DS 3 de mathématiques – Corrigé

1 Exercice – Contrôle technique

1. Soit $x \in \mathbb{Z}$. On remarque que $7 \equiv 1\,[3]$ et $7 \equiv 2\,[5]$. Par le théorème des restes chinois, x est solution des deux premières équations ssi $x \equiv 7\,[15]$. Une relation de Bézout entre 15 et 7 est $1 \times 15 - 2 \times 7 = 1$. Donc, $x_0 = 3 \times 15 - 2 \times 7 \times 7 = -53$ vérifie $x_0 \equiv 3\,[7]$ et $x_0 \equiv 7\,[15]$.
   Par une nouvelle application du théorème des restes chinois, x est solution du système ssi $x \equiv x_0\,[105]$. Si on souhaite une solution positive, on peut remplacer x_0 par $x_0 + 105 = 52$.

2. (a) On a $3^3 = 27 \equiv 2\,[25]$. Donc, $3^9 = (3^3)^3 \equiv 2^3 \equiv 8\,[25]$ et $3^{10} \equiv 3 \times 8 \equiv -1\,[25]$.

   (b) On remarque que $53 \equiv 1\,[4]$. Donc, $53^{2025} \equiv 1\,[4]$. De plus, $53 \equiv 3\,[25]$ donc $53^{2025} \equiv 3^{2025}\,[25]$. On fait la division euclidienne de 2025 par 20 : $2025 = 20 \times 101 + 5$. Donc,

$$53^{2025} \equiv 3^{2025} = 3^5 \times (3^{20})^{101} \equiv 3^5 \equiv 3^3 \times 3^2 \equiv 18\,[25].$$

   On remarque que $93 \equiv 18\,[25]$ et $93 \equiv 1\,[4]$. Donc, par le théorème des restes chinois, $53^{2025} \equiv 93[100]$. Donc, ce nombre se termine par 93 dans son écriture en base 10.

2 Exercice – Théorème des quatre carrés

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

   (a) Si $a, b \in \mathbb{C}$, on rappelle que $|a+b|^2 = |a|^2 + |b|^2 + 2\mathrm{Re}(a\bar{b})$. Donc, avec les notations de l'énoncé,

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

   Les parties réelles se simplifient et par propriété des modules :

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

   (b) Soient $a, b, c, d, p, q, r, s \in \mathbb{Z}$.
   On pose $u = a + ib$, $v = c + id$, $w = p + iq$ et $z = r + is$. Alors, d'un part,

$$(|u|^2 + |v|^2)(|w|^2 + |z|^2) = (a^2 + b^2 + c^2 + d^2)(p^2 + q^2 + r^2 + s^2).$$

D'autre part,

$|uw-vz|^2 = \mathrm{Re}(uw-vz)^2+\mathrm{Im}(uw-vz)^2 = (ap-bq-cr+ds)^2+(aq+bp-cs-dr)^2$

ainsi que

$|u\bar{z}+v\bar{w}|^2 = \mathrm{Re}(u\bar{z}+v\bar{w})^2+\mathrm{Im}(u\bar{z}+v\bar{w})^2 = (ar+bs+cp+dq)^2+(-as+br-cq+dp)^2.$

La formule annoncée est alors obtenue par la question précédente.

2. Soient $u, v \in [\![0, q]\!]$ tels que $\overline{u^2} = \overline{v}^2$ dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi, p divise $u^2-v^2 = (u-v)(u+v)$. Comme p est premier, par le lemme d'Euclide, p divise $u-v$ ou p divise $u+v$. Mais $u-v \in [\![-q, q]\!]$ et $u+v \in [\![0, 2q]\!]$. Le seul multiple de p dans ces intervalles est 0 et on a donc $u = v$. Ainsi, f est injective.

3. D'après la question précédente, $\overline{u^2}$ prend $q+1$ valeurs différentes dans $Z/p\mathbb{Z}$, quand u varie dans $[\![0, q]\!]$. De même, pour $\overline{-v^2-1}$. Or, $\mathbb{Z}/p\mathbb{Z}$ est un ensemble à n éléments et $2q+2 = p+1 > 1$. Il existe donc $u, v \in [\![0, q]\!]$ tels que $\overline{u^2} = \overline{-v^2-1}$ dans $\mathbb{Z}/p\mathbb{Z}$. Et donc, il existe un entier d tel que $u^2+v^2+1 = dp$.
Comme $u, v \in [\![0, q]\!]$, $u^2+v^2+1 \in [\![1, 2q^2+1]\!] = [\![1, \dfrac{(p-1)^2}{2}+1]\!]$. On en déduit que $d \geq 1$ et que $d < \dfrac{(p-1)^2}{2p} \leq p$ (car $(p-1)^2 \leq p^2 \leq 2p^2$)). Ainsi, $d \in [\![1, p-1]\!]$.

