À rendre pour le mardi 22 septembre

PROBLÈME 1

Notations et rappels

Étant donnés deux entiers relatifs a et b, le plus grand diviseur commun de a et b sera noté PGCD (a, b) ou $a \wedge b$. On rappelle que $a \wedge 0 = a$.
a est dit premier avec b si $a \wedge b = 1$.

On notera $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ inversibles pour la multiplication et que $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{k},\ k \in \mathbb{Z} \text{ et } k \wedge n = 1\}$. On rappelle que $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe dont le cardinal est $\phi(n)$, avec ϕ l'indicatrice d'Euler. En particulier si k est dans $\mathbb{Z}$, avec $k \wedge n = 1$, alors dans $\mathbb{Z}/n\mathbb{Z}$, on a : $\overline{k}^{\phi(n)} = \overline{1}$.

Partie I : Étude du groupe $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ quand $n = p^\alpha$

On suppose que n s'écrit sous la forme $n = p^\alpha$, où p est un entier premier, et α un entier naturel supérieur ou égal à 2.
On admet qu'il existe un entier b, dont la classe $\overline{b}$ est d'ordre $p-1$ dans $((\mathbb{Z}/p\mathbb{Z})^*, \times)$, c'est à dire que : $(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{b}, ..., \overline{b}^{p-2}\}$ et $\overline{b}^{p-1} = \overline{1}$.

1. Montrer que l'un au moins des deux entiers b^{p-1} ou $(b+p)^{p-1}$ n'est pas congru à 1 modulo p^2 : on notera c l'un des nombres b ou $b+p$ de façon à ce que c^{p-1} ne soit pas congru à 1 modulo p^2.

2. Montrer par récurrence que, pour tout entier naturel r, il existe un entier k_r, premier avec p tel que $c^{p^r(p-1)} = 1 + k_r \times p^{r+1}$. En déduire que $\overline{c}$ appartient à $(\mathbb{Z}/n\mathbb{Z})^*$.

3. Soit r l'ordre de $\overline{c}$ dans le groupe $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ (le plus petit entier naturel non nul tel que : $\overline{c}^r = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$).

- ***a.*** Expliquer pourquoi r divise $p^{\alpha-1}(p-1)$ et pourquoi $(p-1)$ divise r.
- ***b.*** En déduire qu'il existe un entier naturel β inférieur ou égal à $\alpha - 1$ tel que $r = p^\beta(p-1)$.
- ***c.*** Montrer finalement que $\beta = \alpha - 1$ et que $\overline{c}$ est un générateur de $((\mathbb{Z}/n\mathbb{Z})^*, \times)$.

4. Application : Déterminer un générateur de $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ puis un générateur de $((\mathbb{Z}/49\mathbb{Z})^*, \times)$.

Partie II : Nombres de Carmichaël

L'objet de cette partie est la caractérisation de certains nombres, appelés nombres de Carmichaël.
On rappelle que pour tout entier naturel premier p, et tout a entier premier avec p, $a^{p-1} \equiv 1 \bmod p$.
La réciproque n'est pas vraie ; un nombre n est appelé nombre de Carmichaël si :

a) n n'est pas premier
b) pour tout nombre a premier avec n, a^{n-1} est congru à 1 modulo n.

1. Montrer que si $n = p_1 \times p_2 \times \ldots \times p_k$ où p_1, p_2, ..., p_k sont des nombres premiers deux à deux distincts tels que $(p_i - 1)$ divise $(n-1)$ pour tout i de $\{1, 2, \ldots, k\}$, avec $k \geq 2$, alors n est un nombre de Carmichaël.

Montrer en particulier que 561, 10585 sont des nombres de Carmichaël.

