******The following questions are concerned with Chapter 1 of the notes - Basic Coding Theory.******

1 Let $C = \{00101, 11011, 10100, 10010\} \subseteq \{0,1\}^5$. Find $d(C)$. Give examples of words that do or do not have a unique nearest neighbour in C.

2 Consider the words GOTHS, HARES, HATES, MARES, MARKS, MATES, MATHS, MATEY, MITES, MOTHS, MYTHS, and RITES. Let these be the codewords of the (n, M_1, d_1) code $C_1 \subseteq \{A, B, \ldots Z\}^5$. a) For each of the words PARKS, GOALS and DATES, find its nearest neighbour(s) in C_1.
b) Find n, M_1 and d_1. Now find a (n, M_2, d_2) code $C_2 \subseteq C_1$ such that $d(C_2) = 2$ and $|M_2| \geq 6$.
c) Find three codewords x, y, and z in C_1 such that $d(x, y) = d(x, z) + d(z, y)$.
d) Find three codewords x, y, and z in C_1 such that $d(x, y) < d(x, z) + d(z, y)$.

3 Let $C = \{01010, 10101, 11000, 11111\} \subseteq \{0,1\}^5$. Find $d(C)$.
How many errors can C detect? and how many can it correct?

4 Let $C = \{01234, 12340, 23401, 34012, 40123\} \subseteq \{0,1,2,3,4\}^5$. Find $d(C)$.
How many errors can C detect? and how many can it correct?

5 For fixed $n \geq 1$, how many binary $(n, 2, n)$ codes are there?

6 Let C be an (n, M, d) code with $n \geq d \geq 2$
a) Fix j with $1 \leq j \leq n$ and form C_1 by deleting the jth entry from each word in C.
Show that C_1 is a $(n-1, M, d)$ or $(n-1, M, d-1)$ code.
b) Form C_2 by deleting the last m entries of each word in C.
What can we say about the parameters of C_2 if $m < d$? How about if $m \geq d$?

7 A binary code with block length 4 is transmitted over a channel such that $P(1 \text{ received} \mid 0 \text{ sent}) = 0.1$ and $P(0 \text{ received} \mid 1 \text{ sent}) = 0.05$. Is this channel symmetric? If 0001 is sent what is the chance that 0110 is received?

8 Consider the code $C = \{c_1, c_2, c_3\} = \{000000, 110000, 111111\} \subseteq \{0,1\}^6$, and the words $w_1 = 010100$, $w_2 = 111100, w_3 = 110100, w_4 = 111110$.
a) Perform nearest neighbour decoding for each w_i. When is there no unique nearest neighbour?
b) C is sent over a binary symmetric channel with symbol-error probability p. For each $1 \leq i \leq 3$ and $1 \leq j \leq 4$, find $P(w_j \text{ received} \mid c_i \text{ sent})$.

9 For the binary code $C = \{0000, 1000, 1111\}$, the codeword 1111 is transmitted over a binary symmetric channel with symbol-error probability $p = 0.1$. We decode a received word to its unique nearest neighbour if it has one; otherwise we do not decode. What is the chance that the received word is decoded correctly? Incorrectly?

10 Consider the binary code $C = \{000, 111\}$. Suppose the codewords are transmitted over a binary symmetric channel with symbol-error probability p. Consider the following strategies:
(i) Complete decoding using nearest neighbour decoding.
(ii) Accepting a received word if it is in C but asking for retransmission otherwise.
For each strategy find the chance that, when we send 000, it is decoded correctly, perhaps after several transmissions. If $p = 0.1$, which method is more reliable? Should we therefore use this method?

11 The ternary code $C = \{01, 02, 20\}$ is transmitted over a ternary symmetric channel with error probability $p = 0.02$. We decode received words as the nearest neighbour if that is unique, and ask for retransmission otherwise.
a) If 02 is sent, what is the chance that it is received as a word in the code?
b) If 01 is sent, what is the chance that we ask for retransmission?
(Hint for part b): first find which received words do not have a unique nearest neighbour.)

