L'ENSEMBLE DES NON INVERSIBLES $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$

ÉNONCÉ

Navigation : *Énoncé* *Corrigé*

Dans tout ce problème on désigne par:

- n un entier supérieur ou égal à 2.
- $\overline{a}$ la classe de l'entier a modulo n.
- $(\mathbb{U}_n, \times)$ le groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
- $\mathcal{N}_n$ l'ensemble des éléments non inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$
- $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, a \mapsto \overline{a}$ le morphisme d'anneaux surjectif.
- $\varphi(n) = \textbf{Card}\{k \in [\![1, n]\!] / k \wedge n = 1\}$, l'indicateur d'Euler.

Partie I: Théorème d'Euler

1. (a) Soit $k \in [\![1, n]\!]$, montrer que $\overline{k} \in \mathbb{U}_n \Leftrightarrow k \wedge n = 1$.

   En déduire les cardinaux de $\mathbb{U}_n$ et $\mathcal{N}_n$.

   (b) Montrer que si a est un nombre premier avec n alors: $a^{\varphi(n)} \equiv 1[n]$

   (c) En déduire que si p un nombre premier et a un entier tel que p ne divise pas a alors: $a^{p-1} \equiv 1[p]$

2. **Applications**:

   (a) Déterminer les cardinaux de $\mathbb{U}_{78}$ et $\mathcal{N}_{78}$.

   (b) Montrer que $\overline{2}$ est inversible dans $\mathbb{Z}/11\mathbb{Z}$ et déterminer son ordre dans le groupe $(\mathbb{U}_{11}, \times)$.

   En déduire que $(\mathbb{U}_{11}, \times)$ est cyclique et déterminer tous ses générateurs

   (c) En utilisant des congruences modulo 11, montrer que pour tout entier naturel n, l'entier $2^{n+2013} - 8 \times 7^{3n}$ est divisible par 11

Partie II: Sous-groupes de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$

Soit H un sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$

3. Déterminer $\text{Ker}(\pi_n)$.
4. Montrer qu'il existe un unique $\delta \in \mathbb{N}^*$ tel que $\pi_n^{-1}(H) = \delta\mathbb{Z}$ et que δ divise n.
5. Montrer que $\pi_n(\delta\mathbb{Z}) = \textbf{gr}\left(\overline{\delta}\right)$
6. En déduire que H est cyclique engendré par $\overline{\delta}$
7. Soit $d = \dfrac{n}{\delta}$, montrer que $\circ(\overline{\delta}) = d$ dans le groupe $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$.
8. Montrer que H est l'unique sous-groupe de cardinal d de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$.

Partie III: $\mathcal{N}_n$ est-t-il un sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$?

On dit que n est primaire lorsqu'il existe un nombre premier p et $\alpha \in \mathbb{N}^*$ tel que $n = p^\alpha$

9. Dans cette question on suppose que n n'est pas primaire.

(a) Établir qu'il existe deux entiers n_1 et n_2 tels que $n = n_1.n_2$, $1 < n_1 < n$ et $n_1 \wedge n_2 = 1$

(b) Montrer alors que $(n_1 + n_2) \wedge n = 1$.

(c) Montrer que $\overline{n_1} \in \mathcal{N}_n$ et $\overline{n_2} \in \mathcal{N}_n$

10. Soit p un nombre premier et $\alpha \in \mathbb{N}^*$.

    Soit $k \in \mathbb{Z}$, prouver que: $\overline{k} \in \mathcal{N}_{p^\alpha} \iff p|k$

11. Montrer que $\mathcal{N}_n$ est un sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ si, et seulement si, n est primaire et donner dans ce cas un générateur de $\mathcal{N}_n$

Partie I: Théorème d'Euler

1. (a)
   - Soit $k \in [\![1, n]\!]$, alors

$$\begin{aligned} \overline{k} \in \mathcal{U}_n &\iff \exists u \in \mathbb{Z},\ \overline{k}.\overline{u} = \overline{1} \\ &\iff \exists u \in \mathbb{Z},\ k.u \equiv 1 \quad [n] \\ &\iff \exists u, v \in \mathbb{Z},\ ku + vn = 1 \\ &\iff k \wedge n = 1 \end{aligned}$$

   - **Card** $(\mathcal{U}_n) = \varphi(n)$
   - $\mathcal{U}_n$ et $\mathcal{N}_n$ forment une partition de $\mathbb{Z}/n\mathbb{Z}$, donc **Card** $(\mathcal{N}_n) = n - \varphi(n)$

