Coding and cryptography
Assignment 2

Due **11:00am Tuesday 21st March 2023**

- This assignment is *optional*. It will allow you to get feedback on the standards used in this course.
- You may hand in this assignment in pairs. If you do this then hand in the same copy (with both names on it) for both people in canvas.
- The use of computer programs, etc., is not allowed.
- If you have any questions, email Ronen at `r.z.brilleslijper@vu.nl` .

1. Factorize $x^{10} + x^6 + x^5 + x^4 + x^3 + x + 1$ into irreducible factors in $K[x]$. You may use the list of irreducible polynomials of degree 1, 2, 3 and 4 that were already computed.
2. (a) Find all idempotents in $K[x]$ modulo $1 + x^9$.
   (b) For each idempotent $I(x)$ in which the constant term and the coefficient of x are non-zero, find the generator polynomial of the smallest cyclic linear code containing $I(x)$.
   (c) How many cyclic linear codes (other than $\{00\ldots0\}$ and K^n) are there of length n if $n = 9$? And if $n = 36$?
3. Let $f(x) = 1 + x^3 + x^4$. It is given that $f(x)$ is irreducible in $K[x]$. Let $GF(2^4)$ be $K[x]$ modulo $f(x)$ and let β be x modulo $f(x)$ in $GF(2^4)$.
   (a) By making a table expressing $1, \beta, \beta^2, \ldots, \beta^{14}$ in the form $a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3$ (or $a_0a_1a_2a_3$) with the a_i in K, verify that β is a primitive element of $GF(2^4)$.
   (b) Let $\alpha = \beta^6$. Is α a primitive element of $GF(2^4)$?
   (c) Find the minimal polynomial $m_\alpha(x)$ in $K[x]$ for α as in (b).
4. In this problem, $GF(2^4)$ and β are as in Problem 3 (so make sure your table there is correct as you'll need it for the calculations here). Let C be the 2-error correcting BCH code of length 15 with parity check matrix

$$H = \begin{bmatrix} 1 & 1 \\ \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \vdots \\ \beta^{14} & \beta^{42} \end{bmatrix}.$$

   If w is a received word, determine if $d(v, w) \leq 2$ for some v in C in two cases:
   (a) w has syndrome $wH = [s_1, s_3] = [\beta^9, \beta^7]$;
   (b) w has syndrome $wH = [s_1, s_3] = [\beta, \beta^3]$.