SPÉCIALE MP* : CORRIGÉ DU DEVOIR SURVEILLÉ

PARTIE I

I.1. Soit $\varphi\ : (d_1,d_2)\in D(m)\times D(n)\mapsto d=d_1d_2\in D(mn)$. Si $d\in D(mn)$ alors montrons que l'on peut écrire de manière unique $d=d_1d_2$ où $d_1\in D(m)$ et $d_2\in D(n)$.

Si $m=\prod\limits_{p\in\mathcal{P}}p^{\alpha(m)}$ et $n=\prod\limits_{p\in\mathcal{P}}p^{\alpha(n)}$, comme $m\wedge n=1$ alors $(\mathcal{P}\cap D(m))\cap(\mathcal{P}\cap D(n))=\emptyset$.

On pose alors $d_1=\prod\limits_{p\in\mathcal{P}\cap D(m)}p^{\alpha(d)}$ et $d_2=\prod\limits_{p\in\mathcal{P}\cap D(n)}p^{\alpha(d)}$. Ceci assure l'existence.

Unicité : si $d_1d_2=d_1'd_2'$ alors $d_1\wedge d_2'=1$ (d_1 et d_2' sont des diviseurs de 2 entiers premiers entre eux) donc $d_1|d_1'$. De même $d_1'|d_1$ donc $d_1=d_1'$ et on a $d_2=d_2'$.

On peut poser alors $\psi\ : d\in D(mn)\mapsto(d_1,d_2)\in D(m)\times D(n)$ qui est l'application réciproque de φ.

Conclusion : $D(mn)$ et $D(m)\times D(n)$ sont en bijection. .... $\boxed{4}$

On pouvait aussi poser directement $\psi(d)=(d\wedge m,d\wedge n)$ ce qui donne directement aussi la bijection entre $D_p(mn)$ et $D_p(m)\times D_p(n)$.

I.2. Première égalité :

on a évidemment $[\![1,n]\!]\supset\bigcup_{d|n}\{k\in[\![1,n]\!]\mid k\wedge n=d\}$ puis si $k\in[\![1,n]\!]$ alors on pose $d=k\wedge n$ et on peut conclure à l'inclusion dans l'autre sens.

Les E_d sont évidemment disjoints ! .... $\boxed{1}$

Deuxième égalité :

on a $k\wedge n=d\Leftrightarrow\dfrac{k}{d}\wedge\dfrac{n}{d}=1$. On pose $d'=\dfrac{n}{d}$ et $k'=\dfrac{k}{d}$ alors $k'\wedge d'=1$ et $k=k'd=k'\dfrac{n}{d'}$.

On a alors équivalence entre

$$k\in\bigcup_{d|n}\{k\in[\![1,n]\!]\mid k\wedge n=d\}\text{ et }k\in\bigcup_{d|n}\{\frac{kn}{d},\ k\in[\![1,d]\!]\mid k\wedge d=1\}\text{ (on enlève les ').}\qquad\boxed{2}$$

Là aussi, les F_d sont disjoints.

I.3. **a.** I est de manière évidente l'élément unité de $\mathcal{D}$. .... $\boxed{1}$

b. Si f est inversible alors $f*f^{-1}(1)=1$ d'où $f(1)\neq0$. .... $\boxed{1}$

Réciproque : si $f(1)\neq0$, cherchons $g\in\mathcal{D}$ tq $f*g=I$: Tout d'abord $g(1)=\dfrac{1}{f(1)}$.

On fait alors une récurrence forte : supposons que l'on ait calculé $g(k)$ pour $k\leqslant n$ alors

$$g(k+1)=-\frac{1}{f(1)}\sum_{d|n+1,d<n+1}g(d)f(n+1).$$

On peut ainsi déterminer une seule application $g\in\mathcal{D}$ telle que $f*g=I$ ce qui prouve le résultat. .... $\boxed{3}$

c. Vu le **b** μ est inversible. Si $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ alors

$$\mu*E(n)=\sum_{d=p_{i_1}\dots p_{i_l},i_1<\dots<i_l}(-1)^l\text{ pour }n\geqslant2,$$

les autres termes étant nuls. Or le coefficient $(-1)^l$ se répète autant de fois que l'on peut écrire un sous-ensemble à l éléments pris dans $[1, k]$, par conséquent

$$\mu * E(n) = \sum_{l=0}^{k} C_k^l (-1)^l = 0$$

et on vérifie que $\mu * E(1) = 1$ c.q.f.d. .... $\boxed{4}$

PARTIE II

II.1. a. Soit f une fonction multiplicative et $k \in \mathbb{N}^*$ tel que $f(k) \neq 0$, alors $1 \wedge k = 1$ donc $f(k.1) = f(k)f(1) = f(k)$ d'où $f(1) = 1$. .... $\boxed{1}$

