Composition commune aux ENS Paris et Lyon
ENS MP 1993

Une fois admis les résultats de la partie 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) supérieurs à 1. Le symbole p désignera toujours un **nombre premier**.

On désigne par $v_p(n)$ la valuation p-adique de n. L'entier $[x]$ désigne la partie entière de x. La notation $n \wedge m$ désigne le pgcd de n et m.

La notation $\sum_{d|n} u_d$ désigne la somme des u_d étendue aux entiers d supérieurs à 1 et 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 $\mathbf{Z}/N\mathbf{Z}$ et $m \mod N$ la classe de m modulo N.

Préliminaires

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

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

PARTIE I

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

$$\forall g \in G \qquad \chi\chi'(g) = \chi(g)\chi'(g) \ .$$

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

Pour g dans G, on note φ_g l'élément de $\hat{\hat{G}}$ donné par $\varphi_g(\chi) = \chi(g)$. On veut d'abord démontrer que le morphisme de G dans $\hat{\hat{G}}$ qui à g associe φ_g est injectif.

1. Soit g dans G distinct de 1 et $\langle g \rangle$ le sous-groupe de G engendré par g. Montrer qu'il existe un caractère χ de $\langle g \rangle$ tel que $\chi(g) \neq 1$.
2. Soit F la famille des sous-groupes H de G contenant $\langle g \rangle$ 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 supérieur à 1 tel que y^n appartienne à G', entier dont on justifiera l'existence, montrer que l'on peut prolonger χ au groupe engendré par y et G'. Conclure.
3. Soit χ' dans $\hat{G}$ et g dans G. Comparer les sommes

   $$\sum_{\chi \in \hat{G}} \chi(g) \text{ et } \sum_{\chi \in \hat{G}} \chi\chi'(g) \ .$$

   En choisissant χ' convenablement, montrer les formules :

   $$\sum_{\chi \in \hat{G}} \chi(g) = \mathrm{Card}(\hat{G})\delta_{g,1} \quad \text{et} \quad \sum_{g \in G} \chi(g) = \mathrm{Card}(G)\delta_{\chi,1}$$

   où δ représente le symbole de Kronecker : $\delta_{a,b} = 1$ si $a = b$ et $\delta_{a,b} = 0$ sinon.

4. En considérant $\sum_{\chi,g} \chi(g)$, montrer $\mathrm{Card}(G) = \mathrm{Card}(\hat{G})$. Que dire alors du morphisme $g \mapsto \varphi_g$?

PARTIE 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 $v_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k}\right]$ et en déduire l'inégalité $\frac{n}{p} - 1 < v_p(n!) \leq \frac{n}{p} + \frac{n}{p(p-1)}$.
2. Montrer successivement les majorations $\binom{2m+1}{m} \leq 4^m$ et $\prod_{m+1<p\leq 2m+1} p \leq 4^m$.
3. Montrer par récurrence sur n l'inégalité $\prod_{p\leq n} p \leq 4^n$.
4. En considérant $\ln(n!)$, montrer l'estimation $\sum_{p\leq x} \frac{\ln(p)}{p} = \ln(x) + O(1)$.

PARTIE III

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

1. Soit χ un caractère non trivial. Montrer que les séries $\sum_{n\geq 1} \frac{\chi(n)}{n}$ et $\sum_{n\geq 1} \frac{\chi(n)\ln(n)}{n}$ convergent. On note $L(\chi)$ et $L_1(\chi)$ leurs sommes respectives.
   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 n et m sont premiers entre eux. En déduire les minorations $f(n) \geq 1$ si n est un carré et $f(n) \geq 0$ sinon. Pour x positif, 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 :

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

   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.

PARTIE IV

1. On note $\mu(n)$ l'entier défini par $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier et sinon $\mu(n) = (-1)^r$ où r est le nombre de facteurs premiers distincts de n. Montrer que pour tout n distinct de 1, on a l'égalité $\sum_{d|n} \mu(d) = 0$.

2. Soit H une fonction non nulle de $\mathbf{N}^*$ dans $\mathbf{C}$ telle que pour tous n et m entiers $H(nm) = H(n)H(m)$. Calculer $H(1)$.

   On se donne également deux fonctions F et G de $[1;+\infty[$ dans $\mathbf{C}$ telles que :

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

   Montrer la formule $\forall x \in [1;+\infty[,\ F(x) = \displaystyle\sum_{1\leq k\leq x} \mu(k) G\left(\frac{x}{k}\right) H(k)$.

3. Soit Λ la fonction de $[1;+\infty[$ dans $\mathbf{R}$ 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 :

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

PARTIE V

Soit χ un caractère non trivial (pas forcément à valeurs réelles).

1. Posons $G(x) = \displaystyle\sum_{1\leq n\leq x} \frac{x}{n}\chi(n)$. Montrer que $G(x) - xL(\chi)$ est borné.

   En utilisant la partie IV, montrer que si on a $L(\chi) \neq 0$, alors $\displaystyle\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n}$ est borné.

2. Supposons $L(\chi) = 0$.

   Posons $G_1(x) = \displaystyle\sum_{1\leq n\leq x} \left(\frac{x}{n}\ln\left(\frac{x}{n}\right)\right)\chi(n)$. Montrer $G_1(x) = -xL_1(\chi) + O\left(\ln(x)\right)$ et, comme précédemment, en déduire que si on a $L(\chi) = 0$, alors $L_1(\chi)\displaystyle\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} + \ln(x)$ est borné.

3. En utilisant la partie IV, montrer $L_1(\chi)\displaystyle\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} = \sum_{p\leq x} \frac{\chi(p)\ln(p)}{p} + O\left(1\right)$.

4. Déduire de ce qui précède :

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

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 $\operatorname{Card} G(N) \displaystyle\sum_{\substack{p\leq x \\ p\equiv 1 \pmod N}} \frac{\ln(p)}{p} = (1-T)\ln(x) + O\left(1\right)$ et 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

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

   que $\{p \text{ premier } \mid p \equiv \ell \pmod n\}$ est infini.

PARTIE 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 (respectivement par $\mathbf{Q}$ et ζ). Soit d le degré de P_ζ.
3. Soit $\mathcal{B} = (1, \zeta, \ldots, \zeta^{d-1})$. Montrer que $\mathcal{B}$ 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 $P(X^p) = P^p + pG_p$.

   Pour tout x dans $\mathbf{Z}[\zeta]$, on définit $M(x)$ comme la matrice dans $\mathcal{B}$ de l'endomorphisme du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}[\zeta]$ donné par $y \mapsto xy$.
5. En utilisant la question V.7 et en considérant des matrices $M(x)$ pour x dans $\mathbf{Q}[\zeta]$ convenables, montrer que si ℓ est un entier premier à n, on a $P_\zeta(\zeta^\ell) = 0$.
6. Montrer que la réunion des ensembles donnés par

$$E_d = \left\{ \frac{k}{d} \;\middle|\; k \wedge d = 1 \text{ et } 1 \leq k \leq d \right\},$$

   pour d supérieur à 1 et divisant n, est égale à

$$\left\{ \frac{k}{n} \;\middle|\; k \in [\![1; n]\!] \right\}$$

   et que les ensembles E_d, l'entier d parcourant les diviseurs supérieur à 1 de n, sont deux à deux disjoints. Notons Φ_n le polynôme

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

   Montrer l'identité

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

   En déduire que Φ_n est à coefficients entiers pour tout n.
7. Qu'en déduire sur P_ζ ?

