

# Master Mathématiques, Algèbre et Calcul Formel

Examen du 15 Avril 2011, durée 3 heures

Documents interdits.

**Exercice 1:** Soit  $K$  un corps de caractéristique différente de 2 et contenant une racine primitive  $n$ -ième de l'unité  $\omega$  pour  $n = 2^k$ . Soit  $f(x)$  et  $g(x)$  deux polynômes à coefficients dans  $K$  de degrés inférieurs à  $n$ . On note  $f * g$  l'unique polynôme de degré inférieur à  $n$  et tel que  $f(x)g(x) = (f * g)(x) \bmod x^n - 1$  (autrement dit,  $f * g$  est le reste du produit  $f(x)g(x)$  dans la division par  $x^n - 1$ ). On considère l'algorithme suivant:

---

**Algorithm 1** Convolution rapide

---

**Entrées:**  $n = 2^k$ ;  $\{\omega, \omega^2, \dots, \omega^{n/2-1}\}$ ;  $f, g \in K[x]$ ,  $\deg(f) < n$ ,  $\deg(g) < n$ .

**Sorties:**  $f * g$ .

- 1: Si  $k = 0$ , **sortir**  $fg$ .
  - 2: Calculer  $f_0, g_0$  les restes respectifs de  $f$  et  $g$  modulo  $x^{n/2} - 1$  ainsi que  $f_1, g_1$  les restes respectifs de  $f$  et  $g$  modulo  $x^{n/2} + 1$ .
  - 3: Appeler récursivement l'algorithme pour calculer  $h_0(x) = f_0(x) * g_0(x)$  et  $h_1(\omega x) = f_1(\omega x) * g_1(\omega x)$  à l'ordre  $n/2 = 2^{k-1}$ .
  - 4: **Sortir**  $1/2((h_0 + h_1) + x^{n/2}(h_0 - h_1))$ .
- 

1. Exécutez cet algorithme pour  $n = 4$ ,  $f = 1 + x^3$  et  $g = 1 + x + x^2$  et vérifiez votre résultat.
2. Montrez que  $f = f_0 + (x^{n/2} - 1)q = f_1 + (x^{n/2} + 1)q$  pour  $q = (f_0 - f_1)/2$ .
3. En déduire que  $2fg = f_0g_0(x^{n/2} + 1) - f_1g_1(x^{n/2} - 1) \bmod x^n - 1$ .
4. Montrez que  $h_1(x) = f_1(x)g_1(x) \bmod x^{n/2} + 1$ .
5. Déduire des questions précédentes que la sortie de l'algorithme est correcte.
6. Montrez que sa complexité est en  $O(n \log n)$  opérations dans  $K$ .

**Exercice 2:** Le but de cet exercice est de donner une version dans le cas de la caractéristique 2 de l'algorithme de Cantor-Zassenhaus, que l'on rappelle ci-après:

---

**Algorithm 2** Cantor-Zassenhaus

---

**Entrées:**  $q = p^k$  impair,  $Q \in \mathbb{F}_q[X]$  de degré  $n$  un produit de polynômes irréductibles sur  $\mathbb{F}_q$ , deux à deux distincts, et tous de degré  $d$ .

**Sorties:** Un diviseur de  $Q$  non trivial ou bien "échec".

- 1: Tirer au hasard  $A \in \mathbb{F}_q[X]$  de degré inférieur à  $n$ .
  - 2: Calculer  $D = \gcd(A, Q)$ . Si  $D \neq 1$ , **sortir**  $D$ .
  - 3: Calculer  $B = A^{(q^d-1)/2} - 1 \pmod{Q}$ .
  - 4: Calculer  $D = \gcd(B, Q)$ .
  - 5: **Sortir**  $D$  si  $D \neq 1$ , sinon "échec".
- 

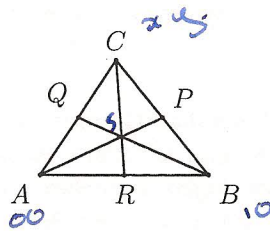
1. Soit  $m \geq 1$  et soit  $T_m = X^{2^{m-1}} + X^{2^{m-2}} + \dots + X^4 + X^2 + X \in \mathbb{F}_2[X]$ .