Si $m \wedge n = 1$, on a vu au I.1 que, si $d|mn$ alors $d = d_1 d_2$ où $d_1|m$ et $d_2|n$, $d_1 \wedge d_2 = 1$ et que l'on a établi une bijection de l'ensemble $D(mn)$ des diviseurs de mn sur l'ensemble $D(m) \times D(n)$. On a alors

$$f * g(mn) = \sum_{d_1|m, d_2|n} f(d_1)f(d_2)g(m/d_1)g(n/d_2) = f * g(m).f * g(n) \qquad \boxed{2}$$

et $f * g(1) = 1 \neq 0$.

b. On raisonne par l'absurde alors $\{mn,\ (m, n) \in \mathbb{N}^{*2} \mid f(mn) \neq f(m)f(n)\}$ est un sous-ensemble non vide de $\mathbb{N}$; il admet donc un élément minimal mn.

Posons $h = f * g$, si $mn = 1$ alors on aurait $f(1)^2 \neq f(1)$ i.e. $f(1) \neq 1$ et donc $h(1) = f(1)g(1) = f(1) \neq 1$ ce qui est impossible. .... $\boxed{1}$

Si $mn > 1$, $ab < mn$ et $a \wedge b = 1$ alors $f(ab) = f(a)f(b)$. On a alors

$$\begin{aligned} h(mn) &= f(mn) + \sum_{ab<mn, a|m, b|n} f(a)g(m/a)f(b)g(n/b) \\ &= h(m)h(n) + f(mn) - f(m)f(n) \\ &\neq h(m)h(n) \end{aligned}$$

ce qui est impossible. On arrive bien à la conclusion attendue. .... $\boxed{3}$

Comme f et I sont multiplicatives et que $f * f^{-1} = I$ on peut déduire de ce qui précède que f^{-1} est multiplicative. .... $\boxed{1}$

c. On trouve immédiatement que $\mathcal{Q} = \{p^s, p \in \mathcal{P}, s \in \mathbb{N}^*\}$. .... $\boxed{3}$

$\mathcal{Q}$ est minimal : en effet s'il existe un ensemble générateur $\mathcal{Q}'$ strictement inclus dans $\mathcal{Q}$ qui ne contient pas p^α alors on peut définir f et g telles que $f = g = 1$ sur $\mathcal{Q} \setminus \{p^\alpha\}$ et $f(p^\alpha) = 0$, $g(p^\alpha) = 1$. On vérifie que f et g sont multiplicatives et que $f \neq g$. . $\boxed{3}$

d. Comme E est multiplicative alors μ l'est aussi. .... $\boxed{2}$

Enfin, on sait que ω_α est fortement multiplicative. .... $\boxed{1}$

II.2. a. Si p premier divise mn avec $m \wedge n = 1$ alors il divise soit m soit n donc

$$\begin{aligned} \Phi_\alpha(mn) &= m^\alpha n^\alpha \prod_{p \in \mathcal{P},\ p|mn} \left(1 - \frac{1}{p^\alpha}\right) \text{ et, en utilisant le I.1} \\ &= m^\alpha \prod_{p \in \mathcal{P},\ p|m} \left(1 - \frac{1}{p^\alpha}\right) n^\alpha \prod_{p \in \mathcal{P},\ p|n} \left(1 - \frac{1}{p^\alpha}\right) \end{aligned}$$

donc Φ est multiplicative. Il suffit alors de vérifier l'égalité pour $n = p^k$ où p est un nombre premier. Or $\Phi_\alpha(p^k) = p^{k\alpha}\left(1 - \dfrac{1}{p^\alpha}\right)$ qui est égal à $\mu * \omega_\alpha(p^k)$ c.q.f.d. .... $\boxed{3}$

b. On sait que ω_α est fortement multiplicative donc on vérifie l'égalité sur $\mathcal{Q}$:

$$\omega_\alpha * (\mu.\omega_\alpha)(p^\beta) = \omega_\alpha(p^\beta)\omega_\alpha(1) - \omega_\alpha(p^{\alpha-1}\omega_\alpha(p) = 0$$

et $\omega_\alpha * (\mu.\omega_\alpha)(1) = 1$ On a donc $\omega_\alpha^{-1} = \mu\omega_\alpha$. .... $\boxed{2}$