   (b) Soit a un nombre premier avec n alors $\overline{a} \in \mathcal{U}_n$. Or $\mathcal{U}_n$ est fini de cardinal $\varphi(n)$, d'après le théorème de Lagrange, alors $\overline{a}$ est d'ordre fini $\circ(a) \mid \varphi(n)$, c'est-à-dire

$$\overline{a}^{\varphi(n)} = \overline{1} \Rightarrow a^{\varphi(n)} \equiv 1[n]$$

   (c) Si p est premier, alors $\varphi(p) = p - 1$ et pour tout a entier tel que p ne divise pas a alors a est premier avec p, puis $a^{p-1} \equiv 1[p]$

2. **Applications**:
   (a)
   - L'indicatrice d'Euler est multiplicative. On écrit $78 = 2.3.13$, donc

$$\textbf{Card}\,(\mathcal{U}_{78}) = \varphi(78) = \varphi(2) \times \varphi(3) \times \varphi(13) = 1 \times 2 \times 12 = 24$$

   - **Card** $(\mathcal{N}_{78}) = 78 - \varphi(78) = 54$

   (b)
   - On a $2 \wedge 11 = 1$, donc $\overline{2}$ est inversible dans $\mathbb{Z}/11\mathbb{Z}$
   - l'ordre de $\overline{2}$ divise 10, $\circ\left(\overline{2}\right) \in \{1, 2, 5, 10\}$. Mais $\overline{2}^1 = \overline{2} \neq \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{2}^5 = \overline{10}$ et $\overline{2}^{10} = \overline{1}$. Bref $\circ\left(\overline{2}\right) = 10$
   - $\mathcal{U}_{11}$ est de cardinal 10 et il contient $\overline{2}$ d'ordre 10, donc $\mathcal{U}_{11} =< \overline{2} >$, ainsi $\mathcal{U}_{11}$ est cyclique
   - Les générateurs de $\mathcal{U}_{11}$ sont exactement les éléments de la forme $\overline{2}^k$ avec $k \in [\![0, 9]\!]$ et $k \wedge 10 = 1$. Or $k \in [\![0, 9]\!]$ et $k \wedge 10 = 1$ équivaut à $k \in \{1, 3, 7, 9\}$, donc les générateurs de $\mathcal{U}_{11}$ sont exactement $\overline{2}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^7 = \overline{3}$ et $\overline{2}^9 = \overline{6}$

   (c) On a $2^7 \equiv 7 \quad [11]$ et $2^3 \equiv 8 \quad [11]$, donc $2^{n+2013} - 8 \times 7^{3n} \equiv 2^{n+2013} - 2^3 \times 2^{21n} \quad [11]$. Soit $2^{n+2013} - 8 \times 7^{3n} \equiv 2^{n+2013} - 2^{21n+3} \quad [11]$.

   Or $2^{10} \equiv 1 \quad [11]$ et $n + 2013 \equiv 21n + 3 \quad [10]$, alors $2^{n+2013} \equiv 2^{21n+3} \quad [11]$ et donc

$$2^{n+2013} - 8 \times 7^{3n} \equiv 0 \quad [11]$$

Partie II: Sous groupes de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$

Soit H un sous groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$

3. Soit $k \in \mathbb{Z}$. On a

$$k \in \mathrm{Ker}(\pi_n) \iff \overline{k} = \pi_n(k) = \overline{0} \iff n \mid k \iff k \in n\mathbb{Z}$$

