DEA Corps finis

1. Déterminer le nombre de facteurs irréductbles des polynômes suivant à coefficients dans le corps $\mathbb{F}_2$: $X^7 + X + 1$, $X^7 + X^4 + 1$, $X^9 + X^7 + X^6 + X^5 + 1$, les factoriser si ils ne sont pas irréductibles et donner leur exposant si ils sont irréductibles.

Les deux premiers sont irréductibles et d'exposant 127 (car 127 est premier). Le second s'crit $(X + X + 1)(X + X + 1)$.

2. Déterminer le nombre de facteurs irréductibles des polynômes suivant à coefficients dans le corps $\mathbb{F}_3$: $X^6 + X^4 + X^3 + 1$, $X^5 + 2X^4 + 1$. Calculer l'exposant des polynômes de la liste qui sont irréductibles.
Les deux polynômes sont irréductibles d'exposant 91 et 242 (ce point était calculatoire, et il y a eu des affirmations gratuites).
Sinon dans ces deux exercices le terme corps de décompostion a t́é utilisé de manière incorrecte.

3. Déterminer le nombre de facteurs irréductbles des polynômes suivant à coefficients dans le corps $\mathbb{F}_5$: $X^5 + 4X + 1$, $X^5 + X^3 + 3X + 2$.
Les deux polynômes sont irréductbles (erreur souvent sur le second)

4. Calculer $\Phi_n(-1)$.

Les calculs ont été prafois incomplets. Diverses méthodes ont été utilisées avec succès. Voici le rśultat :

- $\Phi_1(-1) = -2$,
- $\Phi_2(-1) = 0$,
- $\Phi_{2^h}(-1) = 2$, $h > 1$,
- $\Phi_{2k+1}(-1) = 1$,
- $\Phi_{2k+1}(-1) = 1$,
- $\Phi_{2p^i}(-1) = p$, p premier impair,
- sinon la valeur est 1

Pour faire ce calcul on utilse la formule (avec n pair!)

$$X^{n-1} - X^{n-2} + \cdots + (-1)^{n-1} = fracX^n - 1X + 1 = \prod_{d|n, d\neq 2} \Phi_n(X)$$

soit sous cette hypothse

$$-n = \prod_{d|n, d\neq 2} \Phi_n(-1)$$

5. Factoriser le polynôme suivant, à coefficients dans le corps $\mathbb{F}_2$:

$$P = X^{17} + X^{14} + X^{13} + X^{12} + X^{11} + X^{10} + X^9 + X^8 + X^7 + X^5 + X^4 + X + 1$$

On cherchera d'abord les facteurs multiples, en calculant le *pgcd* de P et P'. On factorisera ce *pgcd* en produit de facteurs irréductibles. On pourra commencer encore une fois par étudier les facteurs multiples puis utiliser l'algorithme de Berlekamp.

$(X^2+X+1)^3(X^3+X+1)^2(X^5+X^4+X^3+X^2+1)$

6. Montrer que le polynôme $P = X^2 - X - 1$ à coefficients dans $\mathbb{F}_3$ est irréductible. Soit $\mathbb{F}_9 \cong \mathbb{F}_3[X]/(P)$, et $\alpha = \bar{X}$.
Trouver un polynôme générateur pour un code BCH de longueur 8 et dimension 4 sur $\mathbb{F}_3$. Déterminer sa distance minimum.

7. Trouver un polynôme générateur pour un code BCH de longueur 12 et distance minimale supérieure ou égale à 5 sur $\mathbb{F}_2$.

8. $\Phi_6(X) = X^2 - X + 1$, $\Phi_{12}(X) = X^4 - X^2 + 1$ et $\Phi_{15}(X)X = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$.