Université de Bordeaux — **Arithmétique – M1MA7W01**
Master 1 CSI — Année 2013–2014

FEUILLE D'EXERCICES n° 3

Exercice 1 – Donner une construction d'un corps fini de cardinal $2^5 = 32$.

Exercice 2 – Soit A un anneau commutatif et a, b deux entiers > 0. Donner la caractéristique des anneaux suivants :

$$\mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{Z}/a\mathbb{Z}, \quad \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \quad A[X].$$

Exercice 3 – On considère $P = X^3 + X + 1$ et $Q = X^3 + X^2 + 1$ dans $\mathbb{F}_2[X]$.

1) Montrer P et Q sont irréductibles.

2) Soit $K = \mathbb{F}_2[X]/\langle P \rangle$. Trouver les racines de Q dans le corps K.

3) En déduire un isomorphisme explicite $\mathbb{F}_2[X]/\langle Q \rangle \to \mathbb{F}_2[X]/\langle P \rangle$.

Exercice 4 – Soit L/K une extension de corps, et $a, b \in L$ algébriques sur K. On note $K' = K(a)$.

1) Montrer que les extensions K'/K et $K'(b)/K'$ sont de degré fini.

2) En déduire que $a + b$ et ab sont algébriques sur K, puis que l'ensemble $\{x \in L : x \text{ algébrique sur } K\}$ est un corps.

Exercice 5 – Soit $\mathbb{F}_q$ un corps fini de caractéristique impaire.

1) Quelles sont les solutions de l'équation $x^2 = 1$ dans $\mathbb{F}_q$?

2) En déduire le nombre de *carrés* dans $\mathbb{F}_q^*$, puis que les carrés de $\mathbb{F}_q^*$ sont exactement les racines de l'équation $x^{(q-1)/2} = 1$.

3) Quels sont les carrés de $\mathbb{F}_{2^k}$?

Exercice 6 – Soit $q \equiv 3 \pmod 4$ une puissance d'un nombre premier. Montrer que si $a \in \mathbb{F}_q^*$ est un carré, alors $a^{(q+1)/4}$ est une racine carrée de a. [*Utiliser l'exercice 5.*]

Exercice 7 – Soit q une puissance d'un nombre premier et d un diviseur de $q-1$.

1) On rappelle que le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique. Montrer que l'équation $x^d = 1$ a exactement d solutions dans $\mathbb{F}_q$.

2) Montrer que les puissances d-ièmes dans $\mathbb{F}_q$ sont exactement les $(q-1)/d$ solutions de l'équation $x^{(q-1)/d} = 1$.

Exercice 8 – [Chiffrement de Pohlig-Hellman]
Soit $K = \mathbb{F}_q$ un corps fini et $m \in K^*$ un message clair. On choisit une clé secrète $k \in \mathbb{Z}/(q-1)\mathbb{Z}$, qui définit l'opération de chiffrement $f : m \mapsto m^k$.

1) Quelle hypothèse faire sur k pour que le déchiffrement soit possible ? (Pour tout $y \in K^*$, il existe $m \in K^*$ unique tel que $y = f(m)$.)

★ **2)** Connaissant k, comment déchiffrer efficacement $f(m)$? Estimer la complexité du déchiffrage. [*Introduire d tel que $kd \equiv 1 \pmod{q-1}$.*]

Exercice 9 – [Logarithme discret]
Soit K le corps fini à q éléments et $g \in K^*$ un élément d'ordre N, engendrant un sous-groupe cyclique $G \subset K^*$.

1) a) Expliquer pourquoi l'application

$$\begin{aligned} \exp_g \colon (\mathbb{Z}/N\mathbb{Z}, +) &\to (G, \times) \\ x &\mapsto g^x \end{aligned}$$

est bien définie, et pourquoi elle réalise un isomorphisme.

b) Montrer que pour $x \in \mathbb{Z}/N\mathbb{Z}$, on peut calculer g^x en utilisant $O(\log N)$ multiplications. [*Écrire x en base 2.*]

2) On note $\log_g \colon (G, \times) \to (\mathbb{Z}/N\mathbb{Z}, +)$ son inverse, qui à g^x associe $\bar{x}$. Montrer que $\log_g(ab) = \log_g(a) + \log_g(b)$ pour tout $a, b \in G$.

3) Les deux systèmes suivants reposent sur l'asymétrie entre le calcul de $\exp_g$ (facile) et de $\log_g$ (pas d'algorithme en temps polynomial connu).

a) [Diffie-Hellman] Alice et Bob choisissent chacun de leur côté un exposant secret, respectivement a et b. Ils se communiquent g^a et g^b, via un canal dont la sécurité n'est pas garantie. Expliquer comment ils peuvent chacun reconstituer la « clé partagée » g^{ab}, à partir des informations dont ils disposent respectivement. Détailler le problème que doit résoudre un attaquant qui veut reconstituer la clé.

b) [Elgamal] Alice choisit une clé secrète $c \in \mathbb{Z}/N\mathbb{Z}$ et publie $h = g^c$. Bob souhaite lui envoyer le « message » $m \in K^*$; il tire k au hasard dans $\mathbb{Z}/N\mathbb{Z}$ et transmet le couple (g^k, mh^k). Expliquer comment Alice peut en déduire m.

★ **4)** [Algorithme de Pohlig-Hellman] Pour calculer $\log_g h$, où $h \in G$, il faut résoudre l'équation $g^x = h$, où $0 \leqslant x < \mathrm{ord}(g) = N$. Soit d un diviseur de N et $e = N/d$.

a) Montrer qu'il existe $0 \leqslant x_0 < e$ et $0 \leqslant x_1 < d$ tels que $x = x_1 e + x_0$.

b) Montrer que $x_0 = \log_{g^d}(h^d)$ et $x_1 = \log_{g^e}(hg^{-x_0})$.

c) Expliquer en quoi cette décomposition aide à calculer $\log_g h$.