On en déduit $\Phi_\alpha^{-1} = \mu^{-1} * \omega_\alpha^{-1} = E * (\mu\omega_\alpha)$ ce qui donne la relation attendue. .... $\boxed{1}$

II.3. **a.** Si (1) est vraie alors, pour $n \in \mathbb{N}^*$ donné, on a

$$g(n) = \prod_{d|n} (f(d))^{a(n/d)} = \prod_{d|n} \exp[a(n/d)\ln(f(d))] = \exp(a * \ln f)(n).$$

Comme $g > 0$ alors on obtient $\ln g = a * \ln f$ qui est directement équivalent à $\ln f = a^{-1} * \ln g$ c.q.f.d. .... $\boxed{2}$

b. En posant $\theta(m) = \dfrac{P(m)}{m^{\varphi(m)}}$ et en tenant compte du fait que $\mu * E = I$, il suffit de prouver la relation

$$\forall n \in \mathbb{N}^*, \frac{n!}{n^n} = \prod_{d|n} \theta(d).$$

Or on a $\dfrac{n!}{n^n} = \displaystyle\prod_{k=1}^{n} \frac{k}{n} = \prod_{d|n} \left(\prod_{k \wedge n = d} \frac{k}{n} \right)$.

Soit $d \in D(n)$, avec $E_d = \{k \in [1, n] | k \wedge n = d\}$ et $F_d = \{k' \in [1, n/d] | k' \wedge (n/d) = 1\}$.

L'application : $k' \in F_d \mapsto dk' \in E_d$ est bijective donc $\displaystyle\prod_{k \in E_d} \frac{k}{n} = \prod_{k' \in F_d} \frac{k'}{(n/d)} = \theta(n/d)$

et comme $\displaystyle\prod_{d|n} \theta(n/d) = \prod_{d|n} \theta(d)$ on en déduit $\dfrac{n!}{n^n} = \displaystyle\prod_{d|n} \theta(d)$ c.q.f.d. .... $\boxed{6}$

c. On a $H(n) = \displaystyle\sum_{d|n} \left(\sum_{k \in E_d} h\left(\frac{k}{n}\right) \right) = \sum_{d|n} \left(\sum_{k' \in F_d} h\left(\frac{k}{(n/d)}\right) \right) = \sum_{d|n} \widetilde{H}\left(\frac{n}{d}\right) = E * \widetilde{H}(n)$

donc $H = E * \widetilde{H}$. .... $\boxed{3}$

On termine par $E^{-1} * H = \widetilde{H}$ i.e. $\widetilde{H} = \mu * H$.

En prenant $h(x) = \exp(2i\pi x)$ alors $\widetilde{H}(n)$ est la somme des racines primitives $n^{\text{ièmes}}$ de l'unité. Cette somme vaut donc $(\mu * H)(n) = \displaystyle\sum_{d|n} \mu(d) H(d/n)$. Mais on sait ici que $H = I$ (calcul classique). On a donc $\widetilde{H}(n) = \mu(n)$ c.q.f.d. .... $\boxed{2}$

PARTIE III

III.1. **a.** Si d désigne un diviseur de N, on note $O_d = \{e^{i2k\pi/n},\ k \in E_d\}$. Vu le I.2, on sait que les $(O_d)_{d|N}$ forment une partition de U_N et, en posant $d' = n/d$, on peut écrire $O_d = \{e^{i2k'\pi/d'},\ k' \wedge d' = 1\}$ ensemble des racines primitives de $\mathbb{U}_{d'}$ d'où

$$X^N - 1 = \prod_{\zeta \in U_N} (X - \zeta) = \prod_{d|N} \left(\prod_{\zeta \in O_d} (X - \zeta) \right) = \prod_{d'|N} \Psi_{d'}(X). \qquad \boxed{4}$$

