DS 3 de mathématiques

Durée : 4h.

- Les calculatrices et autres technologies sont interdites.
- Une attention particulière sera portée à la qualité de la rédaction et à la rigueur du raisonnement. La copie doit être lisible, les pages numérotées, les calculs suffisamment détaillés, les résultats mis en valeur...
- Les 2 exercices et les 2 problèmes sont indépendants et peuvent être traités dans un ordre quelconque.
- Si vous repérez une possible erreur d'énoncé, vous êtes invité(e) à venir le signaler.

Dans tout le sujet, $\mathbb{P}$ désigne l'ensemble des nombres premiers.

1 Exercice – Contrôle technique

1. Déterminer les $x \in \mathbb{Z}$ solutions du système suivant :

$$\begin{cases} x \equiv 1\,[3] \\ x \equiv 2\,[5] \\ x \equiv 3\,[7] \end{cases}$$

2. (a) Montrer que $3^{10} \equiv -1\,[25]$.
   (b) Déterminer les deux derniers chiffres (dans l'écriture en base 10) de 53^{2025}.

2 Exercice – Théorème des quatre carrés

1. **Identité des quatre carrés d'Euler.**

   (a) Soient $u, v, w, z \in \mathbb{C}$. Montrer que

   $$(|u|^2 + |v|^2)(|w|^2 + |z|^2) = |uw - vz|^2 + |u\bar{z} + v\bar{w}|^2.$$

   (b) En déduire[1] que si $a, b, c, d, p, q, r, s \in \mathbb{Z}$, alors

   $$(a^2+b^2 + c^2 + d^2)(p^2 + q^2 + r^2 + s^2) = (ap - bq - cr + ds)^2 + (aq + bp - cs - dr)^2 + (ar + bs + cp + dq)^2 + (-as + br - cq + dp)^2.$$

Soit p un nombre premier impair. On note $q = \dfrac{p-1}{2}$.

2. Montrer que l'application $f : \left\{ \begin{array}{c} [\![0, q]\!] \to \mathbb{Z}/p\mathbb{Z} \\ u \mapsto \overline{u^2} \end{array} \right.$ est une injection.

3. En déduire qu'il existe $u, v \in [\![0, q]\!]$ et $d \in [\![1, p-1]\!]$ tels que $u^2 + v^2 + 1 = dp$.

On note m le plus petit entier naturel non nul tel qu'il existe $(x, y, z, t) \in \mathbb{Z}^4$ vérifiant

$$x^2 + y^2 + z^2 + t^2 = mp$$

et on fixe un tel quadruplet (x, y, z, t). On suppose par l'absurde que $m > 1$.

4. Montrer que m est bien défini et que $m < p$.

5. On note x', y', z', t' les entiers dans $]\!] - \dfrac{m}{2}, \dfrac{m}{2}[\![$ tels que

   $$x \equiv x'\,[m], y \equiv y'\,[m], z \equiv z'\,[m], t \equiv t'\,[m].$$

   Montrer qu'il existe $r \in [\![1, m-1]\!]$ tel que $x'^2 + y'^2 + z'^2 + t'^2 = mr$.

6. En déduire qu'il existe $x_2, y_2, z_2, t_2 \in \mathbb{Z}$, divisibles par m, tels que

   $$x_2^2 + y_2^2 + z_2^2 + t_2^2 = m^2 rp.$$

7. Obtenir une contradiction.

8. Montrer que tout entier naturel est somme de quatre carrés.[2]

[1] La seule vérification de la formule annoncée ne sera pas valorisée.

[2] Théorème dû à Lagrange, démontré en 1770.

3 Problème – Asymptotique de $\sum_{p\leq n} \frac{1}{p}$

Pour tout $n \in \mathbb{N}^*$, on désigne par $\mathbb{P}_n$ l'ensemble $\mathbb{P} \cap [\![1, n]\!]$.
Le but de l'exercice est de déterminer un équivalent de $\sum_{p\in\mathbb{P}_n} \frac{1}{p}$, quand $n \to +\infty$.

3.1 Préliminaires analytiques

1. En comparant, pour tout $k \in [\![1, n]\!]$ les valeurs de $\frac{1}{k}$, $\frac{1}{k+1}$ et $\int_k^{k+1} \frac{dt}{t}$, montrer que $\ln n \leq \sum_{k=1}^{n} \frac{1}{k} \leq \ln n + 1$.

2. Montrer de manière analogue que $\sum_{k=1}^{n} \ln k \geq n \ln n - n$.

   En déduire que $n! \geq \left(\frac{n}{e}\right)^n$.