Composition commune aux ENS Paris et Lyon – ENS MP 1993

Préliminaires

Pour k entier supérieur à 1, on a, en notant $\Delta a_k = a_{k+1} - a_k$ et en soustrayant la seconde colonne à la première,

$$\Delta(Uv)_k = \begin{vmatrix} U_{k+1} & U_k \\ v_k & v_{k+1} \end{vmatrix} = \begin{vmatrix} u_{k+1} & U_k \\ -\Delta v_k & v_{k+1} \end{vmatrix} = u_{k+1}v_{k+1} + U_k \Delta v_k$$

et donc en sommant de 1 à $n-1$ (avec la convention qu'une telle somme est nulle si $n = 1$) et en remarquant que le membre de gauche donne naissance à une somme téléscopique, il vient

$$U_n v_n - U_1 v_1 = \sum_{k=1}^{n-1} U_k(v_{k+1} - v_k) + \sum_{k=1}^{n-1} u_{k+1}v_{k+1}$$

puis, en réindexant la dernière somme et en tenant compte de $U_1 = u_1$,

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

PARTIE I

1. Comme $\langle g \rangle$ est cyclique, il est isomorphe à $\mathbf{Z}/m\mathbf{Z}$ et donc aussi à $\mathbf{U}_m$ (groupe des racines m-ièmes de l'unité dans $\mathbf{C}$) où m est l'ordre de g dans G. Comme g est distinct de 1, m est strictement supérieur à 1. Dans $\mathbf{U}_m$ le morphisme identique est un caractère de $\mathbf{U}_m$ qui ne prend la valeur 1 que sur 1. Via l'isomorphisme on en déduit un caractère de $\langle x \rangle$ qui ne prend la valeur 1 que sur 1_G. En particulier un tel caractère χ de $\langle g \rangle$ vérifie $\boxed{\chi(g) \neq 1.}$

2. L'ensemble $\{\mathrm{Card}(H) \mid H \in F\}$ est une partie de $\mathbf{N}$ puisque G, et donc aussi les éléments de F, est fini. C'est une partie non vide puisque F contient $\langle x \rangle$. Enfin elle est majorée toujours parce que G est fini et donc $\mathrm{Card}(G)$ est un majorant de l'ensemble considéré. Elle admet donc un élément maximal, i.e. $\boxed{F \text{ admet un élément } G' \text{ de cardinal maximal.}}$

   L'ensemble $\{m \in \mathbf{N}^* \mid y^m \in G'\}$ est une partie de $\mathbf{N}$ par définition. Elle est non vide puisqu'elle contient l'ordre de y, qui est fini puisque G l'est, car G' contient 1 en tant que sous-groupe de G. On dispose donc de $\boxed{n \text{ minimal dans } \mathbf{N}^* \text{ tel que } y \in G'.}$

   Soit alors χ' un caractère de G' prolongeant χ et $a = \chi'(y^n)$. Puisque $\mathbf{C}$ est algébriquement clos, d'après le théorème fondamental de l'algèbre, on dispose de b une racine n-ième de a dans $\mathbf{C}$. Pour m dans $\mathbf{Z}$ et g dans G', on pose alors $\chi''(y^m g) = b^m \chi'(g)$. On montre tout d'abord que cette définition est licite, autrement dit que si $y^m g = y^k g'$ pour m et k entiers et g et g' dans G', alors $b^m\chi'(g) = b^k\chi'(g')$. Dans un tel cas, puisque $g'g^{-1}$ est un élément de G, y^{m-k} est à la fois dans $\langle y \rangle$ et G'. En effectuant la division euclidienne de $m-k$ par n, on dispose de q entier et r dans $[\![0; n-1]\!]$ tels que $m - k = qn + r$. Comme y^n et donc aussi y^{qn} appartiennent aux sous-groupes $\langle y \rangle$ et G', on en déduit que c'est aussi le cas de y^r et donc $r = 0$ par minimalité de n. On en déduit $g'g^{-1} = y^{qn} = (y^n)^q$ et donc, puisque χ' est un caractère, $\chi'(g')\chi'(g)^{-1} = \chi'(y^n)^q = a^q = b^{qn} = b^{m-k}$ et il vient donc $\chi'(g')b^k = \chi(g)b^m$. Enfin on a $\chi''_{|G'} = \chi'$ par construction et donc aussi $\chi''_{|G} = \chi'_{|G} = \chi$ puisque χ' prolonge χ à G'. Autrement dit $\boxed{\text{on peut prolonger } \chi \text{ au groupe engendré par } y \text{ et } G'.}$

   L'hypothèse $G' \neq G$ conduit donc à une absurdité car le groupe engendré par G' et y est de cardinal strictement supérieur à celui de G', puisque $y \notin G'$, et on en déduit $G' = G$, i.e. pour tout g dans G distinct de 1, on dispose d'un caractère χ de G tel que $\chi(g)$ soit distinct de 1 et donc aussi $\varphi_g(\chi) \neq 1$. Autrement dit $\varphi_g \neq 1$. Puisqu'on a affaire à un morphisme de groupes, on en déduit que le morphisme de groupes $g \mapsto \varphi_g$ est $\boxed{\text{injectif}}$.

3. Puisque $\hat{G}$ est un groupe la multiplication à droite par χ' est une bijection de $\hat{G}$ dans lui-même. De plus, d'après le théorème de Lagrange, un élément de $\hat{G}$ est à valeurs dans les racines de l'unité d'ordre $|G|$ et donc $\hat{G}$ est un ensemble de fonctions entre deux ensembles finis (de cardinal $|G|$), donc est fini. On en déduit, par réindexation et commutativité de l'addition dans $\mathbf{C}$,

$$\boxed{\sum_{\chi\in\hat{G}} \chi\chi'(g) = \sum_{\chi\in\hat{G}} \chi(g).}$$

Si g est distinct de 1, on dispose d'après ce qui précède de χ' dans $\hat{G}$ tel que $\chi'(g)$ soit distinct de 1. Or, par définition de la loi de groupe dans $\hat{G}$, on a aussi $\sum_{\chi\in\hat{G}} \chi\chi'(g) = \chi'(g) \sum_{\chi\in\hat{G}} \chi(g)$ et donc il vient $(\chi'(g) - 1) \sum_{\chi\in\hat{G}} \chi(g) = 0$. Par hypothèse sur $\chi'(g)$ on en déduit $\sum_{\chi\in\hat{G}} \chi(g) = 0$. Inversement si $g = 1$ alors pour tout χ dans $\hat{G}$ on a $\chi(g) = 1$ et donc la somme précédente vaut $\mathrm{Card}(\hat{G})$. Autrement dit

$$\boxed{\sum_{\chi\in\hat{G}} \chi(g) = \mathrm{Card}(\hat{G})\delta_{g,1}.}$$

Si $\chi = 1$, par définition, on a $\sum_{g\in G} \chi(g) = \sum_{g\in G} 1 = \mathrm{Card}(G)$. Sinon on dispose de g' dans G tel que $\chi(g') \neq 1$. Puisque la multiplication à droite par g' est une bijection de G dans G, on en déduit

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(gg') = \chi(g') \sum_{g\in G} \chi(g)$$

et donc, puisqu'on a $\chi(g) \neq 1$, $\sum_{g\in G} \chi(g) = 0$. Autrement dit $\boxed{\sum_{g\in G} \chi(g) = \mathrm{Card}(G)\delta_{\chi,1}.}$

4. En sommant les deux relations précédentes et en inversant les deux signes de sommation finie, il vient

$$\mathrm{Card}(G) = \sum_{\chi\in\hat{G}} \mathrm{Card}(G)\delta_{\chi,1} = \sum_{\chi\in\hat{G}} \left(\sum_{g\in G} \chi(g) \right) = \sum_{g\in G} \left(\sum_{\chi\in\hat{G}} \chi(g) \right) = \sum_{g\in G} \mathrm{Card}(\hat{G})\delta_{g,1} = \mathrm{Card}(\hat{G})$$

et donc $\boxed{\mathrm{Card}(G) = \mathrm{Card}(\hat{G}).}$

On en déduit, en appliquant ce résultat au groupe $\hat{G}$, qui est aussi un groupe fini abélien, $\mathrm{Card}(G) = \mathrm{Card}(\hat{G}) = \mathrm{Card}(\hat{\hat{G}})$. Puisque $g \mapsto \varphi_g$ est injectif, par égalité des cardinaux des ensembles de départ et d'arrivée, on en déduit que

$$\boxed{\text{le morphisme } g \mapsto \varphi_g \text{ est un isomorphisme entre } G \text{ et } \hat{\hat{G}}.}$$

PARTIE II

1. Soit k dans $\mathbf{N}^*$. On a $p^k\mathbf{N} = \{j \in \mathbf{N} \,|\, v_p(j) \geq k\}$ par définition de la valuation p-adique et donc

$$p^k\mathbf{N} = p^{k+1}\mathbf{N} \cup \{j \in \mathbf{N} \,|\, v_p(j) = k\} \ ,$$

la réunion étant disjointe. En prenant l'intersection avec $[\![1; n]\!]$, il vient

$$p^k \left[\!\left[1; \left[\frac{n}{p^k}\right]\right]\!\right] = p^{k+1} \left[\!\left[1; \left[\frac{n}{p^{k+1}}\right]\right]\!\right] \cup \{j \in [\![1; n]\!] \,|\, v_p(j) = k\} \ ,$$

la réunion étant encore disjointe. Il vient donc en prenant les cardinaux

$$\text{Card}\left(\{j \in [\![1;n]\!] \,|\, v_p(j) = k\}\right) = \left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right] .$$

