EXAMEN DU COURS DE M1 THÉORIE DES NOMBRES 1

Durée : 2h

Tous les appareils électroniques sont interdits

Le seul document autorisé est une feuille A4 recto avec un résumé de formules et résultats de votre choix.

Toutes les réponses doivent être justifiées.

Exercice 1.

(1) Faire la liste de tous les générateurs du groupe cyclique $(\mathbf{Z}/7\mathbf{Z})^\times$.

(2) Déterminer le plus petit entier $\mathrm{N} \geq 2$ tel que le groupe $(\mathbf{Z}/\mathrm{N}\mathbf{Z})^\times$ ne soit pas cyclique.

Exercice 2. Soit $\mathrm{S} \subset \{1, 2, \dots\}$ le sous-ensemble formé des entiers ≥ 1 sans facteur carré.

(1) Démontrer que tout entier $n \geq 1$ s'écrit de façon unique comme le produit du carré d'un entier ≥ 1 et d'un élément de S.

(2) Démontrer que la série $\sum_{n \in \mathrm{S}} \frac{1}{n}$ diverge en utilisant le fait que si a_k et b_ℓ sont des suites des nombres réels positifs sommables, alors $\sum_{k,\ell \geq 1} a_k b_\ell = (\sum_{k \geq 1} a_k)(\sum_{\ell \geq 1} b_\ell)$.

(3) En déduire que la suite

$$\prod_{p < \mathrm{N}} \left(1 + \frac{1}{p}\right),$$

où le produit parcourt les nombres premiers $p < \mathrm{N}$, tend vers l'infini lorsque $\mathrm{N} \to +\infty$.

(4) En utilisant l'inégalité $e^x > 1 + x$ pour tout $x > 0$, conclure que la série $\sum_p \frac{1}{p}$ diverge.

Exercice 3. Soit ℓ un nombre premier. Considérons le polynôme

$$\Phi_\ell(\mathrm{T}) = \mathrm{T}^{\ell-1} + \mathrm{T}^{\ell-2} + \cdots + 1 = \frac{\mathrm{T}^\ell - 1}{\mathrm{T} - 1}.$$

Supposons qu'il existe un nombre *fini* de nombres premiers congrus à 1 modulo ℓ (autrement dit dans la progression arithmétique $1 + n\ell$) et notons-les $p_1, \dots, p_\mathrm{N}$. Posons $a = \ell p_1 \cdots p_\mathrm{N}$.

(1) Démontrer qu'il existe un nombre premier p divisant le nombre entier $\Phi_\ell(a)$.

(2) Démontrer qu'un tel p n'appartient pas à l'ensemble $\{\ell, p_1, \dots, p_\mathrm{N}\}$.

(3) En considérant $\Phi_\ell(a)$, démontrer que $a^\ell \equiv 1 \bmod p$ et $a \not\equiv 1 \bmod p$.

(4) En déduire que ℓ divise $p - 1$.

(5) Conclure qu'il existe une infinité de nombres premiers de la forme $1 + n\ell$.

Exercice 4. Soient $k \geq 1$ un entier et p un nombre premier.

(1) Démontrer l'inégalité $\binom{2k+1}{k} \leq 4^k$.

(2) Démontrer que $\binom{2k+1}{k}$ est divisible par tout nombre premier p tel que $k+2 \leq p \leq 2k+1$.

(3) Soit $n \geq 4$ pair. Démontrer que $\prod_{p \leq n-1} p \leq 4^{n-1}$ implique $\prod_{p \leq n} p \leq 4^n$.

(4) Soit $n = 2k+1 \geq 3$. Démontrer que $\prod_{p \leq k+1} p \leq 4^{k+1}$ implique $\prod_{p \leq n} p \leq 4^n$.

(5) Conclure que l'inégalité $\prod_{p \leq n} p \leq 4^n$ est vraie pour tout $n \geq 2$.

Exercice 5. Soit $p \geq 3$ un nombre premier. Notons $(\frac{\cdot}{p})\colon \mathbf{Z}/p\mathbf{Z} \to \{-1, 0, 1\}$ le symbole de Legendre modulo p et posons

$$\mathrm{N}_p = |\{(x, y) \in (\mathbf{Z}/p\mathbf{Z})^2 \mid x^2 + y^2 = 1\}|.$$

(1) Démontrer l'égalité

$$\sum_{a \in \mathbf{Z}/p\mathbf{Z}} \left(\frac{a}{p}\right) = 0.$$

(2) Soit $a \in \mathbf{Z}/p\mathbf{Z}$. Démontrer que $x^2 = a$ possède exactement $1 + (\frac{a}{p})$ solutions dans $\mathbf{Z}/p\mathbf{Z}$.

(3) Démontrer la formule

$$\mathrm{N}_p = \sum_{\substack{a,b \in \mathbf{Z}/p\mathbf{Z} \\ a+b=1}} |\{x \in \mathbf{Z}/p\mathbf{Z} \mid x^2 = a\}| \cdot |\{y \in \mathbf{Z}/p\mathbf{Z} \mid y^2 = b\}|.$$

(4) En déduire l'égalité

$$\mathrm{N}_p = p + \sum_{\substack{a,b \in \mathbf{Z}/p\mathbf{Z} \\ a+b=1}} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(5) Démontrer les deux égalités

$$\sum_{\substack{a,b \in \mathbf{Z}/p\mathbf{Z} \\ a+b=1}} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \sum_{\substack{a \in \mathbf{Z}/p\mathbf{Z} \\ a \neq 1}} \left(\frac{a(1-a)^{-1}}{p}\right) = -\left(\frac{-1}{p}\right).$$

(6) En déduire la formule

$$\mathrm{N}_p = \begin{cases} p-1 & p \equiv 1 \bmod 4, \\ p+1 & p \equiv 3 \bmod 4. \end{cases}$$