Solutions to MATH247 January 2001

Section A

1. $a \in R$ is a *unit* if there exists $b \in R$ auch that $ab = ba = 1$, and then b is the multiplicative inverse of a - b is, in fact, unique.

a) The only units are ± 1 because $1 \times 1 = (-1) \times (-1) = 1$ but if $n \in \mathbf{Z}$ and $n \neq \pm 1$ then $1/n$ is not an integer.

b) If $x \in \mathbf{R}$ and $x \neq 0$ then $1/x \in \mathbf{R}$ is the multiplicative inverse of x, and x is a unit.

c) If m and n are not both 0, then $(m+ni)^{-1} = (m-ni)/(m^2+n^2)$ exists as a complex number, but this is only in R if $(m,n) = (\pm 1, 0)$ or $(0, \pm 1)$, that is only if $m + ni = \pm 1$ or $\pm i$. So these are the only units in R.

2. We have

$$x^4 + x + 1 = x(x^3 + x + 1) + x^2 + 1,$$

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

So the g.c.d. of $x^4 + x + 1$ and $x^3 + x + 1$ is 1 and

$$1 = x^3 + x + 1 + x(x^2 + 1) = x^3 + x + 1 + x(x^4 + x + 1 + x(x^3 + x + 1))$$

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

So $m(x) = 1$ and $n(x) = x^2 + 1$.

3. If $f(x)$ factorises in $\mathbf{Z}[x]$ then one of the factors must be degree one and must be of the form $x \pm 1$, because the constant coefficient of $f(x)$ is 1 and the coefficient of x^3 is 1. But $f(1) = 3 = f(-1)$. So f is irreducible in $\mathbf{Z}[x]$. then the theory tells us that it is irreducible in $\mathbf{Q}[x]$ also.

However, in $\mathbf{Z}_3$ we have $f(1) = 3 = 0$ and $f(2) == 16 - 2 + 1 = 0$. So $x - 1$ and $x - 2$ are factors and

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

This is the factorization into irreducibles.

4a) We have $x = -2y - 1 = y + 2$. Taking $y = 0$, 1, 2 gives the points $(2,0)$, $(0,1)$, $(1,2)$.

b) We have $Z = -X - 2Y = 2X + Y$. Taking $X = 1$ and $Y = 0$, 1, 2 gives the points $[1:0:2]$, $[1:1:0]$, $[1:2:1]$. Taking $X = 0$ and $Y = 1$ gives $[0:1:1]$. This gives all the four points on the line. c) The parallel lines are $x + 2y = 0$ and $x + 2y + 2 = 0$ (and of course $x + 2y + 1 = 0$ is parallel to itself). d) If $X + 2Y + Z = X + 2Y + 2Z = 0$ then subtracting gives $Z = 0$ and then $X = -2Y = Y$. So the intersection point is $[1:1:0]$.

5a) 5 does not divide 11×3. So there is no 1-design with these parameters. b) The collection of all 5-element subsets of a set V with 10 elements is a 1-design with these parameters. c) the set of lines in $\mathbf{Z}^3$ is a 2-design with parameters $(9,3,1)$ d) A 3-design with parameters $(9,3,2)$ would, by definition, be a collection $\mathbf{B}$ of 3-element subsets of a 9-element set V such that *every* 3-element subset of V is a subset of -and hence equal to - *two* of the sets in $\mathbf{B}$. This is clearly impossible.

6.

$$\begin{array}{ccccccc} 1&1&0&0&1&1&0\\ 1&0&0&1&0&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&0&1&1&1 \end{array} \rightarrow \begin{array}{c} R_1-R_2-R_3\\ .\\ .\\ . \end{array} \begin{array}{ccccccc} 0&0&0&0&0&0&0\\ 1&0&0&1&0&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&0&1&1&1 \end{array}$$

The second matrix is also a check matrix for the code. We may as well delete the first row from now on. It has three nonzero rows in standard row echelon form. So the number of linearly independent rows is 3 and the dimension of the code C is $7-3=4$. The *weight* of a code C' is

$$\min\{\#(\{i : c_i \neq 0\}) : \underline{c} = (c_1, \cdots c_n) \in C', \ \underline{c} \neq \underline{0}\}.$$

the weight of the code C is ≥ 3, because all the columns of H (or the other check matrix) are distinct and not identicaly 0.

To do the computations we can use the second check matrix (which means just deleting the first row of H. a)

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

The righthand side is the fourth column of the check matrix. So the fourth entry of the word is wrong and the corrected word is 1001011. b)

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

So this is a codeword in C.

Section B

7a). S is a *subring* if $S \neq \emptyset$, $S \subset R$ and if x, $y \in S$ then $x-y$, $xy \in S$.