Puisque v_p est à valeurs dans $\mathbf{N}$, on a

$$[\![1;n]\!] = \coprod_{k\geq 0} \{j \in [\![1;n]\!] \,|\, v_p(j) = k\} \ ,$$

la réunion étant en fait finie puisqu'à partir de $k = 1 + \left[\log_p(n)\right]$ les ensembles considérés sont vides. De plus la valuation d'un produit étant la somme des valuations, il vient

$$v_p(n!\,) = \sum_{j=1}^{n} v_p(j) = \sum_{k=0}^{+\infty} \sum_{\substack{j\in[\![1;n]\!] \\ v_p(j)=k}} v_p(j) = \sum_{k=0}^{+\infty} k \cdot \text{Card}\left(\{j \in [\![1;n]\!] \,|\, v_p(j) = k\}\right) ,$$

ou encore $v_p(n!\,) = \displaystyle\sum_{k=1}^{\left[\log_p(n)\right]} U_k(v_k - v_{k+1})$ en posant $u_k = 1$ et $v_k = \left[\frac{n}{p^k}\right]$ puisque, dans la somme précédente, le terme pour $k = 0$ et ceux pour $k > \log_p(n)$ sont nuls. Donc, en utilisant la formule démontrée en préliminaire et en posant $m = 1 + \left[\log_p(n)\right]$, il vient

$$v_p(n!\,) = m\left[\frac{n}{p^m}\right] + \sum_{k=1}^{m}(k-(k-1))\left[\frac{n}{p^k}\right]$$

soit, puisque $\left[\frac{n}{p^m}\right] = 0$ et $\left[\frac{n}{p^k}\right] = 0$ pour $k > m$, $\boxed{v_p(n!\,) = \displaystyle\sum_{k=1}^{+\infty}\left[\frac{n}{p^k}\right].}$

Par positivité des termes, on en déduit directement $v_p(n!\,) \geq \left[\frac{n}{p}\right] \geq \frac{n}{p} - 1$ et

$$v_p(n!\,) \leq \sum_{k=1}^{+\infty} \frac{n}{p^k} = \frac{n}{p}\frac{1}{1-\frac{1}{p}} = \frac{n}{p}\frac{p}{p-1} = \frac{n}{p}\left(1 + \frac{1}{p-1}\right)$$

et donc $\boxed{\frac{n}{p} - 1 < v_p(n!\,) \leq \frac{n}{p} + \frac{n}{p(p-1)}.}$

2. Puisque $2^{2m+1} = (1+1)^{2m+1} = \displaystyle\sum_{k=0}^{2m+1}\binom{2m+1}{k}$ et qu'on affaire à une somme de termes positifs, on a $2^{2m+1} \geq \displaystyle\sum_{k=m}^{m+1}\binom{2m+1}{k}$. Par symétrie dans le triangle de Pascal, on a $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ et il en résulte $\boxed{\binom{2m+1}{m} \leq 4^m.}$

Soit p un nombre premier vérifiant $m+1 < p \leq 2m+1$. Alors p divise $(2m+1)!$, i.e. p divise $m!\,(m+1)!\binom{2m+1}{m}$. Par contre il ne divise ni $m!$, ni $(m+1)!$ donc, d'après le lemme de Gauss, p divise $\binom{2m+1}{m}$. Toujours en utilisant le lemme de Gauss, le produit de ces nombres premiers distincts divise $\binom{2m+1}{m}$ et en particulier $\displaystyle\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m}$. D'après ce qui précède on en déduit

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

3. Soit, pour n dans $\mathbf{N}^*$, $\mathbf{H}_n$ le prédicat $\prod_{p\leq n} p \leq 4^n$. Pour $n=1$, il s'écrit $1\leq 4$ et pour $n=2$ il s'écrit $2\leq 16$. On en déduit qu'il est vrai pour $n\leq 2$. Soit alors n supérieur à 3 tel que $\mathbf{H}_k$ soit vrai pour $0<k<n$. Si n n'est pas premier, alors $\prod_{p\leq n} p = \prod_{p\leq n-1} p \leq 4^{n-1}\leq 4^n$. Sinon n est impair et on dispose de m entier supérieur à 1 tel que $n=2m+1$. On a alors

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

en utilisant $\mathbf{H}_m$ et la propriété démontrée à la question précédente. On en déduit que $\mathbf{H}_n$ est héréditaire et donc, par le principe de récurrence, pour tout entier n supérieur à 1, on a $\boxed{\prod_{p\leq n} p \leq 4^n.}$

4. Soit $n=[x]$. On a donc $x=n+O(1)$ et donc $\dfrac{x}{n}=1+o(1)$, d'où $\ln(x/n)=o(1)$. En utilisant la formule rappelée dans l'énoncé sous la forme $\ln(n)=\dfrac{1}{n}\ln(n!\,)+O(1)$, il vient

$$\begin{aligned}
\sum_{p\leq x}\frac{\ln(p)}{p}-\ln(x) &= \sum_{p\leq n}\frac{\ln(p)}{p}-\ln(n)-\ln(x/n)\\
&= \sum_{p\leq n}\frac{\ln(p)}{p}-\ln(n)+o(1)\\
&= \sum_{p\leq n}\frac{\ln(p)}{p}-\frac{1}{n}\ln(n!\,)+O(1)\\
&= \sum_{p\leq n}\left(\frac{\ln(p)}{p}-\frac{v_p(n!\,)}{n}\ln(p)\right)+O(1)\\
&= \sum_{p\leq n}\frac{\ln(p)}{n}\left(\frac{n}{p}-v_p(n!\,)\right)+O(1)\ .
\end{aligned}$$

Or, d'après l'encadrement de $v_p(n!\,)$ obtenu précédemment, on a

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

et donc, par sommation et puisque $\ln(p)$ est positif pour tout nombre premier p, il vient

$$-\sum_{p\leq n}\frac{\ln(p)}{p(p-1)}\leq \sum_{p\leq n}\frac{\ln(p)}{n}\left(\frac{n}{p}-v_p(n!\,)\right)\leq \sum_{p\leq n}\frac{\ln(p)}{n}=\frac{\ln\left(\prod_{p\leq n}p\right)}{n}\leq \ln(4)\,,$$

par croissance du logarithme et en utilisant la majoration $\prod_{p\leq n} p\leq 4^n$ obtenue précédemment. Comme $\dfrac{\ln(k)}{k(k-1)}=O\left(k^{-3/2}\right)$ la série $\sum_{k\geq 1}\dfrac{\ln(k)}{k(k-1)}$ est convergente par comparaison à une série de Riemann convergente. Ses sommes partielles sont donc bornées. Par positivité des termes on en déduit que $\sum_{p\leq n}\dfrac{\ln(p)}{p(p-1)}$ est borné indépendamment de n et finalement $\boxed{\sum_{p\leq x}\frac{\ln(p)}{p}=\ln(x)+O(1).}$

PARTIE III

1. On pose $u_n = \chi(n)$. D'après la question I.3 et par définition de χ sur $\mathbf{N}$, on a

$$\sum_{n=1}^{N} u_n = \sum_{\substack{1\leq n\leq N\\ n\wedge N=1}} \chi(n) = \sum_{g\in G(N)} \chi(g) = 0$$

et donc, en reprenant les notations des préliminaires, $U_N = 0$. On en déduit, puisque la suite (u_n) est périodique de période N et donc que la somme de ses termes sur une période ne dépend pas de la période choisie, que la suite (U_n) l'est aussi :

$$U_{n+N} - U_n = \sum_{k=n+1}^{n+N} u_k = \sum_{k=1}^{N} u_k = U_N = 0\ .$$

En particulier la suite (U_n) est bornée, i.e. $U_m = O(1)$. En utilisant les préliminaires, il vient en prenant $v_n = \dfrac{1}{n}$

$$\sum_{n=1}^{m} \frac{\chi(n)}{n} = \frac{U_m}{m} + \sum_{k=1}^{m-1} \frac{U_k}{k(k+1)}\ .$$

Le premier terme du membre de droite est dans $O\left(\dfrac{1}{m}\right)$ et le terme général du second membre est dans $O\left(\dfrac{1}{k^2}\right)$. Par comparaison à une série de Riemann convergente, on en déduit que la somme partielle de la série $\displaystyle\sum_{n\geq 1} \frac{\chi(n)}{n}$ est somme d'un terme tendant vers 0 et de la somme partielle d'une série absolument convergente. Il en résulte que la série $\boxed{\displaystyle\sum_{n\geq 1} \frac{\chi(n)}{n} \text{ est convergente.}}$

En prenant cette fois $v_n = \dfrac{\ln(n)}{n}$, il vient

$$\sum_{n=1}^{m} \frac{\chi(n)\ln(n)}{n} = \frac{U_m \ln(m)}{m} + \sum_{k=1}^{m-1} \frac{U_k(k\ln(k+1) - (k+1)\ln(k))}{k(k+1)}\ .$$

