Le candidat peut traiter l'une quelconque des parties en admettant les résultats précédemment énoncés dans les autres parties. On attire l'attention du candidat sur le fait qu'une fois admis les résultats du V, la dernière partie du problème est indépendante des parties précédentes.

Les symboles n, m (respectivement x) désigneront des nombres entiers (respectivement un nombre réel) ≥ 1.

Le symbole p désignera toujours un **nombre premier**.

On désigne par $v_p(n)$ la plus grande puissance, éventuellement nulle, de p divisant n.

L'entier $[x]$ désigne la partie entière de x.

Si f, g sont deux fonctions numériques définies au voisinage de $+\infty$, l'écriture $f = O(g)$ signifie que f est produit de g par une fonction bornée au voisinage de $+\infty$.

De même, si u_n et v_n sont deux suites à valeurs complexes, l'écriture $u_n = O(v_n)$ signifie que la suite u_n est produit de la suite v_n par une suite bornée au voisinage de $+\infty$.

La notation $\sum_{d|n} u_d$ désigne la somme des u_d étendue aux entiers $d \geq 1$ divisant n.

On désigne par ln le logarithme népérien.

On se donne un entier non nul N fixé une fois pour toutes.

On note $G(N)$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/N\mathbb{Z}$.

Préliminaire

1. Soit $\sum_{n\geq 1} u_n$, $\sum_{n \geq 1} v_n$ deux séries de nombres complexes. Soit $U_n = \sum_{k=1}^{n} u_k$ la somme partielle. Vérifier l'égalité

$$\sum_{k=1}^{n} u_k v_k = U_n v_n + \sum_{k=1}^{n-1} U_k (v_k - v_{k+1}).$$

I

Soit G un groupe commutatif fini dont on notera la loi *multiplicativement*. On dit qu'un homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^*$ est un caractère de G. Soient χ et χ' deux caractères de G. Le produit $\chi\chi'$ est défini par la formule :

$$\chi\chi'(g) = \chi(g)\chi'(g) \text{ pour } g \in G.$$

On note 1 le caractère constant de valeur 1. L'ensemble $\hat{G}$ des caractères de G est ainsi muni d'une loi de groupe d'élément neutre 1.

On note $\hat{\hat{G}}$ le groupe des caractères de $\hat{G}$.

On note enfin $\bar{\chi}$ le caractère qui à $g \in G$ associe le conjugué $\overline{\chi(g)}$ de $\chi(g)$.

Pour tout $x \in G$, considérons l'application $\phi_x \in \hat{\hat{G}}$:

$$\begin{cases} \hat{G} & \rightarrow & \mathbb{C}^* \\ \chi & \longmapsto & \chi(x) \end{cases}$$

On veut d'abord prouver que le morphisme

$$(*) \qquad \begin{cases} G & \rightarrow & \hat{\hat{G}} \\ x & \longmapsto & \phi_x \end{cases}$$

est injectif.

1. Soit $x \in G$, $x \neq 1$ et $gr(x)$ le sous-groupe de G engendré par x. Montrer qu'il existe un caractère χ de $gr(x)$ tel que $\chi(x) \neq 1$.

2. Soit F la famille des sous-groupes H de G contenant $gr(x)$ tels que χ se prolonge en un caractère de H. Montrer que F admet un élément G' de cardinal maximal. Supposons $G' \neq G$. Soit y un élément de G qui n'est pas dans G'.
En considérant le plus petit $n \geq 1$ tel que $y^n \in G'$, entier dont on justifiera l'existence, montrer que l'on peut prolonger χ au groupe engendré par y et G'. Conclure.

3. Soit $\chi' \in \hat{G}$ et $x \in G$. Comparer les sommes

$$\sum_{\chi \in \hat{G}} \chi(x) \; et \; \sum_{\chi \in \hat{G}} \chi\chi'(x).$$

En choisissant χ' convenablement, montrer les formules :

$$\sum_{\chi \in \hat{G}} \chi(x) = 0 \; si \; x \neq 1$$

$$\sum_{\chi \in \hat{G}} \chi(x) = \text{card } \hat{G} \; si \; x = 1.$$

Montrer de même les formules :

$$\sum_{x \in G} \chi(x) = 0 \; si \; \chi \neq 1$$

$$\sum_{x \in G} \chi(x) = \text{card } G \; si \; \chi = 1.$$

4. En considérant la somme $\sum_{\chi, x} \chi(x)$, montrer card G = card $\hat{G}$. Que dire alors du morphisme $G \rightarrow \hat{\hat{G}}$ décrit en $(*)$?

II

On rappelle que le symbole p désigne un **nombre premier**.

