Traiter au moins un des deux problèmes suivants – l'indiquer clairement sur la première page

Problème 1 : Autour de la transformée de Fourier discrète

Soient $n, d \in \mathbb{N}^*$. On note $\mathbb{U}_n$ est l'ensemble des racines n-ièmes de l'unité et $\mathbb{U}$ l'ensemble des complexes de module 1.

Le but de ce problème est d'étudier un polynôme complexe $P(X) = \sum_{j=0}^{d} a_j X^j$ de degré d à partir des valeurs qu'il prend sur les racines n-ièmes de l'unité.

1. Expression et majoration des coefficients

1) Montrer l'*inégalité triangulaire généralisée* : pour $(z_1, ..., z_n) \in \mathbb{C}^n$, on a $\left|\sum_{k=1}^{n} z_k\right| \leqslant \sum_{k=1}^{n} |z_k|$, l'égalité ayant lieu si et seulement si tous les z_k non nuls ont même argument *modulo* 2π.

2) Pour $q \in \mathbb{Z}$, montrer que $\frac{1}{n}\sum_{\omega\in\mathbb{U}_n} \omega^q = \begin{cases} 1 & \text{si } n \mid q, \\ 0 & \text{sinon.} \end{cases}$

3) En déduire que pour $k \in [\![0, d]\!]$,
$$\frac{1}{n}\sum_{\omega\in\mathbb{U}_n} P(\omega)\omega^{-k} = \sum_{j\in[\![0,d]\!],\, j\equiv k \bmod n} a_j.$$

4) On suppose uniquement dans cette question que $n > d$. On fixe $k \in [\![0, d]\!]$.
   (a) Etablir l'égalité
   $$a_k = \frac{1}{n}\sum_{\omega\in\mathbb{U}_n} P(\omega)\omega^{-k}.$$
   (b) En déduire l'inégalité
   $$|a_k| \leqslant \max(\{|P(\omega)| \,/\, \omega \in \mathbb{U}_n\}). \tag{1}$$
   et montrer que l'égalité a lieu si P est un monôme de degré k.
   (c) Montrer que l'égalité a lieu dans la formule (1) si et seulement si P est un monôme de degré k.

5) Justifier l'existence de $M(P) = \sup\{|P(z)| \,/\, z \in \mathbb{U}\}$. Montrer que $|a_k| \leqslant M(P)$. Traiter le cas d'égalité.

2. Le principe du maximum pour les polynômes

6) Soient $r \in \mathbb{R}_+^*$, $P \in \mathbb{C}[X]$ non constant et $z_0 \in \mathbb{C}$. Montrer que
$$|P(z_0)| < \sup(\{|P(z)| \,/\, z \in \mathbb{C}, |z - z_0| = r\}).$$
(On pourra utiliser une transformation affine envoyant le cercle de centre 0 et de rayon 1 sur le cercle de centre z_0 et de rayon r.)

3. Une majoration plus forte

On montre ici une majoration plus forte que celle de la première partie :
$$\sum_{k=0}^{d} |a_k|^2 \leqslant M(P)^2,$$

Soient $\overline{P}$ le polynôme conjugué de P et $Q(X) = X^d P(X)\overline{P}\left(\frac{1}{X}\right)$.

7) Montrer que Q est un polynôme et calculer le coefficient devant X^d.

8) Comparer $M(Q)$ et $M(P)$. Démontrer alors l'inégalité voulue.

4. Minoration de $\sup_{[-1,1]} |P|$ pour P unitaire de degré d

On note $\mathcal{N}_d$ l'ensemble des polynômes complexes *normalisés* (ou *unitaires*) de degré d, c'est-à-dire de coefficient dominant $a_d = 1$. On fixe $P \in \mathcal{N}_d$.

9) Etablir l'inégalité $1 \leqslant M(P)$. Quand y-a-t-il égalité ?

10) Justifier l'existence de $N(P) = \sup(\{|P(t)| \,/\, t \in [-1, 1]\})$.

11) Les polynômes de Chebichev sont définis par récurrence par
$$T_0(X) = 1, \qquad T_1(X) = X \qquad \text{et} \quad T_{d+2}(X) = 2XT_{d+1}(X) - T_d(X).$$
   (a) Pour $d \in \mathbb{N}$ et $t \in \mathbb{R}$, vérifier que $T_d(\cos t) = \cos(dt)$.
   (b) Trouver le degré et le coefficient dominant de T_d, pour $d \geqslant 1$.
   (c) Pour $d \geqslant 1$, $S_d(X) = \frac{1}{2^{d-1}} T_d(X)$ appartient à $\mathcal{N}_d$. Montrer que $N(S_d) = \frac{1}{2^{d-1}}$.