12 Consider the codes $C_1 = \{0, 1, 2\}$ and $C_2 = \{000, 111, 222\} \subseteq \{0, 1, 2\}^3$, which are sent over a ternary symmetric channel with symbol-error probability p.
a) Find the minimum distances for C_1 and C_2. How many errors can C_1 and C_2 detect or correct?
b) For C_1 the codeword 0 is sent. What is the chance that the received word is decoded correctly under nearest neighbour decoding?
c) For C_2 the codeword 000 is sent. Determine the chance that the received word is decoded correctly if we do incomplete nearest neighbour decoding, where we only decode a received word x if $d(x, c) \leq 1$ for some $c \in C_2$ and do not do anything otherwise. What is the chance that we do not decode the received word at all?
d) Again, for C_2 the codeword 000 is sent, but now we accept only codewords as received words, and ask for retransmission otherwise. What is the chance that we receive a codeword the first time? What is the chance that we eventually decode the received word correctly, perhaps after several transmissions?
e) Now take $p = 0.1$ and compare the chance of failure for parts b), c) and d), where failure means that we decode either incorrectly or not at all, even after several transmissions.

13 Let the code $C = \{00000, 11111, 22222, 33333\} \subseteq \{0,1,2,3\}^5$ be transmitted over a symmetric 4-ary channel with symbol-error probability $p = 0.1$. We assume that each codeword is equally likely to be sent.
a) Find the nearest neighbours of $w_0 = 00123$ and $w_1 = 00111$.
b) If $c_0 = 00000$ and $c_1 = 11111$, find $\mathbb{P}(w_j \text{ received} \mid c_i \text{ sent})$ for $0 \leq i, j \leq 1$.
c) Find $\mathbb{P}(w_j \text{ received})$ for $j = 0, 1$.
d) Find $\mathbb{P}(c_i \text{ sent} \mid w_j \text{ received})$ for $0 \leq i, j \leq 1$.
e) Comment on the following statement: "If 00000 is sent, we are as likely to receive 00111 as 00123. So if we decode 00123 to 00000, we should also decode 00111 to 00000."
f) Do $\mathbb{P}(00000 \text{ sent} \mid 00111 \text{ received})$ and $\mathbb{P}(11111 \text{ sent} \mid 00111 \text{ received})$ add up to 1? Should they?

14 Consider words of length 3 made using the alphabet $A = \{0, 1, \ldots, q-1\}$ where $q \geq 3$. Describe $S(000, r)$ for $r = 0, 1$ and 2. How many elements are there in each? Do those sets look like spheres if we identify the elements in A with $0, 1, \ldots, q-1$ in $\mathbb{R}$, and view all words in $\mathbb{R}^3$?

15 Let C be a ternary (4, 9, 3)-code. Show that C is perfect.

16 Let C be an $(n, M, 2t)$ code with $M > 1$. (In other words, $d(C)$ is even).
a) Given code words x and y such that $d(x, y) = 2t$, find a word z not in the code such that $d(x, z) = d(y, z) = t$.
b) Can z be in some $S(u, r)$ with u in the code and $r < t$?
c) Conclude that C cannot be a perfect code.

******The following questions are concerned with Chapter 2 of the notes - Linear Codes.******

17 Write out an addition table and a multiplication table for $\mathbb{Z}/5$ and $\mathbb{Z}/6$. Use your tables to show that $\mathbb{Z}/6$ is not a field.

18 Let $C = \{(0,0,2),(1,1,0),(2,2,1)\} \subseteq \mathbb{F}_3^3$. Is C a linear code? Find its span, $\langle C \rangle$, a ternary $[n,k,d]$ code. What are n, k, and d?

19 Show that a q-ary $[n,k,d]$ MDS code satisfies $d = n - k + 1$. Use this to check that the code $C = \{000, 111\} \subset \mathbb{F}_2^3$ is MDS.

20 Let $C = \langle \{(0,1,0,1,0),(1,0,1,1,0),(0,1,1,1,0),(1,0,0,1,0)\} \rangle \subseteq \mathbb{F}_2^5$. Find a basis for C, and its dimension.

