	ANNÉE UNIVERSITAIRE 2022/2023	
	4TMA701U Calcul Formel **Examen terminal session 1** **Date : 13/12/2022 Heure : 9h Durée : 3h** Accès autorisé aux feuilles TD sur Moodle.	**Collège Sciences et Technologies**

Vous rendrez à la fin de l'examen une copie papier ainsi qu'un fichier sage contenant vos programmes (lisible, commenté et nettoyé si possible..) au format EX-Nom-Prenom.ipynb (feuille Jupyter) ou EX-Nom-Prenom.sage (fichier texte). Le fichier est à envoyer par e-mail à christine.bachoc@u-bordeaux.fr

Exercice 1 Nous avons vu en cours qu'il existe des algorithmes (utilisant FFT) de complexité algébrique $\tilde{O}(n)$ pour la multiplication et pour la division euclidienne dans $K[X]$ lorsque le degré des polynômes est inférieur à n, ainsi que des algorithmes (utilisant FFT) de complexité binaire $\tilde{O}(s)$ pour la multiplication et pour la division euclidienne des nombres entiers de taille binaire inférieure à s. À partir de là déterminez la complexité de :

1. La multiplication dans $R = K[X]/(P)$ où $P \in K[X]$ est de degré k (on demande la complexité algébrique, exprimée en fonction de k. Explicitez la représentation des éléments de R et les étapes nécessaires à la multiplication dans R).
2. La multiplication dans $\mathbb{F}_q$ où $q = p^k$, p premier (on demande la complexité binaire, exprimée en fonction de q, ou de p, k. On explicitera la représentation binaire des éléments de $\mathbb{F}_q$).
3. La multiplication dans $A = \mathbb{F}_q[X]/(P)$ où $P \in \mathbb{F}_q[X]$ est de degré d (on demande la complexité binaire, exprimée en fonction de q, d, ou de p, k, d).
4. L'exponentiation dans $A = \mathbb{F}_q[X]/(P)$: calcul de a^n pour $a \in A$ et $n \in \mathbb{N}$ (on demande la complexité binaire, exprimée en fonction de q, d, n, ou de p, k, d, n).

Exercice 2 Cet exercice porte sur un algorithme de partage de secret. Une personne A détient un secret $s \in \mathbb{N}$ qu'elle souhaite partager avec un groupe de n personnes $B_1, \ldots, B_n$. Toutefois elle souhaite que s reste inconnu de chacun des B_i, et même de toute partie incomplète du groupe. Pour cela elle construit à partir de s des valeurs $x_1, \ldots, x_n$, et transmet x_i à B_i $(i = 1, \ldots, n)$. La mise en commun des n valeurs x_i doit permettre au groupe de reconstruire s, mais aucune information sur s ne doit pouvoir être obtenue à partir d'un sous-ensemble strict des x_i.

A procède ainsi : elle fixe un corps fini $\mathbb{Z}/p\mathbb{Z}$, avec $p > n, s$, ainsi que $(t_1, \ldots, t_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ avec $t_i \neq t_j$ pour tout $i \neq j$. Ces données sont publiques. Pour calculer les x_i elle tire au hasard $(a_1, \ldots, a_{n-1}) \in (\mathbb{Z}/p\mathbb{Z})^{n-1}$ et pose $P = s + \sum_{k=1}^{n-1} a_k x^k \in \mathbb{Z}/p\mathbb{Z}[x]$. Puis elle calcule $x_i = P(t_i)$, qu'elle transmet à B_i.

1. Écrire une fonction sage qui prend en entrées p, $(t_1, \ldots, t_n)$, s et rend en sortie $(x_1, \ldots, x_n)$.
2. Quel algorithme vu en cours permettra au groupe de calculer s à partir de leurs données $(x_1, \ldots, x_n)$, et des données publiques p et $(t_1, \ldots, t_n)$? Justifiez votre réponse.
3. Écrire une fonction sage prenant en entrées p, $(t_1, \ldots, t_n)$, $(x_1, \ldots, x_n)$, et retournant en sortie s.

4. Application numérique : calculez s sachant que : $p = 10007$, $n = 10$, $t_i = i$ pour $1 \leq i \leq n$ et $(x_1, \ldots, x_{10}) = [1707, 8016, 4310, 9802, 9049, 5879, 557, 5818, 3247, 7072]$.
5. Expliquez pourquoi un sous-ensemble strict des personnes B_i ne pourra pas obtenir d'information sur s à partir de leurs données et des données publiques (on pourra montrer par exemple que tout autre secret s' peut conduire pour au moins un aléa aux mêmes parts x_i détenues par les membres du sous-ensemble strict des B_i).

