Examen d'algèbre effective (3h)

Exercice 1 : Preuve sans divulgation de connaissance d'une factorisation

Soient p et q deux nombres premiers congrus à 3 modulo 4. On note $n = pq$.

I. Équivalence entre factorisation et calcul de racines carrées

1. On note $\phi_2 : \mathbb{Z}/p\mathbb{Z}^* \to \mathbb{Z}/p\mathbb{Z}^*$, $x \mapsto x^2$. Justifier que ϕ_2 est un morphisme de groupes, puis que pour tout $y \in \mathbb{Z}/p\mathbb{Z}^*$ on a :
$$y \in \mathrm{Im}(\phi_2) \iff y^{(p-1)/2} = 1$$
(On dit alors que y est un carré modulo p.)
2. Soit y un carré modulo p ; on pose $x = y^{(p+1)/4}$. Montrer que $x^2 = y \bmod p$.
3. Soit a un entier premier avec n. Montrer que l'équation $x^2 = a \bmod n$ admet 0 ou 4 solutions dans $\mathbb{Z}/n\mathbb{Z}$ (appelées *racines carrées* de a modulo n) et expliquer comment les calculer efficacement le cas échéant en connaissant la factorisation de n.
4. Inversement, on suppose que l'on a accès à un algorithme $\mathcal{A}$ qui, prenant en entrée un entier a premier avec n, renvoie une solution de l'équation $x^2 = a \bmod n$ (s'il existe une telle solution).
On tire aléatoirement de façon uniforme un élément x_0 dans $(\mathbb{Z}/n\mathbb{Z})^\times$, et on note $x_1 = \mathcal{A}(x_0^2)$.
   (a) Montrer qu'avec probabilité 1/2 on a $x_0 \neq x_1$ et $x_0 \neq -x_1$ (modulo n).
   (b) En déduire qu'avec probabilité 1/2 le pgcd de $x_0 - x_1$ avec n permet d'obtenir la factorisation de n.
5. Expliquer finalement pourquoi savoir calculer des racines carrées modulo n est équivalent à connaître la factorisation de n.

II. Un protocole "zero-knowledge"

Alice veut démontrer à Bob qu'elle connaît la factorisation d'un entier n (de la forme pq avec p et q premiers congrus à 3 mod 4), sans la lui donner. Un protocole interactif possible est le suivant :

— Bob choisit un entier c (premier à n) et envoie $m = c^2$ à Alice.
— Alice choisit aléatoirement uniformément un entier x premier à n et elle envoie $e = x^2c^2$ à Bob.
— Bob envoie ou $b = 0$ ou 1 (au choix) à Alice.
— Si Bob a envoyé 0, Alice renvoie $y = x$; sinon, elle renvoie $y = xc'$ où c' est une racine carrée de m modulo n.
— Bob vérifie que $y^2 m = e$ (cas $b = 0$) ou $y^2 = e$ (cas $b = 1$).

6. On suppose dans cette question qu'Alice est une impostrice qui ne connaît pas la factorisation de n.
   (a) Montrer qu'Alice peut cependant envoyer un élément $e \in (\mathbb{Z}/n\mathbb{Z})^\times$ lui permettant de répondre correctement à la question $b = 0$.
   (b) Montrer de même qu'Alice peut envoyer un élément $e \in (\mathbb{Z}/n\mathbb{Z})^\times$ lui permettant de répondre correctement à la question $b = 1$.
   (c) Montrer qu'il n'existe pas d'élément $e \in (\mathbb{Z}/n\mathbb{Z})^\times$ permettant à Alice de répondre correctement aux deux questions possibles de Bob.

7. Comment Bob peut-il à peu près certain qu'Alice connaît bien la factorisation de n et n'est pas une imposteuse ?
8. Montrer que, quels que soient les choix pour c et b de Bob, la réponse d'Alice ne lui apporte aucune information sur la factorisation de n.
9. On suppose que le protocole est répété plusieurs fois. Que se passe-t-il si Alice choisit toujours la même valeur de x au lieu de le tirer aléatoirement ? Bob peut-il exploiter cette information pour factoriser n ?

Exercice 2 : Cantor-Zassenhauss en caractéristique 2

Soit q un entier de la forme 2^k, avec $k \in \mathbb{N}^*$. On considère un polynôme unitaire $P \in \mathbb{F}_q[X]$ de degré n ; on suppose que P est un produit de plusieurs polynômes irréductibles distincts de même degré $r \geq 1$: $P = \prod_{i=1}^{n/r} P_i$ avec $n/r > 1$.

On note $\mathbb{F}_q[X]_{<n}$ l'ensemble des polynômes à coefficients dans $\mathbb{F}_q$ de degré strictement inférieur à n.