On a $\Psi_1(X) = X - 1$ et raisonnons par récurrence (forte) sur N :

si $\Psi_m \in \mathbb{Z}[X]$ pour $m < N$ alors $\Psi_N(X) = \dfrac{X^N - 1}{F(X)}$ où $F(X) = \displaystyle\prod_{d|N, d<N} \Psi_d(X)$. Or F est un polynôme normalisé donc $\Psi_N \in \mathbb{Z}[X]$. .... $\boxed{4}$

b. On déduit du a) et du résultat du préliminaire que $c_k(n) \in \mathbb{Z}$. Si $n = 1$, $c_k(1)$ n'est autre que $\widetilde{H}(k)$ du I.4.c. et donc $c_k(1) = \mu(k)$. .... $\boxed{2}$

III.2. Soit $g(p) = \frac{1}{k}\sum_{m=0}^{k-1}\widehat{f}(m)\zeta^{-mp}$:

$$\sum_{p=0}^{k-1}\widehat{g}(p)\zeta^{mp} = \frac{1}{k}\sum_{(p,q)\in[0,k-1]} f(q)\zeta^{p(m-q)} = \frac{1}{k}\sum_{q=0}^{k-1} f(q)\left(\sum_{p=0}^{k-1}\zeta^{p(m-q)}\right).$$

Or $\sum_{p=0}^{k-1}\zeta^{p(m-q)} = k$ si $m-q\equiv 0[k]$ et vaut 0 dans les autres cas. Si m est choisi dans $[0,k-1]$ alors la somme considérée vaut $\widehat{f}(m)$ (en remarquant que $\widehat{f}(0) = f(k)$). Ceci prouve bien l'existence de g. L'unicité est en fait assurée par la symétrie des formules. $\boxed{3}$

III.3. a. Comme $(m+k)\wedge k = m\wedge k$ on peut affirmer que s_k est k-périodique. . . . . $\boxed{1}$

On utilise alors la question 2. pour écrire que $s_k(m) = \sum_{p=0}^{k-1}\widehat{a}_k(p)\zeta^{mp}$. On sait que $a_k(p) = \frac{1}{k}\sum_{q=0}^{k-1}\widehat{s}_k(q)\zeta^{-pq}$ d'où, si l'on reporte,

$$a_k(p) = \frac{1}{k}\sum_{q=0}^{k-1}\zeta^{-pq}\left(\sum_{d|q\wedge k} f(d)g(k/d)\right). \tag{a}$$

Si $d|q\wedge k$ alors $d|k$ et si on se donne $d\in D(k)$ alors $d|q\wedge k \Leftrightarrow d|q$ donc on peut réécrire l'égalité (a) sous la forme :

$$a_k(p) = \frac{1}{k}\sum_{d|k}\left(\sum_{d|q,q\in[0,k-1]}\zeta^{-pq}f(d)g(k/d)\right) = \frac{1}{k}\sum_{d|k}f(d)g(k/d)\sum_{d|q,q\in[0,k-1]}\zeta^{-pq}. \tag{b}$$

Maintenant, si $d\in D(k)$ alors l'application : $c\in[0,k/d-1]\mapsto cd\in\{q\in[0,k-1], d|q\}$ est bijective d'où : $\sum_{d|q,q\in[0,k-1]}\zeta^{-pq} = \sum_{c=0}^{k/d-1}\zeta^{-pdc} = \begin{cases}0 & \text{si } pd\not\equiv 0[k]\\ k/d & \text{si } pd\equiv 0[k]\end{cases}$ car $\zeta^{-pd}\in U_{k/d}$ et $\zeta^{-pq}=1$ ssi $qd\equiv 0[k]$.

En reportant dans (b), on obtient

$$a_k(p) = \frac{1}{k}\sum_{d|k}f(d)g(k/d)\left(\sum_{c=0}^{k/d-1}\zeta^{-pdc}\right). \tag{c}$$

Comme $d\mapsto k/d$ est une involution dans $D(k)$, (c) nous donne :

$$a_k(p) = \frac{1}{k}\sum_{d|k}f(k/d)g(d)\left(\sum_{c=0}^{d-1}\zeta^{-pkc/d}\right). \tag{d}$$

