

GROUPE DES INVERSIBLES DE $\mathbb{Z}/n\mathbb{Z}$

Dans tout ce problème on désigne par:

- n un entier naturel supérieur ou égal à 1.
- $\bar{a}$ la classe de l'entier a modulo n .
- $(\mathbb{U}_n, \times)$ le groupe des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
- $\mathcal{N}_n$ l'ensemble des éléments non inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
- $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, a \mapsto \bar{a}$ le morphisme d'anneaux surjectif.
- $\varphi(n) = \text{Card}\{k \in \llbracket 1, n \rrbracket / k \wedge n = 1\}$, l'indicateur d'Euler.

Il résulte du théorème chinois que si $n \in \mathbb{N}^*$, $n \geq 2$ s'écrit $n = \prod_{i=1}^r m_i$ où $m_i = p_i^{\alpha_i}$ avec les p_i premiers distincts et les α_i dans $\mathbb{N}^*$, les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ sont isomorphes. Il s'en suit l'isomorphisme entre les groupes multiplicatifs $\mathbb{U}_n$ et $\mathbb{U}_{m_1} \times \dots \times \mathbb{U}_{m_r}$ où $\mathbb{U}_k = \mathbb{U}(\mathbb{Z}/k\mathbb{Z})$. Nous allons étudier la structure de $\mathbb{U}_{p^\alpha}$ pour p entier naturel premier et $\alpha \in \mathbb{N}^*$

Partie I: Cas où $\alpha = 1$.

1. Montrer que tout sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.
2. Montrer que pour tout diviseur d de n , il existe un unique sous-groupe C_d de $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal d .
3. Soit $(G, .)$ un groupe d'ordre n vérifiant: si $d \mid n$ alors le cardinal de $\{x \in G, x^d = e_G\}$ est inférieur ou égal à d . Montrer que G est cyclique
4. Dédurre que si $(\mathbb{K}, +, \times)$ est un corps fini de cardinal n , alors $(\mathbb{K}^*, \times)$ est un groupe cyclique isomorphe à $(\mathbb{Z}/(n-1)\mathbb{Z}, +)$
5. Que dire de $\mathbb{U}_p$, si p est un nombre premier?

Partie II: Cas où p est premier et impair

6. Montrer que: $\forall k \in \mathbb{N}, (1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$
7. Déterminer l'ordre de $\bar{1+p}$ dans $\mathbb{U}_{p^\alpha}$ où $\alpha \in \mathbb{N}^*$
8. Soient a et b deux éléments d'ordre p et q d'un groupe $(G, .)$. Montrer que si $ab = ba$ et $p \wedge q = 1$, alors ab est d'ordre pq
9. Montrer que $(\mathbb{U}_{p^\alpha}, .)$ est un groupe cyclique

Partie III: Cas où $p = 2$

10. Montrer que: $\forall k \in \mathbb{N}, 5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}$
11. Quel l'ordre de $\bar{5}$ dans $\mathbb{U}_{2^\alpha}$ où α est entier et $\alpha \geq 3$.
12. Montrer que $(\mathbb{U}_{2^\alpha}, .)$ n'est pas cyclique pour $\alpha \geq 3$

Partie IV: Cas général

13. Soit $(H, .)$ et $(K, .)$ deux groupes finis $h \in H, k \in K$. Montrer que l'ordre de (h, k) dans le groupe $(H \times K, .)$ est **ppcm** $(o(h), o(k))$.
14. Montrer que le groupe produit de deux groupes cycliques H et K est cyclique si, et seulement si, leurs ordres sont premiers entre eux
15. Déterminer $n \geq 2$ tel que $(\mathbb{U}_n, .)$ soit cyclique

GROUPE DES INVERSIBLES DE $\mathbb{Z}/n\mathbb{Z}$

Partie I: Cas où $\alpha = 1$.

