# E.P.I.T.A.

## Mathématiques (Obligatoire : durée 3h)

---

Ce problème a pour objectif l'étude de la transformation de Fourier discrète et son application à un algorithme rapide de multiplication des polynômes.
Dans tout la suite, on désigne par $N$ un nombre entier naturel non nul et on convient de noter $n$ le nombre entier $2^N$ et $\omega_n$ le nombre complexe $\exp(2i\pi/n) = \cos(2\pi/n)+i\sin(2\pi/n)$.
On appellera :

- polynôme associé à un $n$-uplet $a = (a_0, a_1, \ldots, a_{n-1})$ de $\mathbf{C}^n$ le polynôme $A$ appartenant à $\mathbf{C}_{n-1}[X]$ et défini par :

$$A(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} = \sum_{i=0}^{n-1} a_i X^i$$

- transformation de Fourier discrète l'application linéaire $F_n$ associant à tout $n$-uplet $a$ de $\mathbf{C}^n$ le $n$-uplet de $\mathbf{C}^n$ défini à l'aide du polynôme $A$ associé au $n$-uplet $a$ par :

$$F_n(a) = (A(1), A(\omega_n), A(\omega_n^2), \ldots, A(\omega_n^{n-1})).$$

L'espace $\mathbf{C}^n$ est muni de sa norme usuelle, défini pour un élément $a = (a_0, a_1, \ldots, a_{n-1})$ par :

$$\|a\|^2 = \sum_{k=0}^{n-1} |a_k|^2 = \sum_{k=0}^{n-1} \overline{a_k} a_k .$$

1°) Etude du cas particulier $n = 4$.

a) Expliciter l'image d'un quadruplet $a = (a_0, a_1, a_2, a_3)$ de $\mathbf{C}^4$ par l'application $F_4$.

b) Expliciter la matrice $M_4$ de l'endomorphisme $F_4$ dans la base canonique de $\mathbf{C}^4$, définie par :
$e_0 = (1, 0, 0, 0)$, $e_1 = (0, 1, 0, 0)$, $e_2 = (0, 0, 1, 0)$, $e_3 = (0, 0, 0, 1)$.

c) Calculer le produit matriciel $M_4 \overline{M_4}$ où $\overline{M_4}$ désigne la matrice d'ordre 4 dont les éléments sont les conjugués de ceux de la matrice $M_4$. En déduire que $F_4$ est inversible; préciser $F_4^{-1}$.

d) Calculer enfin $M_4^2$ et $M_4^4$.

2°) Etude du cas général.

a) Etablir que l'application $F_n$ est bijective de $\mathbf{C}^n$ dans $\mathbf{C}^n$.

b) Expliciter la matrice $M_n$ de l'endomorphisme $F_n$ dans la base canonique de $\mathbf{C}^n$.

c) On désigne par $i, j$ deux nombres entiers vérifiant l'inégalité $-n \le i-j \le n$.
En distinguant les cas $i-j = 0$ et $i-j \neq 0$, calculer la somme $\sum_{k=0}^{n-1} \omega_n^{(i-j)k}$.

d) Calculer le produit matriciel $M_n \overline{M_n}$ où $\overline{M_n}$ désigne la matrice d'ordre $n$ dont les éléments sont les conjugués de ceux de la matrice $M_n$. Préciser alors l'automorphisme $F_n^{-1}$.

e) Calculer $M_n^2$ et $M_n^4$.
L'endomorphisme $F_n$ est-il diagonalisable (cette question est réservée aux candidats MP, PC, PSI) ?

f) Exprimer enfin $\|F_n(a)\|^2$ en fonction de $\|a\|^2$.

3°) Etude des éléments propres de $Fn$.

a) Montrer que les valeurs propres de $F_n$ appartiennent nécessairement à l'ensemble à quatre éléments $\{\sqrt{n}, -\sqrt{n}, i\sqrt{n}, -i\sqrt{n}\}$.

b) On considère pour $N \ge 3$, donc $n \ge 8$, les deux vecteurs $u$ et $v$ de $\mathbf{C}^n$ définis par :

$$u = \sum_{k=0}^{n-1} \cos\frac{2k\pi}{n} e_k \quad \text{et} \quad v = \sum_{k=0}^{n-1} \sin\frac{2k\pi}{n} e_k .$$

- Calculer $F_n(e_1+e_{n-1})$ en fonction de $u$ et en déduire $F_n(u)$.
- Calculer $F_n(e_1-e_{n-1})$ en fonction de $v$ et en déduire $F_n(v)$.
- En déduire les images des quatre vecteurs suivants par $F_n$, puis conclure :

$$\frac{\sqrt{n}}{2}(e_1+e_{n-1})+u,\ \frac{\sqrt{n}}{2}(e_1+e_{n-1})-u,\ \frac{\sqrt{n}}{2}(e_1-e_{n-1})+v,\ \frac{\sqrt{n}}{2}(e_1-e_{n-1})-v.$$

4°) Etude d'un algorithme récursif de calcul de $Fn(a)$.