21 Show that, for a prime p, the p-ary code $C = \{(0,1),(1,1),\ldots,(p-1,1)\} \subseteq F_p^2$, is a $(2,p,1)$ code but not a $[2,1,1]$ code.

22 Show that, in a decoding array constructed according to the algorithm given, every possible received word $\mathbf{y} \in \mathbb{F}_q^n$ appears exactly once. (Hint: Show first that the same $\mathbf{y}$ cannot appear twice in the same row, and then that the same $\mathbf{y}$ cannot appear twice in *different* rows. (This contradiction argument is similar to the proof of Proposition 2.10.))

23 Make a decoding array for the code $C_2 = \{(0,0,0),(1,1,1)\} \subseteq \mathbb{F}_2^3$. If C_2 is transmitted over a symmetric binary channel with symbol-error probability p, use Proposition 2.11 to find the probability that a codeword $\mathbf{c} \in C_2$ will be successfully decoded.

24 Make a decoding array for the code $C_3 = \{(0,0,0),(1,1,1),(2,2,2)\} \subseteq \mathbb{F}_3^3$. Use it to decode the words $(1,2,1)$ and $(1,2,0)$. If C_3 is transmitted over a symmetric ternary channel with symbol-error probability p, use Proposition 2.11 to find the probability that a codeword $c \in C_3$ will be successfully decoded.

25 In making your array for Q24, when did you have to make arbitrary choices? Which of these choices will affect decoding? Which words may be decoded differently by different arrays? Explain by considering a different (but still correct!) array for C_3. Is the situation the same for C_2 of Q23?

26 Suppose we have a decoding array for a q-ary $[n,k,2t+1]$ code C (t any integer). For $\mathbf{c} \in C$ and $r \leq t$, where in the array would we find the the words of the sphere $S(\mathbf{c},r)$? (Look at Q25, and/or draw a general, schematic array).

27 In terms of the definition of a perfect code ("there is some t such that...."), what words are in the first column of a decoding array for a perfect code? Explain why, for perfect codes, all arrays will decode identically.

******The following questions are concerned with Chapter 3 of the notes - Codes as Images.******

28 Let code $C_5 \subseteq \mathbb{F}_5^4$ be the span of the set $\{(0,1,2,3),(1,1,1,1),(3,1,4,2)\}$. Find a generator-matrix for C_5. What is the dimension of C_5?

29 Let code $C_7 \subseteq \mathbb{F}_7^4$ be the span of the set $\{(0,1,2,3),(1,1,1,1),(3,1,4,2)\}$. Find a generator-matrix for C_7. What is the dimension of C_7? (- so, identical to the previous question, except that we are over a different field.)

30 For each of the codes above, C_5 and C_7, write down an alternative generator-matrix.

31 a) Draw 49 points in a square grid, to represent $\mathbb{F}_7^2$. (You could label just the "axes", $S((0,0),1)$). Find the points corresponding to the code C with generator-matrix $(2\ 1)$. Does it look like a "line" in a "plane"? Can you think of a better way to draw (or model?) these vector spaces?
b) Perhaps on a new grid, draw the code C' with generator-matrix $(1\ 3)$. Can you see two different ways to draw the "line"? Is one better than the other?

32 The code $C \subseteq \mathbb{F}_7^5$ has generator matrix $G_1 = \begin{pmatrix} 1 & 2 & 3 & 3 & 3 \\ 0 & 2 & 1 & 5 & 5 \\ 4 & 5 & 0 & 6 & 3 \end{pmatrix}$.
Use this to encode the message $(3,2,1) \in \mathbb{F}_7^3$ to a codeword $\mathbf{c}$. Also, channel-decode codeword $\mathbf{c}' = (4,5,0,0,2)$ to find the corresponding message. (You will need to solve a set of five equations - possibly by row-reducing a suitable augmented matrix.)