12) On prouve ici que, pour $d \geqslant 1$ et $P \in \mathcal{N}_d$, $N(P) \geqslant \frac{1}{2^{d-1}}$, l'égalité ayant lieu si et seulement si $P = S_d$.

(a) On note $R(X) = X^d P\left(\frac{1}{2}\left(X + \frac{1}{X}\right)\right)$. Montrer que R est un polynôme dont on précisera le degré et le coefficient dominant.

(b) Montrer que $M(R) = N(P)$.

(c) Calculer $\sum_{\omega \in \mathbb{U}_{2d}} R(\omega)$ et conclure que $N(P) \geqslant \frac{1}{2^{d-1}}$.

(d) On suppose que $N(P) = \frac{1}{2^{d-1}}$. Pour $\omega \in \mathbb{U}_{2d}$, montrer l'égalité $R(\omega) = \frac{1}{2^{d-1}}$. En déduire que $P = S_d$.

5. Polynômes de $\mathbb{Z}[X]$ majorés par 1 sur $\mathbb{U}_n$

On suppose ici que P est à coefficients dans $\mathbb{Z}$ et que $z \mapsto |P(z)|$ est majorée par 1 sur $\mathbb{U}_n$ et s'annule au moins une fois sur $\mathbb{U}_n$. On va montrer par récurrence sur le degré que P s'annule sur les autres racines n−ièmes de l'unité.

13) On traite d'abord le cas $\deg(P) = d < n$. Montrer à l'aide de (1) que les coefficients de P sont majorés en valeur absolue par $\frac{n-1}{n}$. Conclure.

14) On revient au cas général. En reprenant l'algorithme de la division euclidienne, montrer que le quotient Q et le reste R dans la division de P par $X^n - 1$ sont à coefficients entiers relatifs.

15) Comparer $P(\omega)$ et $R(\omega)$ pour $\omega \in \mathbb{U}_n$. Conclure.

6. Interprétation de la formule (1) pour $k = 0$

16) Si $z_0, ..., z_{n-1}$ sont les affixes des sommets d'un polygone régulier de centre d'affixe 0, montrer que pour tout $P \in \mathbb{C}_{n-1}[X]$, $P(0) = \frac{1}{n}\sum_{p=0}^{n-1} P(z_p)$.

Montrer que la relation (1) lorsque $k = 0$ n'est qu'un cas particulier de cette égalité.

17) On veut établir la réciproque de la question 16. On suppose que $z_0, ..., z_{n-1}$ sont deux-à-deux distincts et que tout $P \in \mathbb{C}_{n-1}[X]$ vérifie la condition

$$P(0) = \frac{1}{n}\sum_{k=0}^{n-1} P(z_k). \tag{2}$$

On introduit les polynômes suivants :

$$\varphi(X) = \prod_{k=0}^{n-1}(X - z_k) \quad \text{et pour } k \in [\![0, n-1]\!], \varphi_k(X) = \prod_{\substack{0 \leqslant l \leqslant n-1 \\ l \neq k}} (X - z_l).$$

(a) Soit $Q \in \mathbb{C}[X]$, $p_1, \ldots, p_r \in \mathbb{N}^*$ et $b_1, \ldots, b_r$ des nombres complexes distincts. On suppose que $\frac{Q'}{Q} = \sum_{k=1}^{r} \frac{p_k}{X - b_k}$. Montrer qu'il existe $\mu \in \mathbb{C}^*$ tel que $Q = \mu \prod_{k=1}^{r} (X - b_k)^{p_k}$.

(b) Pour $(i, j) \in [\![0, n-1]\!]^2$, montrer que $\varphi_i(z_j) = \begin{cases} \varphi'(z_i) & \text{si } i = j, \\ 0 & \text{sinon.} \end{cases}$

(c) Montrer que $\frac{X}{n}\varphi'(X) + \varphi(0)$ et φ ont même degré et même coefficient dominant.

(d) Montrer que $\frac{X}{n}\varphi'(X) + \varphi(0)$ a les mêmes racines que φ. (Utiliser (2).)