4. Avec les notations de la question précédente, on a $x^2+y^2+z^2+t^2 = mp$ en prenant $x = u$, $y = v$, $z = 1$, $t = 0$ et $m = d$. Ainsi, l'ensemble des m considérés est non vide (il contient d) ; et il contient $d < p$. Ceci montre que m est bien défini et que $m < p$.

5. Par opérations usuelles sur les congruences, on a

$$x'^2+y'^2+z'^2+t'^2 \equiv x^2+y^2+z^2+t^2 \equiv 0\,[m].$$

Ainsi, on peut trouver un entier r tel que $x'^2+y'^2+z'^2+t'^2 = mr$. Comme chacun des entiers x', y', z' et t' est dans $]\!]-\dfrac{m}{2}, \dfrac{m}{2}[\![$, on a

$$x'^2+y'^2+z'^2+t'^2 \in [\![0, 4\times\frac{m^2}{4}]\!] = [\![0, m^2]\!].$$

Donc, $r \in [\![0, m]\!]$. Il reste à éliminer les possibilités $r = 0$ et $r = m$.
Si $r = 0$, on a nécessairement $x' = y' = z' = t' = 0$. Mais alors, $x^2+y^2+z^2+t^2$ serait divisible par m^2 et donc p serait divisible par m ; c'est absurde car on a montré que $m < p$ et qu'on a supposé que $m > 1$.
Si $r = m$, on a cette fois $x' = y' = z' = t' = \dfrac{m}{2}$. On peut donc écrire $x = \dfrac{m}{2}+k_x m$, et de même pour y, z et t. Alors,

$$x^2+y^2+z^2+t^2 = m^2+(k_x+k_y+k_z+k_t)m^2+(k_x^2+k_y^2+k_z+k_t)^2m^2$$

est divisible par m^2. De nouveau, on en conclut que m divise p, ce qui est absurde.

6. On multiplie les égalités vérifiées par les deux quadruplets (x, y, z, t) et (x', y', z', t'). On a donc :
$$(x^2 + y^2 + z^2 + t^2)(x'^2 + y'^2 + z'^2 + t'^2) = m^2 rp.$$
Par l'identité des quatre carrés d'Euler, on peut réécrire le membre de gauche sous la forme $x_2^2 + y_2^2 + z_2^2 + t_2^2$, avec

$x_2 = xx' - yy' - zz' + tt'$; $y_2 = xy' + yx' - zt' - z't$; $z_2 = xz' + yt' + zx' + ty'$; $t_2 = -xt' + yz' - zy' + tx'$.

Tel quel, ces nombres ne sont pas tous congrus à 0 modulo m. Mais on peut remplacer y par $-y$ et z par $-z$ (ce qui ne change pas le produit de la somme des 4 carrés) et considérer plutôt les quantités

$x_2 = xx' + yy' + zz' + tt'$; $y_2 = xy' - yx' + zt' - z't$; $z_2 = xz' - yt' - zx' + ty'$; $t_2 = -xt' - yz' + zy' + tx'$.

Alors $x_2 \equiv x^2 + y^2 + z^2 + t^2 \equiv 0\,[m]$ et, on a aussi $y_2 \equiv z_2 \equiv t_2 \equiv 0\,[m]$, ce qui conclut la question.

7. On a donc $\left(\frac{x_2}{m}\right)^2 + \left(\frac{y_2}{m}\right)^2 + \left(\frac{z_2}{m}\right)^2 + \left(\frac{t_2}{m}\right)^2 = rp$, où les nombres dans les parenthèses sont des entiers. Or, r est non nul et $r < m$; ceci contredit la minimalité de m pour la propriété énoncée avant la question 4. D'où la contradiction.

8. Par la question précédente, $m = 1$ et il existe donc 4 entiers x, y, z, t tels que $x^2 + y^2 + z^2 + t^2 = p$. Ainsi, tout nombre premier est somme de 4 carrés.
De plus, par l'identité des quatre carrés d'Euler, le produit de deux nombres qui sont sommes de quatre carrés est aussi somme de quatre carrés ; par récurrence immédiate, le produit d'un nombre quelconque de nombres qui sont sommes de quatre carrés est aussi une somme de quatre carrés.
Par le théorème fondamental de l'arithmétique, tout entier $n \geq 2$ est produit de nombres premiers, donc produit de nombres sommes de quatre carrés. Donc, tout entier naturel $n \geq 2$ est somme de quatre carrés. De plus, on a aussi $0 = 0^2 + 0^2 + 0^2 + 0^2$ et $1 = 0^2 + 0^2 + 0^2 + 1^2$.