33 For the code C of Q32, find an alternative generator-matrix, G_2, in RREF. Use this to encode the message $(3,2,1)$. Also, use G_2 to channel-decode the codeword $(2,1,1,4,0)$.

34 There is a code C' which is permutation equivalent to code C of Q32 but has a generator matrix G_3 in standard form. Use this matrix to encode $(3,2,1)$ to a codeword of C', and channel-decode the codeword $(2,1,4,1,0)$.

35 Equivalent codes have the same rank, redundancy and rate. Find these values for C' and C above.

36 Let C be an (n,M,d) over an alphabet of order q, not necessarily linear. If C_2 is equivalent to C_1, show that C_2 is also an (n,M,d) code over an alphabet of order q.

37 The codes C_1 and C_2 in $\mathbb{F}_5^6$ have generator-matrices G_1 and G_2 respectively, where
$G_1 = \begin{pmatrix} 0 & 3 & 1 & 0 & 3 & 1 \\ 1 & 4 & 0 & 2 & 3 & 4 \\ 2 & 0 & 3 & 4 & 3 & 0 \end{pmatrix}$ and $G_2 = \begin{pmatrix} 3 & 1 & 4 & 1 & 0 & 0 \\ 4 & 4 & 0 & 1 & 4 & 1 \\ 0 & 0 & 2 & 1 & 3 & 2 \end{pmatrix}$.
Show that C_1 and C_2 are monomially equivalent.

38 Given a code $C \subseteq \mathbb{F}_q^n$, prove that $\mathrm{PAut}(C)$ is a group.

39 Let $C \subseteq \mathbb{F}_3^4$ be the code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}.$$

Let $g = (134) \in S_4$. Show that $g \in \mathrm{PAut}(C)$.

40 Consider two maps $\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$. Map $\pi_{s(i,j)}$ swaps the i^{th} and j^{th} entry of each vector, and map $\pi_{m(i,\mu)}$ multiplies the i^{th} entry by $\mu \in \mathbb{F}_q$. Show that for each of these maps, and for any $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ and $\lambda \in \mathbb{F}_q$, we have $\pi(\mathbf{x} + \mathbf{y}) = \pi(\mathbf{x}) + \pi(\mathbf{y})$, and $\pi(\lambda\mathbf{x}) = \lambda\pi(\mathbf{x})$. For this reason we say that these maps "preserve linear structure".

41 Suppose an $[n, k, d]$ code C has a generator-matrix G in RREF. By considering the weights of the rows of G, find a new proof that $d \leq n - k + 1$ (the Singleton bound for linear codes).

42 We know that any generator-matrix for a code C can be row-reduced to a generator-matrix G in RREF, and that this RREF generator-matrix is unique. Thus, if C does have a generator-matrix in standard form $(I \mid A)$, it will be this matrix G. Again by considering weights of rows, show that if C is maximum distance separable then it has a generator-matrix in standard form. (Hint: Prove the contrapositive.)

43 Show (by example or argument) that the converse of Q42,
"If C has a generator-matrix in standard form then it is MDS."
is false.

******The following questions are concerned with Chapter 4 of the notes - Codes as Kernels.******

44 Let $C \subseteq \mathbb{F}_5^6$ have generator-matrix $G = \begin{pmatrix} 1 & 4 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 4 & 2 \end{pmatrix}$. Find a basis for its dual code $C^\perp$.

45 Let $C \subseteq \mathbb{F}_7^6$ have generator-matrix $G = \begin{pmatrix} 2 & 1 & 2 & 1 & 1 & 2 \\ 3 & 0 & 6 & 0 & 3 & 4 \\ 0 & 1 & 5 & 5 & 0 & 1 \end{pmatrix}$. Find a generator-matrix for $C^\perp$.

46 Let $C \subseteq \mathbb{F}_3^5$ have generator-matrix $G = \begin{pmatrix} 0 & 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 2 & 0 \\ 2 & 0 & 1 & 2 & 1 \end{pmatrix}$. Using the $G \leftrightarrow H$ algorithm, find a generator-matrix for $C^\perp$. Could you have used Proposition 4.5? Would you have got the same answer?

