IV054 Coding, Cryptography and Cryptographic Protocols
2020 - Exercises III.

1. *(6 points)* Consider the binary code $C =< 1 + x^2 + x^3 + x^4 >$ in R_7.
   (a) Find generator matrix G.
   (b) Find parity check matrix H.
   (c) Using polynomials encode the message 101.

2. *(4 points)*
   (a) How many binary cyclic codes of length 6 are there?
   (b) How many quinary (5-ary) cyclic codes of length 6 are there?

3. *(4 points)* Consider an $[8, 4]$ extended binary Hamming code, i.e. the binary linear code with the generator matrix
$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$
   Decide whether this code is equivalent to a cyclic code and prove your answer.

4. *(2 points)* Consider a binary cyclic code C with generator polynomial $g(x)$. Show that if $1 + x \mid g(x)$ then each codeword from C has even weight.

5. *(5 points)* Show that the polynomial
$$g(x) = \sum_{i=0}^{n} x^{2i}$$
   is a generating polynomial of a q-ary cyclic code of length $2n + 2$ for any integer n and prime q.

6. *(4 points)* Consider a definition of the Golay G_{24} code from exercise 2.27 in the exercise book. Using the described decoding procedure decode the following:
   (a) 000100001010100000000001
   (b) 110100110100010111100000