TD 5 de mathématiques

1. Montrer (par contradiction) que la caractéristique d'un anneau intègre est soit 0 soit un entier premier.

2. Montrer qu'un idéal propre d'un anneau A ne peut contenir d'éléments inversibles.

3. Montrer qu'un anneau est un corps si et seulement si il n'a pas d'idéal propre non nul.

4. Calculer $(x+1)(x+2)(x^2+1)$ dans $F_3[x]$. Montrer que x^2+1 est irréductible.

5. 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 $\alpha^{12}, \alpha^8, \alpha^{14}$

6. Soit $f(x) = x^3 + x + 1 \in F_2[x]$. Soit α une racine de f. Montrer que α^2 est aussi une racine de f. En déduire toutes les racines de f.

7. Soit p un entier premier. On considère le polynôme $a := x^p + x \in Z_p[x]$. Déterminer $a(\alpha)$ pour tout $\alpha \in Z_p$.

8. Donner un exemple où le degré du produit de deux polynômes a et b est strictement inférieur à $\deg(a) + \deg(b)$.

9. Calculer $a \mod b$ dans F_3, avec $a = x^4 + 2x^3 + x + 2, \quad b = x^3 - 1$.

10. Calculer $a.a' \mod b$ dans F_5, avec $a' = 2x^2 + x + 2$

11. 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)?

0.1 Exercice supplémentaire

Considérons un corps commutatif F. Une courbe elliptique E sur F est définie comme étant l'ensemble des couples $(x, y),\ \ x,\ y \in F$, vérifiant l'équation

$$y^2 = x^3 + ax + b$$

et augmenté artificiellement d'un élément supplémentaire que l'on notera O et qu'on appelle le "point à l'infini". Une droite qui passe par deux points d'une courbe elliptique la recoupe en exactement un point supplémentaire. On peut munir une courbe d'une structure de groupe commutatif. Les éléments du groupes sont les points de la courbe et la loi de groupe est notée $+$. On convient que

1. Le point à l'infini O est l'élement neutre,
2. Soit $P, Q,\ R$ trois points de E. $P + Q + R = O$ si les points P, Q, R sont alignés.

La loi de groupe, notée $+$, peut être définie géométriquement. Si $P \neq O$ est le point (x, y) et Q est le point $(x, -y)$ symétrique par rapport à l'axe des x, on convient que $P + Q = O$. P et Q sont donc des points opposés.
Soient deux points $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ de E différents de O et tels que $x_1 \neq x_2$. Alors la somme $P_1 + P_2 = P_3 = (x_3, y_3)$ est un point de la courbe vérifiant

$$\begin{cases} x_3 = & (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 = & -y_1 + (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) \end{cases}$$

Si $P_2 = P_1$, le point $P_3 = P_1 + P_1$ noté $2.P_1$ a pour coordonnées x_3 et y_3 avec

$$\begin{cases} x_3 = & (\frac{3{x_1}^2 + a}{2y_1})^2 - 2x_1 \\ y_3 = & -y_1 + (\frac{3{x_1}^2 + a}{2y_1})(x_1 - x_3) \end{cases}$$

Soit E la courbe elliptique d'équation $y^2 = x^3 + x + 1$ sur F_{17}.

1. Montrer que $P = (0, 1)$ est un point de la courbe E.
   On constate que le groupe de la courbe est un groupe cyclique à 18 éléments et que P en est un générateur. Ainsi $15.P = (4, 1)$, $17.P = (0, -1)$ et $18.P = O$ appartiennent à la courbe.

2. Calculer $2.P$, $3.P$ et $(0,1)+(-4,1)$

3. Le point $A=(-4,-1)$ appartient-il à la courbe E? Si oui, calculer k tel que $k.P=A$.

Alice et Bob désirent communiquer de manière confidentielle et décident d'utiliser la courbe elliptique pour chiffrer leur communication. Bob rend publics la courbe E, le corps F_{17}, le point P et un point $\Pi = s.P$. L'entier s est la clé secrète de Bob. Un message M est un élément de F_{17} transformé en un point de la courbe et pour le chiffrer, Alice choisit un entier aléatoire k, calcule $k.P$ et transmet le point (C_1, C_2) ou $C_1 = k.P$ et $C_2 = M + k.\Pi$. Pour déchiffrer, Bob calcule $M = C_2 - s.C_1$.

4 Alice veut chiffrer $M=(-4,1)$. Elle choisit $k=3$. La valeur de Π est $(-1,4)$. Quelle est la valeur du chiffré?

5 Calculer $5.P$

Les inconvénients de ce chiffrement sont doubles. Il faut d'abord précoder chaque message en un point de la courbe E, ce qui n'est pas très commode. De plus, le chiffré est quatre fois plus long que le message en clair. (qui est un élément de F_{17}).
Pour corriger ces défauts, Menezes et Vanstone ont proposé cette variante : chaque message en clair M est un couple $M=(M_1,M_2)$ d'éléments de F_{17}.
Pour le chiffrement, Alice choisit un entier k, calcule $k.P$ et $k.\Pi=(x,y)$.
Le message chiffré est le couple $C=(C_1,C_2)$ où $C_1=k.P$ et $C_2=(M_1x, M_2y)$ est un couple d'éléments de F_{17}.

6 Comment Bob va-t-il déchiffrer?

7 Quelle est la longueur du chiffré par rapport à celle du texte clair?