Année universitaire 2013-2014
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. Soit p un nombre premier ne divisant pas q. Posons $\Phi = X^{p-1} + \cdots + X + 1$. On suppose que Φ a une racine a dans K.

a. Déterminer l'ordre de a dans le groupe K^*.

b. En déduire que p divise $q-1$.

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^* ?

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 $P(\alpha^{21}) = 0$.

Exercice 6

Soit p un nombre premier. Soit $F = X^2 - bX + c \in \mathbb{F}_p[X]$ irréductible.

a. Prouver qu'il existe un corps fini K de cardinal p^2 contenant une racine α de F.

b. Montrer que $F(\alpha^p) = 0$ et que $\alpha^p \neq \alpha$, puis exprimer b en fonction de α.

c. En déduire que F divise $X^p + X - b$ dans $\mathbb{F}_p[X]$.

Exercice 7 : 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.