- (a) Montrez que  $T_m(T_m + 1) = X^{2^m} + X$ .
- (b) En déduire que, si  $\alpha \in \mathbb{F}_{2^m}$ , alors  $T_m(\alpha) \in \mathbb{F}_2$ .
- (c) Montrez que l'application  $\alpha \mapsto T_m(\alpha)$  de  $\mathbb{F}_{2^m}$  dans  $\mathbb{F}_2$  est une application linéaire de  $\mathbb{F}_2$ -espaces vectoriels. En déduire que  $\{\alpha \in \mathbb{F}_{2^m} : T_m(\alpha) = 0\}$  et  $\{\alpha \in \mathbb{F}_{2^m} : T_m(\alpha) = 1\}$  ont même cardinal, soit  $2^{m-1}$ .

Soit maintenant  $q = 2^k$ , et  $Q(X) \in \mathbb{F}_q[X]$  de degré  $n$ . On suppose que  $Q$  est le produit de  $r$  polynômes irréductibles sur  $\mathbb{F}_q$  notés  $P_1, \dots, P_r$ , deux à deux distincts et tous de même degré  $d$ . On note  $R = \mathbb{F}_q[X]/(Q)$ ,  $R_i = \mathbb{F}_q[X]/(P_i)$  et  $\phi_i : R \rightarrow R_i$  l'application canonique définie par:  $\phi_i(P \pmod{Q}) = P \pmod{P_i}$ .

2. Soit  $A \in R$ . Montrez que  $\phi_i(T_{kd}(A)) = T_{kd}(\phi_i(A))$ . En utilisant les résultats de la question 1. en déduire que  $\phi_i(T_{kd}(A)) \in \mathbb{F}_2$ , et que, si  $A$  est choisi au hasard et uniformément dans  $R$ ,  $T_{kd}(A)$  appartient à  $\mathbb{F}_2$  avec probabilité  $2^{1-r}$ .
3. En déduire un analogue de l'algorithme de Cantor-Zassenhaus pour factoriser  $Q$  et montrez que sa probabilité d'échec est inférieure à  $1/2$ . On écrira cet algorithme sous la forme conventionnelle.
4. Étudier la complexité de l'algorithme décrit à la question précédente.

**Exercice 3:** Dans cet exercice, on veut démontrer le résultat de géométrie bien connu suivant: les médianes d'un triangle sont concourantes et leur point d'intersection est le centre de gravité du triangle, à l'aide des bases de Gröbner. Soit donc dans le plan un triangle  $ABC$  dont les sommets ont pour coordonnées:  $A = (0,0)$ ,  $B = (1,0)$  et  $C = (x,y)$ . Soit  $P$ ,  $Q$ ,  $R$  les milieux respectifs des côtés  $[BC]$ ,  $[AC]$ ,  $[AB]$ . Soit  $S = (u,v)$  l'intersection des médianes  $AP$  et  $BQ$ .



1. Soit  $f_1 = uy - v(x+1)$  et  $f_2 = (u-1)y - v(x-2)$ . Montrez que  $S = (u,v)$  est l'intersection des droites  $AP$  et  $BQ$  si et seulement si  $f_1 = f_2 = 0$ .
2. Soit  $g_1 = -2uy - (v-y) + 2vx$ . Montrez que  $g_1 = -f_1 - f_2$ . En déduire que les trois médianes sont bien concourantes en  $S$ .
3. Soit  $g_2 = 3u - x - 1$  et  $g_3 = 3v - y$ . Montrez que les conditions:  $\overrightarrow{AS} = 2\overrightarrow{SP}$ ,  $\overrightarrow{BS} = 2\overrightarrow{SQ}$ ,  $\overrightarrow{CS} = 2\overrightarrow{SR}$  sont équivalentes à  $g_2 = g_3 = 0$ .
4. On considère désormais  $x, y, u, v$  comme des variables de polynômes à coefficients réels. Soit  $I = \langle f_1, f_2 \rangle$  l'idéal de  $\mathbb{R}[x, y, u, v]$  engendré par  $f_1$  et  $f_2$ . Calculez une base de Gröbner de  $I$ , relativement à l'ordre lexicographique noté  $\prec$ , pour lequel  $u \succ v \succ x \succ y$ .
5. En déduire que  $yg_2$  et  $g_3$  appartiennent à  $I$  et conclure.