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

3.1 Préliminaires analytiques

1. Soit $k \in [\![1, n]\!]$. Pour tout $t \in [k, k+1]$, on a $\frac{1}{k+1} \leq \frac{1}{t} \leq \frac{1}{k}$. Par propriété de croissance de l'intégrale, on a en intégrant entre k et $k+1$:

$$\frac{1}{k+1} \leq \int_k^{k+1} \frac{dt}{t} \leq \frac{1}{k}.$$

On somme ces inégalités pour k allant de 1 à $n-1$; par relation de Chasles, on a donc :

$$\sum_{k=1}^{n-1} \frac{1}{k+1} \leq \int_1^n \frac{dt}{t} \leq \sum_{k=1}^{n-1} \frac{1}{k}.$$

L'inégalité de droite donne $\ln n \leq \sum_{k=1}^{n-1} \frac{1}{k} \leq \sum_{k=1}^{n} \frac{1}{k}$. En ajoutant 1 à l'inégalité de gauche (et après changement de variable), on a aussi $\sum_{k=1}^{n} \frac{1}{k} \leq \ln n + 1$.

2. Soit $k \in [\![2, n]\!]$. On a $\ln k \geq \int_{k-1}^{k} \ln t dt$ car ln est croissante sur $[k-1, 1]$. En sommant pour k allant de 2 à n, il vient :

$$\sum_{k=1}^{n} \ln k = \sum_{k=2}^{n} \ln k \geq \int_1^n \ln t dt.$$

Or, cette intégrale vaut $\left[t \ln t - t\right]_1^n = n \ln n - n + 1 \geq n \ln n - n$. On a bien :

$$\sum_{k=1}^{n} \ln k \geq n \ln n - n.$$

Par propriété du logarithme, le terme de gauche vaut $\ln\left(\prod_{k=1}^{n} k\right) = \ln n!$. On passe à l'exponentielle (croissante) et on obtient :

$$n! \geq \exp(n \ln n - n) = n^n \times e^{-n} = \left(\frac{n}{e}\right)^n.$$

3. Soit $x > 0$. On montre la formule annoncée par récurrence sur n.

- Pour $n = 0$, la formule devient $e^x = 1 + \int_0^x e^u du$, ce qui est vrai car $\int_0^x e^u du = e^x - e^0 = e^x - 1$.

- Soit $n \in \mathbb{N}$ tel que la formule est vraie. On fait une intégration par parties :

$$\begin{aligned}\int_0^x (x-u)^n e^u du &= -\frac{1}{n+1}\left[(x-u)^{n+1}e^u\right]_{u=0}^{u=x} + \frac{1}{n+1}\int_0^x (x-u)^{n+1}e^u du \\ &= \frac{x^{n+1}}{n+1} + \frac{1}{n+1}\int_0^x (x-u)^{n+1}e^u du.\end{aligned}$$

  Par hypothèse de récurrence, on a

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

  D'où, avec le calcul précédent :

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

  ce qui conclut la récurrence.

Soit $u \in [0, x]$. On a les inégalités $0 \leq (x-u)^n e^u \leq (x-u)^n e^x$. En intégrant entre 0 et x, on a donc :

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

Comme $e^x - \sum_{k=0}^{n} \frac{x^k}{k!} = \frac{1}{n!}\int_0^x (x-u)^n e^u du$, on en déduit les inégalités annoncées.

3.2 Minoration

4. Notons $p_1, \ldots, p_k$ les diviseurs premiers distincts de m ayant une valuation impaire dans m. Comme les p_i sont deux à deux premiers entre eux, $p_1 \ldots p_k$ divise m. Par construction, $\dfrac{m}{p_1 \ldots p_k}$ s'écrit $\prod_{i=1}^{s} q_i^{\alpha_i}$, où les q_i sont des nombres premiers distincts (non nécessairement distincts des p_i) et les α_i sont pairs. On note alors $r = \prod_{i=1}^{s} q_i^{\alpha_i/2}$.
   Alors, r est un entier et $m = r^2 p_1 \ldots p_k$.
   Les p_i sont supérieurs à 1 donc $m \geq r^2$ et $r \leq \sqrt{m}$, donc $r \leq \lfloor \sqrt{m} \rfloor$. De plus, chaque p_i est inférieur à m, donc est dans $\mathbb{P}_m$.