(e) Prouver que $\frac{X}{n}\varphi'(X) + \varphi(0) = \varphi(X)$.

(f) En déduire que $z_0, ..., z_{n-1}$ sont les affixes des sommets d'un polygone régulier centré en 0.

Problème 2 – Polynômes cyclotomiques

Le but du problème est de donner la décomposition en produit d'irréductibles sur $\mathbb{Q}$ de X^n-1 lorsque n est un entier naturel non-nul. Le résultat et la preuve sont dus à Gauss.

On désigne par $\mathbb{Z}[X]$ l'ensemble des polynômes en l'indéterminée X à coefficients entiers relatifs. On prendra garde que $\mathbb{Z}$ n'est pas un corps, donc que certaines propriétés du cours ne s'appliquent pas à $\mathbb{Z}[X]$. Évidemment, $\mathbb{Z}[X]$ est un anneau pour la somme et le produit des polynômes. On désigne par $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ lorsque p est un entier premier.

Soient $n\in\mathbb{N}^*$ et $z_k=\exp\left(2i\pi\dfrac{k}{n}\right)$ avec $k\in\mathbb{Z}$.

Partie 1 : Calculs préliminaires

1) Donner la décomposition de X^n-1 en produits d'irréductibles sur $\mathbb{C}$.
2) Soient $a,b\in\mathbb{C}$. Montrer que $\prod_{k=1}^{n}(a+bz_k)=a^n+(-1)^{n-1}b^n$.
3) Soit $\theta\in\mathbb{R}$. Montrer que $\prod_{k=1}^{n}(z_k^2-2(\cos\theta)z_k+1)=2(1-\cos n\theta)$.

Partie 2 : Réduction *modulo* p

Soit p un entier naturel premier. Pour tout entier relatif k, on note $\overline{k}$ sa classe modulo p. On appelle *réduction modulo p* du polynôme $P=\sum_k a_kX^k$ le polynôme noté $\overline{P}$ de $\mathbb{F}_p[X]$ défini par $\sum_k \overline{a_k}X^k$. On a évidement $\overline{P+Q}=\overline{P}+\overline{Q}$ et $\overline{PQ}=\overline{P}\,\overline{Q}$.

4) On suppose dans cette question que p est le nombre premier 1789. (On ne justifiera pas la primalité de p.) Déterminer une relation de Bézout entre p et $k=2018$. En déduire l'inverse de $\overline{2018}$ dans $\mathbb{F}_p$. (On fera apparaître la méthode et les calculs de la manières la plus concise mais complète possible.)
5) Montrer que pour tout $k\in[\![1,p-1]\!]$, p divise le coefficient binomial $\binom{p}{k}$.
6) En déduire que pour $A,B\in\mathbb{F}_p[X]$, $(A+B)^p=A^p+B^p$.
7) Montrer que si $\sum_{k=0}^{d}a_kX^k\in\mathbb{Z}[X]$, alors $\left(\sum_{k=0}^{d}\overline{a_k}X^k\right)^p=\sum_{k=0}^{d}\overline{a_k}X^{kp}$.

Partie 3 : Racines primitives de l'unité

On rappelle que la *fonction indicatrice d'Euler* φ est définie par $\varphi(n)=\mathrm{Card}\{k\mid 1\leqslant k\leqslant n \text{ et } \mathrm{pgcd}(n,k)=1\}$. Autrement dit, $\varphi(n)$ est le nombre d'entiers $\leqslant n$ premiers à n.

On appelle *racine primitive n-ième de l'unité* toute racine n-ième de l'unité ζ telle que $\zeta^q\neq 1$ si $1\leqslant q\leqslant n-1$. Autrement dit, une racine n-ième de l'unité est primitive si elle n'est pas racine q-ième de l'unité pour un q strictement plus petit. Soit Z_n l'ensemble des racines primitives n-ième de l'unité.

On définit le n-ième *polynôme cyclotomique* Φ_n par

$$\Phi_n=\prod_{\zeta\in Z_n}(X-\zeta).$$

8) A quelle condition sur k a-t-on z_k racine primitive n-ième ?
9) Déterminer les racines primitives n-ièmes de l'unité pour $n=2,3,4,5,6$.
10) Déterminer $\Phi_2,\Phi_3,\Phi_4,\Phi_5,\Phi_6$. (On veut leurs coefficients.)
11) Déterminer $\deg\Phi_n$.
12) Montrer que $X^n-1=\prod_{d\mid n}\Phi_d$.
13) En déduire $\sum_{d\mid n}\varphi(d)$.
14) Soit $A,B\in\mathbb{Z}[X]$ avec B unitaire. Montrer que le quotient et le reste de la division euclidienne de A par B sont encore à coefficients entiers. (On pourra raisonner par récurrence sur $\deg A$.)
15) Montrer que Φ_n est à coefficients entiers.

