****The following questions are concerned with Chapter 6: Polynomials and Codes.****

78 a) Show in general (and by contradiction) that if in a ring R we have $a \neq 0, b \neq 0$, but $ab = 0$, then there is no a^{-1} or b^{-1} in R.
b) Use $R = \mathbb{F}_2[x]/(x^3 + x^2 + x + 1)$ to provide an example of this: for each (nontrivial) factor of $x^3 + x^2 + x + 1$, find all its multiples in R, to show that none of them is 1. (You are finding two rows of the multiplication table for R.)

79 Which elements of $\mathbb{F}_5$ are primitive? Which elements of $\mathbb{F}_7$ are primitive?

80 Working in $\mathbb{F}_7$, express each non-zero element as a power of 3. If $a = 3^i$ then what is a^{-1}, in terms of i? Now find a primitive element of $\mathbb{F}_{11}$, and answer the corresponding question.

81 In $\mathbb{F}_7$, for which $1 \leq i \leq 6$ is 3^i a primitive element? In $\mathbb{F}_{11}$, for which $1 \leq i \leq 10$ is 2^i a primitive element? Can you generalise this idea? If a is a primitive element in $\mathbb{F}_p$, for which $1 \leq i \leq p-1$ is a^i a primitive element?

82 In lectures we used the field $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$. What happens if, instead, we divide $\mathbb{F}_2[x]$ out by other $f(x)$ of degree 3 over $\mathbb{F}_2$? By considering polynomials of smaller degree, show that x^3+x+1 and x^3+x^2+1 are irreducible, but x^3+x^2+x+1 is reducible, and show how it factors. (It follows that $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ is also the field $\mathbb{F}_8$ (see Q83) but $\mathbb{F}_2[x]/(x^3 + x^2 + x + 1)$ is a ring (see Q78).)

83 a) Find all the powers of x in $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x^2 + 1)$. That is, make a table giving each x^i, $0 \leq i \leq 7$, in the form $a_2x^2 + a_1x + a_0$.
b) Use your table to find x^4+x^5 in the form x^i, and $(x^2+x+1)(x^2+x)$ in the form $a_2x^2+a_1x+a_0$.

84 Consider $\mathbb{F}_3[x]/(x^2 + 1)$. Show that in this version of $\mathbb{F}_9$, x is not a primitive element, but $x + 1$ is a primitive element. (Thus, we say that $x^2 + 1$ is not a primitive polynomial over $\mathbb{F}_3$.)

85 By considering possible roots, show that $x^3 + 2x + 1$ is irreducible in $\mathbb{F}_3[x]$. Use Proposition 6.9 to show that $\mathbb{F}_3[x]/(x^3+2x+1)$ is a field $\mathbb{F}_q$, and find q. By writing each x^i, $0 \leq i \leq 13$, in the form $a_2x^2 + a_1x + a_0$, show that $x^3 + 2x + 1$ is a primitive polynomial over $\mathbb{F}_3$. Why do we *not* need to calculate the x^i, $14 \leq i \leq 26$, to know this?

86 Let a be a primitive element in the field $\mathbb{F}_q$, where the prime power $q = p^r$.
a) For which $1 \leq i \leq q-1$ is a^i a primitive element? (See Q81; explain if you can. For a formal proof, you need Lagrange's Theorem - the order of a subgroup divides the order of the group.)
b) Show that if *every* $a \in \mathbb{F}_q, a \neq 0, a \neq 1$ is primitive, then $p = 2$.
c) Show that the converse is not true: for some values of r, $\mathbb{F}_{2^r}$ has other non-primitive elements.
d) Show that any irreducible polynomial of degree 3 or 5 in $\mathbb{F}_2[x]$ is a primitive polynomial over $\mathbb{F}_2$.

87 Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$,
a) Construct a check-matrix, and then a generator-matrix for $\mathrm{Ham}_4(2)$.
b) Decode the received word, $y = (x, x, x+1, 1, x)$.
c) Construct a generator-matrix and a check-matrix for the extended Hamming code $\widehat{\mathrm{Ham}}_4(2)$.
d) Show that for $\widehat{\mathrm{Ham}}_4(2)$, some received words do not have a unique nearest neighbour.

88 Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, let $C \subseteq \mathbb{F}_4^4$ have check-matrix $H = \begin{pmatrix} 1 & x+1 & x & 1 \\ 0 & x+1 & 1 & x \end{pmatrix}$. Find $d(C)$.

89 Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, let $C = \langle(1,1)\rangle \subseteq \mathbb{F}_4^2$.
a) Make a decoding array for C and use it to decode $(x,0)$, $(1,x)$, $(x+1,x)$, and $(0,1)$.
b) C is transmitted over a 4-ary symmetric channel with symbol-error probability p. Find the chance that a received word is successfully decoded by your array.
c) Now make a syndrome look-up table for C, and decode the same words as in a). Does it decode them to the same codewords? If not, could you make a syndrome look-up table that *does* decode like the array?

