

L'ENSEMBLE DES NON INVERSIBLES $\mathbb{Z}/n\mathbb{Z}$

Dans tout ce problème on désigne par:

- n un entier supérieur ou égal à 2.
- $\bar{a}$ 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 $\mathbb{Z}/n\mathbb{Z}$.
- $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, a \mapsto \bar{a}$ le morphisme d'anneaux surjectif.
- $\varphi(n) = \text{Card}\{k \in \llbracket 1, n \rrbracket / k \wedge n = 1\}$, l'indicateur d'Euler.

Partie I: Théorème d'Euler

- (a) Soit $k \in \llbracket 1, n \rrbracket$, montrer que $\bar{k} \in \mathbb{U}_n \Leftrightarrow k \wedge n = 1$.
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: $a^{p-1} \equiv 1[p]$
- Applications:**
 - Déterminer les cardinaux de $\mathbb{U}_{78}$ et $\mathcal{N}_{78}$.
 - Montrer que $\bar{2}$ 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
 - 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 $(\mathbb{Z}/n\mathbb{Z}, +)$

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

- Déterminer $\text{Ker}(\pi_n)$.
- Montrer qu'il existe un unique $\delta \in \mathbb{N}^*$ tel que $\pi_n^{-1}(H) = \delta\mathbb{Z}$ et que δ divise n .
- Montrer que $\pi_n(\delta\mathbb{Z}) = \langle \bar{\delta} \rangle$
- En déduire que H est cyclique engendré par $\bar{\delta}$
- Soit $d = \frac{n}{\delta}$, montrer que $\circ(\bar{\delta}) = d$ dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
- Montrer que H est l'unique sous groupe de cardinal d de $(\mathbb{Z}/n\mathbb{Z}, +)$.

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

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

- Dans cette question on suppose que n n'est pas primaire.
 - Établir qu'il existe deux entiers n_1 et n_2 tels que $n = n_1 \cdot n_2$, $1 < n_1 < n$ et $n_1 \wedge n_2 = 1$
 - Montrer alors que $(n_1 + n_2) \wedge n = 1$.
 - Montrer que $\bar{n}_1 \in \mathcal{N}_n$ et $\bar{n}_2 \in \mathcal{N}_n$
- Soit p un nombre premier et $\alpha \in \mathbb{N}^*$.
Soit $k \in \mathbb{Z}$, prouver que: $\bar{k} \in \mathcal{N}_{p^\alpha} \Leftrightarrow p|k$
- Montrer que $\mathcal{N}_n$ est un sous groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ si, et seulement si, n est primaire et donner dans ce cas un générateur de $\mathcal{N}_n$

L'ENSEMBLE DES NON INVERSIBLES $\mathbb{Z}/n\mathbb{Z}$

Partie I: Théorème d'Euler

1. (a) • Soit $k \in \llbracket 1, n \rrbracket$, alors

$$\begin{aligned}\bar{k} \in \mathcal{U}_n &\iff \exists u \in \mathbb{Z}, \bar{k} \cdot \bar{u} = \bar{1} \\ &\iff \exists u \in \mathbb{Z}, k \cdot u \equiv 1 \pmod{n} \\ &\iff \exists u, v \in \mathbb{Z}, ku + vn = 1 \\ &\iff k \wedge n = 1\end{aligned}$$

• $\text{Card}(\mathcal{U}_n) = \varphi(n)$

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

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

$$\bar{a}^{\varphi(n)} = \bar{1} \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

- (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 $a^{p-1} \equiv 1 \pmod{p}$

2. Applications:

- (a) • L'indicatrice d'Euler est multiplicative. On écrit $78 = 2 \cdot 3 \cdot 13$, donc

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

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

- (b) • On a $2 \wedge 11 = 1$, donc $\bar{2}$ est inversible dans $\mathbb{Z}/11\mathbb{Z}$

• l'ordre de $\bar{2}$ divise 10, $\circ(\bar{2}) \in \{1, 2, 5, 10\}$. Mais $\bar{2}^1 = \bar{2} \neq \bar{1}$, $\bar{2}^2 = \bar{4}$, $\bar{2}^5 = \bar{10}$ et $\bar{2}^{10} = \bar{1}$. Bref $\circ(\bar{2}) = 10$

• $\mathcal{U}_{11}$ est de cardinal 10 et il contient $\bar{2}$ un élément de $\mathcal{U}_{11}$ d'ordre 10, donc $\mathcal{U}_{11} = \langle \bar{2} \rangle$, ainsi $\mathcal{U}_{11}$ est cyclique