   Donc $\mathrm{Ker}(\pi_n) = n\mathbb{Z}$

4. • Existence: Si $H = \{\overline{0}\}$, on pose $\delta = n$. Sinon H est non nul, alors $\pi_n^{-1}(H)$ est un sous-groupe non trivial de $(\mathbb{Z}, +)$, donc il existe $\delta > 0$ tel que $\pi_n^{-1}(H) = \delta\mathbb{Z}$.
   De plus $\{\overline{0}\} \subset H$, donc $\pi_n^{-1}(\{\overline{0}\}) \subset \pi_n^{-1}(H)$, ceci fournit l'inclusion $n\mathbb{Z} \subset \delta\mathbb{Z}$ qui se traduit par divisibilité à $\delta \mid n$
   • Unicité: s'il existe $\delta, \delta' \in \mathbb{N}^*$ tels que $\pi_n^{-1}(H) = \delta\mathbb{Z} = \delta'\mathbb{Z}$, alors δ et δ' sont associés et puisque ils sont positifs alors ils sont égaux .
5. $\delta\mathbb{Z}$ est le sous-groupe de $\mathbb{Z}$ engendré par δ et π_n est un morphisme de groupes, donc $\pi_n(\delta\mathbb{Z})$ est le sous-groupe engendré par $\overline{\delta}$. Autrement $\pi_n(\delta\mathbb{Z}) =< \overline{\delta} >$
6. π_n est surjective, donc $H = \pi_n\left(\pi_n^{-1}(H)\right) =< \overline{\delta} >$. On déduit que H est monogène engendré par $\overline{\delta}$. En outre un sous-groupe d'un groupe fini est aussi fini
7. $\circ\left(\overline{\delta}\right) = \circ\left(\delta.\overline{1}\right) = \dfrac{n}{n \wedge \delta} = \dfrac{n}{\delta} = d$. Donc $\circ(\overline{\delta}) = d$
8. H est un sous groupe de cardinal d car H est cyclique et $\circ(\overline{\delta}) = d$.
   Soit K un sous-groupe $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ de cardinal d.
   Soit $\overline{\alpha} \in K$, alors $d\overline{\alpha} = \overline{0}$, donc $n \mid d.\alpha$ ou encore $\delta = \dfrac{n}{d}$ divise α, donc il existe $\beta \in \mathbb{Z}$ tel que $\alpha = \beta.\delta$ ceci donne $\overline{\alpha} \in <\overline{\delta}>$. Ainsi on a montré que $K \subset <\overline{\delta}> = H$ et puisque ils ont le même cardinal alors l'égalité $K = H$.
   Bref H est l'unique sous groupe de cardinal d de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$.

Partie III: $\mathcal{N}_n$ est-t-il un sous groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$?

9. On suppose que n n'est pas primaire.
   (a) Par hypothèse $n \geqslant 2$. D'après le théorème fondamental de l'arithmétique il existe $r \in \mathbb{N}^*$, une suite $p_1, \cdots, p_r$ de nombres premiers deux à deux distincts et $\alpha_1, \cdots, \alpha_r \in \mathbb{N}^*$ tels que
   $$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$
   n est supposé non primaire donc $r \geqslant 2$. On pose $n_1 = p_1^{\alpha_1}$ et $n_2 = \prod_{i=2}^{r} p_i^{\alpha_i}$. On a $n = n_1.n_2$, $1 < n_1 < n$ et $n_1 \wedge n_2 = 1$
   (b) Soit $d = (n_1 + n_2) \wedge n$, alors d divise n et $n_1 + n_2$. Écrivons $n_2^2 = n_2(n_1 + n_2) - n$ et $n_1^2 = n_1(n_1 + n_2) - n$, donc d divise à la fois n_1^2 et n_2^2, puis d divise $n_1^2 \wedge n_2^2 = 1$. Donc $d = 1$
   (c) les deux entiers n_1 et n_2 ne sont pas premiers avec n, donc $\overline{n_1}, \overline{n_2} \notin \mathcal{U}_n$, alors $\overline{n_1} \in \mathcal{N}_n$ et $\overline{n_2} \in \mathcal{N}_n$
10. $\Leftarrow$) Si $p \mid k$, alors $k \wedge p^\alpha \neq 1$. Donc $\overline{k} \notin \mathcal{U}_{p^\alpha}$, autrement-dit $\overline{k} \in \mathcal{N}_{p^\alpha}$
    $\Rightarrow$) Par contraposée, si p ne divise pas k, alors $p \wedge k = 1$ et aussi avec toutes les puissances de p, c'est-à-dire $p^\alpha \wedge k = 1$, par suite $\overline{k} \in \mathcal{U}_{p^\alpha}$, d'où $\overline{k} \notin \mathcal{N}_{p^\alpha}$
11. $\Rightarrow$) Par contraposée. Si n n'est pas primaire, alors il existe $\overline{n_1}, \overline{n_2} \in \mathcal{N}_n$ sans que $\overline{n_1} + \overline{n_2}$ soit dans $\mathcal{N}_n$. Ce qui montre que $\mathcal{N}_n$ n'est pas un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$
    $\Leftarrow$) Si n est primaire: il existe p premier et $\alpha \in \mathbb{N}^*$ tel que $n = p^\alpha$. D'après la question précédente, on a:
    $$\overline{k} \in \mathcal{N}_{p^\alpha} \Longleftrightarrow p \mid k \overset{n=p^\alpha}{\Longleftrightarrow} \overline{k} \in <\overline{p}>$$
    ce qui montre que $\mathcal{N}_{p^\alpha} =< \overline{p} >$ qui est un sous-groupe engendré par $\overline{p}$