A tout élément $a = (a_0, a_1, \dots, a_{n-1})$ de $\mathbf{C}^n$, on associe l'élément $b = (a_0, a_2, a_4, \dots, a_{n-2})$ et l'élément $c = (a_1, a_3, a_5, \dots, a_{n-1})$ de $\mathbf{C}^{n/2}$. On considère alors les transformées de Fourier discrètes de ces deux derniers éléments $b$ et $c$, notées :

$$F_{n/2}(b) = (\beta_0, \beta_1, \dots, \beta_{\frac{n}{2}-1}),\ F_{n/2}(c) = (\gamma_0, \gamma_1, \dots, \gamma_{\frac{n}{2}-1}).$$

a) On suppose connus $F_{n/2}(b)$ et $F_{n/2}(c)$ et l'on considère l'algorithme suivant :

> $E := 1$
> **Pour** $p := 0$ **à** $(n/2)-1$ **faire** :
> **Début** $F := \gamma_p E$ ; $\alpha_p := \beta_p + F$ ; $\alpha_{p+\frac{n}{2}} := \beta_p - F$ ; $E := \omega_n E$ **Fin**

Comparer l'élément $(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ ainsi obtenu à l'issue de cet algorithme à $F_n(a)$, transformée de Fourier discrète de l'élément $a$.

b) On convient d'appeler "opération complexe" l'une des quatre opérations +, –, x, / dans $\mathbf{C}$. On désigne alors par $u_N$ le nombre des opérations complexes nécessaires au calcul de $F_n(a)$ par l'algorithme récursif décrit ci-dessous (sans tenir compte du calcul des nombres $\omega_n$, qui sont supposés connus) :
- Si $N = 0$, on a $F_1(a) = (a)$ et il est donc clair que $u_0 = 0$.
- Sinon, on calcule récursivement $F_{n/2}(b)$ et $F_{n/2}(c)$, ce qui nécessite $2u_{N-1}$ opérations, et l'on obtient $F_n(a)$ par l'algorithme décrit ci-dessus à la question (a).

Exprimer $u_N$ en fonction de $u_{N-1}$ et $N$, et en déduire $u_N$ en fonction de $N$, puis de $n$.

5°) Application au produit rapide de deux polynômes.

On considère ici deux polynômes $P$ et $Q$ à coefficients réels ou complexes dont la somme des degrés respectifs est strictement inférieure à $n$, et le polynôme $R = PQ$. On note :

$$P(X) = \sum_{i=0}^{n-1} p_i X^i,\ Q(X) = \sum_{j=0}^{n-1} q_j X^j,\ R(X) = \sum_{k=0}^{n-1} r_k X^k$$

(les coefficients des polynômes $P$, $Q$, $R$ d'indices strictement supérieurs à leurs degrés respectifs sont nuls) et $p$, $q$ et $p*q$ les trois éléments de $\mathbf{C}^n$ associés aux polynômes $P$, $Q$ et $R = PQ$, soit : $p = (p_0, p_1, \dots, p_{n-1})$, $q = (q_0, q_1, \dots, q_{n-1})$, $p * q = (r_0, r_1, \dots, r_{n-1})$.

Enfin, on note $pq = (p_0q_0, p_1q_1, \dots, p_{n-1}q_{n-1})$ le produit de deux éléments $p$ et $q$ de $\mathbf{C}^n$.

a) Etablir l'égalité $F_n(p*q) = F_n(p)F_n(q)$.

b) On calcule le produit $R = PQ$ en calculant successivement :
- les transformées de Fourier discrètes $F_n(p)$ et $F_n(q)$ par l'algorithme étudié au 4°.
- le produit $F_n(p)F_n(q)$, et donc $F_n(p*q)$.
- la transformée de Fourier discrète inverse $F_n^{-1}(F_n(p*q))$.

Déterminer le nombre d'opérations complexes nécessaires à la réalisation de chacune de ces trois étapes, et en déduire en fonction de $n$ un équivalent du nombre d'opérations nécessaires au calcul du produit $R = PQ$ par cette méthode.

c) Comparer du point de vue du nombre d'opérations effectuées cette méthode à la méthode usuelle de calcul du produit $R = PQ$.

***