ALGORITHMIQUE ALGÉBRIQUE **MU4MA023** **Examen**

P. V. Koseleff – P. Charollois

Examen

Jeudi 6 mai 2021
Durée : 2 heures. Le polycopié du cours est autorisé.

Rappels

Le polynôme cyclotomique Φ_n est le polynôme unitaire dont les racines sont les $\varphi(n)$ racines primitives n-èmes de 1 (dans $\mathbf{C}^*$). Φ_n est de degré $\varphi(n)$ et on a

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Φ_n est un polynôme à coefficients entiers, irréductible dans $\mathbf{Z}[X]$. Lorsque p est un entier premier qui ne divise par n, les facteurs irréductibles de Φ_n sont tous de même degré r : l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$.

Exercice 1.1. — Extension de degré 2^n sur $\mathbf{F}_5$

1. (a) Montrer que $X^{2^n} - 1 = (X-1) \cdot \prod_{i=0}^{n-1} (X^{2^i} + 1)$, pour tout $n \in \mathbf{N}$.

   (b) Montrer que $\Phi_{2^n}(X) = X^{2^{n-1}} + 1$ pour tout $n \geq 1$.

2. (a) Montrer que $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$, pour tout $n \geq 3$.

   (b) En déduire que l'ordre de 5 dans $(\mathbf{Z}/2^n\mathbf{Z})^*$ est 2^{n-2}, pour tout $n \geq 3$.

3. (a) Montrer que dans $\mathbf{F}_5[X]$ on a $\Phi_4 = (X-2)(X+2)$.

   (b) En déduire que dans $\mathbf{F}_5[X]$, on a $\Phi_{2^n} = (X^{2^{n-2}} - 2)(X^{2^{n-2}} + 2)$, pour tout $n \geq 2$.

   (c) En déduire la décomposition en facteurs irréductibles de Φ_{2^n} dans $\mathbf{F}_5[X]$.

4. Soit n un entier positif, $P_n = X^{2^n} + 2 \in \mathbf{F}_5[X]$ et $K_n = \mathbf{F}_5[X]/(P_n)$.

   (a) Montrer que K_n est un corps. Quel est son cardinal q ?

   (b) Soit $\alpha = X \pmod{P_n} \in K_n^*$. Quel est l'ordre de α ?

5. Soit $A \in \mathbf{F}_5[X]$ un polynôme de degré d exprimé dans la base canonique $(X^i, i \geq 0)$.

   (a) Soit $B_N \in \mathbf{F}_5[X]$ un polynôme quelconque de degré N. Donner un majorant du nombre d'opérations arithmétiques nécessaires dans $\mathbf{F}_5$ pour exprimer $A \pmod{B_N}$ dans la base $(1, X, \ldots, X^{N-1})$?

   (b) On pose $N = 2^n$. Donner un majorant du nombre d'opérations arithmétiques nécessaires dans $\mathbf{F}_5$ pour exprimer $A \pmod{P_n}$ dans la base $(1, X, \ldots, X^{N-1})$?
   (*on pourra écrire* $A = A_0 + X^{2^n} A_1 + \cdots + X^{r \cdot 2^n} A_r$, *où* $r \cdot 2^n \leq d < (r+1) \cdot 2^n$).

En informatique il est très important de construire des polynômes irréductibles de degré N dans $\mathbf{F}_p$ pour tout premier p et tout degré N *ayant un nombre de termes aussi petit que possible*.

Exercice 1.2. — Paramétrisation rationnelle d'une conique

1. Soit $\mathcal{C}$ une courbe admettant une paramétrisation rationnelle $x(t) = \dfrac{F(t)}{H(t)}, y(t) = \dfrac{G(t)}{H(t)}$, où $F, G, H \in \mathbf{R}[t]$ sont des polynômes de degrés inférieurs ou égaux à 2.
   (a) Montrer que F^2, FG, G^2, FH, GH et H^2 sont liés dans $\mathbf{R}[t]$.
   (b) Montrer que la courbe $\mathcal{C}_1$, paramétrée par $x = \dfrac{t^2-1}{t^2+t+1}, y = -\dfrac{t(t+2)}{t^2+t+1}$ admet une équation de degré 2.
   (c) Expliquer comment obtenir l'équation de la conique $\mathcal{C}_1$ (on ne demande pas l'équation).
2. On considère la conique $\mathcal{C}_a$ d'équation $x^2 + y^2 + axy = 1$.
   (a) Montrer que les points $I = (1,0)$, $I' = (-1,0)$, $J = (0,1)$ et $J' = (-1,0)$ appartiennent à $\mathcal{C}_a$.
   (b) Montrer que la droite $\mathcal{D}_t$, d'équation $y = t(x-1)$ coupe $\mathcal{C}_a$ en I et en un second point $I_a(t)$. Exprimer les coordonnées de $I_a(t)$ en fonction de t et de a.
   (c) Montrer que $I_a(0) = I', I_a(-1) = J, I_a(1) = J'$.
   (d) Pour quelle valeur de t a-t-on $I_a(t) = I$? En déduire l'équation de la tangente $\mathcal{C}_a$ en I.
3. (a) Montrer que $t \mapsto I_a(t)$ est une paramétrisation rationnelle de $\mathcal{C}_a$.
   (b) À quelle condition, portant sur le réel a, la courbe $\mathcal{C}_a$ est-elle bornée (une ellipse) ?