47 Prove the following (which we might call Proposition 4.5 a):
If $C \subseteq \mathbb{F}_q^n$ has generator-matrix $G = (A \mid I_k)$, then it has a check-matrix $H = (I_{n-k} \mid -A^t)$. (*Hint:* Consider the code C' which has generator-matrix $H = (I_{n-k} \mid -A^t)$, and use Propositions 4.5 and 4.7.)

48 A code is a subspace of a vector space. The first example of this you ever met was lines through the origin in $\mathbb{R}^2$, which can be written as $ax + by = 0$. Later you learned that such a line could also be given as any multiple of some vector, $\lambda\binom{c}{d}$.
a) Explain how these two ways correspond to specifying a code using either a generator- or a check-matrix.
b) Give two ways to specify a line through $(0, 0, 0)$ in $\mathbb{R}^3$, and explain how these also correspond to generator and check-matrices.
c) What about planes in $\mathbb{R}^3$?

49 In each case, find a check-matrix and then a generator-matrix for the code.
a) $C = \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 \mid x_1 + x_2 + x_4 = 0,\ x_3 + x_4 = 0\}$
b) $C = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_7^5 \mid x_1 + x_2 + x_3 + x_4 + x_5 = 0,\ x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 = 0\}$
c) $C = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_5^5 \mid x_1 + x_3 = 0,\ x_2 + x_4 = 0,\ 2x_1 + 3x_2 + x_5 = 0\}$

50 Until 2007, an ISBN (International Standard Book Number) was ten digits $x_1 \dots x_{10}$, with $0 \leq x_i \leq 9$ for $1 \leq i \leq 9$, and $0 \leq x_{10} \leq 10$, but writing X for 10. It was also required that $x_1 + 2x_2 + \cdots + 10x_{10} \equiv 0$ mod 11. We can regard the ISBN numbers as a code $C_{ISBN} \subseteq \mathbb{F}_{11}^{10}$.
a) Why is C_{ISBN} not a linear code?
b) By thinking about codewords (that is, ISBN numbers) show that $d(C_{ISBN}) \leq 2$, and then show that $d(C_{ISBN}) \neq 1$.
c) If instead we allow $0 \leq x_i \leq 10$ for $1 \leq i \leq 10$, we have a linear code $C \subseteq \mathbb{F}_{11}^{10}$. Write down its check-matrix, and show using Theorem 4.11 that $d(C) = 2$.
d) One particularly common human error is to swap two adjacent digits. This is an error of weight two. Show that, nonetheless, for C (or C_{ISBN}) this error will be detected. What about swapping non-adjacent digits?

51 Let $C = \subseteq \mathbb{F}_2^5$ have check-matrix $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$. Make a syndrome look-up table for C, and decode the received words $\mathbf{y}_1 = (1,0,0,1,1)$ and $\mathbf{y}_2 = (0,1,1,1,0)$. Show how a different syndrome look-up table could decode $\mathbf{y}_2$ differently. Why could this not happen for $\mathbf{y}_1$?

52 Let $C = \{\mathbf{x} \in \mathbb{F}_5^4 \mid \mathbf{x}H^t = 0\}$, where $H = \begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 1 \end{pmatrix}$.
a) Make a shortened syndrome look-up table for C, and decode the received words $\mathbf{y}_1 = (1,2,3,4)$, $\mathbf{y}_2 = (3,1,2,0)$, and $\mathbf{y}_3 = (2,4,3,1)$.
b) A normal look-up table has q^{n-k} rows. How many rows in this kind of shortened table?

53 Show that syndrome decoding is nearest-neighbour decoding. (Do this by contradiction - similar to the proof for array decoding)

54 Suppose that matrix A is in $M_{m,n}(\mathbb{F}_q)$. How can we check whether some set of d columns of A is linearly dependent? In general, we could write them as *rows* in a $d \times m$ matrix, and row-reduce. But for some values of d there are other ways. How can we check when:
a) $d = 1$ b) $d = 2$ c) $d = m$ d) $d > m$?