J is an *ideal* if $J \neq \emptyset$, $J \subset R$ and if x, $y \in J$, $z \in R$ then $x-y$, $xz \in J$.

a)(i) If $2f_1(x)$, $2f_2(x) \in J$ and $g(x) \in \mathbf{Z}[x]$ then $2f_1(x)-2f_2(x) = 2(f_1(x)-f_2(x)) \in J$ and $(2f_1(x))g(x) = 2(f_1(x)g(x)) \in J$. So J is an ideal in $\mathbf{Z}[x]$ - and hence also a subring, since this is a weaker property.

a)(ii) If $2f_1(x)$, $2f_2(x) \in J$ then $2f_1(x)-2f_2(x) \in J$ (as in (i)) and $(2f_1(x))(2f_2(x)) = 2(2f_1(x)f_2(x)) \in J$. So J is a subring in $\mathbf{R}[x]$. Alternatively, we can get this by using (i): since J is a subring in $\mathbf{Z}[x]$, it is closed under subtraction and multiplication, and hence is a subring in $\mathbf{R}[x]$ also. But J is not an ideal in $\mathbf{R}[x]$ because we can find at least one $f(x) \in J$ and $g(x) \in \mathbf{R}[x]$ such that $f(x)g(x) \notin J$: for example, take $f(x) = 2x \in J$ and $g(x) = 1/2 \in \mathbf{R}[x]$ (the constant polynomial). Then $f(x)g(x) = x \notin J$.

b) Take any $g(x) \in J$. then

$$g(x) = q(x)f(x) + r(x)$$

for some $q(x)$, $r(x) \in \mathbf{Q}[x]$ with degree$(r(x)) <$ degree$(f(x)$ or $r(x) = 0$. But then

$$r(x) = g(x) - q(x)f(x) \in J.$$

Since $f(x)$ has minimal degree among nonzero elements of j, we must have $r(x) = 0$ and $g(x) = f(x)q(x) \in f(x)\mathbf{Q}[x]$. So $J \subset f(x)\mathbf{Q}[x]$. Since $f(x) \in J$ we also have $f(x)\mathbf{Q}[x] \subset J$. So $f(x)\mathbf{Q}[x] = J$.

8a) We have

$$\begin{array}{cccc} a = & 0 & 1 & 2 \\ f_1(a) & 171 & 1 & . \\ f_2(a) & 2 & 2 & 2 \end{array}$$

So f_1 and f_2 have no degree one factors in $\mathbf{Z}_3[x]$ and are irreducible.

If $y = 2x+1$ then $2x = y-1$ and $x = 2(2x) = 2y - 2 = 2y + 1$. Also,

$$2f_1(2x+1) = 2((2x+1)^3 + 2(2x+1) + 1)$$

$$= 2(8x^3 + 12x^2 + 12x + 1 + 4x + 2 + 1) = 2(2x^3 + x + 1) = x^3 + 2x + 2 = f_2(x).$$

b)

$$f_1(J_1 + x) = J_1 + x^3 + 2x + 1 = J_1 = 0$$

as required. We also have

$$J_1 + g_1(x) = J_1 + g_2(x) \Leftrightarrow f_1(x)|g_1(x) - g_2(x) \Leftrightarrow f_1(y)|g_1(y) - g_2(y)$$

(for $y = 2x+1$)

$$\Leftrightarrow 2f_1(y) = f_2(x)|g_1(2x+1) - g_2(2x+1))$$

(because 2 is a unit in $\mathbf{Z}_3$ and in $\mathbf{Z}_3[x]$)

$$\Leftrightarrow J_2 + g_1(2x+1) = J_2 + g_2(2x+1).$$

Now define

$$\varphi(J_1 + g(x)) = J_2 + g(2x+1).$$

By the above line of equivalences this is well-defined and one-to-one. The inverse homomorphism φ^{-1} satisfies

$$\varphi^{-1}(J_2 + g(y)) = J_1 + g(2y+1),$$

since, if $y = 2x+1$, then $x = 2y+1$, by a).

9a) There are four sets of parallel lines in $\mathbf{Z}_3^2$: $x+c=0$, $y+c=0$, $x+y+c=0$ and $x+2y+c=0$ with, in each set, $c=0$, 1 or 2. The wine testers correspond to these different values of c. The wines correspond to the 9 points in $\mathbf{Z}_3^2$. tghe scedule is then as follows, where 1 indicates that a wine is tested by the tester, and 0 indicates that it is not.

