UGA Master 1-Algèbre effective 2026

Examen du mercredi 13 mai, 9h-12h.
Documents interdits à l'exception d'une feuille manuscrite A4 recto-verso.
Calculatrice ou smartphone **en mode avion** *autorisé.*
Autres appareils électroniques interdits.
Ce sujet est composé de 3 exercices (barême indicatif non contractuel : 8, 7, 8). Veuillez rédiger l'exercice 1 sur une copie séparée.

Exercice 1 : Corps finis avec générateur multiplicatif

Le but de cet exercice est de calculer efficacement dans le corps K à 2^n éléments pour n relativement petit, on posera pour la plupart des questions $n = 6, N = 2^n = 64$. Les éléments de K peuvent être représentés de deux manières différentes :

— (représentation additive) :
comme des entiers j entre 0 et $N-1$ dont l'écriture en base 2 représente les coefficients d'un polynôme de degré au plus $n-1$ à coefficients dans $\mathbb{Z}/2\mathbb{Z}$

— (représentation multiplicative) :
on représente 0_K par $N-1$ et un élément non nul g^k par l'entier k correspondant compris entre 0 et $N-2$ (où g est un générateur de K^*).

On peut alors calculer efficacement (en quelques cycles de temps CPU) la somme (=la différence) de 2 éléments de K avec la première représentation, et la produit ou l'inverse d'un élément avec la deuxième représentation, et faire toutes les opérations de base sur K efficacement en construisant deux tables permettant de passer de j à k et inversement.

1. Expliquer comment on calcule la somme de deux éléments de K en représentation additive. Donner un algorithme en langage naturel qui permet de calculer le produit et l'inverse avec la représentation multiplicative.
2. Déterminer un polynôme M de degré $n = 6$ irréductible dans $\mathbb{Z}/2\mathbb{Z}[x]$, en justifiant que ce polynôme est bien irréductible : pour justifier, on pourra donner directement le résultat d'instructions telles que `powmod` ou `gcd` mais pas de `factor` ou `is_irreducible` (qu'on peut quand même utiliser pour vérifier).
Dans la suite, on notera $\alpha = x \pmod M$ vu donc comme élément de K.
3. Que doit-on vérifier pour savoir si un élément de K^* est un générateur de K^* ? Quelle est la probabilité qu'un élément de K^* choisi au hasard soit générateur ? Tester si c'est le cas pour α en décrivant les instructions données à la calculatrice.
4. Si α est générateur, expliquer comment déterminer la table qui permet de passer de la représentation multiplicative vers la représentation additive. Peut-on construire la table inverse en temps $O(N)$?
5. Si α n'est pas générateur, on pourrait essayer de construire un autre polynôme irréductible M de degré n jusqu'à ce que $x \pmod M$ le soit. mais c'est en fait peu efficace. On va plutôt chercher un polynôme non constant P pris au hasard et tester si $P(\alpha)$ est générateur de K^* puis calculer son polynôme minimal sur $\mathbb{Z}/2\mathbb{Z}$.
Déterminer un tel polynôme P (différent de x si dans votre cas α est déjà générateur).
6. Pour calculer le polynôme minimal de $P(\alpha)$, on cherche le noyau de la matrice dont les colonnes sont les coefficients de $1, P, ..., P^n \bmod M$. Montrer que ce noyau est exactement de dimension 1 et que l'on peut en déduire un polynôme $\tilde{M}$ tel que $\beta = x \pmod{\tilde{M}}$ soit générateur de $\tilde{K}^* = \mathbb{Z}/2\mathbb{Z}[x]/\tilde{M}$. Faire le calcul pour $n = 6$ et $P \neq x$.
7. Estimer pour n quelconque la complexité du calcul précédent, comparer au coût d'un test d'irréductibilité et justifier que cette méthode est effectivement plus efficace que de prendre des polynômes irréductibles au hasard et attendre que $x \pmod M$ soit générateur de K^*.

Exercice 2 : Test de primalité de Pocklington

On prend ici p premier fixé, $n \geq 1$ et N pris sous la forme $N = Kp^n + 1$ avec K entier.
On considère q un facteur premier de N.

1. Supposons qu'on ait trouvé $a > 0$ entier vérifiant l'hypothèse
$(H) : (\ a^{N-1} \equiv 1 \mod N$ et $\text{pgcd}(a^{\frac{N-1}{p}} - 1, N) = 1)$.
Montrer que $a^{N-1} \equiv 1 \mod q$ mais $a^{\frac{N-1}{p}} \neq 1 \mod q$.

