DM 20

à rendre le mardi 23 avril 2024

Arithmétique modulaire

Partie A - Étude de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition – Ensemble $\mathbb{Z}/n\mathbb{Z}$
On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour la relation de congruence à n.
Pour $x \in \mathbb{Z}$, on note $\overline{x}$ la classe d'équivalence de x.

Exemples :
- $\overline{x} = \overline{2} \quad \Leftrightarrow \quad x \equiv 2\ [n]$
- $\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$

Proposition - Définition – Ordre d'un groupe, d'un élément, groupe cyclique
*On appelle **ordre** d'un groupe fini, le nombre de ses éléments.*
Soit $(G, +)$ un groupe fini (notation additive) et $x \in G$. L'ensemble $\langle x \rangle = \{kx : \ k \in \mathbb{N}\}$ est fini et forme un sous-groupe de G : c'est le sous-groupe engendré par x.
*On appelle **ordre** de l'élément x, l'ordre de $\langle x \rangle$, le sous-groupe qu'il engendre. En particulier, l'ordre de x est $\min\{k \in \mathbb{N}^*; kx = 0\}$.*
*On dit qu'un groupe est **cyclique**, s'il est fini et engendré par un élément.*

Exemples :
- $(\mathbb{Z}/8\mathbb{Z}, +)$ est cyclique car engendré par $\overline{1}$
- $\overline{3}$ est aussi un générateur de $(\mathbb{Z}/8\mathbb{Z}, +)$: $\{\overline{3}, 2 \times \overline{3} = \overline{6}, 3 \times \overline{3} = \overline{1}, 4 \times \overline{3} = \overline{4}, 5 \times \overline{3} = \overline{7}, 6 \times \overline{3} = \overline{2}, 7 \times \overline{3} = \overline{5}, 8 \times \overline{3} = \overline{0}\}$.

1. Montrer que les opérations définies ci-après sont deux lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$.
Pour tout $x, y \in \mathbb{Z}$:
$$\overline{x} + \overline{y} = \overline{x+y} \qquad \text{et} \qquad \overline{x} \times \overline{y} = \overline{x \times y}$$
Il s'agit de vérifier que ces opérations ne dépendent pas des représentants des classes utilisées :
$$\overline{x} = \overline{x'} \text{ et } \overline{y} = \overline{x'} \quad \Rightarrow \quad \overline{x+y} = \overline{x'+y'} \text{ et } \overline{x \times y} = \overline{x' \times y'}$$
2. Montrer que $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$ est un anneau (commutatif). Lister toutes les propriétés et en montrer quelques unes.
3. Montrer que pour $x \in \mathbb{Z}$, $\overline{x}$ est inversible dans le magma $(\mathbb{Z}/n\mathbb{Z}, \times)$ si et seulement si $x \wedge n = 1$.
4. Montrer que pour $x \in \mathbb{Z}$, si $x \wedge n = 1$ alors $\overline{x}$ est d'ordre n dans $(\mathbb{Z}/n\mathbb{Z}, +)$
5. En déduire que $\overline{x}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\overline{x} \in U(\mathbb{Z}/n\mathbb{Z})$.
6. Résoudre :
   - $(E_1) \quad : \quad \overline{6} \times x = \overline{7}$ dans $\mathbb{Z}/55\mathbb{Z}$
   - $(E_2) \quad : \quad \overline{6} \times x = \overline{11}$ dans $\mathbb{Z}/34\mathbb{Z}$
   - $(E_3) \quad : \quad \overline{6} \times x = \overline{15}$ dans $\mathbb{Z}/27\mathbb{Z}$
7. Montrer que les assertions suivantes sont équivalentes :
   (i) $\mathbb{Z}/n\mathbb{Z}$ est un corps
   (ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre
   (iii) n est premier
8. Donner un contre-exemple prouvant que $\mathbb{Z}/15\mathbb{Z}$ n'est pas intègre.
9. Résoudre $E_4 \quad : \quad x^2 - \overline{6}x + \overline{12} = 0$ dans $\mathbb{Z}/19\mathbb{Z}$.