Comme $\dfrac{U_m \ln(m)}{m} = O\left(\dfrac{\ln(m)}{m}\right) = o(1)$ et

$$k\ln(k+1) - (k+1)\ln(k) = \begin{vmatrix} k & k+1 \\ \ln(k) & \ln(k+1) \end{vmatrix} = \begin{vmatrix} k & 1 \\ \ln(k) & \ln\left(1+\dfrac{1}{k}\right) \end{vmatrix} = \begin{vmatrix} k & 1 \\ \ln(k) & O\left(\dfrac{1}{k}\right) \end{vmatrix}$$

et donc

$$\frac{U_k(k\ln(k+1) - (k+1)\ln(k))}{k(k+1)} = O\left(\frac{\ln(k) + O(1)}{k(k+1)}\right) = O\left(\frac{1}{k^{3/2}}\right)\ ,$$

on en déduit que la somme partielle de la série $\displaystyle\sum_{n\geq 1} \frac{\chi(n)\ln(n)}{n}$ est somme d'un terme tendant vers 0 et de la somme partielle d'une série absolument convergente, par comparaison à une série de Riemann convergente. Il en résulte que la série $\boxed{\displaystyle\sum_{n\geq 1} \frac{\chi(n)\ln(n)}{n} \text{ est convergente.}}$

2. On suppose que n et m sont premiers entre eux et on considère l'application $(d,d') \mapsto dd'$ pour d divisant n et d' divisant m. Puisque $d \mid n$ et $d' \mid m$, on a $dd' \mid mn$. Réciproquement si a est un diviseur de mn, on pose $d = a \wedge n$, alors par définition du pgcd d divise n et a. De plus $\dfrac{a}{d}$ est premier à n et divise a donc aussi mn. Puisque m et n sont premiers entre eux, d'après le lemme de Gauss, $\dfrac{a}{d}$ divise m et donc tout diviseur de mn s'écrit comme le produit d'un diviseur de m et d'un diviseur de n. Cette décomposition est de plus unique car si $dd' = DD'$ avec d, D des diviseurs de n et d', D' des diviseurs de m, alors d divise DD' et est premier à m donc aussi à D' et donc, d'après le lemme de Gauss, $d \mid D$. Par symétrie de l'égalité, on en déduit $D \mid d$ et donc $d = D$ puisqu'on a affaire à des nombres naturels. Il vient alors, puisque d est non nul, $d' = D'$. On conclut qu'il y a une bijection entre les couples formés d'un diviseur de n et d'un diviseur de m et les diviseurs de mn donnée par $(d,d') \mapsto dd'$. Il vient alors

$$f(n)f(m) = \sum_{d|n} \sum_{d'|m} \chi(d)\chi(d') = \sum_{\substack{d|n \\ d'|m}} \chi(dd') = \sum_{d|mn} \chi(d)\,,$$

i.e. $\boxed{f(nm) = f(n)f(m) \text{ si } n \text{ et } m \text{ sont premiers entre eux.}}$

Si n n'est pas premier à N, on a $\chi(n) = 0$ et sinon si a est l'ordre de la classe de n dans $G(N)$, on a $1 = \chi(1) = \chi(n^a) = \chi(n)^a$ et donc $\chi(n)$ est une racine a-ième de l'unité. Puisqu'on suppose χ à valeurs réelles, $\chi(n)$ est donc égal à 1 ou -1. En conclusion χ est à valeurs dans $\{-1,0,1\}$.

Si $\chi(p) = 0$, i.e. si p divise N, $f(p^n) = \displaystyle\sum_{k=0}^{n} \chi(p)^k = 1$. Si $\chi(p) = 1$, alors $f(p^n) = \displaystyle\sum_{k=0}^{n} \chi(p)^k = n+1$. Enfin si $\chi(p) = -1$, alors $f(p^n) = \displaystyle\sum_{k=0}^{n} \chi(p)^k = \frac{1+(-1)^n}{2}$. On en tire, par multiplicativité, en décomposant n en facteurs premiers,

$$f(n) = \prod_{p|n} f(p^{v_p(n)})$$

et chacun des termes est positif d'après ce qui précède et même supérieur à 1 si $v_p(n)$ est pair. On en conclut $\boxed{f(n) \geq 0 \text{ et } f(n) \geq 1 \text{ si } n \text{ est un carré.}}$

D'après ce qui précède, pour $x \geq m^2$, on a par positivité de tous les termes

$$g(x) \geq \sum_{n=1}^{m^2} \frac{f(n)}{\sqrt{n}} \geq \sum_{n=1}^{m} \frac{1}{m}$$

et donc, par divergence de la série harmonique $\boxed{\lim_{+\infty} g = +\infty.}$

3. L'application $(d,d') \mapsto (dd',d)$ de l'ensemble des couples (d,d') de $\mathbf{N}^* \times \mathbf{N}^*$ vérifiant $dd' \leq x$ dans l'ensemble des couples (n,d) de $\mathbf{N}^* \times \mathbf{N}^*$ vérifiant $n \leq x$ et $d \mid n$ est bien définie et bijective de réciproque $(n,d) \mapsto (d, n/d)$. On en déduit

$$g(x) = \sum_{n \leq x} \sum_{d|n} \frac{\chi(d)}{\sqrt{n}} = \sum_{dd' \leq x} \frac{\chi(d)}{\sqrt{dd'}}$$

où la seconde somme est prise sur l'ensemble des couples (d,d') d'entiers supérieurs à 1 tels que $dd' \leq x$. Pour de tels entiers on a $d \leq \dfrac{x}{d'} \leq x$ et $d' \leq \dfrac{x}{d} \leq x$ et $d' < \sqrt{x} \iff d > \sqrt{x}$. En coupant en deux la

somme selon que d est inférieur à $\sqrt{x}$ ou pas, il vient

$$\begin{aligned} g(x) &= \sum_{\substack{dd'\leq x\\ d>\sqrt{x}}} \frac{\chi(d)}{\sqrt{dd'}} + \sum_{\substack{dd'\leq x\\ d\leq\sqrt{x}}} \frac{\chi(d)}{\sqrt{dd'}} = \sum_{\substack{dd'\leq x\\ d'<\sqrt{x}}} \frac{\chi(d)}{\sqrt{dd'}} + \sum_{\substack{dd'\leq x\\ d\leq\sqrt{x}}} \frac{\chi(d)}{\sqrt{dd'}} \\ &= \sum_{d'<\sqrt{x}} \sum_{\sqrt{x}<d\leq\frac{x}{d'}} \frac{1}{\sqrt{d'}}\frac{\chi(d)}{\sqrt{d}} + \sum_{d\leq\sqrt{x}} \sum_{d'\leq\frac{x}{d}} \frac{1}{\sqrt{d'}}\frac{\chi(d)}{\sqrt{d}} \\ &= \sum_{d'<\sqrt{x}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{x}<d\leq\frac{x}{d'}} \frac{\chi(d)}{\sqrt{d}} + \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{d'\leq\frac{x}{d}} \frac{1}{\sqrt{d'}} \end{aligned}$$

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

La fonction g est en escalier par définition et donc continue par morceaux sur son domaine de définition ; la fonction $x \mapsto g(x) - 2\sqrt{x}L(\chi)$ est donc également continue par morceaux sur son domaine de définition et il suffit donc de montrer qu'elle est majorée au voisinage de l'infini, ce qu'on notera $g(x) - 2\sqrt{x}L(\chi) = O(1)$.
Pour $m = [x]$ on a $g(x) = g(m)$ et donc

$$g(x) - 2\sqrt{x}L(\chi) = g(m) - 2\sqrt{m}L(\chi) - 2L(\chi)\frac{x-m}{\sqrt{x}+\sqrt{m}} = g(m) - 2\sqrt{m}L(\chi) + o(1)$$

puisque $0 \leq x-m < 1$ et $\sqrt{x}+\sqrt{m} \geq \sqrt{x} > 0$. On se ramène donc à démontrer $g(x)-2\sqrt{x}L(\chi) = O(1)$ dans le cas où x est un entier. Par ailleurs, par définition, on a

$$2\sqrt{m}L(\chi) = 2\sqrt{m}\sum_{d=1}^{+\infty}\frac{\chi(d)}{d} = 2\sum_{d=1}^{+\infty}\frac{\chi(d)}{\sqrt{d}}\sqrt{\frac{m}{d}}$$

et donc

$$\begin{aligned} g(m) - 2\sqrt{m}L(\chi) &= \sum_{d'<\sqrt{m}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{m}<d\leq\frac{m}{d'}} \frac{\chi(d)}{\sqrt{d}} \\ &\quad + \sum_{d\leq\sqrt{m}} \frac{\chi(d)}{\sqrt{d}} \left(\sum_{d'\leq\frac{m}{d}} \frac{1}{\sqrt{d'}} - 2\sqrt{\frac{m}{d}} \right) \\ &\quad -2\sqrt{m} \sum_{d>\sqrt{m}} \frac{\chi(d)}{d}\ . \end{aligned}$$

On va démontrer que chacun des termes du membre de droite de cette égalité est borné avec m, ce qui permet de conclure.