1. L'ensemble $A = \{k \in \mathbb{N}^*, \bar{k} \in H\}$ est non vide car il contient n , donc il admet un plus petit élément p . L'inclusion $\mathcal{G}\mathbf{r}(\bar{p}) \subset H$, car $\bar{p} \in H$. Inversement soit $\bar{h} \in H$, avec $h \in \mathbb{Z}$, on effectue la division euclidienne de h par δ , il existe $(q, r) \in \mathbb{Z}^2$ tel que $h = q\delta + r$ avec $0 \leq r < \delta$. Par passage aux classes on obtient $\bar{h} = q\bar{\delta} + \bar{r}$, soit $\bar{r} = \bar{h} - q\bar{\delta} \in H$. Si $r \neq 0$, alors $r \in A$, donc $r \geq \delta$. Absurde.
2. On écrit $n = d\delta$. Le groupe $\mathcal{G}\mathbf{r}(\bar{\delta})$ est un sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ d'ordre $\circ(\bar{\delta}) = \frac{n}{n \wedge \delta} = \frac{n}{\delta} = d$.
soit C_d un sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ d'ordre d . D'après la question précédente C_d est cyclique, alors il existe $x \in \mathbb{Z}$ tel que $C_d = \mathcal{G}\mathbf{r}(\bar{x})$. Par le théorème de Lagrange $d\bar{x} = \bar{0}$, donc $n \mid dx$, puis $\delta \mid x$. On tire donc $\mathcal{G}\mathbf{r}(\bar{x}) \subset \mathcal{G}\mathbf{r}(\bar{\delta})$ et par égalité des cardinaux, on obtient l'égalité des sous-groupes.
3. Pour $d \in \mathbb{N}^*$ divisant n , on pose H_d l'ensemble des éléments de G d'ordre d .
— S'il n'existe pas d'éléments de G tel que $\circ(x) = d$, alors $H_d = \emptyset$;
— Sinon il existe $x \in G$ d'ordre d , alors d'une part $\mathcal{G}\mathbf{r}(x) \subset \{x \in G, x^d = e_G\}$ et par égalité des cardinaux $\mathcal{G}\mathbf{r}(x) \subset \{x \in G, x^d = e_G\}$, par conséquent H_d est l'ensemble des générateurs de $\mathcal{G}\mathbf{r}(x)$, donc il est de cardinal $\varphi(d)$.

Bref $\mathbf{Card}(H_d) \leq \varphi(d)$. Mais $G = \bigcup_{d|n} H_d$ est une union disjointe, on obtient alors

$$\sum_{d|n} \mathbf{Card}(H_d) = n$$

On sait aussi que

$$\sum_{d|n} \varphi(d) = n$$

Alors $\sum_{d|n} (\varphi(d) - \mathbf{Card}(H_d)) = 0$, donc pour tout d diviseur de n , on a $\mathbf{Card}(H_d) = \varphi(d)$. En particulier $\mathbf{Card}(H_n) = \varphi(n) \geq 1$, donc G est cyclique.

4. Quel que soit d un diviseur de $n-1$, l'ensemble des x de $\mathbb{K}^*$ tels que $x^d = 1_{\mathbb{K}}$ admet au plus d solutions; d'après la question précédente $\mathbb{K}^*$ est cyclique d'ordre $n-1$, donc il est isomorphe à $\left(\mathbb{Z}/(n-1)\mathbb{Z}, +\right)$.
5. Si p est premier $\left(\mathbb{Z}/p\mathbb{Z}, +, \cdot\right)$ est un corps de cardinal p . Donc le groupe $(\mathbb{U}_p, \cdot)$ est cyclique et isomorphe au groupe $\left(\mathbb{Z}/(p-1)\mathbb{Z}, +\right)$.

Partie II: Cas où p est premier et impair

6. Faisons un raisonnement par récurrence sur $k \in \mathbb{N}$.
— Pour $k = 0$, l'égalité est vérifiée.
— Soit $k \in \mathbb{N}$, on fait appel à l'hypothèse de récurrence puis à la formule de binôme de Newton

$$\begin{aligned} (1+p)^{p^{k+1}} &= \left[(1+p)^{p^k}\right]^p \\ &= (1+p^{k+1} + \lambda p^{k+2})^p \\ &= (1+p^{k+1}(1+\lambda p))^p \\ &= 1 + p^{k+1}(1+\lambda p) + \sum_{\ell=2}^p C_p^\ell p^{(k+1)\ell} (1+\lambda p)^\ell \\ &= 1 + p^{k+1} + \lambda p^{k+2} + \underbrace{\sum_{\ell=2}^p C_p^\ell p^{(k+1)\ell} (1+\lambda p)^\ell}_{= \beta p^{k+2}} \end{aligned}$$