5. Le produit $\prod_{p\in\mathbb{P}_n}\left(1+\frac{1}{p}\right)$ se développe en une somme de termes de la forme $\frac{1}{p_1\dots p_k}$ où les p_i sont des premiers distincts dans $\mathbb{P}_n$. Si $m\in[\![1,n]\!]$, on peut écrire $m = r^2p_1\dots p_k$ où $r\leq\lfloor\sqrt{m}\rfloor\leq\lfloor\sqrt{n}\rfloor$ et où chaque p_i est dans $\mathbb{P}_m\subset\mathbb{P}_n$. Donc, $\frac{1}{m}$ se retrouve dans un des termes du membre de droite $\sum_{r=1}^{\lfloor\sqrt{n}\rfloor}\frac{1}{r^2}\left(\prod_{p\in\mathbb{P}_n}\left(1+\frac{1}{p}\right)\right)$, une fois développé.
Donc, la somme des $\frac{1}{m}$, pour $m\in[\![1,n]\!]$ est inférieure à la somme de droite (car tous ses termes sont positifs). Ainsi,

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

6. Soit $N\geq 1$. Pour tout $r\in[\![2,N]\!]$, on a $\frac{1}{r^2}\leq\frac{1}{r(r-1)}$. On somme ces inégalités :

$$\sum_{r=2}^{N}\frac{1}{r^2}\leq\sum_{r=2}^{N}\frac{1}{r(r-1)}=\sum_{r=2}^{N}\frac{1}{r-1}-\frac{1}{r}=1-\frac{1}{N}.$$

En ajoutant le terme pour $r=1$, on obtient $\sum_{r=1}^{N}\frac{1}{r^2}\leq 2-\frac{1}{N}\leq 2$.

7. On sait que pour tout réel x, on a $e^x\geq 1+x$. Donc, par produit de quantités positives,

$$\prod_{p\in\mathbb{P}_n}\left(1+\frac{1}{p}\right)\leq\prod_{p\in\mathbb{P}_n}e^{1/p}=e^{A_n}.$$

Par la question 5, on a donc $H_n\leq e^{A_n}\sum_{r=1}^{\lfloor\sqrt{n}\rfloor}\frac{1}{r^2}$ et par la question 6, ceci est inférieur à $2e^{A_n}$. Donc, $e^{A_n}\geq\frac{1}{2}H_n$.

3.3 Majoration

8. Un entier m est dans l'image de f_i ssi il s'écrit comme produit d'exactement i nombres premiers (non nécessairement distincts) dans $\mathbb{P}_n$ (par définition). Soit m un tel entier dans l'image ; on peut donc l'écrire $m=p_1\dots p_i$, où les p_k sont dans $\mathbb{P}_n$.
Si m s'écrit aussi $q_1\dots q_i$, avec des q_k dans $\mathbb{P}_n$, alors le i-uplet $(p_1,\dots,p_i)$ est égal au i-uplet $(q_1,\dots,q_i)$ à permutation près des termes ; c'est en effet une conséquence de l'unicité de la décomposition en facteurs premiers de m. Comme il y a au maximum

$i!$ tels i-uplets permutés (*au maximum, car certains peuvent être identiques si les p_k ne sont pas deux à deux distincts*), m admet au plus $i!$ antécédents.

9. Soit $i \in [\![1, k]\!]$. En développant A_n^i, on a :

$$A_n^i = \sum_{p_1,\dots,p_i \in \mathbb{P}_n} \frac{1}{p_1 \dots p_i}.$$

D'après la question précédente, on a donc :

$$A_n^i \leq i! \sum_{m \in \mathrm{Im}(f_i)} \frac{1}{m}.$$

On divise par $i!$ et on somme ces inégalités de 1 à k :

$$\sum_{i=1}^{k} \frac{A_n^i}{i!} \leq \sum_{i=1}^{k} \sum_{m \in \mathrm{Im}(f_i)} \frac{1}{m}.$$

Or, pour tout $i \in [\![1, k]\!]$, $\mathrm{Im}(f_i) \subset [\![2, n^k]\!]$ (un élément de l'image est un produit de i nombres premiers dans $[\![1, n]\!]$) et les images des f_i sont deux à deux disjointes (car si $m \in \mathrm{Im}(f_i)$, i est la somme totale des valuations p-adiques de m, pour $p \in \mathbb{P}$). Ainsi,

$$\sum_{i=1}^{k} \frac{A_n^i}{i!} \leq \sum_{m=2}^{n^k} \frac{1}{m}.$$

On obtient l'inégalité annoncée en ajoutant 1 des deux côtés.
Par la question 3, on a alors

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

10. On utilise la question 4.

$$\frac{A_n^{k(n)+1}}{(k(n)+1)!} \leq \left(\frac{A_n e}{k(n)+1}\right)^{k(n)+1} \leq \left(e\frac{A_n}{k(n)}\right)^{k(n)+1}.$$

Or, $\dfrac{A_n}{k(n)} \to 0$ quand $n \to +\infty$ car $0 < \dfrac{A_n}{k(n)} \leq \dfrac{C \ln(\ln n)}{\ln^2(\ln n) - 1}$, donc $e\dfrac{A_n}{k(n)}$ aussi. Comme $k(n) \to +\infty$, $\left(e\dfrac{A_n}{k(n)}\right)^{k(n)+1}$ tend aussi vers 0 (*pas de forme indéterminée ici*).