On applique le raisonnement de la question 1 avec $u_m = \chi(m)$. On reprend la notation $U_m = \sum_{d=1}^{m}\chi(d)$.
On a vu durant la réponse à la question 1 que la suite (U_m) est bornée et on dispose donc d'un réel positif A tel que, $|U_m| \leq A$. Supposons que la suite (v_m) soit de signe constant et décroissante en valeur absolue. Alors Pour $n \leq m$, on a donc

$$\sum_{n<d\leq m} u_d v_d = \sum_{d\leq m} u_d v_d - \sum_{d\leq n} u_d v_d = U_m v_m - U_n v_n + \sum_{d=n}^{m-1} U_d(v_d - v_{d+1})$$

et, par hypothèse de monotonie et de signe sur (v_m),

$$\left|\sum_{n<d\leq m} u_d v_d\right| \leq A\,|v_m| + A\,|v_n| + A\sum_{d=n}^{m-1}(|v_d| - |v_{d+1}|) = 2A\,|v_n|\ ,$$

i.e. $\displaystyle\sum_{n<d\leq m} u_d v_d = O\,(v_n)$. Si, de plus, la série $\sum u_d v_d$ converge, alors on peut passer à la limite dans l'inégalité précédente et il vient $\displaystyle\sum_{n<d} u_d v_d = O\,(v_n)$.

On prend d'abord $v_m = \dfrac{1}{m}$, qui constitue le terme général d'une suite positive, décroissante. Avec ce qui précède et puisque la série définissant $L(\chi)$ converge, il vient

$$\left|-2\sqrt{m}\sum_{d>\sqrt{m}}\frac{\chi(d)}{d}\right| = \sqrt{m}O\left(\frac{1}{[\sqrt{m}]}\right) = O\,(1)$$

puisque $\sqrt{m}\sim\sqrt{[m]}$.

On prend ensuite $v_m = \dfrac{1}{\sqrt{m}}$, qui est également le terme général d'une suite positive décroissante. Il vient alors

$$\sum_{\sqrt{m}<d\leq\frac{m}{d'}}\frac{\chi(d)}{\sqrt{d}} = O\left(\frac{1}{\sqrt{[\sqrt{m}]}}\right)\ .$$

Or, par comparaison entre une série (de Riemann) divergente et une intégrale dans le cas d'une fonction continue positive et décroissante, on a $\displaystyle\sum_{d'<\sqrt{m}}\frac{1}{\sqrt{d'}} \sim 2\sqrt{\left[\sqrt{m}\right]}$ et donc

$$\sum_{d'<\sqrt{m}}\frac{1}{\sqrt{d'}}\sum_{\sqrt{m}<d\leq\frac{m}{d'}}\frac{\chi(d)}{\sqrt{d}} = O\,(1)\ .$$

Pour étudier le dernier terme, on constate

$$\sum_{d'\leq\frac{m}{d}}\frac{1}{\sqrt{d'}} - 2\sqrt{\frac{m}{d}} = \sum_{d'\leq\frac{m}{d}}\left(\frac{1}{\sqrt{d'}} - \int_{d'-1}^{d'}\frac{\mathrm{d}t}{\sqrt{t}}\right) + 2\sqrt{\left[\frac{m}{d}\right]} - 2\sqrt{\frac{m}{d}}\ .$$

Or

$$\sqrt{\left[\frac{m}{d}\right]} - \sqrt{\frac{m}{d}} = \frac{\left[\dfrac{m}{d}\right] - \dfrac{m}{d}}{\sqrt{\left[\dfrac{m}{d}\right]} + \sqrt{\dfrac{m}{d}}} = O\left(\sqrt{\frac{d}{m}}\right)$$

et donc

$$\begin{aligned}\sum_{d\leq\sqrt{m}}\frac{\chi(d)}{\sqrt{d}}\left(\sum_{d'\leq\frac{m}{d}}\frac{1}{\sqrt{d'}} - 2\sqrt{\frac{m}{d}}\right) \quad &= \quad \sum_{d\leq\sqrt{m}}\frac{\chi(d)}{\sqrt{d}}\sum_{d'\leq\frac{m}{d}}\int_{d'-1}^{d'}\left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right)\mathrm{d}t \\ &\quad + \sum_{d\leq\sqrt{m}}\frac{\chi(d)}{\sqrt{d}}O\left(\sqrt{\frac{d}{m}}\right)\ .\end{aligned}$$

On remarque qu'on a

$$\sum_{d\leq\sqrt{m}} \frac{\chi(d)}{\sqrt{d}} O\left(\sqrt{\frac{d}{m}}\right) = \sum_{d\leq\sqrt{m}} O\left(\sqrt{\frac{1}{m}}\right) = O(1)$$

et que le terme $\displaystyle\int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right) \mathrm{d}t$ est négatif par décroissance de la fonction $t \mapsto t^{-1/2}$. On en déduit que

$$d \mapsto \sum_{d'\leq\frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right) \mathrm{d}t$$

est négative et croissante (i.e. décroissante en valeur absolue), par décroissance de $d \mapsto \dfrac{m}{d}$. On pose donc, enfin,

$$v_d = \frac{1}{\sqrt{d}} \sum_{d'\leq\frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right) \mathrm{d}t$$

de sorte que (v_d) est négative et décroissante en valeur absolue en tant que produit de deux termes tous deux décroissants en valeur absolue, l'un positif et l'autre négatif. On obtient donc

$$\sum_{d\leq\sqrt{m}} \frac{\chi(d)}{\sqrt{d}} \sum_{d'\leq\frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right) \mathrm{d}t = O\left(\int_0^m \frac{\mathrm{d}t}{\sqrt{t}} - \sum_{d'=1}^{m} \frac{1}{\sqrt{d'}}\right)$$

l'intégrale s'entendant comme une limite. Or, par comparaison entre série et intégrale, on a

$$\int_1^{m+1} \frac{\mathrm{d}t}{\sqrt{t}} \leq \sum_{d'=1}^{m} \frac{1}{\sqrt{d'}} \leq \int_0^m \frac{\mathrm{d}t}{\sqrt{t}}$$

et donc, puisque $\sqrt{m} - \sqrt{m+1} + 1 = 1 - \dfrac{1}{\sqrt{m}+\sqrt{m+1}} = O(1)$, on en déduit

$$\sum_{d\leq\sqrt{m}} \frac{\chi(d)}{\sqrt{d}} \sum_{d'\leq\frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right) \mathrm{d}t = O(1)$$

et ainsi $\boxed{g(x) - 2\sqrt{x}L(\chi) \text{ est bornée.}}$

4. On déduit des deux question précédentes que la fonction $x \mapsto 2\sqrt{x}L(\chi)$ tend vers l'infini en $+\infty$ et donc que $L(\chi)$ est strictement positif. En particulier $\boxed{L(\chi) \text{ est non nul.}}$

