, b) \neq (0, 0)$. [Not required, but essential knowledge for part b): (a_1, b_1) and (a_2, b_2) give the same line $\Leftrightarrow$ $(a_2, b_2) = \lambda(a_1, b_1)$ for some $\lambda \neq 0$.]

[2 marks.]

b)

$$x + 2y + 1 = 0 \;\Leftrightarrow\; x = -2y - 1.$$

$y = 0$ gives $(x, y) = (2, 0)$, $y = 1$ gives $(x, y) = (0, 1)$ and $y = 2$ gives $(x, y) = (1, 2)$. These are all the points on the line

[2 marks.]

To find all lines through $(2, 1)$: we must have

$$a(x - 2) + b(y - 1) = 0,$$

where, by scaling, we can take $a = 1$, with $(a, b) = (1, 0)$ or $(1, 1)$ or $(1, 2)$, or $(a, b) = (0, 1)$. So the lines are

$$x - 2 = x + 1 = 0 \text{ (from } (a, b) = (1, 0)),$$

$$x + y = 0 \text{ (from } (a, b) = (1, 1)),$$

$$x + 2y + 2 = 0 \text{ (from } (a, b) = (1, 2)),$$

$$y + 2 = 0 \text{ (from } (a, b) = (0, 1)).$$

[4 marks.]

[$10 = 2 + 2 + 2 + 4$ marks.]

Standard homework exercises.

5a) True.

[1 mark.]

b) False, because 6 is not a prime power.

[1 mark.]

c) False because 7 does not divide 10×3

[2 marks.]

d) True: lines in $P^2(\mathbf{Z}_2)$, for example.

[2 marks.]

e) True: for example, one can take the Hamming code of length 7, that is, the one with check matrix

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

The code in question 6 is isomorphic to this one, and could also be cited.

[2 marks.]

[$8 = 1 + 1 + 2 + 2 + 2$ marks.]

Parts c) and d) are similar to homework exercises. Parts a), b) and e) are theory. No explanations are required BUT a student who attempts to explain an answer has a chance of some credit even if the answer is actually wrong.

6. This code corrects one error because all columns are distinct and not identically zero.

[2 marks.]

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

[3 marks.]

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

The righthand side is the fourth column of the check matrix. So the fourth entry needs to be corrected, and the corrected codeword is 0011010.

[4 marks.]

[$9 = 2 + 3 + 4$ marks.]

The whole question is a standard homework exercise, althought the first part of the question is also standard theory.

SECTION B

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

[2 marks.]

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

[2 marks.]

(ii) a) $\sqrt{2} \in S$ but $\sqrt{2} \times \sqrt{2} \notin S$. So S is not a subring or ideal.

[2 marks.]

(ii) b) $2x - 2y = 2(x - y) \in S$ for all $x,\ y \in R$ - that is, $2x,\ 2y \in S$.

$(2x)y = 2(xy) \in S$ for all $x,\ y \in R$- that is, $2x \in S,\ y \in R$.

So S is an ideal - and hence also a subring.

[2 marks.]

(ii) c) S is not closed under subtraction, because, for any $x \in S,\ x - x = 0 \notin S$. So S is not a subring or ideal.

[2 marks.]

(ii) d)

$$S = \{2p + n\sqrt{2} : p, n \in \mathbf{Z}\} = \{\sqrt{2}(n + p\sqrt{2}) : p + n\sqrt{2} \in \mathbf{Z}[\sqrt{2}\} = \sqrt{2}\mathbf{Z}[\sqrt{2}].$$

$x,\ y \in \mathbf{Z}[\sqrt{2}] \ \Leftrightarrow\ \sqrt{2}x,\ \sqrt{2}y \in S \ \Rightarrow\ \sqrt{2}(x - y) \in S = \sqrt{2}\mathbf{Z}[\sqrt{2}]$.

$x,\ y \in \mathbf{Z}[\sqrt{2}] \ \Leftrightarrow\ \sqrt{2}x \in S,\ y \in \mathbf{Z}[\sqrt{2}] \ \Rightarrow\ \sqrt{2}xy \in S$.

So S is an ideal - and hence also a subring.

[3 marks.]

(iii) $\varphi(m+n\sqrt{2}) = m \bmod 2 = 0 \Leftrightarrow m$ is even. So $\mathrm{Ker}(\varphi)$ is the ideal S as in (ii)d).
[2 marks.]
[$15 = 2+2+2+2+2+3+2$ marks.]
(i) Standard theory for (i), standard homework for (ii) and (iii).

8(i) $x^4+x+1 \neq 0$ at $x = 0,\ 1$. So there are no degree 1 factors. So the only way x^4+x+1 can be reducible in $\mathbf{Z}_2[x]$ is if $x^4+x+1 = (x^2+x+1)^2$. But $(x^2+x+1)^2 = x^4+x^2+1$. So x^4+x+1 is irreducible in $\mathbf{Z}_2[x]$.
[3 marks].
(ii)

$$F = \{J + a_0 + a_1x + a_2x^2 + a_3x^3 : a_i \in \mathbf{Z}_2,\ i = 0,\ 1,\ 2\}.$$

[1 mark.]
So F has $2^4 = 16$ elements.
[1 mark.]
$F^* = F \setminus \{0\}$ has $16-1 = 15$ elements.
[1 mark.]
The orders of the elements of F^* are the divisors of 15, that is, 1,3,5,15.
[2 marks.]
(iii) For $\alpha = J+x$, $\alpha^3 = J+x^3$, $\alpha^4 = J+x^4 = J+x+1$, $\alpha^5 = (J+x)(J+x+1) = J+x^2+x$. So α does not have order 1, 3 or 5, and must have order 15.
[3 marks.]
The other elements of order 15 are α^n for n coprime to 15, that is, $n = 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14$.
[2 marks.]
(iv) If $\beta^4+\beta+1 = 0$ then $\beta^4 = \beta+1$ and $\beta^8 = \beta^5+\beta^4$. So

$$(\beta^2)^4+\beta^2+1 = \beta^8+\beta^2+1 = \beta^5+\beta^4+\beta^2+1 = \beta^2+\beta+\beta^4+\beta^2+1$$
$$= \beta^4+\beta+1 = 0.$$

[2 marks.]
[$15 = 3+1+1+1+2+3+2+2$ marks.]
Standard homework exercises except for part (iii), which is not quite so standard.