1. Expliquer rapidement comment vérifier que P est sans facteur carré, et que tous les facteurs irréductibles de P sont de même degré r.
2. On note dans la suite $m = kr$. Justifier que dans $\mathbb{F}_2[x]$:
$$x^{2^m} - x = (x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^4 + x^2 + x)(x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^4 + x^2 + x + 1)$$
3. Soit a un élément de $\mathbb{F}_{2^m}$ tiré aléatoirement de façon uniforme. Montrer que la quantité $\sum_{j=0}^{m-1} a^{2^j}$ vaut 0 avec probabilité 1/2 et 1 avec probabilité 1/2.
4. On considère un polynôme $Q \in \mathbb{F}_q[X]_{<n}$, et on note $T = \sum_{j=0}^{m-1} Q^{2^j} \bmod P$. Donner une estimation de la complexité du calcul de T.
5. Avec les notations de la question précédente, on pose $t_i = T \bmod P_i$ pour tout $i \in [\![1; n/r]\!]$. Montrer que si Q est tiré aléatoirement de façon uniforme dans $\mathbb{F}_q[X]_{<n}$, alors le n/r-uplet $(t_1, \ldots, t_{n/r})$ est uniformément distribué dans $\{0,1\}^{n/r}$.
6. En déduire que la probabilité que le pgcd de T avec P soit non trivial (i.e. différent de 1 et de P) est égale à $1 - \dfrac{1}{2^{n/r-1}}$.
7. Écrire, sous forme de pseudo-code, un algorithme probabiliste prenant en entrée un polynôme $P \in \mathbb{F}_q[X]$ et un entier r, où P est supposé être unitaire et produit de polynômes irréductibles distincts de même degré r, et renvoyant la liste des facteurs irréductibles de P.
Donner sa complexité en moyenne.
8. Une simplification.
On s'intéresse dans la suite au cas où P est simplement scindé (i.e. $r = 1$). On considère deux racines distinctes x_1 et x_2 de P. On note S le polynôme $X^{2^{k-1}} + X^{2^{k-2}} + \cdots + X^2 + X$.
   (a) Justifier que la fonction $x \mapsto S(x)$ est une application $\mathbb{F}_2$-linéaire non nulle de $\mathbb{F}_q$ dans $\mathbb{F}_2$.
   (b) Soient x_1 et x_2 deux racines distinctes de P. Montrer que si a est un élément de $\mathbb{F}_q$ tiré aléatoirement de façon uniforme, alors $a(x_1 + x_2)$ est uniformément distribué dans $\mathbb{F}_q$.
   (c) En déduire que $S(ax_1) \neq S(ax_2)$ avec probabilité 1/2.
   (d) Montrer finalement que la probabilité que le pgcd de P avec $S(aX)$ soit non trivial est supérieure ou égale à 1/2.
   (e) Comment modifier en conséquence l'algorithme proposé en 7 ? Quel est l'intérêt ?

Exercice 3 : polynôme énumérateur des poids

Soit n un entier. Pour tout n-uplet ou mot $w \in \mathbb{F}_2^n$, on note $h(w)$ son poids de Hamming, c'est-à-dire son nombre de composantes non nulles.
Soit $\mathcal{C} \subset \mathbb{F}_2^n$ un code linéaire binaire, de longueur n. Pour tout i entre 0 et n, on note a_i le nombre de mots du code de poids i :

$$a_i = \#\{w \in \mathcal{C} : h(w) = i\}.$$

Le *polynôme énumérateur des poids* (ou polynôme énumérateur tout court) du code $\mathcal{C}$ est le polynôme bivarié

$$W_{\mathcal{C}}(X, Y) = \sum_{i=0}^{n} a_i X^i Y^{n-i} \in \mathbb{Z}[X, Y]$$

C'est un polynôme homogène de degré n, qui donne des informations non seulement sur le code $\mathcal{C}$, mais aussi sur le code orthogonal $\mathcal{C}^\perp$.

1. Premières propriétés.
   (a) Déterminer le polynôme énumérateur $W_{\mathcal{C}}$ pour le code par répétition $\mathcal{C} = \{0 \dots 0, 1 \dots 1\}$ et pour le code trivial $\mathcal{C} = \mathbb{F}_2^n$.
   (b) Donner le polynôme énumérateur du code par bit de parité.
   (c) Donner les valeurs de $W_{\mathcal{C}}(0, 1)$ et de $W_{\mathcal{C}}(1, 1)$.
   (d) Montrer que le polynôme énumérateur d'un code $\mathcal{C}$ est symétrique (i.e. $W_{\mathcal{C}}(Y, X) = W_{\mathcal{C}}(X, Y)$) si et seulement si le mot $11 \dots 1$ appartient à $\mathcal{C}$.

On note $\langle ., . \rangle$ la forme bilinéaire symétrique standard sur $\mathbb{F}_2^n$, définie par $\langle v, w \rangle = \sum_{i=1}^{n} v_i w_i$.
On considère un code linéaire $\mathcal{C} \subset \mathbb{F}_2^n$, de dimension k. On rappelle que son orthogonal est

$$\mathcal{C}^\perp = \{v \in \mathbb{F}_2^n : \forall w \in \mathcal{C},\ \langle v, w \rangle\}$$

L'*identité de MacWilliams*, donnée ci-dessous, relie les polynômes énumérateurs de $\mathcal{C}$ et de $\mathcal{C}^\perp$:

$$W_{\mathcal{C}^\perp} = \frac{1}{2^k} W_{\mathcal{C}}(Y - X, Y + X)$$

2. Soit $\mathcal{C}_1$ le code polynomial de longueur 4, engendré par le polynôme $g = X^2 + 1$.
   (a) Ce code est-il cyclique ?
   (b) Déterminer son polynôme énumérateur et donner sa distance minimale.
   (c) Déterminer la distance minimale du code orthogonal $\mathcal{C}_1^\perp$.
3. Soit $\mathcal{C}_2$ le code polynomial de longueur 4, engendré par le polynôme $g = X^2 + X$. Comme à la question précédente, déterminer le polynôme énumérateur et la distance minimale de $\mathcal{C}_2$, puis la distance minimale de $\mathcal{C}_2^\perp$.
4. Que peut-on en conclure sur les distance minimales d'un code et de son orthogonal ?