Année universitaire 2014-2015
Licence 3 de mathématiques
Cryptographie et arithmétique - Feuille 8

Exercice 1

a. Quels sont, dans $\mathbb{F}_3[X]$, les polynômes unitaires irréductibles de degré 2 ?

b. L'anneau $\mathbb{F}_3[X]/\langle X^4+1\rangle$ est-il un corps ?

Exercice 2
Soit K un corps fini de cardinal q impair. Soit $a \in K^*$.

a. Vérifier que si a est un carré dans K^*, alors $a^{(q-1)/2} = 1$.

b. Supposons $a^{(q-1)/2} = 1$ et $q \equiv 3 \bmod 4$. Trouver un entier n tel que $(a^n)^2 = a$.

Exercice 3
On pose $K = \mathbb{F}_2[Y]/\langle Y^5+Y^2+1\rangle$.

a. Démontrer que K est un corps.

b. Soit $x \in K^*$ tel que $x \neq 1$. Prouver que x engendre le groupe K^*.

Exercice 4
Posons $K = \mathbb{F}_2[Y]/\langle Y^4+Y^3+Y^2+Y+1\rangle$ et notons α la classe de Y dans K.

a. Vérifier que K est un corps.

b. Calculer $(\alpha+1)^5$, puis montrer que $\alpha+1$ engendre le groupe K^*.

c. L'élément α engendre-t-il K^* ?

d. Déterminer l'inverse de $\alpha^3+\alpha+1$.

Exercice 5
On pose $A = \mathbb{F}_2[Y]/\langle Y^6+Y+1\rangle$ et on désigne par α la classe de Y dans A.

a. Calculer α^9, α^{21} et α^{63}.

b. Quel est l'ordre de α ? En déduire que A est un corps.

c. Trouver un polynôme $P \in \mathbb{F}_2[X]$ de degré 2 tel que $P(\alpha^{21}) = 0$.

d. Calculer l'inverse de $\alpha^3 + \alpha + 1$.

Exercice 6

Soit p un nombre premier. Soit $F = X^2 - bX + c \in \mathbb{F}_p[X]$ irréductible. Soit α une racine de F dans un corps fini K de cardinal p^2.

a. Démontrer que $F(\alpha^p) = 0$ et que $\alpha^p \neq \alpha$.

b. En déduire que $\alpha^{p+1} = c$.

c. On suppose maintenant $p = 17$ et $F = X^2 - X + 2$. Trouver un élément $\beta \in K$ tel que $\beta^2 = 2$.

Exercice 7 : algorithme $p + 1$ de Williams

Soit p un nombre premier. Soit $F = X^2 - bX + c \in \mathbb{Z}[X]$ tel que la réduction $\bar{F}$ de F modulo p soit irréductible dans $\mathbb{F}_p[X]$. On pose $G_1 = 1$ et $G_2 = b$; on définit par récurrence la suite d'entiers $(G_n)_{n\geq 1}$ en posant $G_{n+2} = bG_{n+1} - cG_n$ pour tout $n \geq 1$.

a. Notons $K = \mathbb{F}_p[X]/\langle \bar{F} \rangle$ et désignons par α la classe de X dans K. Posons $\beta = b - \alpha$. Montrer que $(\beta - \alpha)G_n = \beta^n - \alpha^n$ pour tout $n \geq 1$.

b. Soit $n \geq 3$ un multiple de $p + 1$. En utilisant l'exercice 6, prouver que p divise G_n.

c. Soit $N \geq 2$ un multiple de p. Soit m un entier ≥ 3 tel que pour tout facteur premier q de $p+1$, on ait $q^{v_q(p+1)} \leq m$. Notons M le ppcm de $1, 2, \cdots, m$. Montrer que $N \wedge G_M$ est un diviseur > 1 de N. Cet algorithme trouve donc un facteur non trivial de N si $G_M \not\equiv 0 \bmod N$.

Exercice 8 : Data Encryption Standard

Soit n un entier ≥ 1 ; notons B l'ensemble des blocs de n bits. Soient K un ensemble de clefs et $f : K \times B \to B$ une application. Pour chiffrer un message $(l_0; m_0)$ avec les clefs $k_1, \cdots, k_t$, on effectue t tours. Au tour $i \in \{1; \cdots; t\}$, on calcule $l_i = m_{i-1}$ et $m_i = l_{i-1} \oplus f(k_i; m_{i-1})$. Le chiffré est $(l_t; m_t)$.

Déterminer l'algorithme de déchiffrement de ce cryptosystème symétrique.