PARTIE IV

1. Soit $n = \displaystyle\prod_{i=1}^{m} p_i^{a_i}$ la décomposition en facteurs premiers de n. Puisque n est supérieur à 2, m est non nul. De plus si d est un entier naturel, alors $d \mid n$ et $\mu(d) \neq 0$ si et seulement si $d = \displaystyle\prod_{i\in J} p_i$ avec $J \subset [\![1;m]\!]$ et alors $\mu(d) = (-1)^{|J|}$. On en déduit

$$\sum_{d|n} \mu(d) = \sum_{J\subset[\![1;m]\!]} (-1)^{|J|} = (1-1)^m = 0\,.$$

On a donc $\boxed{\displaystyle\sum_{d|n} \mu(d) = 0.}$

2. On a par hypothèse $H = H(1)H$ et donc, puisque H est non nulle, $\boxed{H(1) = 1.}$
Par définition pour $x \geq 1$, on a

$$\begin{aligned}\sum_{1\leq k\leq x} \mu(k)G\left(\frac{x}{k}\right)H(k) &= \sum_{1\leq k\leq x}\sum_{1\leq \ell\leq \frac{x}{k}} \mu(k)F\left(\frac{x}{k\ell}\right)H(\ell)H(k)\\ &= \sum_{\substack{k\ell\leq x\\ 1\leq k,\ell}} \mu(k)F\left(\frac{x}{k\ell}\right)H(k\ell)\\ &= \sum_{1\leq m\leq x}\sum_{k|m}\mu(k)F\left(\frac{x}{m}\right)H(m)\\ &= \sum_{1\leq m\leq x} F\left(\frac{x}{m}\right)H(m)\sum_{k|m}\mu(k)\\ &= F(x)H(1)\end{aligned}$$

d'après ce qui précède et puisque $\mu(1) = 1$. On en déduit, avec $H(1) = 1$,

$$\boxed{F(x) = \sum_{1\leq k\leq x} \mu(k)G\left(\frac{x}{k}\right)H(k).}$$

3. On applique ce qui précède à $F = \Lambda$ et $H = 1$ (qui est bien multiplicative). Alors on a, pour $x \geq 1$ et k entier supérieur à 1, $\Lambda\left(\frac{x}{k}\right)$ est non nul si et seulement si x est entier de la forme kp^n avec n entier supérieur à 1, et nécessairement inférieur à $v_p(x)$, d'où

$$G(x) = \sum_{1\leq k\leq x}\Lambda\left(\frac{x}{k}\right) = \mathbb{1}_{\mathbf{N}}(x)\sum_{p^n\leq x}\ln(p) = \mathbb{1}_{\mathbf{N}}(x)\sum_{p|x} v_p(x)\ln(p) = \mathbb{1}_{\mathbf{N}}(x)\ln(x)$$

et donc

$$\Lambda(x) = \sum_{1\leq k\leq x}\mu(k)\mathbb{1}_{\mathbf{N}}\left(\frac{x}{k}\right)\ln\left(\frac{x}{k}\right)\ .$$

En particulier, puisque $\frac{m}{k}$ est entier si et seulement si k divise m, $\boxed{\Lambda(m) = \sum_{d|m}\mu(d)\ln\left(\frac{m}{d}\right).}$

PARTIE V

1. La fonction G est produit de l'identité avec une fonction en escalier, elle est donc continue par morceaux sur son domaine de définition et il suffit de démontrer qu'elle est bornée au voisinage de l'infini. D'après III.1, la série $\sum_{1\leq n\leq x}\frac{\chi(n)}{n}$ converge et en utilisant les inégalités démontrées en question III.3, il vient par positivité et décroissance de $(\frac{1}{n})$,

$$G(x) - xL(\chi) = -x\sum_{n>x}\frac{\chi(n)}{n} = O\left(\frac{x}{[x]}\right) = O\left(1\right)\ ,$$

i.e. $\boxed{G(x) - xL(\chi) \text{ est borné.}}$

Le caractère χ étant multiplicatif, on applique la question IV.2 avec $F = \mathrm{Id}$, $H = \chi$ et donc les applications notées G dans cette question et dans la question IV.2 sont identiques. On en déduit

$$x = \sum_{1\leq k\leq x} \mu(k) G\left(\frac{x}{k}\right)\chi(k)$$

et donc

$$x - xL(\chi)\sum_{1\leq k\leq x}\mu(k)\frac{\chi(k)}{k} = \sum_{1\leq k\leq x}\mu(k)\chi(k)\left(G\left(\frac{x}{k}\right) - \frac{x}{k}L(\chi)\right) = O\left(\sum_{1\leq k\leq x}|\mu(k)\chi(k)|\right).$$

Or μ et χ sont bornés par 1 (on a déjà remarqué que χ est prend ses valeurs non nulles dans les racines de l'unité), donc $xL(\chi)\displaystyle\sum_{1\leq k\leq x}\mu(k)\frac{\chi(k)}{k} = O(x)$ et $L(\chi)\displaystyle\sum_{1\leq k\leq x}\mu(k)\frac{\chi(k)}{k} = O(1)$. Par conséquent, si $L(\chi)$ est non nul et puisqu'on a affaire à une fonction en escalier, donc continue par morceaux sur son domaine de définition, $\boxed{\displaystyle\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} \text{ est borné.}}$

2. Par définition et par convergence des séries définissant $L(\chi)$ et $L_1(\chi)$, on a, en tenant compte de $L(\chi) = 0$,

$$G_1(x) + xL_1(\chi) = G_1(x) + xL(\chi) + xL_1(\chi) = -x\ln(x)\sum_{n>x}\frac{\chi(n)}{n} + x\sum_{n>x}\frac{\chi(n)\ln(n)}{n}.$$

Or, pour $n \geq 3$, on a $\ln(n) \geq 1$ et donc

$$\ln(n+1) = \ln(n) + \ln\left(1+\frac{1}{n}\right) \leq \ln(n) + \frac{1}{n} \leq \ln(n)\left(1+\frac{1}{n}\right) = \ln(n)\frac{n+1}{n},$$

les suites $(1/n)$ et $(\ln(n)/n)_{n\geq 3}$ sont donc positives et décroissantes. Il résulte alors des relations obtenues en question III.3 (pour $x > 2$ dans le second cas)

$$\sum_{n>x}\frac{\chi(n)}{n}O\left(\frac{1}{x}\right) \quad \text{et} \quad \sum_{n>x}\frac{\chi(n)\ln(n)}{n} = O\left(\frac{\ln(x)}{x}\right),$$

d'où $\boxed{G_1(x) = -xL_1(\chi) + O(\ln(x)).}$

On applique la question IV.2 avec $F = \mathrm{Id}\times\ln$ et $H = \chi$. Les applications notées G_1 dans cette question et G dans la question IV.2 coïncident alors et on en déduit

$$x\ln(x) = \sum_{1\leq k\leq x}\mu(k)G_1\left(\frac{x}{k}\right)\chi(k)$$

et donc, en utilisant la formule rappelée en partie II,

$$\begin{aligned} x\ln(x)+xL_1(\chi)\sum_{1\leq k\leq x}\mu(k)\frac{\chi(k)}{k} &= \sum_{1\leq k\leq x}\mu(k)\chi(k)\left(G_1\left(\frac{x}{k}\right)+\frac{x}{k}L_1(\chi)\right)\\ &= O\left(\sum_{1\leq k\leq x}\ln\left(\frac{x}{k}\right)\right)\\ &= O\left(x\ln(x)-\ln(([x])!\,)\right)\\ &= O\left(x\ln(x)-[x]\ln([x])+O\left(x\right)\right)\\ &= =O\left((x-[x])\ln(x)-[x]\ln\left(\frac{x}{[x]}\right)+O\left(x\right)\right)\\ &= O\left(1\right)O\left(\ln(x)\right)+O\left(x\right)O\left(1\right)+O\left(x\right)=O\left(x\right) \end{aligned}$$

et donc

$$\ln(x)+L_1(\chi)\sum_{1\leq k\leq x}\mu(k)\frac{\chi(k)}{k}=O\left(1\right)$$

et ainsi, puisqu'on a affaire à des fonctions continues par morceaux sur leur domaine de définition,

$$\boxed{L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n}+\ln(x)\text{ est borné.}}$$

3. Puisque la suite $(\ln(n)/n)$ est positive et décroissante à partir de $n=3$, en utilisant les relations de la question III.3, on obtient

$$\sum_{n>m}\frac{\chi(n)\ln(n)}{n}=O\left(\frac{\ln(n)}{n}\right)\ .$$

Par définition et par associativité, on a, puisque la seconde somme est finie et par multiplicativité de χ,

$$\begin{aligned} L_1(\chi)\sum_{d\leq x}\frac{\mu(d)\chi(d)}{d} &= \sum_{d\leq x}\left(\sum_{n=1}^{+\infty}\frac{\chi(n)\ln(n)}{n}\frac{\mu(d)\chi(d)}{d}\right)\\ &= \sum_{d\leq x}\sum_{n\leq\frac{x}{d}}\frac{\chi(n)\ln(n)}{n}\frac{\mu(d)\chi(d)}{d}+\sum_{d\leq x}\sum_{n>\frac{x}{d}}\frac{\chi(n)\ln(n)}{n}\frac{\mu(d)\chi(d)}{d}\\ &= \sum_{m\leq x}\sum_{d|m}\mu(d)\ln\left(\frac{m}{d}\right)\frac{\chi(m)}{m}+\sum_{d\leq x}O\left(\frac{d\ln\left(\frac{x}{d}\right)}{x}\right)\frac{\mu(d)\chi(d)}{d} \end{aligned}$$

en utilisant la bijection $(d,n)\mapsto(nd,d)$.
En utilisant la question IV.3, il vient

$$L_1(\chi)\sum_{d\leq x}\frac{\mu(d)\chi(d)}{d}=\sum_{m\leq x}\Lambda(m)\frac{\chi(m)}{m}+\frac{1}{x}\sum_{d\leq x}O\left(\ln\left(\frac{x}{d}\right)\right)\ .$$

