UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

FLMA607 Calcul Formel – 2009–2010

Examen 2nde session (21 juin 2010)

Durée : 2h00. Justifiez toutes vos réponses. Documents, calculatrices et téléphones portables sont interdits.

Exercice 1

Soit $\mathcal{C}$ la courbe de $\mathbb{R}^2$ paramétrée par $\begin{cases} x(t) &= \frac{2}{1+t^2} \\ y(t) &= \frac{(1+t)^2}{1+t^2} \end{cases}$ où t parcourt $\mathbb{R}$.

1) Énoncer le théorème d'élimination.
2) Trouver un polynôme $P(X,Y) \in \mathbb{R}[X,Y]$ tel que pour tout point (x_0, y_0) de $\mathcal{C}$ on ait $P(x_0, y_0) = 0$. On justifiera rigoureusement que P convient. [*Indication : Utiliser le théorème d'élimination avec les polynômes* $(1+T^2)X - 2$ *et* $(1+T^2)Y - (1+T)^2$.]
3) Représenter graphiquement la courbe $P(x, y) = 0$.

Problème

Ce problème décrit un algorithme permettant de trouver les racines d'un polynôme sur un corps fini de cardinal impair. À l'exception des questions 14 et 15, chaque question peut être résolue indépendamment des autres si l'on admet les résultats donnés dans les questions qui la précèdent.

Partie 1 : Résultats préliminaires sur les corps finis

1) Soit $\mathbb{F}_q$ un corps fini de cardinal q *impair*. Soit $\alpha \in \mathbb{F}_q^*$. Montrer que $\alpha^{\frac{q-1}{2}} \in \{\pm 1\}$.
2) On note

$$\begin{aligned} S &= \{\alpha \in \mathbb{F}_q^* \mid \alpha^{\frac{q-1}{2}} = 1\} \\ T &= \{\alpha \in \mathbb{F}_q^* \mid \alpha^{\frac{q-1}{2}} = -1\}. \end{aligned}$$

Montrer que S est exactement l'ensemble des carrés dans $\mathbb{F}_q^*$, et que

$$\operatorname{Card} S = \operatorname{Card} T = \frac{q-1}{2}.$$

[*Indication : On pourra utiliser l'application* $x \mapsto x^2$ *de* $\mathbb{F}_q^*$ *dans lui-même.*]
3) En déduire les égalités

$$X^{\frac{q-1}{2}} + 1 = \prod_{\alpha \in T} (X - \alpha) \quad \text{et} \quad X^{\frac{q-1}{2}} - 1 = \prod_{\alpha \in S} (X - \alpha).$$

4) Montrer que

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha).$$

Partie 2 : Premières étapes (déterministes) de l'algorithme

On cherche maintenant un algorithme permettant de trouver toutes les racines, dans le corps $\mathbb{F}_q$, d'un polynôme $f \in \mathbb{F}_q[X]$ donné.

5) On pose $g = \text{pgcd}\,(f, X^q - X)$. Montrer que f a les mêmes racines que g dans le corps $\mathbb{F}_q$, et que g est scindé sur $\mathbb{F}_q$, c'est-à-dire que tous ses facteurs irréductibles sont de degré 1.
6) On suppose maintenant que le polynôme f est scindé sur $\mathbb{F}_q$. On peut donc écrire

$$f = \prod_{i=1}^{d}(X - s_i)$$

où les $s_i \in \mathbb{F}_q$ sont inconnus. Donner un algorithme permettant de se ramener au cas où les s_i sont deux à deux distincts. *[Indication : Les s_i sont deux à deux distincts si et seulement si le polynôme f est sans facteur carré...]*
7) On peut aussi supposer les s_i non nuls. Pourquoi ?

Partie 3 : Un algorithme probabiliste

8) Soit $f = \prod_{i=1}^{d}(X - s_i)$ un polynôme séparable et scindé de $\mathbb{F}_q[X]$ tel que $f(0) \neq 0$. Montrer que

$$f = \text{pgcd}\,(f, X^{\frac{q-1}{2}} + 1).\text{pgcd}\,(f, X^{\frac{q-1}{2}} - 1).$$

9) À quelle condition cette factorisation est-elle triviale ? Si $d = 2$, montrer que l'on a au moins une chance sur deux de trouver les racines ainsi. (On supposera que les deux racines $s_1 \neq s_2$ ont été choisies aléatoirement et indépendamment dans $\mathbb{F}_q^*$.)
10) Dans le cas où la factorisation obtenue est triviale, on recommence en remplaçant $f(X)$ par $f_a(X) = f(X - a)$ pour $a \in \mathbb{F}_q$ choisi au hasard. Expliquer comment on peut obtenir une factorisation de f à partir d'une factorisation de f_a.
11) On admettra que, pour chaque tirage de a, la probabilité d'obtenir une factorisation triviale de f_a est de l'ordre de 2^{1-d}. Si $d = 3$, quelle est la probabilité de ne pas avoir réussi à factoriser f après 10 tirages de a ?

Partie 4 : Coût de l'algorithme

On note d le degré de f.

12) Avec les notations de la question 5) combien d'opérations dans $\mathbb{F}_q$ doit-on effectuer pour calculer g par l'algorithme d'Euclide (donner une estimation de la forme $O(...)$) ? Ce coût est-il polynomial en la taille des entrées ?
13) Au lieu de calculer directement $\text{pgcd}\,(f, X^q - X)$ par l'algorithme d'Euclide, on propose de calculer d'abord $X^q \mod f$ par l'algorithme d'exponentiation rapide. Montrer que le coût de ce premier calcul est de $O(d^2 \log q)$ opérations dans $\mathbb{F}_q$, puis donner une estimation du coût global du calcul de g.
14) En vous inspirant du résultat de la question 13), donner une majoration du coût du calcul de $\text{pgcd}\,(f, X^{\frac{q-1}{2}} + 1)$.
15) Avec les notations de la partie 3, on suppose que l'on a beaucoup de chance à chaque tirage de a. Plus précisément on suppose que l'on obtient toujours une factorisation non triviale et que les deux facteurs $\text{pgcd}\,(f_a, X^{\frac{q-1}{2}} + 1)$ et $\text{pgcd}\,(f_a, X^{\frac{q-1}{2}} - 1)$ sont de degré $\frac{d}{2}$ (au passage on suppose donc que d est une puissance de 2)[1]. Sous ces hypothèses, montrer que le coût de la partie probabiliste de l'algorithme est en $O(d^2 \log q)$. [*Indication : On pourra procéder par récurrence. On négligera le coût du calcul des coefficients de f_a.*]
16) Faire un bilan du coût global de l'algorithme. (On admettra que l'étape décrite à la question 6 nécessite au plus $O(d^2 \log q)$ opérations dans $\mathbb{F}_q$.)

[1] Cette hypothèse apparemment idéaliste n'est pas complètement déraisonnable. Elle correspond à peu près à ce qu'il se passe en pratique lorsque d est grand.