$\mathbb{Z}/n\mathbb{Z}$

Dans toute la feuille on fixe un entier $n \in \mathbb{N}$.

L'idée : on change l'égalité sur $\mathbb{Z}$. Notre nouvelle égalité sera la congruence modulo n. On rappelle qu'on dispose d'une construction purement mathématique pour formaliser cela : échanger nos entiers relatifs contre leurs classes d'équivalences (pour la congruence modulo n). Rappel de notation : pour $k \in \mathbb{Z}$, on notera $\overline{k}$ la classe d'équivalence de k pour la relation de congruence modulo n et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de ces classes d'équivalences.

0 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

1. Rappeler comment on note d'habitude l'ensemble $\overline{k}$ (commencer par $k = 0$).

2. À l'aide du théoème de division euclidienne, rappeler le cardinal de $\mathbb{Z}/n\mathbb{Z}$ et décrire le plus simplement possible cet ensemble.

1 Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$

3. Justifier que l'application $+ : \left\{ \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^2 & \to & \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) & \mapsto & \overline{a+b} \end{array} \right.$ est bien définie[1].

4. Justifier que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe.

5. Exemple : donner la table d'addition de $(\mathbb{Z}/4\mathbb{Z}, +, \times)$.

6. Donner un sous-groupe bien connu isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

2 Les anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

7. Justifier que l'application $\times : \left\{ \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^2 & \to & \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) & \mapsto & \overline{a \times b} \end{array} \right.$ est bien définie[1].

8. Justifier que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau.

9. Exemple : donner la table de multiplication de $(\mathbb{Z}/4\mathbb{Z}, +, \times)$. Est-ce un anneau intègre ? Quels sont ses inversibles ?

10. Autre exemple : on regarde $(\mathbb{Z}/5\mathbb{Z}, +, \times)$. Est-ce un anneau intègre ? Quels sont ses inversibles, qu'en déduire ?

3 Les corps $(\mathbb{Z}/p\mathbb{Z}, +, \times)$

11. Dans cette question on fixe un entier $p \geqslant 2$. Montrer l'équivalence entre :
    i/ $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps ;
    ii/ $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un anneau intègre ;
    iii/ p est premier.
    Indication : Bézout et Gauss sont nos amis.

Énoncé disponible à l'adresse suivante : http://mpsi.daudet.free.fr/.

N'hésitez pas à me poser *tout type de question sur un point qui ne vous paraît pas clair* par mail à l'adresse abbrug@gmail.com.

1. Rappel : on a déjà fait ce genre de choses dans le cours sur $\mathbb{Q}$.