Feuille d'exercices n°3

Les groupes $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^*$

A - Groupes finis

On rappelle que l'*ordre* d'un groupe G est, par définition, le cardinal de G. L'*ordre* d'un élément $x \in G$ est l'ordre du sous-groupe de G engendré par x.

1 - Théorème de Lagrange

Si G est groupe fini, et H un sous-groupe de G, montrer que l'ordre de H divise celui de G. *Indication: montrer que les classes modulo H possèdent toutes le même nombre d'éléments que H.*

2 - Ordre d'un élément

Soit G un groupe fini (on notera multiplicativement la loi de G). Soit x un élément de G et m l'ordre de x.

1. Montrer que :

a. m divise l'ordre de G,

b. m est le plus petit entier positif tel que $x^m = 1_G$,

c. le sous-groupe de G engendré par x est $\{1_G, x, x^2, \ldots, x^{m-1}\}$.

2. Soit q un entier positif. Montrer que $x^q = 1_G$ si et seulement si m divise q.

3. Soit k un entier positif. Montrer que x^k est d'ordre m/d où $d = pgcd(m, k)$.

3 - Ordre des éléments dans un groupe commutatif

Soit G un groupe fini commutatif. Soient x, y deux éléments de G d'ordres respectifs p et q.

1. Dans le cas où p et q sont premiers entre eux, montrer que $z = xy$ est d'ordre pq, et que le sous-groupe engendré par z contient x et y.

2. Dans le cas général, montrer qu'il existe un élément $t \in G$ d'ordre $ppcm(p, q)$.

B - Groupes cycliques

4 - Sous-groupe d'un groupe cyclique

Soit G un groupe cyclique d'ordre n (on notera G multiplicativement, mais les résultats s'applique bien sûr au cas où $G = \mathbb{Z}/n\mathbb{Z}$). Soit d un entier strictement positif qui divise n. On note

$$U_d = \{x \in G \mid x^d = 1\}$$

1. Montrer que U_d est un sous-groupe d'ordre d de G, et que c'est le seul.

2. Combien U_d possède-t-il d'éléments ? de générateurs ?

C - Le groupe $\mathbb{Z}/n\mathbb{Z}$

5 - Deux groupes d'ordre 4 non-isomorphes

Montrer que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ sont tous les deux commutatifs et d'ordre 4, mais ne sont pas isomorphes.

6 - Sous-groupes de $\mathbb{Z}/54\mathbb{Z}$

Déterminer les sous-groupes de $\mathbb{Z}/54\mathbb{Z}$. Pour chaque sous-groupe, en donner les générateurs.

7 - Comparaison avec la situation dans $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

Soit $G = (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. Quel est l'ordre de G ? Déterminer $U_3 = \{x \in G \mid 3.x = 1_G\}$. Déterminer l'ensemble des éléments d'ordre 3 de G. Comparer aux résultats de l'exercice **??**.

8 - Isomorphisme entre $\mathbb{Z}/pq\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$.

1. Soient p et q deux entiers premiers entre eux. Montrer que l'application

$$\Phi : (\bar{x} \bmod pq) \mapsto (\bar{x} \bmod p, \bar{x} \bmod q)$$

défini un isomorphisme entre $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$.

2. Écrire explicitement l'isomorphisme précédent pour $p = 4$ et $q = 3$.

D - Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$

On rappelle que, pour p premier différent de 2 et n quelconque, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique d'ordre $(p-1).p^{n-1}$. En particulier, $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$.

9 - Inverses modulo n

Quel est l'inverse de 5 modulo 12 ? de 8 modulo 27 ? de 14 modulo 25 ? de 10 modulo 15 ?

10 - Étude de $(\mathbb{Z}/13\mathbb{Z})^*$

1. Trouver un générateur, puis tous les générateurs de $(\mathbb{Z}/13\mathbb{Z})^*$.
2. Trouver tous les sous-groupes de $(\mathbb{Z}/13\mathbb{Z})^*$ (on gardera en mémoire les résultats de l'exercice 4).
3. Parmi les éléments de $(\mathbb{Z}/13\mathbb{Z})^*$, lesquels sont des carrés ? Combien y en a-t-il ?