Comme les quantités sont positives, on obtient que $\dfrac{A_n^{k(n)+1}}{(k(n)+1)!} \to 0$, quand $n \to +\infty$, par théorème d'encadrement.

11. D'après la question 1, on a

$$k(n)\ln n = \ln n^{k(n)} \leq H_{n^{k(n)}} \leq \ln n^{k(n)} + 1 = k(n)\ln n + 1.$$

On passe au logarithme (croissant) :

$$\ln(\ln n)+\ln(k(n)) \leq \ln H_{n^{k(n)}} \leq \ln(k(n)\ln n+1) = \ln(\ln n)+\ln(k(n))+\ln(1+k(n)^{-1}\ln^{-1} n).$$

Or, $\ln(k(n)) \leq \ln(\ln^2(\ln n)) = 2\ln(\ln(\ln n)) = o(\ln(\ln n))$. Et le terme $\ln(1 + k(n)^{-1}\ln^{-1} n)$ tend vers 0 donc est aussi $o(\ln(\ln n))$. Ainsi, quand on divise les inégalités par $\ln(\ln n)$, les deux membres extrêmes tendent vers 1, donc par encadrement $\ln H_{n^{k(n)}} \sim \ln(\ln n)$.

3.4 Conclusion

12. On reprend l'inégalité de la question 9, avec $k(n)$ au lieu de k. En passant au logarithme :

$$A_n \leq \ln H_{n^{k(n)}} - \ln\left(1 - \frac{A_n^{k(n)+1}}{(k(n)+1)!}\right).$$

Dans le membre de droite, le premier terme est équivalent à $\ln(\ln n)$ par la question 11, le deuxième tend vers 0 par la question 10. Ainsi, le membre de droite est équivalent à $\ln(\ln n)$. On a donc majoré A_n par une suite équivalente à $\ln(\ln n)$.
Mais à la question 7, on a montré que $A_n \geq \ln(H_n) - \ln 2$, qui est aussi équivalent à $\ln(\ln n)$ (*conséquence immédiate de la question 1, en plus simple*). Ainsi, A_n est encadrée par deux quantités équivalentes à $\ln(\ln n)$; par théorème d'encadrement A_n est aussi équivalent à $\ln(\ln n)$.

4 Problème – Groupes de cardinal p^2 et pq

4.1 Théorème de Lagrange

1. - Réflexivité. Soit $x \in G$. Comme $x^{-1}x = e_G \in H$, $x \mathcal{R}_H x$.
   - Symétrie. Soient $x, y \in G$ tels que $x \mathcal{R}_H y$. On a donc $x^{-1}y \in H$. Par stabilité de H par passage à l'inverse, $(x^{-1}y^{-1}) = yx^{-1} \in H$. Donc, $y \mathcal{R}_H x$.
   - Transitivité. Soient $x, y, z \in G$ tels que $x \mathcal{R}_H y$ et $y \mathcal{R}_H z$. Alors $x^{-1}y, y^{-1}z \in H$. Par stabilité de H par produit, $x^{-1}z \in H$. Donc $x \mathcal{R}_H z$.

   Comme la relation $\mathcal{R}_H$ est réflexive, symétrique et transitive, c'est une relation d'équivalence sur G.

2. L'application $\tau : g \mapsto xg$ définit une permutation de G, sa bijection réciproque étant $g \mapsto x^{-1}g$. De plus, $g \in H \iff x^{-1}(xg) \in H \iff x \mathcal{R}_H xg \iff xg \in \mathrm{cl}_{\mathcal{R}_H}(x)$. Ainsi, τ induit une bijection de H vers $\mathrm{cl}_{\mathcal{R}_H}(x)$.

3. Les classes d'équivalence pour $\mathcal{R}_H$ forment une partition de G. Si G est fini, elles ont toutes le même cardinal $|H|$ d'après la question précédente. S'il y a K classes d'équivalence, on a donc $|G| = K \times |H|$. En particulier, $|H|$ divise $|G|$.

4. Soit $x \in G \setminus \{e\}$. Notons $H = \langle x \rangle$. C'est un sous-groupe de G donc, d'après la question précédente, $|H|$ divise p. Or, H a au moins deux éléments : x et e ; donc $|H| = p$, c'est-à-dire $\langle x \rangle = G$.
Ainsi, G est monogène et de cardinal p ; il est donc isomorphe au groupe additif $\mathbb{Z}/p\mathbb{Z}$.

