ÉNONCÉ

Navigation : *Énoncé* *Corrigé*

Dans tout ce problème on désigne par:

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

Il résulte du théorème chinois que si $n \in \mathbb{N}^*$, $n \geqslant 2$ 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 $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ sont isomorphes. Il s'en suit l'isomorphisme entre les groupes multiplicatifs $\mathbb{U}_n$ et $\mathbb{U}_{m_1} \times \cdots \times \mathbb{U}_{m_r}$ où $\mathbb{U}_k = \mathbb{U}\left(\mathbb{Z}/k\mathbb{Z}\right)$. 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 $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est cyclique.
2. Montrer que pour tout diviseur d de n, il existe un unique sous-groupe C_d de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ 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. Déduire que si $(\mathbb{K}, +, \times)$ est un corps fini de cardinal n, alors $(\mathbb{K}^*, \times)$ est un groupe cyclique isomorphe à $\left(\mathbb{Z}/(n-1)\mathbb{Z}, +\right)$
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: $\forall k \in \mathbb{N}, \quad (1+p)^{p^k} \equiv 1 + p^{k+1} \quad \left[p^{k+2}\right]$
7. Déterminer l'ordre de $\overline{1+p}$ 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: $\forall k \in \mathbb{N}, \quad 5^{2^k} \equiv 1 + 2^{k+2} \quad \left[2^{k+3}\right]$
11. Quel l'ordre de $\overline{5}$ dans $\mathbb{U}_{2^\alpha}$ où α est entier et $\alpha \geqslant 3$.
12. Montrer que $(\mathbb{U}_{2^\alpha}, .)$ n'est pas cyclique pour $\alpha \geqslant 3$

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** $(\circ(h), \circ(k))$.
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 $n \geqslant 2$ tel que $(\mathbb{U}_n,.)$ soit cyclique

Partie I: Cas où $\alpha = 1$.

1. L'ensemble $A = \left\{k \in \mathbb{N}^* \ , \ \overline{k} \in H\right\}$ est non vide car il contient n, donc il admet un plus petit élément p. L'inclusion $\mathbf{gr}\left(\overline{p}\right) \subset H$, car $\overline{p} \in H$. Inversement soit $\overline{h} \in H$, 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 $0 \leqslant r < \delta$. Par passage aux classes on obtient $\overline{h} = q.\overline{\delta} + \overline{r}$, soit $\overline{r} = \overline{h} - q\overline{\delta} \in H$. Si $r \neq 0$, alors $r \in A$, donc $r \geqslant \delta$. Absurde
2. On écrit $n = d\delta$. Le groupe $\mathbf{gr}\left(\overline{\delta}\right)$ est un sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ d'ordre $\circ\left(\overline{\delta}\right) = \dfrac{n}{n \wedge \delta} = \dfrac{n}{\delta} = d$.
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 $C_d = \mathbf{gr}\left(\overline{x}\right)$. Par le théorème de Lagrange $d\overline{x} = \overline{0}$, donc $n \mid dx$, puis $\delta \mid x$. On tire donc $\mathbf{gr}\left(\overline{x}\right) \subset \mathbf{gr}\left(\overline{\delta}\right)$ 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 $\mathbf{gr}(x) \subset \{x \in G \ , \ x^d = e_G\}$ et par égalité des cardinaux $\mathbf{gr}(x) \subset \{x \in G \ , \ x^d = e_G\}$, par conséquent H_d est l'ensemble des générateurs de $\mathbf{gr}(x)$, donc il est de cardinal $\varphi(d)$

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

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

   On sait aussi que

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

   Alors $\sum_{d|n} \left(\varphi\left(d\right) - \mathbf{Card}\left(H_d\right)\right) = 0$, donc pour tout d diviseur de n, on a $\mathbf{Card}\left(H_d\right) = \varphi(d)$. En particulier $\mathbf{Card}\left(H_n\right) = \varphi(n) \geqslant 1$, 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 $\left(\mathbb{Z}/p\mathbb{Z}, +, .\right)$ est un corps de cardinal p. Donc Ie groupe $(\mathbb{U}_p, .)$ 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

