Généralités sur les groupes.

Exercice 1. Lesquels de ces ensembles sont-ils des groupes pour les lois de composition données ?
1. $(\mathbf{N}, +)$;
2. $(\mathbf{Z}, +)$;
3. $(\mathbf{Z}, \times)$;
4. $(\mathbf{Z} - \{0\}, \times)$;
5. $(\mathbf{R} - \{0\}, \times)$.

Exercice 2. Soit G un groupe. Montrer que l'intersection de deux sous-groupes de G est un sous-groupe de G. Que peut-on dire de la réunion de deux sous-groupes de G ?

Exercice 3. Soient G un groupe et H un sous-ensemble fini de G stable pour la loi de composition du groupe G. Montrer que H est un sous-groupe de G.

Exercice 4. Montrer que l'application exponentielle $x \mapsto e^x$ est un isomorphisme du groupe additif R sur le groupe multiplicatif R^*. Quel est l'isomorphisme réciproque ?

Exercice 5. Exhiber un isomorphisme de groupes entre $\mathbf{Z}/n\mathbf{Z}$ et l'ensemble des racines complexes n-ièmes de l'unité.

Exercice 6. Ecrire les tables d'addition de $\mathbf{Z}/5\mathbf{Z}$ et $\mathbf{Z}/12\mathbf{Z}$. Déterminer tous les sous-groupes de chacun de ces groupes.

Exercice 7. Les groupes $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/4\mathbf{Z}$ sont-ils isomorphes ?

Exercice 8. Soit G un groupe commutatif fini, noté multiplicativement.
1. Montrer que l'application $x \mapsto x^{-1}$ est une bijection de G sur lui-même.
2. Soit g le produit de tous les éléments de G. Montrer que $g^2 = 1$.
3. Montrer par des exemples que g peut être égal ou non à 1.

Algorithme d'Euclide et relation de Bézout. PGCD et PPCM.

Exercice 9. Soient $a = da'$ et $b = db'$. Montrer : $d = \mathrm{pgcd}(a, b) \Longleftrightarrow 1 = \mathrm{pgcd}(a', b')$.

Exercice 10. Soient p un nombre premier et a un entier. Montrer que si p ne divise pas a alors a et p sont premiers entre eux.

Exercice 11. Soient a, b, c et d des entiers ; démontrer les implications :
1. $\mathrm{pgcd}(a, b) = d \implies \mathrm{pgcd}(ac, bc) = dc$;
2. $\mathrm{pgcd}(a, b) = 1$ et $\mathrm{pgcd}(a, c) = 1 \implies \mathrm{pgcd}(a, bc) = 1$;
3. $\mathrm{pgcd}(a, b) = 1 \implies \forall m \geq 2,\ \forall n \geq 2,\ \mathrm{pgcd}(a^m, b^n) = 1$;
4. $\mathrm{pgcd}(a, b) = d \implies \forall m \geq 2,\ \mathrm{pgcd}(a^m, b^m) = d^m$.

Exercice 12. **1.** Ecrire les suites (r_i), (u_i) et (v_i) pour $a = 1234$ et $b = 832$. En déduire u et v tels que $\text{pgcd}(a, b) = a.u + b.v$.
2. Même question pour $a = 2431$ et $b = 1342$.

Exercice 13. Montrer que si $d = \text{pgcd}(a, b)$ et si le couple $(u_0, v_0) \in \mathbf{Z}^2$ vérifie $au_0 + bv_0 = d$, les autres couples (u, v) vérifiant $au + bv = d$ sont les (u_k, v_k) définis pour tout $k \in \mathbf{Z} - \{0\}$ par

$$\begin{cases} u_k = u_0 + kb' \\ v_k = v_0 - ka' \end{cases}$$

où a' et b' sont définis par $a = da'$, $b = db'$.

Exercice 14. Résoudre dans $\mathbf{Z}^2$ les équations suivantes : $5x - 18y = 4$ et $6x + 15y = 28$.

Exercice 15. Si a et b sont des entiers positifs, déterminer le *pgcd* de $2^a - 1$ et $2^b - 1$.

Exercice 16. Par combien de zéros le nombre $283!$ se termine-t-il ?

Exercice 17. Si p est premier, et $1 \leq k \leq p-1$, montrer que p divise le coefficient binomial $\mathcal{C}_p^k$.

Exercice 18. **1.** Soient a et b deux entiers. Exprimer le *pgcd* et le *ppcm* de a et b en fonction des décompositions respectives de a et b en facteurs premiers.
2. Calculer le *pgcd* et le *ppcm* de 15288 et 2772.
3. Quels sont (à permutation près) les couples d'entiers naturels (a, b) qui admettent 165 pour *pgcd* et 4950 pour *ppcm* ?

Exercice 19. Trouver tous les couples d'entiers naturels (x, y) vérifiant

$$\text{pgcd}(\mathrm{x}, \mathrm{y}) + 10\text{ppcm}(\mathrm{x}, \mathrm{y}) = 341.$$

Exercice 20. Soit m le *ppcm* de deux entiers a et b ; montrer qu'il existe un diviseur a' de a, un diviseur b' de b, tels que $\text{pgcd}(a', b') = 1$ et $m = a'b'$.

Groupes finis. Ordres.

Exercice 21. Montrer que si p est premier, tout groupe d'ordre p^n possède un élément d'ordre p, donc un sous-groupe d'ordre p.

Exercice 22. Soit G un groupe fini commutatif, soit $x \in G$ un élément d'ordre p, et $y \in G$ un élément d'ordre q. Montrer que
1. L'ordre du sous-groupe $< x, y >$ de G engendré par x et y est majoré par pq.
2. Si p et q sont premiers entre eux, le produit $z = xy$ est d'ordre pq et le sous-groupe de G engendré par z contient x et y.
3. Il existe $t \in G$ dont l'ordre est égal au *ppcm* de p et q.