9(i) A 2-design with parameters (v,k,r) is a collection $\mathbf{B}$ of k-element subsets of a v-element set V such that every pair of elements of V is contained in exactly r of the sets in $\mathbf{B}$.
[3 points.]
(ii). Label the seven varieties a, b, c, d, e, f g by the points in the projective plane $P^2(\mathbf{Z}_2)$, and the seven locations by the lines in $P^2(\mathbf{Z}_2)$. The three varieties grown in a location are the varieties corresponding to the three points on the line corresponding to the location. The incidence matrix of varieties in locations is therefore the same as the incidence matrix of points in lines, which is shown below.
[3 points.] Each pair of varieties is grown together in exactly one location because there is exactly one line through any two points in $P^2(\mathbf{Z}_2)$: that is, the set of lines in $P^2(\mathbf{Z}_2)$ is a two-design.

[2 points.]

The incidence matrix is as shown.

.	.	$[1,0,0]$	$[0,1,0]$	$[0,0,1]$	$[1,1,0]$	$[1,0,1]$	$[0,1,1]$	$[1,1,1]$
$X=0$	.	0	1	1	0	0	1	0
$Y=0$	.	1	0	1	0	1	0	0
$Z=0$	.	1	1	0	1	0	0	0
$X+Y=0$	.	0	0	1	1	0	0	1
$Y+Z=0$	.	1	0	0	0	0	1	1
$X+Z=0$	.	0	1	0	0	1	0	1
$X+Y+Z=0$	.	0	0	0	1	1	1	0

[7 points.]

[$15 = 3+2+7+3$ points.]

(i) is standard theory, (ii) is a standard homework exercise.

10(i)

$x^7+1 = (x+1)(x^6+x^5+x^4+x^3+x^2+x+1) = (x+1)(x^3+x+1)(x^3+x^2+1)$.

x^3+x+1 and x^3+x^2+1 are irreducible in $\mathbf{Z}_2[x$ because neither vanishes at 0 or 1, and hence neither has a degree one factor.

An alternative acceptable argument is: using general theory, since $7 = 2^3-1$, x^7+1 is the product of all degree 3 and degree 1 irreducible polynomials in $\mathbf{Z}_2[x]$, apart from $x+1$ (since 3 and 1 are the only divisors of 3 in $\mathbf{Z}$). So the degree 3 factors in the product above must be irreducible.

[4 marks.]

(ii) A cyclic code of dimension 4 must have generator $g(x)$ of degree $7-4=3$, that is, $g(x) = x^3+x+1$ or $g(x) = x^3+x^2+1$.

Case $g(x) = x^3+x+1$. Then $g(x)h(x) = x^7+1$ where $h(x) = x^4+x^2+x+1$.

Case $g(x) = x^3+x^2+1$. Then $g(x)h(x) = x^7+1$ where $h(x) = x^4+x^3+x^2+1$.

[3 marks for either.]

Case $g(x) = x^3+x+1$.So the generator matrix G and check matrix H are given by

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

Case $g(x) = x^3+x^2+1$. Then $g(x)h(x) = x^7+1$ where $h(x) = x^4+x^3+x^2+1$. Then the generator matrix G and check matrix H are given by

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

[3 marks for G, 4 marks for H in either case.]

Both these codes correct one error because, in each case, all the columns of the check matrix H are distinct and not identically 0.

[1 mark]

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

Standard homework exercise.

11(i) *Kirkman's Schoolgirls Problem.* 15 girls go out walking 7 days in a row. They walk in threes. The problem is to arrange them in groups of three (on seven successive days) so that every pair of girls is in the same group of three exactly once.

[3 marks.]

(ii) The matrix A has 15 columns and 35 rows - since there are 7 days and 5 groups of three on each day.

[2 marks.]

Because A is the incidence matrix of a 2-design with parameters $(15,3,1)$, no two rows have more than one girl in common. So for any two rows of A there is at most one column in which both rows have a 1 (and this does happen). So the minimum distance between any two rows of A is 4.

[2 marks]

Similarly for any two rows of A'. there is at most one column in which both rows have a 0 (and this does happen) So the minimum distance between any two rows of A' is 4.

[1 mark]

Any row of A has exactly 3 1's and any row of A' has exactly 12 1's. So the minimum distance between any row of A and any row of A' is ≥ 9. So the code of all rows has minimum distance 4.

[2 marks]

(iii) Any column of A has 7 1's. If 2 columns have 1 in rows R_1 and R_2 (corresponding to girls) then this pair of girls are together in two different rows, which is impossible. So there is at most one row in which both columns have a 1 (and this does happen). So the minimum distance between columns of A is 12.

[2 marks]

Similarly the minimum distance between any two columns of A' is 12

[1 mark]

Any column of A has 7 1's and any column of A' has $35-7=28$ 1's. So the minimum distance between any column of A and any column of A' is $\geq 28-7=21$. So the code of all columns has minimum distance 12.

[2 marks.]

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

(i) is standard theory and (ii) and (iii) are standard homework exercises.