3. Montrer que pour tout réel $x > 0$, on a l'égalité

$$e^x = \sum_{k=0}^{n} \frac{x^k}{k!} + \frac{1}{n!} \int_0^x (x-u)^n e^u du.$$

   En déduire que, pour tout réel $x > 0$,

$$0 \leq e^x - \sum_{k=0}^{n} \frac{x^k}{k!} \leq e^x \frac{x^{n+1}}{(n+1)!}.$$

3.2 Minoration

Soit $n \in \mathbb{N}^*$. Jusqu'à la fin du problème, on note $A_n = \sum_{p\in\mathbb{P}_n} \frac{1}{p}$ et $H_n = \sum_{k=1}^{n} \frac{1}{k}$.

4. Soit $m \in \mathbb{N}^*$. Montrer qu'il existe $r \in [\![1, \lfloor\sqrt{m}\rfloor]\!]$, $k \in \mathbb{N}$ et $p_1, \ldots, p_k$ deux à deux distincts dans $\mathbb{P}_m$ tels que $m = r^2 p_1 \ldots p_k$.

5. En déduire l'inégalité suivante :

$$H_n \leq \sum_{r=1}^{\lfloor\sqrt{n}\rfloor} \frac{1}{r^2} \left(\prod_{p\in\mathbb{P}_n} \left(1 + \frac{1}{p}\right) \right).$$

6. Montrer que $\displaystyle\sum_{r=1}^{N} \frac{1}{r^2} \leq 2$, pour tout $N \geq 1$.

7. En déduire que $e^{A_n} \geq \dfrac{1}{2} H_n$.

3.3 Majoration

Soit $n \in \mathbb{N}^*$. Pour tout $i \in \mathbb{N}^*$, on note f_i l'application définie de $(\mathbb{P}_n)^i$ dans $\mathbb{N}^*$ par

$$f_i : (p_1, \ldots, p_i) \mapsto p_1 \ldots p_i.$$

8. Soit $i \in \mathbb{N}^*$. Identifier les éléments de l'image de f_i et montrer qu'un élément dans l'image de f_i a au plus $i!$ antécédents.

9. Soit $k \in \mathbb{N}^*$. Déduire de la question précédente que :

$$\sum_{i=0}^{k} \frac{A_n^i}{i!} \leq H_{n^k} \quad \text{puis que} \quad e^{A_n} \left(1 - \frac{A_n^{k+1}}{(k+1)!}\right) \leq H_{n^k}.$$

On admet[3] qu'il existe une constante $C > 0$ telle que, pour tout $n \geq 3$, $A_n \leq C \ln(\ln n)$. Pour tout $n \geq 3$, on pose $k(n) = \lfloor \ln^2(\ln n) \rfloor$.

10. Montrer que $\dfrac{A_n^{k(n)+1}}{(k(n)+1)!} \to 0$, quand $n \to +\infty$.

11. Montrer[4] que $\ln\left(H_{n^{k(n)}}\right) \sim \ln(\ln n)$.

3.4 Conclusion

12. Montrer[5] que $\displaystyle\sum_{p \in \mathbb{P}_n} \frac{1}{p} \sim \ln(\ln n)$, quand $n \to +\infty$.

[3] Ceci mériterait d'être dans le sujet mais une erreur s'était glissée et a été détectée un peu tard...

[4] On rappelle que $u_n \sim v_n$ signifie que $\dfrac{u_n}{v_n} \to 1$, quand $n \to +\infty$.

[5] Résultat dû à Euler, publié en 1744.

4 Problème – Groupes de cardinal p^2 et pq

4.1 Théorème de Lagrange

Soit G un groupe, soit H un sous-groupe de G. On définit une relation $\mathcal{R}_H$ sur G par

$$\forall x, y \in G, x \,\mathcal{R}_H\, y \iff x^{-1}y \in H.$$

1. Montrer que $\mathcal{R}_H$ est une relation d'équivalence sur G.
2. Soit $x \in G$. Définir une bijection de H vers $\mathrm{cl}_{\mathcal{R}_H}(x)$.
3. En déduire que, si G est fini, alors $|H|$ divise $|G|$.
4. Soit G un groupe de cardinal p, où $p \in \mathbb{P}$. Montrer que, pour tout $x \in G \setminus \{e\}$, $G = \langle x \rangle$. À quel groupe G est-il isomorphe ?