90 Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, let $C \subseteq \mathbb{F}_4^6$ have check-matrix $H = \begin{pmatrix} 1 & 0 & 0 & 1 & x & 0 \\ 0 & 1 & 0 & 0 & 1 & x \\ 0 & 0 & 1 & x & 0 & 1 \end{pmatrix}$.
a) Find $d(C)$.
b) How many rows would there be in a syndrome look-up table for C? To cut the table shorter, let us only include syndromes $S(\mathbf{x})$ with $w(\mathbf{x}) \le 1$. Also, we can condense several lines into one by using $\lambda\mathbf{e}_j$ as our $\mathbf{x}$'s, where λ stands for any non-zero element of $\mathbb{F}_4$.
c) Make a shortened table like this and use it to decode (if possible) the received words $(1,1,1,1,1,1)$, $(0,\ 0,\ 0,\ x,\ 1,\ x+1), (x,\ 1,\ 0,\ x+1,\ x,\ 1)\ (0,\ x+1,\ 0,\ x+1,\ x,\ 1), (1,\ 0,\ x,\ 1,\ 0,\ x), (1,\ x,\ 0,\ x+1,\ x,\ 1)$.
d) How many received words can we decode using this table?

91 This question uses $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$. To help you do arithmetic in this field, first make or find the table expressing each x^i, $0 \le i \le 7$, in the form $a_2x^2 + a_1x + a_0$.
a) Let $C = \langle\{(x,\ x^2,\ x^2+x,\ x^2+1), (0,\ 0,\ x^2,\ x), (x+1,\ x^2+x,\ 0,\ x^2+1)\}\rangle \subseteq \mathbb{F}_8^4$. Find a generator- and a check-matrix for C, and its parameters $[n,k,d]$.
b) Use your generator-matrix to encode $(x^2,\ x^2+1)$, and to channel-decode $(x,\ x^2,\ x^2+x,\ x^2+1)$.

92 This question uses $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+x+2)$. To help you do arithmetic in this field, first make or find the table expressing each x^i, $0 \le i \le 8$, in the form $a_1x + a_0$.
Let $C = \langle\{(0,\ x+1,\ 2x+1,\ x,\ 1), (1,\ 0,\ 0,\ 2,\ x), (2,\ 1,\ 0,\ x+2,\ x)\}\rangle \subseteq \mathbb{F}_9^5$. Find a generator- and a check-matrix for C, and its parameters $[n,k,d]$. (To find d, it may help to re-write H with entries x^i.)

93 Prove that for $f(x)$ in $\mathbf{R}_n = \mathbb{F}_q[x]/(x^n-1)$, its span $\langle f(x)\rangle$ is a cyclic code. (This is Proposition 6.14. Use Proposition 6.12 to prove it.)

94 Let $g(x) \in \mathbf{R}_n = \mathbb{F}_q[x]/(x^n-1)$ be monic, of degree r, and be a factor of x^n-1.
a) By considering the check-polynomial $h(x)$, show that any element of $C = \langle g(x)\rangle$ has degree $\ge r$.
b) Show that, with these conditions, $g(x)$ is the generator-polynomial of $\langle g(x)\rangle$.
c) Deduce that there is a 1-1 correspondence between monic factors of x^n-1 and cyclic codes in $\mathbf{R}_n$.

95 Find all ternary cyclic codes of block-length 3. These can be regarded as both subrings (in fact, ideals) in the ring $\mathbf{R}_3 = \mathbb{F}_3[x]/(x^3-1)$ and subspaces of the vector space $\mathbb{F}_3^3$. So, first find the generator-polynomial of each, and then a generator-matrix for each. Two of the codes are trivial. For the two which are not trivial, find their parameters $[n,k,d]$. How are they related?

96 a) By considering possible roots, factor $x^3 - 1$ in the ring of polynomials $\mathbb{F}_7[x]$.
b) Using these factors, find all the non-trivial 7-ary cyclic codes of block-length 3. (There are six of them). Give a generator-polynomial and a generator-matrix for each.
c) Let C be the one of these codes with generator-matrix $G = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}$. By finding x_1 and x_2 such that $x_1(3,1,0) + x_2(0,3,1) = (1,2,6)$, show that $(1,2,6) \in C$. (In effect, you are channel decoding.) In the same way, show that $(2,6,1)$ and $(6,1,2)$ (the cyclic shifts of $(1,2,6)$) are in C, but $(1,6,2)$ is not.

97 Consider the code C of Q96c. Write down its generator-polynomial $g(x)$ and its check-polynomial $h(x)$. Use Proposition 6.20 to find out which of these polynomials are in C: $a(x) = 6x^2 + 2x + 1$, $b(x) = 2x^2 + 6x + 1$. Do your answers agree with Q96c?