Or on a vu à la question précédente $\displaystyle\sum_{d\leq x}\ln\left(\frac{x}{d}\right)=O\left(x\right)$ et donc

$$L_1(\chi)\sum_{d\leq x}\frac{\mu(d)\chi(d)}{d}=\sum_{m\leq x}\Lambda(m)\frac{\chi(m)}{m}+O\left(1\right)\ .$$

Enfin on a

$$\begin{aligned}\sum_{m\leq x}\Lambda(m)\frac{\chi(m)}{m} &= \sum_{p\leq x}\ln(p)\sum_{n\leq\frac{\ln(x)}{\ln(p)}}\frac{\chi(p)^n}{p^n}\\ &= \sum_{p\leq x}\frac{\chi(p)\ln(p)}{p}+\sum_{p\leq x}\ln(p)\sum_{2\leq n\leq\frac{\ln(x)}{\ln(p)}}\frac{\chi(p)^n}{p^n}\\ &= \sum_{p\leq x}\frac{\chi(p)\ln(p)}{p}+\sum_{p\leq x}\ln(p)\sum_{2\leq n\leq\frac{\ln(x)}{\ln(p)}}O\left(\frac{1}{p^n}\right)\\ &= \sum_{p\leq x}\frac{\chi(p)\ln(p)}{p}+\sum_{p\leq x}\ln(p)O\left(\frac{1}{p^2}\frac{1}{1-\frac{1}{p}}\right)\\ &= \sum_{p\leq x}\frac{\chi(p)\ln(p)}{p}+O(1)\end{aligned}$$

puisque $\ln(p)\dfrac{1}{p^2}\dfrac{1}{1-\frac{1}{p}}\sim\dfrac{\ln(p)}{p^2}=O\left(p^{-3/2}\right)$ et donc, par comparaison avec une série de Riemann convergente $\sum\ln(p)\dfrac{1}{p^2}\dfrac{1}{1-\frac{1}{p}}$ est absolument convergente. Il en résulte

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

4. Il découle des trois questions précédentes qu'on a

$$\boxed{\sum_{p\leq x}\frac{\chi(p)\ln(p)}{p}=L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n}+O(1)=\begin{cases}O(1) & \text{si } L(\chi)\neq 0\\ -\ln(x)+O(1) & \text{si } L(\chi)=0\,.\end{cases}}$$

5. D'après la question II.4, si χ est trivial, on a $\displaystyle\sum_{p\leq x}\frac{\chi(p)\ln(p)}{p}=\sum_{p\leq x}\frac{\ln(p)}{p}=\ln(x)+O(1)$ et donc, en utilisant le résultat précédent

$$\sum_{\chi\in G(N)}\sum_{p\leq x}\frac{\chi(p)\ln(p)}{p}=(1-T)\ln(x)+O(1)\ .$$

Puisqu'on affaire à des sommes finies, on peut les échanger et donc, en utilisant la question I.3, on obtient $\boxed{\operatorname{Card}G(N)\sum_{\substack{p\leq x\\ p\equiv 1\pmod N}}\frac{\ln(p)}{p}=(1-T)\ln(x)+O(1).}$ Comme le membre de gauche est positif en tant que somme de termes positifs, celui de droite l'est aussi et donc $\boxed{T\leq 1.}$

6. Si χ est non trivial et à valeurs réelles, alors $L(\chi)\neq 0$ d'après la question III.4. Si χ n'est pas à valeurs réelles, alors $\overline{\chi}$ est distinct de χ et $L(\overline{\chi})=\overline{L(\chi)}$, de sorte que les deux sont simultanément nuls ou non. Comme $T\leq 1$, aucun des deux n'est nul et, finalement $\boxed{T=0.}$

7. On déduit de ce qui précède que, pour χ non trivial, on a $\displaystyle\sum_{p\leq x}\frac{\chi(p)\ln(p)}{p}=O(1)$ et donc

$$\sum_{\chi\in G(N)}\sum_{p\leq x}\overline{\chi}(\ell)\frac{\chi(p)\ln(p)}{p}=\sum_{p\leq x}\frac{\ln(p)}{p}=\ln(x)+O(1)\ .$$

Puisque ℓ est premier à N, on dispose d'une relation de Bézout $a\ell+bN=1$ avec a et b entiers et alors $\chi(a)\chi(\ell)=1$. De plus si d est l'ordre de la classe de ℓ modulo N dans $G(N)$, alors $\ell^d\equiv 1\pmod N$ et donc $\chi(\ell)^d=\chi(1)=1$ et $\chi(\ell)$ est une racine de l'unité et donc $\overline{\chi(\ell)}=\chi(\ell)^{-1}=\chi(a)$. Il en résulte $\displaystyle\sum_{\chi\in G(N)}\overline{\chi}(\ell)\chi(p)=\sum_{\chi\in G(N)}\chi(ap)$ et cette dernière somme est nulle sauf si $ap\equiv 1\pmod N$, auquel cas elle vaut $\operatorname{Card}G(N)$, d'après la question I.3. Enfin $ap\equiv 1\pmod N\iff p\equiv\ell\pmod N$ et donc

$$\sum_{p\leq x}\sum_{\chi\in G(N)}\overline{\chi}(\ell)\frac{\chi(p)\ln(p)}{p}=\operatorname{Card}G(N)\sum_{\substack{p\leq x\\ p\equiv\ell\pmod N}}\frac{\ln(p)}{p}\ .$$

Si l'ensemble $\{p \text{ premier } \mid p\equiv\ell\pmod n\}$ est fini, alors la seconde somme est bornée (et même constante) au voisinage de l'infini, et ne saurait donc être équivalente à $\ln(x)$. Par conséquent $\boxed{\{p \text{ premier } \mid p\equiv\ell\pmod n\}}$

PARTIE VI

1. Soit P un polynôme non nul à coefficients entiers et a un entier naturel. Par définition on a $c(aP)=ac(P)$ et si a divise $c(P)$, alors $\frac{1}{a}P$ est à coefficients entiers et $c(P)=ac\left(\frac{1}{a}P\right)$. En particulier en posant $\tilde{P}=\frac{1}{c(P)}P$ alors $\tilde{P}$ est à coefficients entiers et $c(\tilde{P})=1$. On pose de même, pour Q un polynôme non nul à coefficients entiers, $\tilde{Q}=\frac{1}{c(Q)}Q$. Si on démontre $c(\tilde{P}\tilde{Q})=1$ alors, puisque $PQ=c(P)c(Q)\tilde{P}\tilde{Q}$, on aura $c(PQ)=c(P)c(Q)c(\tilde{P}\tilde{Q})=c(P)c(Q)$. Il suffit dont de traiter le cas $c(P)=c(Q)=1$. Soit p un nombre premier. Puisque $c(P)=1$, l'image de P dans $\mathbf{Z}/p\mathbf{Z}[X]$ par le morphisme canonique (qui aux coefficients de P associe leur classe modulo p) est non nulle, et il en va de même pour Q. Puisque $\mathbf{Z}/p\mathbf{Z}$ est un corps, $\mathbf{Z}/p\mathbf{Z}[X]$ est intègre et donc PQ est non nul modulo p, ce qui signifie que p ne divise pas $c(PQ)$. Comme c'est vrai pour tout nombre premier, c'est que $c(PQ)$ vaut 1. On a donc $\boxed{c(PQ)=c(P)c(Q).}$

Remarque : plus simplement si $P=\sum a_mX^m$ et $Q=\sum b_nX^n$, on dispose de

$$m=\min\{m\in\mathbf{N}\mid a_m\wedge p=1\}\ \text{ et }\ n=\min\{n\in\mathbf{N}\mid b_n\wedge p=1\}$$

et alors le coefficient d'indice $m+n$ de PQ est somme de a_mb_n et de termes divisibles par p, donc est premier à p, donc $p\wedge c(PQ)=1$.

2. Soit I l'ensemble des polynômes dans $\mathbf{Q}[X]$ annulant ζ. C'est un idéal de $\mathbf{Q}[X]$. Comme X^n-1 appartient à I, c'est un idéal non nul et comme $\mathbf{Q}[X]$ est principal P_ζ en est le générateur unitaire.