4.2 Groupes d'ordre p^2

5. - Réflexivité. Soit $x \in G$. $x = e^{-1}xe$, donc $x \mathcal{R} x$.
   - Symétrie. Soient $x, y \in G$ tels que $x \mathcal{R} y$. Alors, il existe $g \in G$ tel que $y = g^{-1}xg$. En multipliant à gauche par g et à droite par g^{-1} : $x = gyg^{-1} = (g^{-1})^{-1}yg^{-1}$. Donc, $y \mathcal{R} x$.
   - Transitivité. Soient $x, y, z \in G$ tels que $x \mathcal{R} y$ et $y \mathcal{R} z$. On peut trouver $g, g' \in G$ tels que $y = g^{-1}xg$ et $z = g'^{-1}yg'$. Alors $z = g'^{-1}g^{-1}xgg' = (gg')^{-1}x(gg')$. Donc, $x \mathcal{R} z$.

   Donc, $\mathcal{R}$ est une relation d'équivalence sur G.

6. Soient $g, g' \in C(x)$. Alors,

$$(gg')x = g(g'x) = g(xg') = (gx)g' = (xg)g' = x(gg'),$$

en utilisant plusieurs fois l'associativité de la loi de G et le fait que $g, g' \in C(x)$. Donc, $gg' \in C(x)$.
De plus, en multipliant par g^{-1} des deux côtés dans la relation $gx = xg$, on obtient $xg^{-1} = g^{-1}x$. Donc, $g^{-1} \in C(x)$.
Enfin, $C(x)$ contient e car $ex = xe = x$.
Ainsi, $C(x)$ est un sous-groupe de G.

7. Par définition, $y \in G$ est dans $\mathrm{cl}_{\mathcal{R}}(x)$ ssi il existe $g \in G$ tel que $y = g^{-1}xg$ ssi g est un antécédent de y pour l'application p_x. Ceci montre à la fois que p_x est bien définie et qu'elle est surjective.
Soient $g, g' \in G$. On a

$$\begin{aligned} p_x(g) = p_x(g') &\iff gxg^{-1} = g'xg'^{-1} \\ &\iff x(g^{-1}g'') = (g^{-1}g')x \\ &\iff g^{-1}g' \in C(x) \\ &\iff g \mathcal{R}_{C(x)} g'. \end{aligned}$$

8. L'application p_x est surjective de G dans $\mathrm{cl}_{\mathcal{R}}(x)$. D'après la question précédente, deux éléments ont même image par p_x ssi ils sont dans la même classe d'équivalence pour la relation $\mathcal{R}_{C(x)}$. Or, d'après la question 2, toutes ces classes sont de cardinal $|C(x)|$.
   Ainsi, exactement $|C(x)|$ éléments de G correspondent par p_x à un élément de $\mathrm{cl}_{\mathcal{R}}(x)$. Donc, $|G| = |\,\mathrm{cl}_{\mathcal{R}(x)}\,| \times |C(x)|$.

9. On a les équivalences suivantes :

$$\begin{aligned} x \in Z_G &\iff \forall h \in G, x \in C(h) \\ &\iff \forall h \in G, hx = xh \\ &\iff \forall h \in G, x = h^{-1}xh \\ &\iff \mathrm{cl}_{\mathcal{R}}(x) = \{x\}. \end{aligned}$$

10. Les classes d'équivalence pour $\mathcal{R}$ forment une partition de G. Elles sont de deux types : les singletons, qui correspondent à des éléments de Z_G (il y en a donc $|Z_G|$) ; les autres, qui sont par définition les $\mathrm{cl}_{\mathcal{R}}(x_i)$, pour $i \in [\![1, K]\!]$.
    On a donc $|G| = |Z_G| \times 1 + \sum_{i=1}^{G} |\,\mathrm{cl}_{\mathcal{R}}(x_i)|$. Et donc l'égalité annoncée car $|G| = p^n$.

11. Comme Z_G est un sous-groupe de G, son cardinal divise $|G|$ par la question 3. Il est donc de la forme p^k avec $k \in [\![0, n]\!]$. Il reste à éliminer le cas $|Z_G| = 1$.
    Si $i \in [\![1, K]\!]$, on a d'après la question 8, $p^n = |\,\mathrm{cl}_{\mathcal{R}}(x)| \times |C(x)|$. Par définition des x_i, $|\,\mathrm{cl}_{\mathcal{R}}(x)| > 1$, donc $|C(x)| < p^n$. Comme $C(x)$ est un sous-groupe, son cardinal est de la forme p^k pour un $k < n$. Et donc, le cardinal de $\mathrm{cl}_{\mathcal{R}}(x)$ est de la forme p^j, pour un $j > 0$. En particulier, p divise le cardinal de $\mathrm{cl}_{\mathcal{R}}(x_i)$.
    En considérant l'égalité de la question 10 modulo p, on en déduit que $|Z_G| \equiv 0\,[p]$, ce qui permet de conclure.