4.2 Groupes d'ordre p^2

Soit G un groupe. On définit une relation $\mathcal{R}$ sur G par

$$\forall x, y \in G, x \,\mathcal{R}\, y \iff \exists g \in G : y = g^{-1}xg.$$

5. Montrer que $\mathcal{R}$ est une relation d'équivalence sur G.

Soit $x \in G$. On définit :

- le centralisateur de x par $C(x) = \{g \in G \mid gx = xg\}$;
- l'application $p_x : G \to \mathrm{cl}_{\mathcal{R}}(x)$ par : $\forall g \in G, p_x(g) = gxg^{-1}$.

6. Montrer que $C(x)$ est un sous-groupe de G.
7. Montrer que p_x est surjective et que

$$\forall g, g' \in G, p_x(g) = p_x(g') \iff g \,\mathcal{R}_{C(x)}\, g'.$$

8. On suppose G fini. En déduire que $|G| = |\,\mathrm{cl}_{\mathcal{R}}(x)| \times |C(x)|$.

On définit le centre de G par $Z_G = \bigcap_{h \in G} C(h)$. On rappelle que c'est un sous-groupe de G.

9. Montrer que $x \in Z_G \iff \mathrm{cl}_{\mathcal{R}}(x) = \{x\}$.

On suppose désormais que G est fini de cardinal p^n, où $p \in \mathbb{P}$ et $n \geq 1$. On note K le nombre de classes d'équivalence – pour $\mathcal{R}$ – *non réduites à un singleton* et on fixe un élément x_i dans chacune de ces classes, pour $i \in [\![1, K]\!]$.

10. Montrer que $p^n = |Z_G| + \sum_{i=1}^{K} |\operatorname{cl}_{\mathcal{R}}(x_i)|$.

11. En déduire que $|Z_G|$ est de la forme p^k, pour un $k \in [\![1, n]\!]$.

On suppose maintenant que G est de cardinal p^2 – avec $p \in \mathbb{P}$ – et que G n'est pas monogène. On fixe $x \in Z_G \setminus \{e\}$ et $y \in G \setminus \langle x \rangle$.

12. Montrer que les éléments $x^k y^\ell$, avec $(k, \ell) \in [\![0, p-1]\!]^2$, sont deux à deux distincts. En déduire que G est abélien.

On définit $f : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G, (\bar{k}, \bar{\ell}) \mapsto x^k y^\ell$.

13. Montrer que f est bien définie et que c'est un isomorphisme de groupes.

4.3 Groupes d'ordre pq

Soient H et K deux groupes, dont la loi de groupe est notée multiplicativement. On note $\mathrm{Aut}(H)$ le groupe des automorphismes de H – pour la composition – et on se donne un morphisme $f : K \to \mathrm{Aut}(H)$. Sur l'ensemble $H \times K$, on définit une loi de composition interne $*$ par $\quad \forall (h,k),(h',k') \in H \times K, (h,k) * (h',k') = (hf(k)(h'), kk')$.

14. Montrer que $*$ définit une structure de groupe sur l'ensemble $H \times K$.

15. On suppose que H et K sont abéliens.
Montrer que $(H \times K, *)$ est abélien ssi $\forall k \in K, f(k) = \mathrm{id}_H$.
Quelle structure de groupe retrouve-t-on sur $H \times K$ dans ce cas ?

16. Soit $n \geq 2$ un entier.

    (a) Soit $k \in \mathbb{Z}$ tel que $k \wedge n = 1$. Montrer que $m_k : \left\{ \begin{array}{c} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ \overline{u} \mapsto k\overline{u} \end{array} \right.$ est un automorphisme de $\mathbb{Z}/n\mathbb{Z}$.

    On rappelle qu'on note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. C'est l'ensemble des $\overline{k}$ tels que $k \wedge n = 1$ et c'est un groupe pour la multiplication.

    (b) Montrer que $f : \left\{ \begin{array}{c} (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ \overline{k} \mapsto m_k \end{array} \right.$ est bien défini et que c'est un isomorphisme de groupes.

On considère $p < q \in \mathbb{P}$. On admet que le groupe $\left((\mathbb{Z}/q\mathbb{Z})^\times, \times\right)$ est monogène.

17. Montrer qu'il existe un morphisme non trivial[6] de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ ssi $p \mid q-1$.

18. En déduire l'existence d'un groupe non abélien de cardinal pq si $p \mid q-1$.

19. Expliciter la construction d'un groupe non abélien de cardinal 21.

[6] c'est-à-dire différent de l'application constante égale à $\mathrm{id}_{\mathbb{Z}/q\mathbb{Z}}$