TD Polynômes et extensions de corps

1. Montrer (par contradiction) que la caractéristique d'un anneau intègre est soit 0 soit un entier premier.
2. Soit p un entier premier. On considère le polynôme $a := x^p + x \in Z_p[x]$. Déterminer $a(\alpha)$ pour tout $\alpha \in Z_p$.
3. Donner un exemple où le degré du produit de deux polynômes a et b est strictement inférieur à $\deg(a) + \deg(b)$.
4. Calculer $a \mod b$ dans F_3, avec $a = x^4 + 2x^3 + x + 2, \quad b = x^3 - 1$.
5. Calculer $a.a' \mod b$ dans F_5, avec $a' = 2x^2 + x + 2$
6. Montrer qu'un idéal propre d'un anneau commutatif A ne peut contenir d'éléments inversibles.
7. Montrer qu'un anneau commutatif est un corps si et seulement si il n'a pas d'idéal propre non nul.
8. Soit α une racine de $x^3 + x^2 + 1 \in F_2[x]$. Quelles sont les autres racines de ce polynôme (en fonction de α)?
9. Calculer $(x + 1)(x + 2)(x^2 + 1)$ dans $F_3[x]$. Montrer que $x^2 + 1$ est irréductible. Construire un corps de neuf éléments. Soit α un élément de ce corps, calculer α^4.
10. Soit $f(x) = x^4 + x + 1 \in F_2[x]$. Soit α une racine de f.
    (a) Calculer α^5, α^6, α^7, α^8, α^9, α^{10}, ...
    (b) Calculer $(\alpha^4 + \alpha + 1)^2$.
    (c) Calculer les inverse de $\alpha^{12}, \alpha^8, \alpha^{14}$
    (d) Construire le corps $F_2[x]/(f(x))$.
    (e) Quel est le polynôme minimal de α^3?
    (f) Trouver un polynôme binaire de degré 9 qui factorise $x^{15} - 1$.
    (g) Combien existe-t-il de polynômes binaires de degré 10 qui factorise $x^{15} - 1$?
11. Soit f un polynome irréductible primitif dans $GF(3)$. $f = x^2 + 2x + 2$. Factoriser $X^8 - 1$ dans $GF(3)[x]$.
12. (facultatif) Soit f un polynôme irréductible primitif dans Z_4. $f = x^3 + 2x^2 + x + 3$. Factoriser $x^7 - 1$ dans $Z_4[x]$.
13. On considère le polynôme $f = x^3 + 2x + 1$ dans F_3.
    (a) Montrez que f est irréductible dans $F_3[x]$.
    (b) Quel est le nombre de facteurs irréductibles de $x^{26} - 1$ sur F_3 ? quel est leur degré respectif?
    (c) Afin de définir le corps F_{27}, on traduit la représentation polynômiale des éléments du corps en puissance d'une racine α. La racine est telle que $\alpha^3 + 2\alpha + 1 = 0$. On a

$2\alpha^2 = \alpha^{15}$	$1 + 2\alpha^2 = \alpha^{25}$
$\alpha + \alpha^2 = \alpha^{10}$	$1 + \alpha = \alpha^9$
$\alpha + 2\alpha^2 = \alpha^{17}$	$2 + 2\alpha^2 = \alpha^8$
$2\alpha = \alpha^{14}$	$2 + \alpha = \alpha^3$
$2\alpha + \alpha^2 = \alpha^4$	$2 + \alpha + \alpha^2 = \alpha^{11}$
$2\alpha + 2\alpha^2 = \alpha^{23}$	$2 + \alpha + 2\alpha^2 = \alpha^5$
$1 + \alpha^2 = \alpha^{21}$	$2 + 2\alpha = \alpha^{22}$

Traduisez en puissances de α :
$2 + 2\alpha + 1\alpha^2$
$2 + 2\alpha + 2\alpha^2$
$2 + \alpha^2$
$1 + \alpha + \alpha^2$
$1 + \alpha + 2\alpha^2$
$1 + 2\alpha$
$1 + 2\alpha + \alpha^2$
$1 + 2\alpha + 2\alpha^2$

(d) Quel est le polynôme minimal de α, de α^2, de α^{24}, de α^{20}?

(e) Quel est l'inverse de α^{13}, l'inverse de $1 + \alpha + \alpha^2$, l'inverse de $1 + 2\alpha + \alpha^2$?

(f) Combien de polynômes de degré 5 factorisent-ils $x^{26} - 1$?