On rappelle la formule $\ln n! = n\ln n - n + O(\ln n)$.

1. Montrer l'égalité

$$v_p(n!) = \sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right].$$

En déduire l'inégalité

$$\frac{n}{p} - 1 < v_p(n!) \leq \frac{n}{p} + \frac{n}{p(p-1)}$$

2. En considérant l'expression $(1+1)^{2m+1}$, montrer $C_{2m+1}^{m} \leq 4^m$. En déduire la majoration

$$\prod_{m+1<p\leq 2m+1} p \leq 4^m.$$

3. Montrer par récurrence sur n l'inégalité $\prod_{p\leq n} p \leq 4^n$.

4. En considérant $\ln(n!)$, montrer l'estimation

$$\sum_{p\leq x}\frac{\ln p}{p} = \ln x + O(1).$$

III

Par caractère, on entendra toujours caractère de $G(N)$. On dira qu'un caractère $\chi \neq 1$ est non trivial. On notera encore χ la fonction de $\mathbf{N}$ dans $\mathbf{C}$ définie par $\chi(m) = \chi(m \bmod N)$ si m et N sont premiers entre eux et $\chi(m) = 0$ sinon. On a la formule $\chi(ab) = \chi(a)\chi(b)$ pour tout a, b.

1. Soit χ un caractère non trivial. Montrer que la série $\sum_{n\geq 1}\frac{\chi(n)}{n}$ (respectivement $\sum_{n\geq 1}\frac{\chi(n)\ln(n)}{n}$) converge. On note $L(\chi)$ (respectivement $L_1(\chi)$) sa somme.

Dans cette partie χ est désormais un caractère non trivial à valeurs **réelles**.

2. Soit $f(n) = \sum_{d|n}\chi(d)$. Montrer $f(nm) = f(n)f(m)$ si $\mathrm{pgcd}(n, m) = 1$. En déduire les minorations

$$f(n) \geq 1 \text{ si } n \text{ est un carré et } f(n) \geq 0 \text{ sinon.}$$

Pour $x \geq 0$, soit $g(x) = \sum_{n\leq x}\frac{f(n)}{\sqrt{n}}$. Quel est le comportement de g au voisinage de $+\infty$?

3. Montrer très soigneusement l'égalité :

$$g(x) = \sum_{d'\leq\sqrt{x}}\frac{1}{\sqrt{d'}}\sum_{\sqrt{x}<d\leq\frac{x}{d'}}\frac{\chi(d)}{\sqrt{d}} + \sum_{d\leq\sqrt{x}}\frac{\chi(d)}{\sqrt{d}}\sum_{d'\leq\frac{x}{d}}\frac{1}{\sqrt{d'}}.$$

Grâce à une analyse minutieuse des deux membres de la somme, montrer que la différence $g(x) - 2\sqrt{x}L(\chi)$ est bornée.

4. Montrer que $L(\chi)$ est non nul dans ce cas.

IV

1. On note $\mu(n)$ l'entier défini par :

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier} \\ (-1)^r & \text{si } r \text{ est le nombre de facteurs premiers distincts de } n, \\ & n \text{ non divisible par le carré d'un nombre premier} \end{cases}$$

Montrer que pour tout $n \neq 1$, on a l'égalité $\sum_{d|n} \mu(d) = 0$.

2. Soit H une fonction non nulle de $\mathbb{N}^*$ dans $\mathbb{C}$ telle que $\forall n, m \in \mathbb{N}, H(nm) = H(n)H(m)$.
Calculer $H(1)$.
On se donne également deux fonctions F et G de $[1, +\infty[$ dans $\mathbb{C}$ telles que :

$$\forall x \in [1, +\infty[, G(x) = \sum_{1 \leq k \leq x} F(\frac{x}{k})H(k)$$

Montrer la formule :

$$\forall x \in [1, +\infty[, F(x) = \sum_{1 \leq k \leq x} \mu(k)G(\frac{x}{k})H(k)$$

3. Soit Λ la fonction de $[1, +\infty[$ dans $\mathbb{R}$ qui à p^n associe $\ln p$ et qui est nulle sur tous les réels qui ne sont pas des entiers de la forme p^n. Montrer la formule :

$$\Lambda(m) = \sum_{d|m} \mu(d) \ln (\frac{m}{d}).$$

V

Soit χ un caractère non trivial (pas forcément à valeurs réelles).
1. Posons $G(x) = \sum_{1 \leq n \leq x} \frac{x}{n}\chi(n)$. Montrer que $G(x) - xL(\chi)$ est borné.