11 - Un critère pour déterminer si un nombre est un carré

On considère un nombre premier p différent de 2, et un élément $x \in (\mathbb{Z}/p\mathbb{Z})^*$. Le but de l'exercice est de montrer que

$$(x \text{ est un carré dans } (\mathbb{Z}/p\mathbb{Z})^*) \Leftrightarrow (x^{\frac{p-1}{2}} = 1 \text{ dans } (\mathbb{Z}/p\mathbb{Z})^*)$$

1. Montrer que, si x est un carré, alors $x^{\frac{p-1}{2}} = 1$.
2. Montrer que 1 et -1 sont les seules racines carrées de 1 dans $(\mathbb{Z}/p\mathbb{Z})^*$.

3. En déduire que l'image du morphisme $\Phi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ défini par $\Phi(x) = x^2$ est un sous-groupe d'ordre $\frac{p-1}{2}$.

4. En utilisant l'exercice 4, en déduire qu'un nombre $x \in (\mathbb{Z}/p\mathbb{Z})^*$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$ (dans $(\mathbb{Z}/p\mathbb{Z})^*$).

12 - Existence de solution pour l'équation $ax^2 + b = y^2$.

Soit p un nombre premier différent de 2. Soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$ et $b \in \mathbb{Z}/p\mathbb{Z}$.

1. Combien y a-t-il de carrés dans $\mathbb{Z}/p\mathbb{Z}$? (utiliser l'exercice précédent).

2. En déduire que l'équation $ax^2 + b \equiv y^2$ admet toujours au moins une solution $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2$.

13 - Quand -1 est-il un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$?

Soit p un nombre premier différent de 2. En utilisant l'exercice 11, montrer que

$$(-1 \text{ est un carré dans } (\mathbb{Z}/p\mathbb{Z})^*) \Leftrightarrow (p \equiv 1 \bmod 4)$$

14 - Une infinité de nombre premiers congrus à 1 modulo 4

1. Soit n un entier au moins égal à 3, et p un nombre premier qui divise $(n!)^2 + 1$. Montrer que $p \geq n$. En utilisant l'exercice précédent, montrer que $p \equiv 1[4]$.

2. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

15 - Le groupe $(\mathbb{Z}/2^n\mathbb{Z})^*$ n'est pas cyclique

Soit n un entier supérieur ou égal à 3.

1. Montrer que $(2^{n-1} + 1)^2 \equiv 1 \bmod 2^n$.

2. En déduire que $(\mathbb{Z}/2^n\mathbb{Z})^*$ n'est pas cyclique.

16 - Le groupe $(\mathbb{Z}/pq\mathbb{Z})^*$

1. Soient p et q deux nombres premiers entre eux. Rappeler pourquoi l'application

$$\Phi : (\bar{x} \bmod pq) \mapsto (\bar{x} \bmod p, \bar{x} \bmod q)$$

définit un isomorphisme de $(\mathbb{Z}/pq\mathbb{Z})^*$ vers $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$.

2. Soient p et q deux nombres permiers distincts, tous les deux congrus à 3 modulo 4. En utilisant la question précédente, montrer que $(\mathbb{Z}/pq\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/\frac{p-1}{2}\mathbb{Z}) \times (\mathbb{Z}/\frac{q-1}{2}\mathbb{Z})$. En déduire que $(\mathbb{Z}/pq\mathbb{Z})^*$ n'est pas cyclique.

3. En utilisant la question 1, montrer qu'il existe des entiers m, n distincts tels que les groupes $(\mathbb{Z}/m\mathbb{Z})^*$ et $(\mathbb{Z}/n\mathbb{Z})^*$ sont isomorphes. *Indication : prendre $n = 2m$.*

17 - Nombre de solutions de l'équation $x^4 = 1$ dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Soit $n = 23275 = 3.5^3.7^2$.

1. Montrer que $(\mathbb{Z}/n\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/100\mathbb{Z}) \times (\mathbb{Z}/42\mathbb{Z})$.

2. Combien l'équation $x^4 = 1$ admet-elle de solution dans $(\mathbb{Z}/n\mathbb{Z})^*$?