• Les générateurs de $\mathcal{U}_{11}$ sont exactement les éléments de la forme $\bar{2}^k$ avec $k \in \llbracket 0, 9 \rrbracket$ et $k \wedge 10 = 1$. Or $k \in \llbracket 0, 9 \rrbracket$ et $k \wedge 10 = 1$ équivaut à $k \in \{1, 3, 7, 9\}$, donc les générateurs de $\mathcal{U}_{11}$ sont exactement $\bar{2}$, $\bar{2}^3 = \bar{8}$, $\bar{2}^7 = \bar{3}$ et $\bar{2}^9 = \bar{6}$

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

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

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

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

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

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

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

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

4. • Existence: Si $H = \{\bar{0}\}$, 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 $\{\bar{0}\} \subset H$, donc $\pi_n^{-1}(\{\bar{0}\}) \subset \pi_n^{-1}(H)$, ceci fournit l'inclusion $n\mathbb{Z} \subset \delta\mathbb{Z}$ qui se traduit par divisibilité à $\delta \mid n$

• Unicité: s'il existe $\delta, \delta' \in \mathbb{N}^*$ tel 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 $\bar{\delta}$. Autrement $\pi_n(\delta\mathbb{Z}) = \langle \bar{\delta} \rangle$

L'ENSEMBLE DES NON INVERSIBLES $\mathbb{Z}/n\mathbb{Z}$

6. π_n est surjective, donc $H = \pi_n(\pi_n^{-1}(H)) = \langle \bar{\delta} \rangle$. On déduit que H est monogène engendré par $\bar{\delta}$. En outre un sous-groupe d'un groupe fini est aussi fini
7. $\circ(\bar{\delta}) = \circ(\bar{\delta} \cdot 1) = \frac{n}{n \wedge \delta} = \frac{n}{\delta} = d$. Donc $\circ(\bar{\delta}) = d$
8. H est un sous groupe de cardinal d car H est cyclique et $\circ(\bar{\delta}) = d$.
Soit K un sous-groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal d .
Soit $\bar{\alpha} \in K$, alors $d\bar{\alpha} = \bar{0}$, donc $n \mid d\alpha$ ou encore $\delta = \frac{n}{d}$ divise α , donc il existe $\beta \in \mathbb{Z}$ tel que $\alpha = \beta\delta$ ceci donne $\bar{\alpha} \in \langle \bar{\delta} \rangle$. Ainsi on a montré que $K \subset \langle \bar{\delta} \rangle = H$ et puisque ils ont le même cardinal alors l'égalité $K = H$.
Bref H est l'unique sous groupe de cardinal d de $(\mathbb{Z}/n\mathbb{Z}, +)$.

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

9. On suppose que n n'est pas primaire.
- (a) Par hypothèse $n \geq 2$. D'après le théorème fondamental de l'arithmétique il existe $r \in \mathbb{N}^*$, une suite $p_1, \dots, p_r$ de nombres premiers deux à deux distincts et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$ tels que

$$n = \prod_{i=1}^r p_i^{\alpha_i}$$

n est supposé non primaire donc $r \geq 2$. On pose $n_1 = p_1^{\alpha_1}$ et $n_2 = \prod_{i=2}^r p_i^{\alpha_i}$. On a $n = n_1 \cdot n_2$, $1 < n_1 < n$ 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 $\bar{n}_1, \bar{n}_2 \notin \mathcal{U}_n$, alors $\bar{n}_1 \in \mathcal{N}_n$ et $\bar{n}_2 \in \mathcal{N}_n$
10. $\Leftarrow$ Si $p \mid k$, alors $k \wedge p^\alpha \neq 1$. Donc $\bar{k} \notin \mathcal{U}_{p^\alpha}$, autrement-dit $\bar{k} \in \mathcal{N}_{p^\alpha}$
- $\Rightarrow$ 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 $\bar{k} \in \mathcal{U}_{p^\alpha}$, d'où $\bar{k} \notin \mathcal{N}_{p^\alpha}$
11. $\Rightarrow$ Par contraposée. Si n n'est pas primaire, alors il existe $\bar{n}_1, \bar{n}_2 \in \mathcal{N}_n$ sans que $\bar{n}_1 + \bar{n}_2$ 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:

$$\bar{k} \in \mathcal{N}_{p^\alpha} \iff p \mid k \xLeftrightarrow{n=p^\alpha} \bar{k} \in \langle \bar{p} \rangle$$

ce qui montre que $\mathcal{N}_{p^\alpha} = \langle \bar{p} \rangle$ qui est un sous-groupe engendré par $\bar{p}$