Or on a vu que la somme entre parenthèses valait d si $d|m$ et 0 autrement. On peut alors conclure, à l'aide de (d) que

$$a_k(p) = \frac{1}{k}\sum_{d|k,d|m} df(k/d)g(d).$$ $\boxed{8}$

b. On prend ici $f=\omega_1$ et $g=\mu$ et on veut prouver que $s_k(n) = c_k(n)$. D'après les résultats ci-dessus, on a $s_k(n) = \sum_{p=0}^{k-1}\widehat{a}_k(p)\zeta^{pm}$ où

$$a_k(p) = \sum_{d|(p\wedge k)}\frac{d}{k}\omega_1(k/d)\mu(d) = \sum_{d|(p\wedge k)}\mu(d) = E*\mu(p\wedge k) = I(p\wedge k).$$

Ceci nous donne donc $s_k(n) = \sum_{p\wedge k=1, p\in[0,k-1]} \zeta^{pn} = c_k(n)$ car $a \in \mathcal{R}_k \mapsto a^p \in \mathcal{R}_k$ pour $p \wedge n = 1$ est une bijection, on a bien le résultat annoncé. . . . . $\boxed{4}$

III.4. a. $\Gamma(a)$ et $\Delta(a)$ sont les fonctions de a respectivement à gauche et à droite de l'égalité. La fonction Δ est clairement multiplicative, prouvons qu'il en est de même pour $\Gamma(a)$: définissons pour cela la fonction χ par $\chi(x) = \begin{cases} 1 & \text{si } x \wedge N = 1 \\ 0 & \text{si } x \wedge N \neq 1 \end{cases}$. χ est fortement multiplicative (propriétés de divisibilité), la fonction $\chi.\mu$ est aussi multiplicative et comme $\Gamma = (\chi.\mu) * \omega_1$, on sait (I - 2 ° - a) que Γ est multiplicative. . . . . $\boxed{3}$

Il suffit donc de prouver que $\Gamma(p^s) = \Delta(p^s)$ pour $p \in \mathcal{P}$ et $s \in \mathbb{N}^*$: or

$$\Delta(p^s) = \begin{cases} p^s\left(1 - \dfrac{1}{p}\right) & \text{si } p \notin D(N) \\ p^s & \text{si } p|N \end{cases}$$

$$\Gamma(p^s) = \begin{cases} p^s\mu(1) + p^{s-1}\mu(p) = p^s - p^{s-1} & \text{si } p \notin D(N) \\ p^s\mu(1) = p^s & \text{si } p|N \end{cases}$$

et donc $\Gamma(p^s) = \Delta(p^s)$ c.q.f.d. . . . . $\boxed{3}$

b. On reprend l'expression de $c_k(n)$ du 3 ° - b) ci-dessus,

$$(e) \qquad c_k(n) = \sum_{d|a} d\mu(aN/d) = \sum_{d|a} \frac{a}{d}\mu(dN)$$

en utilisant l'involution $d \mapsto a/d$ de $D(a)$.

Si $d \wedge N \neq 1$ alors on a $\mu(dN) = 0$ et si $d \wedge N = 1$ alors $\mu(dN) = \mu(d)\mu(N)$ donc (e) s'écrit :

$$c_k(n) = \sum_{d|a, d\wedge N=1} \frac{a}{d}\mu(d)\mu(N) = \mu(N) \sum_{d|a, d\wedge N=1} \frac{a}{d}\mu(d)$$

et, grâce au a) ci-dessus,

$$(f) \qquad c_k(n) = a\mu(N) \prod_{p\in\mathcal{P}, p|a, p\notin D(N)} \left(1 - \frac{1}{p}\right).$$

Or $\mathcal{A} = \{p \in \mathcal{P}, p|a \text{ et } p \in D(N)\}$ et $\mathcal{B} = \{p \in \mathcal{P}, p|N\}$ forment un partage de $\mathcal{C} = \{p \in \mathcal{P}, p|aN\}$. Comme $\varphi(N) = N \prod_{p\in\mathcal{B}} \left(1 - \dfrac{1}{p}\right)$ et $\varphi(aN) = aN \prod_{p\in\mathcal{C}} \left(1 - \dfrac{1}{p}\right)$ alors $a \prod_{p\in\mathcal{A}} \left(1 - \dfrac{1}{p}\right) = \dfrac{\varphi(aN)}{\varphi(N)}$ et donc

$$\boxed{c_k(n) = \mu(N)\frac{\varphi(aN)}{\varphi(N)} = \mu(N)\frac{\varphi(aN)}{\varphi(N)}.} \qquad \boxed{5}$$