Supposons $L(\chi) \neq 0$. En utilisant le IV, déduire que $\sum_{n \leq x} \frac{\mu(n)\chi(n)}{n}$ est borné.
2. Supposons $L(\chi) = 0$. Posons $G_1(x) = \sum_{1 \leq n \leq x} (\frac{x}{n} \ln \frac{x}{n})\chi(n)$.
Montrer que $G_1(x) = -xL_1(\chi) + O(\ln (x))$. Comme en 1, déduire que la fonction

$$L_1(\chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} + \ln (x)$$

est bornée.

3. En utilisant le IV, montrer

$$L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n}=\sum_{p\leq x}\frac{\chi(p)\ln p}{p}+O(1).$$

4. Déduire de ce qui précède :

$$\sum_{p\leq x}\frac{\chi(p)\ln (p)}{p}=\begin{cases}O(1) & \text{si } L(\chi)\neq 0\\ -\ln (x)+O(1) & \text{si } L(\chi)=0\end{cases}$$

5.Soit T le nombre de caractères non triviaux tels que $L(\chi) = 0$. En considérant l'expression :

$$\sum_{\chi\in G(N)}\sum_{p\leq x}\frac{\chi(p)\ln p}{p},$$

montrer l'estimation

$$\text{card } G(N). \sum_{\substack{p\leq x\\ p\equiv 1 \bmod N}}\frac{\ln p}{p}=(1-T)\ln x+O(1).$$

En déduire $T\leq 1$.

6. Montrer que T est nul (on distinguera le cas où χ est à valeurs réelles ou complexes).

7. Soit l un entier premier à N. Montrer en considérant la somme

$$\sum_{\chi\in G(N)}\sum_{p\leq x}\bar{\chi}(l)\frac{\chi(p)\ln p}{p}$$

que $\{p$ premier/ $p\equiv l \mod n\}$ est infini.

VI

Soit P un polynôme non nul à coefficients entiers. On note $c(P)$ le plus grand diviseur commun des coefficients de P.

1. Montrer que si P et Q sont deux polynômes non nuls à coefficients entiers, alors

$$c(PQ)=c(P)c(Q).$$

(On pourra se ramener à $c(P)=c(Q)=1$ et considérer alors un éventuel diviseur premier de $c(PQ)$).

2. Soit ζ une racine n-ième de l'unité. Soit P_ζ le polynôme à coefficients dans $\mathbf{Q}$ unitaire de plus petit degré qui annule ζ. Montrer que P_ζ est à coefficients entiers.

On note $\mathbf{Z}[\zeta]$ (resp. $\mathbf{Q}[\zeta]$) le sous-anneau de $\mathbf{C}$ engendré par $\mathbf{Z}$ et ζ (resp. par $\mathbf{Q}$ et ζ). Soit d le degré de P_ζ.

3. Montrer que $\mathcal{B} = (1, \zeta, \ldots, \zeta^{d-1})$ est une base du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}[\zeta]$.

4. Soit P un polynôme à coefficients entiers. Montrer que pour tout nombre premier p, il existe un polynôme G_p à coefficients entiers tel que

$$P(X^p) = P(X)^p + pG_p(X).$$

Pour tout $x \in \mathbf{Z}[\zeta]$, on définit $M(x)$ comme la matrice dans $\mathcal{B}$ de l'application $\mathbf{Q}$-linéaire

$$\begin{cases} \mathbf{Q}[\zeta] & \to & \mathbf{Q}[\zeta] \\ y & \longmapsto & xy \end{cases}$$

5. En utilisant V.7 et en considérant des matrices $M(x)$ pour $x \in \mathbf{Q}[\zeta]$ convenables, montrer que si l est un entier premier à n, on a

$$P_\zeta(\zeta^l) = 0.$$

6. Montrer que la réunion des ensembles

$$E_d = \left\{ \frac{k}{d},\ \mathrm{pgcd}(k, d) = 1 \text{ et } 1 \leq k \leq d \right\}$$

pour $d \geq 1$ divisant n est égale à

$$\left\{ \frac{k}{n},\ k = 1, \ldots, n \right\}$$

et que les ensembles E_d, l'entier d parcourant les diviseurs ≥ 1 de n, sont deux à deux disjoints. Notons $\Phi_n(X)$ le polynôme

$$\Phi_n(X) = \prod_{\substack{\mathrm{pgcd}(k,n)=1 \\ 1 \leq k \leq n}} \left(X - \exp(\frac{2ik\pi}{n}) \right).$$

Montrer l'identité

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

En déduire que Φ_n est à coefficients entiers pour tout n.

7. Qu'en déduire sur P_ζ ?