GROUPE DES INVERSIBLES DE $\mathbb{Z}/n\mathbb{Z}$

Avec $\beta = \lambda + \sum_{\ell=2}^p C_p^\ell p^{(k+1)\ell-k-2} (1+\lambda p)^\ell$. Récurrence achevée

7. Comme $(1+p)^{p^{\alpha-1}} \equiv 1 + p^\alpha \pmod{p^{\alpha+1}}$, l'ordre de $\overline{1+p}$ dans $\mathbb{U}_{p^\alpha}$ divise $p^{\alpha-1}$ et donc de la forme p^k où $k \in \llbracket 1, \alpha-1 \rrbracket$. Mais comme $(1+p)^{p^{\alpha-2}} \equiv 1 + p^{\alpha-2} \pmod{p^\alpha}$, $[p^\alpha] \not\equiv 1 \pmod{p^\alpha}$, alors l'ordre de $\overline{1+p}$ est $p^{\alpha-1}$.
8. Comme $ab = ba$, alors $(ab)^{pq} = a^{pq}b^{pq} = e$, donc ab est d'ordre fini d divisant pq . Inversement si $n \in \mathbb{Z}$ tel que $(ab)^n = e$, alors $b^{np} = (ab)^{np} = e$, donc $q \mid np$ et par le théorème de Gauss, puisque $p \wedge q = 1$, on conclut que $q \mid n$. De même $p \mid n$ et par suite $pq \mid n$. Ceci permet l'égalité l'ordre de ab est pq .
9. L'ordre de $\mathbb{U}_{p^\alpha}$ est évidemment $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. D'autre part on sait que $\mathbb{U}_p$ est cyclique et on fixe alors $a \in \mathbb{Z}$ un représentant d'un générateur de $\mathbb{U}_p$, alors $a \wedge p = 1$ et par conséquent $a \wedge p^\alpha = 1$. On tire que $\bar{a}$ est inversible dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ et soit k son ordre, alors $a^k \equiv 1 \pmod{p^\alpha}$ et donc aussi $a^k \equiv 1 \pmod{p}$. Or $p-1$ est l'ordre de la classe de a dans $\mathbb{Z}/p\mathbb{Z}$, donc $p-1$ divise k , donc on peut écrire $k = m(p-1)$. Soit $\bar{b} = \bar{a}^m$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ et $\bar{x} = \overline{b(1+p)}$. Cet élément est d'ordre $p^{\alpha-1}(p-1)$, car $\bar{b}$ et $\overline{1+p}$ commutent et ils sont d'ordres premiers entre eux à savoir $p-1$ et $p^{\alpha-1}$. On conclut donc $\mathbb{U}_{p^\alpha}$ est cyclique.

Partie III: Cas où $p = 2$

10. Faisons un raisonnement par récurrence sur $k \in \mathbb{N}$.

— Pour $k = 0$, l'égalité est vérifiée

— Soit $k \in \mathbb{N}$. Par hypothèse de récurrence il existe $\lambda \in \mathbb{Z}$ tel que $5^{2^k} = 1 + 2^{k+2} + \lambda 2^{k+3}$ alors

$$\begin{aligned} 5^{2^{k+1}} &= \left(5^{2^k}\right)^2 = \left(1 + 2^{k+2} + \lambda 2^{k+3}\right)^2 \\ &= 1 + 2^{k+3} + 2^{k+4} + 2^{2k+4} + 2^{k+4}\lambda + 2^{k+4}\lambda \\ &= 1 + 2^{k+3} + 2^{k+4}(\lambda + 2^k(1 + 2\lambda)^2) \end{aligned}$$