Partie B - Étude de l'anneau $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

10. Montrer que $\big(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +, \times\big)$ muni des lois ci-dessous est un anneau.
Pour tout $\left(\,\widehat{x}\,,\,\widetilde{y}\,\right) + \left(\,\widehat{u}\,,\,\widetilde{v}\,\right) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$,

$$\left(\,\widehat{x}\,,\,\widetilde{y}\,\right) + \left(\,\widehat{u}\,,\,\widetilde{v}\,\right) = \left(\,\widehat{x}+\widehat{u}\,,\,\widetilde{y}+\widetilde{v}\,\right) \text{ et } \left(\,\widehat{x}\,,\,\widetilde{y}\,\right) \times \left(\,\widehat{u}\,,\,\widetilde{v}\,\right) = \left(\,\widehat{x}\times\widehat{u}\,,\,\widetilde{y}\times\widetilde{v}\,\right)$$

On citera toutes propriétés, mais on pourra se limiter à en montrer deux ou trois.

Soit $n, m \in \mathbb{N}^*$ et $\begin{array}{rccc}\psi : & \mathbb{Z}/nm\mathbb{Z} & \longmapsto & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & \overline{x} & \longmapsto & \left(\,\widehat{x}\,,\,\widetilde{x}\,\right)\end{array}$
avec $\overline{x}$, $\widehat{x}$ et $\widetilde{x}$ respectivement les classes de $x \in \mathbb{Z}$ dans $\mathbb{Z}/nm\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$.

11. Vérifier que ψ définit bien une application, c'est-à-dire que l'image dépend seulement de la classe et non du représentant utilisé :

$$\overline{x} = \overline{x'} \quad \Rightarrow \quad \psi\big(\overline{x}\big) = \psi\big(\overline{x'}\big)$$

12. Monter que ψ est un morphisme d'anneau.

On suppose pour la suite que n et m sont premiers entre eux.

13. Montrer que ψ est injective.
14. Montrer que ψ est surjective.
15. En déduire que $U(\mathbb{Z}/nm\mathbb{Z})$ et $U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$ sont équipotents.

Partie C - Indicatrice d'Euler et de Carmichael

Définition – Indicatrice d'Euler
On appelle ***indicatrice d'Euler*** *la fonction* $\varphi : \mathbb{N}^* \to \mathbb{N}$ *qui à* n *associe le nombre d'entier de* $[\![1, n]\!]$ *qui sont premiers avec* n *:*

$$\varphi(n) = \mathrm{Card}\big(k \in [\![1, n]\!];\ k \wedge n = 1\big)$$

Définition – Indicatrice de Carmichael - 1910
On appelle ***indicatrice de Carmichael*** *la fonction* $\lambda : \mathbb{N}^* \to \mathbb{N}$ *qui à* n *associe le plus petit* $m \in \mathbb{N}^*$ *tel que pour tout* k *premier avec* n, $k^m \equiv 1\ [n]$ *:*

$$\lambda(n) = \min\big(m \in \mathbb{N}^*;\ k \wedge n = 1 \quad \Rightarrow \quad k^m \equiv 1\ [n]\big)$$

16. Justifier que $\varphi(n) = \mathrm{Card}\big(U(\mathbb{Z}/n\mathbb{Z})\big)$.
17. En utilisant le théorème de Lagrange (vu en TD), déduire le théorème d'Euler qui est une généralisation du petit théorème de Fermat qui ne traite que la cas où n est premier :

Théorème – d'Euler
Pour tout $n \in \mathbb{N}^*$ et tout a premier avec n, alors $a^{\varphi(n)} \equiv 1\ [n]$.

18. Justifier que $\lambda(n)$ divise $\varphi(n)$.
19. Calculer $\varphi(8)$ et $\lambda(8)$.
20. Soit $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$, déterminer $\varphi(p)$, puis $\varphi(p^\alpha)$.
21. Montrer que φ est ***multiplicative*** c'est-à-dire : si n et m sont premiers entre eux, alors

$$\varphi(nm) = \varphi(n)\varphi(m)$$

22. Considérant la décomposition en facteurs premiers de n, donner l'expression de $\varphi(n)$.