Partie 4 : Irréductibilité sur $\mathbb{Q}$

On appelle *contenu* du polynôme $P\in\mathbb{Z}[X]$ le $pgcd$ des coefficients de P. On note $c(P)$ le contenu de P. Un polynôme est *primitif* si son contenu est 1.

16) Montrer que si $P,Q\in\mathbb{Z}[X]$ sont primitifs, PQ aussi. (Raisonner par l'absurde : sinon il existerait un diviseur premier p de $c(PQ)$; considérer alors le plus grand coefficient non divisible par p de P et Q - ou réduire modulo p, ce qui revient au même.)

17) Montrer que si $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$.

18) Soit $P \in \mathbb{Z}[X]$. On suppose que P n'est pas irréductible sur $\mathbb{Q}$. Montrer qu'il existe $A, B \in \mathbb{Z}[X]$ de degrés $\geqslant 1$ tels que $P = AB$.

19) On se propose de montrer le *critère d'Eisenstein* : soit $d \in \mathbb{N}^*$ et $P \in \mathbb{Z}[X]$, $P = a_d X^d + \cdots + a_1 X + a_0$ avec $a_d \neq 0$. On suppose qu'il existe un nombre premier p tel que :
   (a) p ne divise pas a_d ;
   (b) p divise $a_0, a_1, \ldots, a_{d-1}$;
   (c) p^2 ne divise pas a_0.
   Montrer que P est irréductible sur $\mathbb{Q}$. (Regarder modulo p et utiliser l'unicité de l'écriture comme produit d'irréductibles dans $\mathbb{F}_p[X]$.)

20) Application 1 : Montrer que $X^n - 2$ est irréductible sur $\mathbb{Q}$. *(Il existe donc des polynômes irréductibles de tout degré sur $\mathbb{Q}$.)*

21) Application 2 : Soit p premier. Déterminer $\Phi_p \circ (X+1)$. Montrer que ce polynôme est irréductible sur $\mathbb{Q}$ et en déduire que Φ_p est irréductible sur $\mathbb{Q}$.

22) Soit p un nombre premier et $\zeta = \exp\dfrac{2i\pi}{p}$. Montrer que pour tout $P \in \mathbb{Q}[X]$, $P(\zeta) = 0$ si et seulement si Φ_p divise P.

23) Soient $P, Q \in \mathbb{Q}[X]$ unitaires tels que $PQ \in \mathbb{Z}[X]$. Montrer que $P, Q \in \mathbb{Z}[X]$.

Partie 5 : Irréductiblité de Φ_n

On considère le lemme suivant :

Lemme 1 *Soit p un nombre premier ne divisant pas n, $A \in \mathbb{Q}[X]$ un facteur unitaire irréductible sur $\mathbb{Q}$ de Φ_n et ζ une racine primitive n-ième de l'unité telle que $A(\zeta) = 0$. Alors $A(\zeta^p) = 0$.*

24) On considère $\overline{\Phi_n} \in \mathbb{F}_p[X]$. Montrer qu'il n'existe pas de polynôme non-constant $B \in \mathbb{F}_p[X]$ tel que B^2 divise $\overline{X^n - 1}$. (Considérer $X(X^n-1)' - n(X^n-1)$.)

25) Soient $U, V \in \mathbb{Q}[X]$ et $z \in \mathbb{C}$ tels que $U(z) = V(z) = 0$. Montrer que si U est irréductible sur $\mathbb{Q}$, U divise V.

26) Sous les hypothèses du lemme : soit B unitaire tel que $\Phi_n = AB$. Montrer par l'absurde que $B(\zeta^p) \neq 0$. (Sinon $B \circ X^p = AC$; réduire modulo p et considérer un facteur irréductible sur $\mathbb{F}_p$ de $\overline{A}$.) En déduire le lemme.

27) Montrer que $A = \Phi_n$.

Donc Φ_n est irréductible sur $\mathbb{Q}$.