Une attention particulière sera portée à la qualité de la rédaction. Les documents sont interdits ainsi que les appareils électroniques.

**Exercice 1.** Soit $a \in \mathbf{Z}$ et $m, n \in \mathbf{N}^*$ avec $pgcd(m,n) = 1$. Montrer qu'il existe $b \in \mathbf{Z}$ tel que $n$ divise $a - bm$.

**Exercice 2.**
*1.* Donner les éléments d'ordre 4 de $\mathbf{Z}/4\mathbf{Z}$ et donner l'ordre de chaque élément de $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
*2.* Montrer que les groupes $\mathbf{Z}/4\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ ne sont pas isomorphes.

**Exercice 3.**
*1.* Donner les entiers $n$ de $\{0,1,2,3,4,5,6\}$ tels qu'il existe $m \in \mathbf{Z}$ vérifiant $n \equiv_7 m^3$.
*2.* Donner les entiers $n$ de $\{0,1,2,3,4,5,6\}$ tels qu'il existe $m \in \mathbf{Z}$ vérifiant $n \equiv_7 m^6$.
*3.* En déduire que si $(x,y,z) \in \mathbf{Z}^3$ alors $7x + y^3 + z^6 \neq 5$.

**Exercice 4.** Soit $p$ un entier naturel premier, $n \in \mathbf{N}^*$ et $m \in \{1, ..., p^n\}$.
*1.* Montrer que $m$ est premier avec $p^n$ si et seulement si $m$ est premier avec $p$.
*2.* Montrer que $m$ est premier avec $p$ si et seulement si pour tout $k \in \{1, ..., p^{n-1}\}$ on a $m \neq kp$.

**Exercice 5.** On rappelle que si $n = p_1^{r_1} \cdot ... \cdot p_k^{r_k}$ avec $1 < p_1 < ... < p_k$ premiers alors le nombre de générateurs de $(\mathbf{Z}/n\mathbf{Z}, +)$ est $n(1 - \frac{1}{p_1}) \cdot ... \cdot (1 - \frac{1}{p_k})$.
*1.* Calculer le nombre de générateurs de $(\mathbf{Z}/10\mathbf{Z}, +)$.
*2.* Vérifier si les classes $\overline{1}$, $\overline{3}$, $\overline{7}$ et $\overline{9}$ (modulo 10) sont générateurs ou pas de $(\mathbf{Z}/10\mathbf{Z}, +)$.
*3.* Calculer $(\overline{2})^k$ (modulo 11) si $k = 1, ..., 11$ et donner un isomorphisme entre $(\mathbf{Z}/10\mathbf{Z}, +)$ et $(\mathbf{Z}/11\mathbf{Z}^*, \times)$.
*4.* En déduire la liste des générateurs de $(\mathbf{Z}/11\mathbf{Z}^*, \times)$.

**Exercice 6.** Rechercher $x \in \mathbf{N}$ tel que $x - 2$ est divisible par 5, $x - 3$ est divisible par 8 et $x < 40$.

**Exercice 7.** (Chiffrement de El Gamal) Soit $m, g, s \in \mathbf{N}$ tels que $0 \leq m \leq 30$, $g^s \equiv_{31} 8$ et $m(g^s)^3 \equiv_{31} 27$. Trouver $a, b \in \mathbf{N}$ tels que $0 \leq a, b \leq 30$, $a \equiv_{31} (g^s)^3$ et $ab \equiv_{31} 1$ puis en déduire $m$.

**Exercice 8.** Soit $(a,b,c,d) \in \mathbf{C}^4$ de module 1 et tous différents. Montrer que le birapport $\frac{c-a}{d-a} \cdot \frac{d-b}{c-b}$ est réel.

**Exercice 9.** Soit $x \in \mathbf{R}$ strictement positif.
*1.* On suppose $0 < x < 1$. Comment construire à la règle et au compas un segment de longueur $\sqrt{x}$ si on dispose d'un segment de longueur 1 et d'un segment de longueur $x$ ?
*2.* Répondre à la même question lorsque $x > 1$.

**Exercice 10.** Si $F$ et $F'$ sont les deux foyers d'une ellipse $C$ alors un point $M$ appartient à $C$ si et seulement si $FM + F'M$ est égal à la longueur du grand axe. A partir de cette propriété calculer (en expliquant) les coordonnées des foyers de l'éllipse d'équation $(\frac{x}{a})^2 + (\frac{y}{b})^2 = 1$ avec $0 < b < a$.

**Exercice 11.** Soit $H$ l'hyperbole d'équation $4x^2 - y^2 = 1$. Donner en justifiant la réponse une application linéaire $f$ qui ne soit pas une isométrie et telle que $f(H) = H$.

**Exercice 12.** Soit $D_1 = \{x = 0\}$, $D_2 = \{y = 0\}$ et $D_3 = \{3x + 4y = 5\}$. Caractériser l'ensemble $C$ des points $M$ tels que $d(M, D_1)^2 + d(M, D_2)^2 = 5 \cdot d(M, D_3)$ et $3x + 4y < 5$ (nature, centre et axes de symétrie othogonale éventuels).