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

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

7. Comme $(1+p)^{p^{\alpha-1}} \equiv 1+p^\alpha \quad [p^{\alpha+1}]$, l'ordre de $\overline{1+p}$ dans $\mathbb{U}_{p^\alpha}$ divise $p^{\alpha-1}$ et donc de la forme p^k où $k \in [\![1, \alpha-1]\!]$. Mais comme $(1+p)^{p^{\alpha-2}} \equiv 1+p^{\alpha-2} \quad [p^\alpha] \not\equiv 1 \quad [p^\alpha]$, 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 conlut 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 évidement $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. 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 $\overline{a}$ est inversible dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ et soit k son ordre , alors $a^k \equiv 1 \quad [p^\alpha]$ et donc aussi $a^k \equiv 1 \quad [p]$. 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 $\overline{b} = \overline{a}^m$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ et $\overline{x} = \overline{b(1+p)}$. Cet élément est d'ordre $p^{\alpha-1}(p-1)$, car $\overline{b}$ 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

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

    Récurrence achevée
11. Pour $\alpha \geqslant 3$. Comme $5^{2^{\alpha-2}} \equiv 1+2^\alpha \quad [2^{\alpha+1}]$, l'ordre de $\overline{5}$ dans $\mathbb{U}_{2^\alpha}$ divise $2^{\alpha-2}$ et donc de la forme 2^k où $k \in [\![1, \alpha-2]\!]$. Mais comme $5^{2^{\alpha-3}} \equiv 1+2^{\alpha-1} \quad [2^\alpha] \not\equiv 1 \quad [2^\alpha]$, alors l'ordre de $\overline{5}$ est $2^{\alpha-2}$
12. Soit $\alpha \geqslant 3$. Remarquons d'abord que $-\overline{1} \notin \mathbf{gr}(\overline{5})$, car sinon il existera $j \in \mathbb{N}$ tel que $5^j \equiv -1 \quad [2^\alpha]$ et puisque $\alpha \geqslant 2$, alors $5^j \equiv -1 \quad [4]$, ce qui est impossible. Soit G le groupe engendré par $-\overline{1}$ et $\overline{5}$. Vu que $-\overline{1}$ et $\overline{5}$ commutent, alors $G = \mathbf{gr}(\{-\overline{1}, \overline{5}\}) = \left\{\varepsilon\overline{5}^k,\ \varepsilon = \pm 1 \text{ et } k \in [\![0, 2^{\alpha-2}-1]\!]\right\}$. Avec $\mathbf{gr}(\overline{5}) \subsetneq G \subset \mathbb{U}_{2^\alpha}$, alors

$2^{\alpha-2} < \textbf{Card}(G) \leqslant \textbf{Card}\left(\mathbb{U}_{2^\alpha}\right) = 2^{\alpha-1}$. En outre $\textbf{Card}(G)$ divise $2^{\alpha-1}$, donc forcément $\textbf{Card}(G) = 2^{\alpha-1}$, puis $G = \mathbb{U}_{2^\alpha}$. Mais pour tout $x \in G = \mathbb{U}_{2^\alpha}$, on a $x^{2^{\alpha-2}} = 1$, donc $(\mathbb{U}_{2^\alpha}, .)$ n'est pas cyclique

Partie IV: Cas général

13. Posons $m = \textbf{ppcm}(p,q)$, avec $p = \circ(h)$ et $q = \circ(k)$ 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 $\circ((h,k)) = m$

14. Soit h et k respectivement les générateurs de H et K et p et q sont respectivement leurs ordres
    - $\Leftarrow$) Si $p \wedge q = 1$, alors (h,k) est d'ordre pq, avec $(h,k) \in H \times K$ et $\textbf{Card}(H \times K) = pq$, 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 $\textbf{ppcm}(p,q) < pq = \textbf{Card}(H \times K) = pq$. 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 $\mathbb{U}_2 = \{\overline{1}\}$ et $\mathbb{U}_4 = \{\overline{1}, \overline{3}\}$ sont cycliques et pour tout $\alpha \geqslant 3$ 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 deébut du problème, $\mathbb{U}_n$ est cyclique si, et seulement si, les $\mathbb{U}_{m_i}$ le sont les m_i sont deux a? 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 $p \geqslant 3$. 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 $\varphi\left(2^\beta\right) = 2^{\beta-1}$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ et $(p-1) \wedge 2^{\beta-1} = 1$.

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