12. Soient $(k, \ell), (k', \ell') \in [\![0, p-1]\!]^2$ tels que $x^k y^\ell = x^{k'} y^{\ell'}$. Alors, $y^{\ell-\ell'} = x^{k'-k} \in \langle x\rangle \cap \langle y\rangle$. Comme c'est un sous-groupe de G, $\langle x\rangle \cap \langle y\rangle$ doit être de cardinal 1, p ou p^2. Mais $\langle x\rangle$ est de cardinal p (car on a supposé G non monogène) et, comme $y \notin \langle x\rangle$, $\langle x\rangle \cap \langle y\rangle$ est strictement inclus dans $\langle x\rangle$. Ainsi, $\langle x\rangle \cap \langle y\rangle = \{e\}$.
    Donc, $y^\ell = y^{\ell'}$ et $x^k = x^{k'}$. On en déduit, comme les entiers sont dans $[\![0, p-1]\!]$ que $k = k'$ et $\ell = \ell'$ (sinon on aurait trouvé une puissance de x ou y strictement inférieure à p et valant e ; par division euclidienne, on en déduirait que $\langle x\rangle$ ou $\langle y\rangle$ serait de cardinal $< p$, ce qui est absurde).
    Donc, tous les éléments $x^k y^\ell$ sont différents. Comme il y en a $p^2 = |G|$, ce sont tous les éléments de G. Mais deux tels éléments commutent :

$$(x^k y^\ell)(x^{k'} y^{\ell'}) = x^k (x^{k'} y^\ell) y^{\ell'} = x^{k+k'} y^{\ell+\ell'},$$

    en utilisant seulement que $x \in Z_G$. Et de même, $(x^{k'} y^{\ell'})(x^{k'} y^{\ell'}) = x^{k+k'} y^{\ell+\ell'}$.

13. En utilisant par exemple le fait que $\langle x\rangle$ et $\langle y\rangle$ sont tous les deux isomorphes à $\mathbb{Z}/p\mathbb{Z}$, on a que $x^p = y^p = e$. On en déduit que si $k \equiv k'\,[p]$, alors $x^k = x^{k'}$; de même pour y. Donc, f est bien définie.
De plus, f est injective par la question précédente. Comme les ensembles et d'arrivée sont de cardinal p^2, f est bijective.
Enfin, f est un morphisme. En effet, si k, ℓ, k', ℓ' sont des entiers, on a $(x^k y^\ell)(x^{k'} y^{\ell'}) = x^{k+k'} y^{\ell+\ell'}$ par commutativité ; et donc $f((\bar{k},\bar{\ell}) + (\bar{k}',\bar{\ell}')) = f((\bar{k},\bar{\ell}))f((\bar{k}',\bar{\ell}'))$.

4.3 Groupes d'ordre pq

14.
- L'élément (e_H, e_K) est neutre pour $*$. En effet, si $(h,k) \in H \times K$, on a $(h,k) * (e_H, e_K) = (hf(k)(e_H), ke_K) = (h,k)$ et $(e_H, e_H) * (h,k) = (e_H f(e_K)(h), e_K k) = (\mathrm{id}_H(h), k) = (h,k)$. On utilise que $f(k)$ envoie e_H sur e_H (car c'est un automorphisme de H) et que $f(e_K) = \mathrm{id}_H$ (car f est un morphime de groupes).
- Soit $(h,k) \in H \times K$. On définit $(h',k') = (f(k^{-1})(h^{-1}), k^{-1})$. Alors,

$$(h,k) * (h',k') = (hf(k) \circ f(k^{-1})(h^{-1}), kk^{-1}) = (hh^{-1}, kk^{-1}) = (e_H, e_K).$$

$$(h',k') * (h,k) = (f(k^{-1})(h^{-1})f(k^{-1})(h), k^{-1}k) = (f(k^{-1})(e_H)), e_K) = (e_H, e_K).$$

De nouveau, on utilise que f est un morphisme et que $f(k^{-1})$ est un automorphisme de H.
- Il reste à montrer l'associativité. On considère $(h,k), (h',k'), (h'',k'')$ dans $H \times K$. La deuxième composante ne pose pas de problème ; on se concentre sur la première.
La première composante de $\big((h,k) * (h',k')\big) * (h'',k'')$ vaut $hf(k)(h')f(kk')(h'')$. Celle de $(h,k) * \big((h',k') * (h'',k'')\big)$ vaut $hf(k)(h'f(k')(h''))$. Mais comme $f(k)$ est un morphisme, on a

$$f(k)(h'f(k')(h'')) = f(k)(h')f(k) \circ f(k')(h'').$$

Et comme f est un morphisme, $f(k) \circ f(k') = f(kk')$. Finalement, les deux premières composantes sont égales, ce qui conclut.