Récurrence achevée

11. Pour $\alpha \geq 3$. Comme $5^{2^{\alpha-2}} \equiv 1 + 2^\alpha \pmod{2^{\alpha+1}}$, l'ordre de $\bar{5}$ dans $\mathbb{U}_{2^\alpha}$ divise $2^{\alpha-2}$ et donc de la forme 2^k où $k \in \llbracket 1, \alpha-2 \rrbracket$. Mais comme $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}$, $[2^\alpha] \not\equiv 1 \pmod{2^\alpha}$, alors l'ordre de $\bar{5}$ est $2^{\alpha-2}$.
12. Soit $\alpha \geq 3$. Remarquons d'abord que $-\bar{1} \notin \text{Gr}(\bar{5})$, car sinon il existera $j \in \mathbb{N}$ tel que $5^j \equiv -1 \pmod{2^\alpha}$ et puisque $\alpha \geq 2$, alors $5^j \equiv -1 \pmod{4}$, ce qui est impossible. Soit G le groupe engendré par $-\bar{1}$ et $\bar{5}$. Vu que $-\bar{1}$ et $\bar{5}$ commutent, alors $G = \text{Gr}(\{-\bar{1}, \bar{5}\}) = \left\{ \varepsilon \bar{5}^k, \varepsilon = \pm 1 \text{ et } k \in \llbracket 0, 2^{\alpha-2} - 1 \rrbracket \right\}$. Avec $\text{Gr}(\bar{5}) \subsetneq G \subset \mathbb{U}_{2^\alpha}$, alors $2^{\alpha-2} < \text{Card}(G) \leq \text{Card}(\mathbb{U}_{2^\alpha}) = 2^{\alpha-1}$. En outre $\text{Card}(G)$ divise $2^{\alpha-1}$, donc forcément $\text{Card}(G) = 2^{\alpha-1}$, puis $G = \mathbb{U}_{2^\alpha}$. Mais pour tout $x \in G = \mathbb{U}_{2^\alpha}$, on a $x^{2^{\alpha-2}} = 1$, donc $(\mathbb{U}_{2^\alpha}, \cdot)$ n'est pas cyclique.

Partie IV: Cas général

13. Posons $m = \text{ppcm}(p, q)$, avec $p = o(h)$ et $q = o(k)$ alors il existe $a, b \in \mathbb{N}$ tels que $m = ap$ et $m = bq$. Par définition du groupe produit

$$(h, k)^m = (h^m, k^m) = (e_H, e_K)$$

donc (h, k) est d'ordre fini.

Soit $k \in \mathbb{Z}$, on a:

$$\begin{aligned} (h, k)^\alpha = (e_H, e_K) &\iff (h^\alpha, k^\alpha) = (e_H, e_K) \\ &\iff \begin{cases} h^\alpha = e_H \\ k^\alpha = e_K \end{cases} \\ &\iff \begin{cases} p \mid \alpha \\ q \mid \alpha \end{cases} \\ &\iff m \mid \alpha \end{aligned}$$

On conclut donc que $o((h, k)) = m$

GROUPE DES INVERSIBLES DE $\mathbb{Z}/n\mathbb{Z}$

14. Soit h et k respectivement les générateurs de H et K et p et q sont respectivement leurs ordres
- $\Leftrightarrow$ Si $p \wedge q = 1$, alors (h, k) est d'ordre pq , avec $(h, k) \in H \times K$ et $\text{Card}(H \times K) = pq$, on conclut que $H \times K$ est cyclique de générateur (h, k)
 - $\Rightarrow$ Par contraposée, si p et q ne sont pas premiers entre eux, alors tout élément de $H \times K$ est d'ordre inférieur au $\text{ppcm}(p, q) < pq = \text{Card}(H \times K) = pq$. Le groupe $H \times K$ n'est pas cyclique
15. On discute d'abord selon le nombre premier p

- Si $p = 2$. On vérifie aisément que $\mathbb{U}_2 = \{\bar{1}\}$ et $\mathbb{U}_4 = \{\bar{1}, \bar{3}\}$ sont cycliques et pour tout $\alpha \geq 3$ le groupe $\mathbb{U}_{2^\alpha}$ n'est pas cyclique
- Si p est premier supérieur à 3, alors $\mathbb{U}_{p^\alpha}$ est cyclique d'après (9)
- Si p est premier supérieur à 3, alors $\mathbb{U}_{2p^\alpha}$ est cyclique d'après (14)

En utilisant les notations du début du problème, $\mathbb{U}_n$ est cyclique si, et seulement si, les $\mathbb{U}_{m_i}$ le sont les m_i sont deux à deux premiers entre eux et compte tenu de (14). Ceci impose que n admet au plus un diviseur premier impair puisque $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ est pair si $p \geq 3$. Si de plus n admet deux diviseurs premiers, l'un d'eux doit être égal à 2 et d'exposant 1 dans la décomposition de n en facteurs premiers car $\varphi(2^\beta) = 2^{\beta-1}$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ et $(p-1) \wedge 2^{\beta-1} = 1$.

Bref $(\mathbb{U}_n, \cdot)$ est cyclique si, et seulement, si $n \in \{2, 4, p^\alpha, 2p^\alpha\}$ où p est premier impair