2. Quel est le coût en opérations binaires de vérification de l'hypothèse (H) pour un a entre 1 et N ?
   (bien préciser comment on calcule efficacement le pgcd demandé).
3. Pour un a vérifiant (H), on note d l'ordre multiplicatif de a dans $(\mathbb{Z}/q\mathbb{Z})^*$. Montrer que d divise $N-1$ mais pas $(N-1)/p$, et en déduire que p^n divise d.
4. Conclure que si (H) est satisfaite pour un certain a, tout facteur premier de N est congru à 1 modulo p^n.
5. On suppose maintenant que $K < p^n$. Montrer que si (H) est satisfaite pour un certain $a > 0$, N est premier.
6. Dans le cas où N est premier, quelle est la proportion d'entiers a entre 1 et N vérifiant (H) ?
7. Appliquer cette méthode pour montrer (en décrivant les calculs utilisés à la calculatrice) que

$$4 \cdot 7^{17} + 1 = 930522055948829$$

   est premier.

Exercice 3 : Codes de Reed-Solomon

On pose p premier et $n \in \{1, \cdots, p-1\}$.
On choisit $x_1, \cdots, x_n$ des éléments distincts de $\mathbb{F}_p$ et on définit $\varphi : \mathbb{F}_p[X]_{<n} \to \mathbb{F}_p^n$ par

$$\varphi(P) := (P(x_1), \cdots, P(x_n)).$$

1. Montrer que φ est un isomorphisme d'espaces vectoriels sur $\mathbb{F}_p$.
   Pour tout $k \in \{1, \cdots, n\}$, on note $C_k = \varphi(\mathbb{F}_p[X]_{<k})$.
2. Donner la longueur et la dimension de C_k.
3. Montrer que la distance de Hamming minimale de C_k est $n-k+1$, et en déduire que C est un code correcteur de paramètres $(n, k, n-k+1)$.
4. Pour tout $(y_1, \cdots, y_n) \in \mathbb{F}_p^n$, expliquer comment calculer $\varphi^{-1}(y_1, \cdots, y_n)$ par interpolation. Quel est le coût de ce calcul en nombre d'opérations dans $\mathbb{F}_p$? (on n'attend pas de détails de chaque étape)
5. Fixons $k < n-1$, $P_0 \in \mathbb{F}_p[X]_{<k}$ et $y = (y_1, \cdots, y_n) \in \mathbb{F}_p^n$. Supposons qu'au cours de la transmission, ce n-uplet est transformé en $y' = (y'_1, \cdots, y'_n)$ avec au moins une et au plus $n-k-1$ erreurs (coordonnées changées). En considérant le degré de $\varphi^{-1}(y')$, comment peut-on détecter qu'il y a eu des erreurs de transmission grâce à la question précédente ?

   Supposons qu'il y a eu exactement une erreur de transmission (c'est-à-dire un $i \in \{1, \cdots, n\}$ tel que $y_i \neq y'_i$), on cherche à trouver quel est ce i et réparer l'erreur.

   Pour $j \in \{1, \cdots, n\}$, on note $\varphi^{(j)}$ qui à $P \in \mathbb{F}_p[X]_{<n-1}$ associe $(P(x_0), \cdots, \widehat{P(x_j)}, \cdots, P(x_n)) \in \mathbb{F}_p^{n-1}$) (c'est-à-dire qu'on enlève la j-ième coordonnée à l'arrivée par rapport à φ).
   On note enfin $(y')^{(j)}$ le vecteur y' privé de sa j-ième cooordonnée et de même pour y.
6. Montrer que $(\varphi^{(i)})^{-1}((y')^{(i)}) = (\varphi^{(i)})^{-1}((y)^{(i)}) = P_0$.
7. Si $j \neq i$, on pose $P_j = (\varphi^{(j)})^{-1}((y')^{(j)})$.
   Montrer que $P_j \neq P_0$ et $P_j - P_0$ a au moins $n-2$ racines, en déduire que $\deg(P_j) \geq k > \deg(P_0)$.
8. Utiliser les deux questions précédentes pour trouver l'indice i et corriger l'erreur algorithmiquement.
9. (*Bonus*) Pour $p = 7$ et $(x_1, x_2, x_3, x_4, x_5) = (1, 2, 3, 4, 5) \in \mathbb{F}_7^5$, le message transmis avec exactement une erreur avec $n = 5, k = 3$ est $(6, 5, 4, 6, 3)$. Retrouver le polynôme P_0 initialement choisi pour ce message, de degré au plus 2.