# congruences, notion de groupe

## exercices

**1.** *a*) Trouvez le reste de la division de 58 473 625 par 7 ; par 11 ; par 13 ; par 37.

*b*) Soit $n$ un nombre entier. Combien de valeurs peut prendre $n^3$ modulo 8 ?

**2.** *a*) Soit $x$ un nombre entier. Quelles sont les valeurs possibles de $x^2$ modulo 4 ?

*b*) Montrez qu'il n'existe aucun couple $(x, y)$ de nombres entiers vérifiant $x^2 + y^2 = 2007$.

**3.** On munit $\mathbf{R}$ de la loi de composition interne, notée $*$ et définie comme suit : quels que soient $x, y \in \mathbf{R}$,

$$x * y = x + y - xy.$$

*a*) Cette loi est-elle associative ? commutative ? Admet-elle un élément neutre ?

*b*) Est-ce que $\mathbf{R}$ est un groupe pour la loi $*$ ?

**4.** *a*) On note $U_4$ l'ensemble constitué des nombres complexes $1, -1, i, -i$. Montrez que c'est un groupe commutatif pour la multiplication.

*b*) Soit $n$ un entier $> 0$. On note $U_n$ l'ensemble des racines $n$-ièmes de l'unité, c'est-à-dire des nombres complexes qui vérifient $z^n = 1$. Montrez que c'est un groupe pour la multiplication.

*c*) Soit U l'ensemble des nombres complexes $z$ possédant la propriété suivante : il existe un entier $m > 0$ tel que $z^m = 1$. Est-ce que U est un groupe pour la multiplication ?

**5.** Soit E l'ensemble des applications $f$ de $\mathbf{R}^2$ dans $\mathbf{R}^2$ qui vérifient la propriété suivante : il existe $a \in \mathbf{R}^*$ et $b \in \mathbf{R}$ tels que, pour tout $x$ de $\mathbf{R}$, on ait

$$f(x) = ax + b.$$

*a*) Montrez que E est un groupe pour la composition des applications.

*b*) Le groupe $(E, \circ)$ est-il commutatif ?

**6.** Soit $n$ un entier $> 0$ ; on note $\mathrm{GL}(n, \mathbf{R})$ l'ensemble des matrices carrées inversibles d'ordre $n$ à coefficients réels.

*a*) Montrez que $\mathrm{GL}(n, \mathbf{R})$ est un groupe pour la multiplication matricielle.

*b*) Montrez que les matrices carrées d'ordre 2 de la forme $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $x$ appartenant à $\mathbf{R}$, constituent un sous-groupe commutatif de $\mathrm{GL}(2, \mathbf{R})$.

**7.** *a*) Soit G un groupe, en notation multiplicative. Montrez que l'intersection de deux sous-groupes de G est un sous-groupe de G.

*b*) Montrez que la réunion de deux sous-groupes de G *n'est pas* un sous-groupe de G, à moins que l'un d'eux soit contenu dans l'autre.

*Indication.* Soient A et B ces sous-groupes. Supposez qu'on n'ait ni $A \subset B$, ni $B \subset A$. Dans chacun d'eux, prenez un élément qui n'appartienne pas à l'autre, et demandez-vous où se trouve leur produit.