.	$(0,0)$	$(1,0)$	$(2,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(0,2)$	$(1,2)$	$(2,2)$
Session 11	.	.	.	.	.	.	.	.	.
$x=0$	1	0	0	1	0	0	1	0	0
$x+1=0$	0	0	1	0	0	1	0	0	1
$x+2=0$	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	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
$x+2y+1=0$	0	0	1	1	0	0	0	1	0
$x+2y+2=0$	0	1	0	0	0	1	1	0	0

9b) There is a field F with $4=2^2$ elements. (In fact, $\mathbf{Z}_2[x]/(x^2+x+1)\mathbf{Z}_2[x]$ is such a field.) The F^2 has $4^2=16$ elements and there are $(4^2-1)/(4-1)=5$ sets of parallel lines $\{ax+by+c=0 : c \in F\}$ for different choices of $(a,b) \neq (0,0)$. This is obtained by counting the number of pairs $(a,b) \in F^2$ with $(a,b) \neq (0,0)$ up to a nonzero multiple, that is, if we count (a,b) then we do not count $\lambda(a,b)$ for $\lambda \neq 1$. As before, we would take the wimesaters corresponding to the values of c, the sessions corresponding to the sets of parallel lines, and the bottles of wime corresponding to the poits in F^2.

10a). Let $0<k<n$. A *Check matrix* of C is given by the matrix with k rows and n columns:

$$\begin{pmatrix} h_{n-k} & . & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{n-k} & \cdots & h_1 & h_0 & \cdots & 0 \\ . & . & \cdots & . & . & \cdots & 0 \\ . & . & \cdots & . & . & \cdots & 0 \\ . & . & \cdots & \cdots & h_{n-k} & \cdots h_0 & \end{pmatrix}$$

When $k=0$, $C=\mathbf{Z}_2^n$, and when $k=n$, $C=\{\underline{0}\}$.

b)

$$1+x^{20}=(1+x^{10})^2=(1+x^5)^4$$
$$=((1+x)(1+x+x^2+x^3+x^4))^4=(1+x)^4(1+x+x^2+x^3+x^4)^4.$$

The polynomial $1+x+x^2+x^3+x^4$ does not vanish at 0 or 1 and hence has no degree one factors. It is also not the product of two irreducible degree two factors, because the only irreducible degree two polynomial in $\mathbf{Z}_2[x]$ is $1+x+x^2$ and $(1+x+x^2)^2 = 1+x^2+x^4$. So $1+x+x^2+x^3+x^4$ is irreducible in $\mathbf{Z}_2[x]$ and we have factorized $1+x^{20}$ as a product of irreducibles. So the possibilities for $g(x)$ are

$$(1+x)^r(1+x+x^2+x^3+x^4)^s$$

for $0 \leq r \leq 4$ and $0 \leq s \leq 4$. These are also the possibilities for $h(x)$.
c) For $h(x)$ of degree 9, we must have $s = 2$ and $r = 1$, that is,

$$h(x) = (1 + x^5)(1 + x + x^2 + x^3 + x^4)$$
$$= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9.$$

The 20 columns of the correspondin check matrix each have 11 rows, with either a string of ≤ 10 1's followed by a string of 0's, or the other way round. All 20 possibilities occur. So the coluumns are all distinct and not identically 0. So the code has weight ≥ 3.

11a) There are $\binom{v}{2}$ 2-element subsets of V. If $C \in \mathbf{B}$ then $\#(C) = k$. So C has $\binom{k}{2}$ 2-element subsets. Each 2-element subset of V occurs in exactly one $C \in \mathbf{B}$. So there must be

$$\frac{\binom{v}{2}}{\binom{k}{2}} = \frac{(v(v-1)}{k(k-1)}$$

sets in $\mathbf{B}$.
b) Each row has k 1's because each row is indexed by some $C \in \mathbf{B}$, and the 1's in the row occur precisly in the columns indexed by the k elements of C. If we fixe two rows indexed by sets C and $C' \in \mathbf{B}$ there cannot be more than one column where both rows have a 1, because otherwise there are at least two, indexed by elements x and $y \in V$ and then the 2-element set $\{x, y\}$ is contained in both C and C' - which is impossible because the 2-design $\mathbf{B}$ has parameters (v,k,1). So there are $\geq 2(k-1) = 2k - 2$ entries where exactly one of the rows has a 1. So the distance between the rows is $\geq 2k - 2$.
c) Fix $\underline{c} \in \mathbf{Z}_2^v$. The number of words in $\mathbf{Z}_2^v$ which differ from $\underline{c}$ inexactly i places is the number if i-element subsets of a set with v elements, that is, $\binom{v}{i}$. So the number of $\underline{c}' \in \mathbf{Z}_2^v$ which differ from $\underline{c}$ in i places for some $0 \leq i \leq k-2$, is

$$1 + \binom{v}{1} + \cdots + \binom{v}{k-2}.$$

If the minimum distance of C' is $\geq 2k - 3$, then all such sets for the different $\underline{c} \in C'$ are disjoint. So

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

If C is obtained from a 2-design as in a) and b), the minimum distance is $\geq 2k-2 > 2k-3$. So putting $m = \frac{v(v-1)}{k(k-1)}$ gives

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