Exercice 3 Soit $F = \mathbb{Z}/17\mathbb{Z}$ et soit $Q \in F[x]$ le polynôme de degré 18 dont les coefficients rangés par degré croissant sont :

$$[13, 3, 9, 10, 1, 8, 4, 16, 13, 4, 8, 16, 16, 1, 11, 12, 5, 3, 1]$$

Le but de l'exercice est de factoriser Q grâce à l'algorithme de Cantor-Zassenhaus.

1. Q est un polynôme sans facteur carré, produit de trois polynômes irréductibles sur F de degrés 6. Cette affirmation peut être vérifiée par le calcul de quatre pgcd de polynômes ; lesquels ? justifiez votre réponse et faites ces calculs dans Sage.
2. Expliquez pourquoi le quotient $F[x]/(Q)$ est le produit direct de trois copies du corps fini F_{17^6}.
3. Rappelez pourquoi, si $a \in F_{17^6}^*$, alors $a^{\frac{17^6-1}{2}} \in \{1, -1\}$.
4. On propose l'algorithme suivant :

   Algorithme 1 [FACTORISATION DE Q]
   Entrée : Q.
   Sortie : Un facteur irréductible de Q de degré 6 ou "échec"
   1. Choisir au hasard $A \in F[x]$, $1 \leq \deg(A) \leq 17$
   2. Calculer $D = \text{pgcd}(A, Q)$. Si $\deg(D) = 6$, sortir D. Si $\deg(D) = 12$, sortir Q/D.
   3. Calculer $R = A^{\frac{17^6-1}{2}} \mod Q$.
   4. Si $R = 1$ ou $R = -1$, sortir "échec".
   5. Calculer $D = \text{pgcd}(R - 1, Q)$. Si $\deg(D) = 6$, sortir D. Si $\deg(D) = 12$, sortir Q/D.

   Expliquez pourquoi cet algorithme sort avec une probabilité supérieure à $0,75$ un facteur irréductible de Q de degré 6. Effectuez-le dans Sage plusieurs fois pour obtenir les trois facteurs irréductibles de Q.

Exercice 4 Soit $g = x^2 + 2y^2 - 3$ et $h = x^2 + xy + y^2 - 3$ deux polynômes de $\mathbb{Q}[x, y]$. Soit I l'idéal de $\mathbb{Q}[x, y]$ engendré par g et h. On munit $\mathbb{Q}[x, y]$ de l'ordre lexicographique tel que $x > y$.

1. Montrez à la main que (g, h) n'est pas une base de Groebner de I.
2. Soit B la base de Groebner réduite de I, calculez B avec Sage.
3. A l'aide de cette base, calculez l'ensemble $V(I)$ des solutions dans $\mathbb{C}$ du système suivnt (vous expliquerez votre démarche).

$$\begin{cases} x^2 + 2y^2 = 3 \\ x^2 + xy + y^2 = 3 \end{cases}$$

Vous devez trouver 4 points.

4. Les monômes standards sont les monômes de $\mathbb{Q}[x,y]$ qui ne sont divisibles par aucun des termes dominants des éléments de B. Déterminez les monômes standards de B et expliquez pourquoi ils forment une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[x,y]/I$. Quelle est la dimension de ce quotient et comment se compare-t-elle au cardinal de $V(I)$?

Exercice 5 Dans le cas de l'exercice 4, on constate que le cardinal de $V(I)$ est égal à la dimension du quotient $\mathbb{C}[x,y]/I$ (qui est ici la même que celle de $\mathbb{Q}[x,y]/I$). Vous allez maintenant démontrer cette propriété dans un cadre général.

Soit K un corps et soit I un idéal de $K[x,y]$. On note $V(I)$ l'ensemble des zéros de I :

$$V(I) = \{p = (a,b) \in K^2 \mid f(a,b) = 0 \text{ pour tout } f \in I\}$$

On suppose que $V(I)$ est fini et on note $V(I) = \{p_1, \ldots, p_n\}$ ses éléments. On suppose que I vérifie la propriété suivante :

$$(R) \text{ Pour tout } f \in K[x,y], \quad \text{si } \forall p_i \in V(I),\ f(p_i) = 0, \text{ alors } f \in I.$$

Un idéal qui vérifie (R) est dit *radical.*

1. Construire un polynôme $P_1 \in K[x,y]$ tel que $P_1(p_1) = 1$ et $P_1(p_i) = 0$ pour tout $i \geq 2$. (indication : puisque $p_i \neq p_1$, ils diffèrent en l'une des deux coordonnées..).
2. Déduire de 1. qu'il existe n polynômes $P_1, \ldots, P_n$ tels que pour tout $i \neq j$, $1 \leq i,j \leq n$, $P_i(p_i) = 1$ et $P_i(p_j) = 0$.
3. Montrez que ces n polynômes sont K-linéairement indépendants modulo I.
4. Soit $g \in K[x,y]$. Montrez que $g - \sum_{k=1}^{n} g(p_k)P_k$ appartient à I (utilisez (R)).
5. Déduire des questions 3. et 4. que $n = \dim(K[x,y]/I)$.