ANNÉE UNIVERSITAIRE 2023/2024

4TMA701U Calcul Formel
Examen terminal session 1
Date : 13/12/2023 Heure : 9h Durée : 3h

Documents autorisés

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 l'adresse christine.bachoc@u-bordeaux.fr

Exercice 1 Soit p un nombre premier. Cet exercice étudie un algorithme qui calcul l'inverse d'un entier modulo p^n à partir de l'inverse de cet entier modulo p.

Soit donc $n \geq 1$. On suppose que n est une puissance de 2, il existe donc $k \geq 0$ tel que $n = 2^k$. Soit $a \in \mathbb{Z}$ tel que $1 \leq a < p^n$. On suppose qu'il existe b, $1 \leq b < p$ tel que $ab \equiv 1 \bmod p$.

On note comme d'habitude $\mathrm{rem}(c, d)$ pour le reste dans la division euclidienne de c par d. Soit l'algorithme suivant :

Algorithme 1 [INV]
Entrées : p, k, a, b comme ci-dessus.
Sortie : L'inverse de a modulo p^n.
1. Initialisation : $b_0 = b$.
2. Pour i de 1 à k : Calculer $b_i = \mathrm{rem}(2b_{i-1} - ab_{i-1}^2, p^{2^i})$
3. Sortir b_k.

1. Rappelez pourquoi a est inversible modulo p si et seulement si a est inversible modulo p^n.
2. Exécutez à la main l'algorithme INV pour calculer l'inverse modulo 81 de 5.
3. Avec les notations de l'algorithme, montrez que, pour tout $i \geq 1$,
$$1 - ab_i = (1 - ab_{i-1})^2 \bmod p^{2^i}.$$
4. Déduire de la question précédente que, pour tout $i \geq 1$, $ab_i = 1 \bmod p^{2^i}$, et donc que l'algorithme INV est correct.
5. Implémentez l'algorithme INV dans Sage puis testez-le avec $a = 5$, $p = 3$ et différentes valeurs de k.
6. On suppose ne disposer que des algorithmes naifs pour la multiplication et la division euclidienne des entiers. Montrez que la complexité binaire de l'algorithme INV est $O((\log(p^n))^2)$.
7. Quel autre algorithme connaissez-vous pour calculer l'inverse de a modulo p^n et quelle est sa complexité ?

Exercice 2 Soit $F = \mathbb{Z}/23\mathbb{Z}$ et soit $Q \in F[x]$ le polynôme de degré 18 dont les coefficients rangés par degré croissant sont :

$$[21, 19, 22, 13, 10, 2, 2, 7, 5, 18, 20, 13, 21, 3, 10, 4, 20, 0, 1]$$

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

1. On a les informations suivantes :
   a) $\text{pgcd}(x^{23^2} - x, Q) = 1$
   b) $\text{pgcd}(x^{23^3} - x, Q) = 1$
   c) $\text{pgcd}(x^{23^6} - x, Q) = Q$

   Vérifiez ces affirmations dans Sage, puis expliquez soigneusement pourquoi vous pouvez en déduire que Q est le produit de trois polynômes irréductibles deux à deux distincts et de degrés 6.
2. Expliquez pourquoi le quotient $F[x]/(Q)$ est le produit direct de trois copies du corps fini F_{23^6}.
3. Expliquez pourquoi, si $a \in F^*_{23^6}$, alors $a^{\frac{23^6-1}{2}} \in \{1, -1\}$.
4. Dans Sage, choisissez au hasard un polynôme A de $F[x]$, de degré inférieur à 18, et premier avec Q, puis calculez $D = \text{pgcd}(A^{\frac{23^6-1}{2}} - 1, Q)$. Recommencez jusqu'à obtenir la factorisation complète de Q.
5. Dans la question précédente, quelle est la probabilité que $D \in \{1, Q\}$? Justifiez votre réponse.

Exercice 3 Soit $f = x^3 + y^3 - 3xy - 1$ et $g = x^2 + y^2 - 4$ deux polynômes de $\mathbb{Q}[x, y]$. Soit I l'idéal de $\mathbb{Q}[x, y]$ engendré par f et g. On munit $\mathbb{Q}[x, y]$ de l'ordre lexicographique tel que $x > y$.

1. Montrez à la main que (f, g) 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 les solutions dans $\mathbb{R}^2$ du système suivant (vous expliquerez votre raisonnement).
$$\begin{cases} x^3 + y^3 - 3xy = 1 \\ x^2 + y^2 = 4 \end{cases}$$
4. Le polynôme $h = x^6 + y^6 - 28$ appartient-il à I ?
5. Donnez une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[x, y]/I$. Quelle est la dimension de ce quotient ?