55 Let $H = \begin{pmatrix} 3 & 4 & 1 \\ 1 & 4 & 2 \end{pmatrix}$. Find the minimum distance of the codes:
a) $C_5 = \{\mathbf{x} \in \mathbb{F}_5^3 \mid \mathbf{x}H^t = \mathbf{0}\}$
b) $C_7 = \{\mathbf{x} \in \mathbb{F}_7^3 \mid \mathbf{x}H^t = \mathbf{0}\}$

56 Let $H = \begin{pmatrix} 1 & 0 & 4 & 1 \\ 2 & 3 & 0 & 1 \\ 0 & 4 & 3 & 2 \end{pmatrix}$. Find the minimum distance of the codes:
a) $C_5 = \{\mathbf{x} \in \mathbb{F}_5^4 \mid \mathbf{x}H^t = \mathbf{0}\}$
b) $C_7 = \{\mathbf{x} \in \mathbb{F}_7^4 \mid \mathbf{x}H^t = \mathbf{0}\}$

57 Using Theorem 4.11, find yet another proof that $d \leq n - k + 1$ (the Singleton bound for linear codes). (*Hint*: Although the theorem is also true for acting check-matrices, it helps to consider a proper check-matrix.)

58 Students sometimes confuse the way to find $d(C)$ from a check-matrix (see Theorem 4.11) with the definition of the rank of a matrix. How are these ideas similar and different? Find two (or more) matrices $H_1, H_2, \ldots$ which have the same rank, but the codes $C_i = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H_i^t = \mathbf{0}\}$, for which they are check-matrices, have different $d(C_i)$. (*Hint:* There are small examples - e.g. in $M_{2,3}(\mathbb{F}_2)$)

59 Suppose code C has generator-matrix $G \in M_{k,n}(\mathbb{F}_q)$ and check-matrix $H \in M_{n-k,n}(\mathbb{F}_q)$. If C is monomially equivalent to C' we know we can make a generator-matrix G' for C' by permuting and multiplying columns of G. Can we make a check-matrix H' for C' in a similar way?
Adapting the notation of Q40, let us say that for a matrix $A \in M_{k,n}(\mathbb{F}_q)$, $\pi_{s(i,j)}(A)$ is A with columns i and j swapped, and $\pi_{m(i,\mu)}(A)$ is A with column i multiplied by non-zero $\mu \in \mathbb{F}_q$. Then if C_s has generator-matrix $\pi_{s(i,j)}(G)$,and C_m has generator-matrix $\pi_{m(i,\mu)}(G)$, both these codes are monomially equivalent to C. In terms of $\pi_{s(i,j)}$ and $\pi_{m(i,\mu)}$, find a check-matrix for C_s and for C_m. For each code, justify your answer by showing that any row of the generator matrix is orthogonal to any row of the check matrix.

60 Consider the code $C' \subseteq \mathbb{F}_{11}^{10}$, $C' = \{\mathbf{x} \in \mathbb{F}_{11}^{10} \mid x_1 + x_2 \cdots + x_{10} = 0\}$. Show that C' is equivalent to the code C of Q50 in two ways:
a) For any word $\mathbf{c} = (c_1, \ldots, c_{10}) \in C$ apply suitable changes to make a word $\mathbf{c}' \in C'$. This shows that C is equivalent to a subset of C'. Now do the same in reverse.
b) Consider check matrices, and see Q59.
c) If C and C' are equivalent, and C' seems simpler, why did we use C for books?

****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 $w(\mathbf{x}) \leq 1$. 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, $0 \leq i \leq 7$, 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, $0 \leq i \leq 8$, 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 $\geq r$.
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 $\mathrm{Ham}_2(3)$ 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 $\mathsf{RS}_k(\mathbf{a}, \mathbf{b}) \subseteq \mathbb{F}_7^5$, $1 \leq k \leq 4$. 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 $\mathsf{RS}_2(\mathbf{a}, \mathbf{b}) \subseteq \mathbb{F}_4^3$,