CODING THEORY: SOLUTIONS 2

(1) (a) $w(x_1) = 0$, $\{1\, marks\}$

(b) $w(x_2) = 1$, $\{1\, marks\}$

(c) $w(x_3) = 3$, $\{1\, marks\}$

(d) $w(x_4) = 6$. $\{1\, marks\}$

(2) $4^{44} = (4^2)^{22} = 16^{22}$. But in $\mathbb{Z}_5$ we have $16 \cong 1$, thus $16^{22} \cong 1^{22} \cong 1$, that is $4^{44} \cong 1$. $\{1\, marks\}$

Similarly $3^{23} = (3^2)^{10} \times 3^3 = 9^{10} \times 27$. But in $\mathbb{Z}$ we have $9 \cong 4$, so $9^{10} \cong 4^{10} \cong (4^2)^5 \cong 1$ (by above). Hence $3^{23} \cong 1 \times 27 \cong 2$. Now use these in the problems to get: $\{1\, marks\}$

(a) $4^{44} + 3^{23} \cong 1 + 2 \cong 3$, $\{1\, marks\}$

(b) $4^{44} - 3^{23} \cong 1 - 2 \cong -1 \cong 4$, $\{1\, marks\}$

(c) $4^{88} \times 3^{46} \cong 1^2 \times 2^2 \cong 4$, $\{1\, marks\}$

(d) $4^{45} \div 3^{26} \cong (1 \times 4) \div (2 \times 3^3) \cong 4 \div (1 \times 2) \cong 1$. $\{1\, marks\}$

(3)

$\mathbb{Z}_7$:

x	x^{-1}	
1	1	
2	4	$(2 \times 4 = 8 \cong 1)$
3	5	$(3 \times 5 = 15 \cong 1)$
4	2	(commutativity)
5	3	(commutativity)
6	6	$(6 \times 6 = 36 \cong 1)$

$\{1\, marks\}$

$\mathbb{Z}_{17}$:

x	x^{-1}	
1	1	
2	9	$(2 \times 9 = 18 \cong 1)$
3	6	$(3 \times 6 = 18 \cong 1)$
4	13	$(4 \times 13 = 52 \cong 1)$
5	7	$(5 \times 7 = 35 \cong 1)$
6	3	(commutativity)
7	5	(commutativity)
8	15	$(8 \times 15 = 120 \cong 1)$
9	2	(commutativity)
10	12	(as $10 \times 12 = 120 \cong 1$)
11	14	$(11 \times 14 = 154 \cong 1)$
12	10	(commutativity)
13	4	(commutativity)
14	11	(commutativity)
15	8	(commutativity)
16	16	$(16 \times 16 = 256 \cong 1)$

$\{2\, marks\}$

(4) (a) Yes, as 19 is prime $\mathbb{Z}_{19}$ is a field by Theorem 3.40. $\{1\ \textit{marks}\}$

(b) No, 200 is not a prime nor can we find prime p such that $200 = p^e$ where $e \in \mathbb{N}$. $\{1\ \textit{marks}\}$

(c) Yes, although 625 is not prime, we can write $625 = 5^4$ and so there exists a field of order 625 by Theorem 3.40 (however, this field will not be $\mathbb{Z}_{625}$. $\{1\ \textit{marks}\}$

(d) No, as 1026 is even the only way we can write it as a power of a prime is as a power of 2. However $2^{10} = 1024$ and $2^{11} = 2048$ so 1026 cannot be written as 2^e for $e \in \mathbb{N}$. $\{1\ \textit{marks}\}$

(5) (a) The only coefficients we are allowed to use are 0 and 1. Therefore there are 4 degree 2 polynomials over $\mathbb{Z}_2$, these are $f_1(x) = x^2$, $f_2(x) = x^2 + x$, $f_3(x) = x^2 + 1$ and $f_4(x) = x^2 + x + 1$. $\{2\ \textit{marks}\}$

(b) We have $f_1(0) = 0$, $f_2(1) = 1 + 1 \cong 0$ and $f_3(1) = 1 + 1 \cong 0$. However $f_4(0) = 1$ and $f_4(1) = 1 + 1 + 1 \cong 1$. As $0, 1$ are the only elements of $\mathbb{Z}_2$ and neither solve f_4 it must be irreducible over $\mathbb{Z}_2$. $\{2\ \textit{marks}\}$

(6) There are two ways to do this. One way would be to use the method given in lectures by setting a to be a solution of the polynomial $f(x) = x^2 + x + 1$ then using the fact that $a^2 + a + 1 = 0$ to determine $b = a + 1$ (as we need $ab = 1$) and to calculate the multiplication and addition tables.

Another way we can proceed is as follows. Starting with the multiplication tables we know the first row and column will be all 0, as $0\dot{x} = 0$ for any x. We also know that $1\dot{x} = x$ for any x hence the second row and column are also clear. We are left to determine $a^2, ab = ba$ and b^2. Starting with ab we know $ab \neq a$ else $b = 1$. Similarly $ab \neq b$ else $a = 1$ and $ab \neq 0$ else either $a = 0$ or $b = 0$ hence $ab = 1$. Now $a^2 \neq 0$ else $a = 0$ and $a^2 \neq 1$ else $a = a(ab) = a^2b = b$. $a^2 \neq a$ else $a = 1$ hence we must have $a^2 = b$. Finally $b^2 = bb = a^2b = a(ab) = a$ and the table is complete.

We work in a similar way for the addition table. The first row and column are again clear as $0 + x = 0$ for any x. We need to calculate the rest. We start with $a + b$, which we already know is not a or b else $b = 0$ or $a = 0$ respectively. If $a + b = 0$ then $0 = a(a + b) = a^2 + ab = b + 1$ but then $a = a + (b + 1) = 1$ so $a + b \neq 0$ and hence it must be 1. Now $b = (a + b)b = ab + b^2 = 1 + a$ and $a = a(a + b) = a^2 + ab = a + 1$. $1 + 1 = (a + b) + ab = b + a(1 + b) = b + a^2 = b + b = b(1 + 1)$ but as $b \neq 1$ we must have $1 + 1 = 0$. Then $a + a = a(1 + 1) = 0$ and finally $b + b = b(1 + 1) = 0$ completes the table.

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\{3\ \textit{marks}\}$

×	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$\{2\ \textit{marks}\}$