UGA Master 1-Algèbre effective 2025

Examen du mercredi 14 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 à rédiger sur des feuilles séparées (exercice 1 d'un côté, exercices 2 et 3 de l'autre)** *(barême indicatif non contractuel : 9,4,9).*

Exercice 1

Soit K=GF(p,n) un corps fini de caractéristique p un nombre premier. On représente les éléments de K comme des polynômes en y modulo un polynôme $M(y)$ de degré n irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Par complexité dans cet exercice, on entend complexité en terme du nombre d'opérations binaires effectuées.

On s'intéresse au calcul efficace du produit de deux polynômes A et B de degré strictement inférieurs à N à coefficients dans K lorsque N est grand.

1. Pour $K = GF(5,2)$, donner un polynôme M qui convient en justifiant. Quelle est la complexité de votre méthode de justification sur $GF(p,2)$ en fonction de p ?
2. Si la complexité le permet, donner un M convenable pour $p = 2013265921$.
3. Rappeller la complexité du calcul du produit de A et B par la méthode naïve, en fonction de N, n, p.
4. Peut-on appliquer la méthode de Karatsuba pour accélérer le calcul lorsque N est grand ? Quelle est alors la complexité du calcul ?
5. Peut-on effectuer un calcul de produit par FFT avec une racine 2^t-ième de l'unité dans K^* ? (on pourra en particulier considérer le cas où $p = 2$).
6. On associe à un polynôme $P \in K[x]$ un polynôme $\tilde{P} \in \mathbb{Z}/p\mathbb{Z}[z]$ en substituant $x = z^{2n}$ et $y = z$:

$$P = \sum_{i<N} p_i x^i,\ p_i = \sum_{j<n} p_{i,j} y^j, p_{i,j} \in \mathbb{Z}/p\mathbb{Z}, \quad \to \quad \tilde{P} = \sum_{i<N, j<n} p_{i,j} z^{2in+j}$$

   Calculer $\tilde{P}$ lorsque $K = GF(5,2)$ et $P = x^2 + (3y-5)x + 7$.
   Quel est le degré de $\tilde{P}$ génériquement ?
   N.B. : on pourrait prendre $x = z^{2n-1}$, le choix $x = z^{2n}$ a été fait pour alléger les notations.
7. Pour effectuer le produit de A par B, on calcule $\tilde{A}\tilde{B}$, on l'écrit

$$\tilde{A}\tilde{B} = \sum_{i<N} z^{2in} c_i, \quad c_i = \sum_{j<2n} c_{i,j} z^j$$

   on substitue $z = y$ dans c_i et on calcule le reste $r_i(y)$ modulo $M(y)$.
   Tester sur $K = GF(5,2)$ avec $A = B = P$ où P est le polynôme de la question 3.
8. Montrer que le coefficient de degré i de AB est r_i.
9. Supposons que l'on puisse effectuer le calcul du produit $\tilde{A}\tilde{B}$ par un algorithme ayant la même complexité que la FFT, quelle complexité peut-on espérer pour calculer AB ?

Exercice 2

Pour tout $n \geq 0$, on définit le n-ième nombre de Fermat $F_n = 2^{2^n} + 1$.
Cet exercice porte sur le critère de Pépin : pour tout $n \geq 1$,

$$\text{« } F_n \text{ est premier si et seulement si } 3^{(F_n-1)/2} \equiv -1 \mod F_n \text{. »}$$

1. En admettant le critère de Pépin, déterminer quels nombres de Fermat parmi F_3, F_4, F_5, F_6, F_7 sont premiers.

2. En admettant le critère de Pépin, donner un algorithme pour tester la primalité de F_n. Quelle est la complexité de cet algorithme ? Est-il efficace en fonction de la taille de F_n ?
3. La suite et fin de cet exercice vise à montrer l'implication réciproque du critère de Pépin (on admettra l'implication directe, obtenue grâce au symbole de Legendre). On suppose donc que $3^{(F_n-1)/2} \equiv -1 \mod F_n$. En déduire que l'ordre multiplicatif de 3 est exactement $F_n - 1$.
4. En déduire que $(\mathbb{Z}/F_n\mathbb{Z})^\times$ est de cardinal au moins $F_n - 1$, puis finalement que F_n est premier.

Exercice 3

On s'intéresse ici au calcul de valeurs d'une suite récurrente linéaire dans un corps K.
Les complexités seront à donner dans cet exercice uniquement en termes d'opérations dans K.
On fixe $d \geq 1$ et des coefficients $c_0, \cdots, c_{d-1} \in K$. On considère la suite $(a_n)_{n\in\mathbb{N}}$ définie avec un choix fixé de $a_0, \cdots, a_{d-1}$, puis par la récurrence linéaire de degré d

$$a_{n+d} = c_{d-1}a_{n+d-1} + \cdots + c_1 a_{n+1} + c_0 a_n = \sum_{i=0}^{d-1} c_i a_{n+i} \tag{1}$$

pour tout $n \in \mathbb{N}$.

1. Montrer que pour $d = 2$, $a_0 = a_1 = 1$ et $c_0 = c_1 = 1$, on retrouve la suite de Fibonacci, et en donner les dix premiers termes.
2. Pour une suite $(a_n)_{n\in\mathbb{N}}$ donnée, on note pour tout $n \in \mathbb{N}$,

$$A_n = \begin{pmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+d-1} \end{pmatrix},$$

et on pose

$$M = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 \\ & & & \ddots & \\ 0 & & \cdots & 0 & 1 \\ c_0 & c_1 & c_2 & \cdots & c_{d-1} \end{pmatrix} \in M_d(K)$$

Montrer que $(a_n)_{n\in\mathbb{N}}$ vérifie (1) si et seulement si $A_{n+1} = MA_n$.

3. En déduire un algorithme pour calculer a_n en fonction du choix initial de A_0, et donner sa complexité.
4. Montrer que le polynôme non nul unitaire P de plus petit degré tel que $P({}^tM)(e_1) = 0$ avec e_1 le premier vecteur de la base canonique est

$$P = X^d - c_{d-1}X^{d-1} - \cdots - c_1 X - c_0.$$

5. En déduire que P est le polynôme minimal et le polynôme caractéristique de ${}^tM$ donc de M.
6. Comment peut-on calculer efficacement le reste de la division euclidienne de X^n par P pour n grand ? Justifier en donnant la complexité de la méthode.
7. En déduire un algorithme pour calculer A_n plus efficace que celui de la question 3 lorsque n est grand, et donner sa complexité.
8. Supposons que $d = 2$, et $P = (X - \lambda)(X - \mu)$ avec $\lambda, \mu \in K$ distincts.
   Donner une formule pour retrouver un polynôme Q modulo P en fonction de $Q(\lambda)$ et $Q(\mu)$ (plusieurs méthodes sont possibles, par exemple l'interpolation ou les coefficients de Bézout).
9. En déduire une formule pour X^n modulo P, puis pour M^n. L'appliquer au cas où $c_0 = -2$ et $c_1 = 3$.
10. Pour conclure, donner la complexité du calcul de A_n en utilisant cette formule.