Ainsi, $*$ définit bien une loi de groupe sur $H \times K$.

15. Si pour tout $k \in K$, $f(k) = \mathrm{id}_H$, alors la définition de $*$ se simplifie en $(h,k)*(h',k') = (hh', kk')$. On retrouve alors la loi produit sur $H \times K$ et $H \times K$ est abélien car H et K le sont.
Réciproquement, supposons que $*$ munit de $H \times H$ d'une structure de groupe abélien. Soient $h \in H$, $k \in K$. On a $(e_H, k) * (h, e_K) = (h, e_K) * (e_H, k)$. Donc, $(f(k)(h), k) = (h,k)$. Ainsi, $f(k)(h) = h$. Ceci étant vrai pour tous k et tous h, on a $f(k) = \mathrm{id}_H$, pour tout $k \in K$.

16. (a) C'est un morphisme car $k(\overline{u+v}) = k\overline{u} + k\overline{v}$ si $\overline{u}, \overline{v}$ sont dans $\mathbb{Z}/n\mathbb{Z}$. Il est bijectif car sa bijection réciproque est manifestement m_{-k}.

(b) Si $k \in \mathbb{Z}$ et $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$, $k\overline{u} = \overline{ku}$. Donc, m_k ne dépend que de la classe de k dans $\mathbb{Z}/n\mathbb{Z}$. Ceci montre que f est bien définie.
C'est un morphisme de groupes car si $\overline{k}, \overline{\ell} \in (\mathbb{Z}/n\mathbb{Z})^\times$ et si $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$, alors $(k\ell)\overline{u} = k(\ell\overline{u})$, ce qui montre que $f(\overline{k\ell}) = m_{k\ell} = m_k \circ m_\ell = f(\overline{k}) \circ f(\overline{\ell})$.
Si $m_k = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$, on a $k\overline{u} = \overline{u}$ pour tout $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$. En particulier, avec $u = 1$, on trouve que $k = 1$. Donc, m_k est injective.
Considérons enfin g un automorphisme de $\mathbb{Z}/n\mathbb{Z}$. Si k est l'image de $\overline{1}$ par f, on a (par récurrence immédiate), $g(\overline{u}) = k\overline{u}$ pour tout u. De plus, si comme g est surjective, il existe $\overline{u}$ tel que $k\overline{u} = \overline{1}$. Ceci montre que k est inversible modulo n. Ainsi, $g = m_k$; donc g est dans l'image de f.
Bilan : f est un isomorphisme de groupes.

17. Le groupe $(\mathbb{Z}/q\mathbb{Z})^*$ est monogène de cardinal $q-1$. Il est donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$. Comme les groupes $(\mathbb{Z}/q\mathbb{Z})^\times$ et $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ sont isomorphes, il revient au même de se donner un morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$; ou dans $(\mathbb{Z}/q\mathbb{Z})^\times$; ou dans $\mathbb{Z}/(q-1)\mathbb{Z}$ (en composant avec des isomorphismes de groupes).
On se demande donc quand il existe un morphisme non trivial de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/(q-1)\mathbb{Z}$. On a vu en TD (*à refaire !*) qu'un tel morphisme existe ssi p et $q-1$ ne sont pas premiers entre eux. Comme p est premier, cela revient à dire que p divise $q-1$.

18. On note f un morphisme non trivial comme à la question précédente. Ceci définit une loi de groupe sur $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par la procédure décrite en début de partie. Comme f est non trivial, ce groupe est non abélien d'après la queston 15.

19. Il s'agit essentiellement d'expliciter un morphisme non trivial de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$. Déjà, on montre rapidement que $\overline{3}$ est un générateur de $(\mathbb{Z}/7\mathbb{Z})^\times$. Avec l'isomorphisme de la question 16.b), m_3 est un générateur de $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$.
Un morphisme non trivial $f : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$ est construit en envoyant la classe de 1 modulo 3 sur m_3 et donc la classe de 2 sur $m_3 \circ m_3 = m_9$.
Sur l'ensemble $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, on définit donc une loi $*$ par

$$(\overline{k}, \overline{\ell}) * (\overline{k'}, \overline{\ell'}) = (\overline{k \times 3^\ell k'}, \overline{\ell\ell'}).$$

Les classes de k, k' sont modulo 7 ; celles de ℓ, ℓ' sont modulo 3.