2. Dans toute cette question, on suppose que n est un nombre de Carmichaël et l'on désire établir la réciproque du résultat obtenu en question 1.

a. On suppose tout d'abord que n est une puissance de 2, $n = 2^\alpha$, où α est un entier ≥ 2.
Quel est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$? En déduire que pour tout entier a impair, on ne peut avoir $a^{2^{\alpha-1}} \equiv 1[n]$ sauf si $a \equiv 1[n]$; que peut-on conclure ?

b. On suppose désormais que n admet au moins un facteur premier impair p_1 et l'on note p_1, p_2, …, p_k les facteurs premiers de n ; la décomposition de n est alors $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

i. Soit ω un entier dont la classe modulo $p_1^{\alpha_1}$ est un générateur de $((\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^*, \times)$; ω existe d'après la partie I. Montrer qu'on peut trouver un entier t tel que :
$t \equiv \omega \bmod p_1^{\alpha_1}$ et, pour tout i (s'il en existe) tel que $2 \leq i \leq k$, $t \equiv 1 \bmod p_i^{\alpha_i}$.
Montrer qu'alors $t^{n-1} \equiv 1[n]$.

ii. En déduire que $p_1^{\alpha_1 - 1}(p_1 - 1)$ divise $(n-1)$, puis que $\alpha_1 = 1$, et enfin que $(p_1 - 1)$ divise $(n-1)$.

iii. Montrer que n est nécessairement impair et que n peut s'écrire sous la forme $n = p_1 \times p_2 \times \ldots \times p_k$ où p_1, p_2, …, p_k sont des nombres premiers deux à deux distincts tels que $(p_i - 1)$ divise $(n-1)$ pour tout i de $\{1, 2, \ldots, k\}$. Conclure.

3. Montrer qu'un nombre de Carmichaël admet au moins trois facteurs premiers.

4. Résoudre l'équation $85p - 16k = 1$, où (k, p) appartient à $\mathbb{Z}^2$.
Déterminer le plus petit nombre de Carmichaël divisible par 5 et 17.

PROBLÈME 2

Notations

On note $\lfloor x \rfloor$ la partie entière du nombre réel x, c'est à dire le plus grand nombre entier inférieur ou égal à x.
On note $\mathcal{P}$ l'ensemble des nombres premiers.
On note $m \wedge n$ le plus grand commun diviseur (pgcd) des entiers naturels n et m.
Si a et b sont des entiers relatifs, on note $[\![a, b]\!] = \{k \in \mathbb{Z},\ a \leqslant k \leqslant b\}$.
L'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{C}$ est noté $\mathcal{M}_n(\mathbb{C})$.
La matrice identité de $\mathcal{M}_n(\mathbb{C})$ est notée I_n.
Le terme d'indice (i, j) d'une matrice $M \in \mathcal{M}_n(\mathbb{C})$ est noté $m_{i,j}$ et on note $M = (m_{i,j})_{(i,j)\in[\![1,n]\!]^2}$ ou plus simplement $M = (m_{i,j})$ lorsque la taille de M est implicite.
Pour $n \in \mathbb{N}^*$, on note $\mathcal{D}_n$ l'ensemble des nombres entiers naturels divisant n et on écrit $\sum_{d|n} = \sum_{d\in\mathcal{D}_n}$ la somme sur tous les nombres entiers naturels d divisant n.
Une *fonction arithmétique* est une fonction $f : \mathbb{N}^* \to \mathbb{C}$. L'ensemble des fonctions arithmétiques est noté $\mathbb{A}$.
On dit qu'une fonction arithmétique $f \in \mathbb{A}$ est *multiplicative* si

$$\begin{cases} f(1) \neq 0 \\ \forall (m, n) \in\ (\mathbb{N}^*)^2,\ m \wedge n = 1 \implies f(mn) = f(m)f(n) \end{cases}$$

On note $\mathbb{M}$ l'ensemble des fonctions arithmétiques multiplicatives.
On note $\mathbf{1}$, δ et $\mathbf{I}$ les fonctions arithmétiques

$$\mathbf{1} : \begin{cases} \mathbb{N}^* \to \mathbb{C} \\ n \mapsto 1 \end{cases} \quad , \quad \delta : \begin{cases} \mathbb{N}^* \to \mathbb{C} \\ n \mapsto \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geqslant 2 \end{cases} \end{cases} \quad , \quad \mathbf{I} : \begin{cases} \mathbb{N}^* \to \mathbb{C} \\ n \mapsto n \end{cases}$$

On remarque que ces trois fonctions arithmétiques sont multiplicatives.
Si f et g sont deux fonctions arithmétiques, le *produit de convolution* de f et g est la fonctions

arithmétique notée $f * g$ définie par

$$\forall n \in \mathbb{N}^*,\ (f*g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

A. Propriétés générales de la loi $*$

1. Vérifier que δ est un élément neutre pour la loi $*$.

Pour tout $n \in \mathbb{N}^*$, on note $\mathcal{C}_n = \{(d_1, d_2) \in (\mathbb{N}^*)^2,\ d_1 d_2 = n\}$.