98 In lectures, we found all the ternary cyclic codes of length 4. The codes we found (see Example 54) come in dual pairs, C and $C^\perp$. Find these pairs, and show that they are duals,
a) by considering their generator- and check-matrices, and using ideas from Chapter 4,
b) by considering their generator- and check-polynomials and using Proposition 6.22. (Remember that a polynomial can generate a code even if it is not that code's unique, official generator-polynomial.)

99 a) In $\mathbb{F}_2[x]$, $x^7 - 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$. Let $g(x) = (x^3 + x + 1) \in \mathbb{F}_2[x]$, and write out the generator-matrix G_1 for the cyclic code $C_1 = \langle g(x) \rangle \subseteq \mathbf{R}_7 = \mathbb{F}_3[x]/(x^7 - 1)$.
b) Using just 3 EROs, row-reduce G_1 to standard form $(A \mid I)$. Find a check matrix H_1 for C_1, and explain why C_1 is a $\mathsf{Ham}_2(3)$ code.
c) Using Proposition 6.22 find a check-polynomial $h_1(x)$ for C_1, and a generator-polynomial $g_2(x)$ for code $C_2 = C_1^\perp$. Write out a generator-matrix G_2 for the cyclic code C_2.
d) But of course H_1 is also a generator-matrix for C_2. Use just one ERO to change G_2 to H_1.

100 In $\mathbf{R}_n$, let $g(x)$ and $h(x)$ be monic, and $g(x)h(x) = x^n - 1$. Then we know by Q94b that $g(x)$ and $h(x)$ are the generator-polynomials for $C_1 = \langle g(x) \rangle$ and $C_2 = \langle h(x) \rangle$ respectively.
a) Specify polynomials which generate $C_1^\perp$ and $C_2^\perp$ respectively.
b) By considering generator-matrices for C_1 and $C_2^\perp$, show that these codes are equivalent.
(So, we might say that $C_1 = \langle g(x) \rangle$ and $C_2 = \langle h(x) \rangle$ are "almost dual" to each other.)
c) Conclude that in general, if $g(x)$ is monic and divides $x^n - 1$, then the codes $\langle g(x) \rangle$ and $\langle \overline{g}(x) \rangle$ are equivalent.

101 We can construct the Golay codes as cyclic codes. In $\mathbb{F}_2[x]$, $x^{23} - 1$ factors as

$$(x-1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) = (x-1)g_1(x)g_2(x).$$

Use Q100 to show that $\langle g_1(x) \rangle$ and $\langle g_2(x) \rangle$, cyclic codes in $R_{23} = \mathbb{F}_2[x]/(x^{23} - 1)$, are equivalent. In fact, they are both equivalent to the binary Golay code $\mathcal{G}_{23}$ of Section 5.3.

102 Let $\mathbf{a} = (1,0,4,7), \mathbf{b} = (1,2,3,4) \in \mathbb{F}_{11}^4$. Find the minimum distance and a basis for the Reed-Solomon code $\mathsf{RS}_3(\mathbf{a},\mathbf{b}) \subseteq \mathbb{F}_{11}^4$.

103 Let $\mathbf{a} = (0,1,2,3,4), \mathbf{b} = (1,1,1,1,1) \in \mathbb{F}_7^5$. Find a generator-matrix for each code $\mathsf{RS}_k(\mathbf{a},\mathbf{b}) \subseteq \mathbb{F}_7^5$, $1 \le k \le 4$. Then find a check-matrix for each code.

104 Let $\mathbf{a}, \mathbf{b}$, and $\mathbf{b}'$ be vectors in $\mathbb{F}_q^n$. Show that if $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ and $\mathsf{RS}_k(\mathbf{a},\mathbf{b}')$ are two Reed-Solomon codes, they are (monomially) equivalent. Deduce from this and Proposition 6.25 that $[\mathsf{RS}_k(\mathbf{a},\mathbf{b})]^\perp$ and $\mathsf{RS}_{n-k}(\mathbf{a},\mathbf{b})$ are equivalent.

105 Let $\mathbf{a}, \mathbf{a}'$, and $\mathbf{b}$ be vectors in $\mathbb{F}_q^n$, and $\mathsf{RS}_k(\mathbf{a}, \mathbf{b})$ and $\mathsf{RS}_k(\mathbf{a}', \mathbf{b})$ be two Reed-Solomon codes. How could we pick $\mathbf{a}$ and $\mathbf{a}'$ to make the codes (monomially) equivalent?

106 Of course, there are Reed-Solomon codes over non-prime fields. But we have a clash of notation: in Section 6.2 we used x as an element of $\mathbb{F}_q$, and now in 6.5 it is the variable for our polynomials $f(x) \in \mathbf{P}_k$. So here is just one small, easy question: Let $\mathbf{a} = (1, x, x+1), \mathbf{b} = (1, 1, 1) \in \mathbb{F}_4^3$. Find a generator-matrix and then a check-matrix for $\mathsf{RS}_2(\mathbf{a}, \mathbf{b}) \subseteq \mathbb{F}_4^3$,