Puisque P_ζ est à coefficients rationnels, on dispose de a tel que aP_ζ soit à coefficients entiers et alors en divisant aP_ζ par $c(aP_\zeta)$ on obtient un polynôme P et un rationnel r tels que $P_\zeta=rP$, P est un polynôme non nul à coefficients entiers et $c(P)=1$. Comme X^n-1 appartient à I, on dispose de Q_ζ dans $\mathbf{Q}[X]$ tel que $X^n-1=P_\zeta Q_\zeta$. On dispose alors d'un polynôme Q et d'un rationnel s tels que $Q_\zeta=sQ$, Q est un polynôme non nul à coefficients entiers et $c(Q)=1$. On a alors $c(PQ)=1$ et $X^n-1=rsPQ$. Soit $rs=\frac{p}{q}$ une écriture irréductible du rationnel rs avec p dans $\mathbf{Z}$ et q dans $\mathbf{N}^*$,

alors $q(X^n-1)=pRS$ et donc $q=c(q(X^n-1))=c(pRS)=|p|$ et donc $rs=\pm 1$, i.e. $X^n-1=\pm PQ$. Comme on a affaire à des polynômes à coefficients entiers, ceci entraîne que les coefficients dominants de P et Q sont des unités de $\mathbf{Z}$, de sorte que $P_\zeta=\pm P$ et donc $\boxed{P_\zeta \text{ est à coefficients entiers.}}$

3. Par définition $\mathbf{Q}[\zeta]=\{P(\zeta)\,|\,P\in\mathbf{Q}[X]\}$. Puisque $P\mapsto P(\zeta)$ est un morphisme de $\mathbf{Q}$-algèbres, $\mathbf{Q}[\zeta]$ est un $\mathbf{Q}$-espace vectoriel. Par minimalité de P_ζ la famille $\mathcal{B}$ est libre. Par division euclidienne par le polynôme non nul P_ζ, pour tout P dans $\mathbf{Q}[X]$ on dispose de R dans $\mathbf{Q}[X]$ de degré strictement inférieur à d tel que $P-R$ soit un multiple de P_ζ et en particulier $P(\zeta)=R(\zeta)$. Donc $\mathcal{B}$ est également générateur, i.e. $\boxed{\mathcal{B} \text{ est une base de } \mathbf{Q}[\zeta].}$

4. On démontre l'assertion en montrant qu'elle est vraie pour les monômes et que l'ensemble des polynômes qui la vérifie est stable par addition. Soit a entier, n dans $\mathbf{N}$ et $P=aX^n$, alors $P(X^p)-P^p=(a-a^p)X^{np}$. Or, d'après le (petit) théorème de Fermat, $a-a^p$ est divisible par p et l'assertion s'ensuit. Soit P et Q vérifiant l'assertion. On dispose donc de G_p et H_p dans $\mathbf{Z}[X]$ tel que $P(X^p)=P^p+pG_p$ et $Q(X^p)=Q^p+pH_p$. On a alors

$$(P+Q)(X^p)-(P+Q)^p=p(G_p+H_p)+\sum_{k=1}^{p-1}\binom{p}{k}P^kQ^{p-k}\ .$$

Or, pour k dans $[\![1;p-1]\!]$, on a $k!\,(p-k)!\binom{p}{k}=p!$. D'après le lemme de Gauss, puisque p divise $p!$, mais ne divise pas (et donc premier avec) tous les facteurs de $k!$ et $(p-k)!$, il divise $\binom{p}{k}$. Puisque P^kQ^{p-k} est à coefficients entiers, on en déduit que $(P+Q)(X^p)-(P+Q)^p$ s'écrit pK_p avec K_p dans $\mathbf{Z}[X]$ et donc, pour tout polynôme P à coefficients entiers et tout nombre premier p, il existe un polynôme G_p à coefficients entiers tel que $\boxed{P(X^p)=P^p+pG_p.}$

Pour tout x dans $\mathbf{Z}[\zeta]$, on définit $M(x)$ comme la matrice dans $\mathcal{B}$ de l'endomorphisme du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}[\zeta]$ donné par $y\mapsto xy$.

5. Soit ℓ un entier premier à n. D'après la question V.7, avec $N=n$, on dispose d'une infinité de nombres premiers p tels que $p\equiv\ell\pmod n$. Pour de tels p on a $\zeta^\ell=\zeta^p$. Soit alors $x=P_\zeta(\zeta^\ell)$. Pour p comme précédemment on dispose de G_p à coefficients entiers tel que $x=P_\zeta(\zeta)^p+pG_p(\zeta)=pG_p(\zeta)$. En posant $y=G_p(\zeta)$, on a donc $x=py$ avec x et y dans $\mathbf{Z}[\zeta]$. On a donc $M(x)=M(p)M(y)$. Or $M(p)=p\mathrm{Id}$ et donc $M(x)=pM(y)$. Comme x et y sont dans $\mathbf{Z}[\zeta]$, $M(x)$ et $M(y)$ sont à coefficients entiers. On en déduit que tous les coefficients de $M(x)$ sont divisibles par p. Comme c'est vrai pour une infinité de nombres premiers, c'est que $M(x)$ est nul, i.e. $x=0$ et donc $\boxed{P_\zeta(\zeta^\ell)=0.}$

6. L'application $k\mapsto\left(\frac{n}{n\wedge k},\frac{k}{n\wedge k}\right)$, pour k dans $[\![1;n]\!]$ est une bijection avec l'ensemble des couples de la forme (d,k') vérifiant $d\mid n$, $k\in[\![1;d]\!]$ et $k'\wedge d=1$, de bijection réciproque $(d,k')\mapsto\frac{n}{d}k'$, comme on le vérifie directement. Comme $\frac{k}{n}=\frac{k'}{d}$ avec ces notations, on en déduit que $\boxed{(E_d)_{d|n} \text{ est une partition de } \left\{\frac{k}{n}\ \middle|\ k\right.}$

La partition précédente, compte tenu du fait que les racines n-ièmes de l'unité sont exactement les nombres complexes de la forme $\exp(2i\pi k/n)$ avec $k\in[\![1;n]\!]$, donne

$$X^n-1=\prod_{k=1}^{n}\left(X-\exp\left(\frac{2i\pi k}{n}\right)\right)=\prod_{d|n}\prod_{\substack{k\wedge d=1\\1\leq k\leq d}}\left(X-\exp\left(\frac{2ik\pi}{d}\right)\right)$$

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

On démontre par récurrence forte sur n dans $\mathbf{N}^*$ l'assertion $(\mathbf{H}_n)$: Φ_n est unitaire à coefficients entiers. On a $\Phi_1 = X - 1$ et donc $(\mathbf{H}_1)$ est vrai. Si $(\mathbf{H}_d)$ est vrai pour $d < n$, alors $\prod_{\substack{d|n \\ d\neq n}} \Phi_d$ est un polynôme unitaire à coefficients entiers, que l'on note P. Alors on peut effectuer la division euclidienne de $X^n - 1$ par P dans $\mathbf{Z}[X]$ puisque P est unitaire. C'est la même que dans $\mathbf{Q}[X]$ et donc le quotient est Φ_n. Il en résulte que Φ_n est unitaire à coefficients entiers. Par le principe de récurrence on en déduit en particulier que $\boxed{\Phi_n \text{ est à coefficients entiers.}}$

7. Puisque $\zeta^n = 1$, l'ordre de ζ est fini dans $\mathbf{C}^*$ et est un diviseur de n. On le note d. On a donc $\zeta^d = 1$ et, pour $m < d$, $\zeta^m \neq 1$. Pour m divisant d, puisque $X^m - 1 = \prod_{k|m} \Phi_k$, si $\Phi_m(\zeta) = 0$ alors $\zeta^m = 1$ et donc ζ n'est racine d'aucun Φ_m pour m divisant d et distinct de d. Il en résulte que ζ est racine de Φ_d. Soit ℓ premier à d. En appliquant le résultat de la question 5 avec $n = d$ et puisque ζ est racine de $X^d - 1$, on en déduit que ζ^ℓ est racine de P_ζ. Or pour k premier à d, l'application $\ell \mapsto k\ell$ est une bijection de $G(d)$ dans lui-même et donc, puisque ζ est de la forme $\exp(2i\pi k/d)$ avec k premier à d, pour tout ℓ premier à d, ζ^ℓ est racine de Φ_d et en fait on obtient ainsi toutes les racines de Φ_d, i.e. Φ_d est un polynôme à coefficients entiers, unitaire et dont toutes les racines sont des racines de P_ζ. On en déduit $\Phi_d \mid P_\zeta$ puis $P_\zeta = \Phi_d$ par minimalité de P_ζ. En conclusion $\boxed{P_\zeta = \Phi_d \text{ où } d \text{ est l'ordre de } \zeta \text{ dans } \mathbf{C}^*.}$