2. Justifier que, pour tout $n \in \mathbb{N}^*$,

$$(f*g)(n) = \sum_{(d_1,d_2)\in\mathcal{C}_n} f(d_1) g(d_2)$$

3. En déduire que $*$ est commutative.

4. De même, en exploitant l'ensemble $\mathcal{C}'_n = \{(d_1, d_2, d_3) \in (\mathbb{N}^*)^3,\ d_1 d_2 d_3 = n\}$, montrer que $*$ est associative.

5. Que peut-on dire de $(\mathbb{A}, +, *)$?

6. Écrire un programme en PYTHON qui à deux fonctions f, g, renvoie la fonction $f * g$.

B. Groupe des fonctions multiplicatives

7. Soient f et g deux fonctions multiplicatives. Montrer que si

$$\forall p \in \mathcal{P},\ \forall k \in \mathbb{N}^*,\ f(p^k) = g(p^k)$$

alors $f = g$.

8. Soient m et n deux entiers naturels premiers entre eux. Montrer que l'application

$$\pi : \begin{cases} \mathcal{D}_n \times \mathcal{D}_m \to \mathcal{D}_{mn} \\ (d_1, d_2) \mapsto d_1 d_2 \end{cases}$$

est bien définie et réalise une bijection entre $\mathcal{D}_n \times \mathcal{D}_m$ et $\mathcal{D}_{mn}$.

9. En déduire que si f et g sont deux fonctions multiplicatives, alors $f * g$ est encore multiplicative.

10. Soit f une fonction multiplicative. Montrer qu'il existe une fonction multiplicative g telle que

$$\forall p \in \mathcal{P},\ \forall k \in \mathbb{N}^*,\ g(p^k) = -\sum_{i=1}^{k} f(p^i) g(p^{k-i})$$

et qu'elle vérifie $f * g = \delta$.

11. Que dire de l'ensemble $\mathbb{M}$ muni de la loi $*$?

C. La fonction de Möbius

Soit μ la fonction arithmétique définie par

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

12. Montrer que μ est multiplicative.

13. Montrer que $\mu * \mathbf{1} = \delta$.

14. Soit $f \in \mathbb{A}$ et soit $F \in \mathbb{A}$ telle que, pour tout $n \in \mathbb{N}^*$, $F(n) = \sum_{d|n} f(d)$. Montrer que pour tout $n \in \mathbb{N}^*$,

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

On note φ la fonction indicatrice d'Euler, définie par :

$$\forall n \in \mathbb{N}^*,\ \varphi(n) = \text{card}\{k \in [\![1, n]\!],\ k \wedge n = 1\}$$

15. Démontrer que $\varphi = \mu * \mathbf{I}$.

D. Déterminant de Smith

Soient f une fonction arithmétique, $n \in \mathbb{N}^*$ et $g = f * \mu$. On note $M = (m_{i,j})$ la matrice de $\mathcal{M}_n(\mathbb{C})$ de terme général $m_{i,j} = f(i \wedge j)$. On définit aussi la *matrice des diviseurs* $D = (d_{i,j})$ par

$$d_{i,j} = \begin{cases} 1 & \text{si } j \text{ divise } i, \\ 0 & \text{sinon} \end{cases}$$

Soit M' la matrice de terme général $m'_{i,j} = \begin{cases} g(j) & \text{si } j \text{ divise } i, \\ 0 & \text{sinon} \end{cases}$.

16. Montrer que $M = M' D^\top$ où $D^\top$ est la transposée de D.

17. En déduire que le déterminant de M vaut

$$\det(M) = \prod_{k=1}^{n} g(k)$$