Agrégation Externe

L'anneau $\mathbb{Z}/n\mathbb{Z}$

Ce problème est en relation avec les leçons d'oral suivantes :

- 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 121 : Nombres premiers. Applications.
- 126 : Exemples d'équations diophantiennes.

On pourra consulter les ouvrages suivants.

- P. Boyer, J. J. Risler : *Algèbre pour la licence 3. Groupes, anneaux, corps.* Dunod (2006).
- F. Combes — *Algèbre et géométrie.* Bréal (2003).
- M. Demazure. *Cours d'algèbre.* Cassini. (1997).
- S. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).
- S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1.* Masson (1994).
- H. Gianella, F. Krust, F. Taieb, N. Tosel : *Problèmes choisis de mathématiques supérieures.* Springer (2001).
- X. Gourdon. *Les Maths en tête. Algèbre.* Ellipses.
- K. Madere. *Préparation à l'oral de l'agrégation. Leçons d'algèbre.* Ellipses (1998).
- P. Ortiz. *Exercices d'algèbre.* Ellipses (2004).
- D. Perrin. *Cours d'algèbre.* Ellipses (1996).
- G. Rauch. *Les groupes finis et leurs représentations.* Ellipses (2000).

1 Énoncé

Pour tout entier naturel $n \geq 0$, on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes résiduelles modulo n et, pour $n \neq 1$, $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \left\{\overline{0}\right\}$.

Pour $n = 0$, l'anneau $\mathbb{Z}_0$ est isomorphe à $\mathbb{Z}$ et pour $n = 1$, le groupe $\mathbb{Z}_1$ est réduit à $\left\{\overline{0}\right\}$.

Pour ce qui suit, on suppose que $n \geq 2$ et on note $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}_n$.

Si k est un entier relatif, on note $\overline{k} = k + n\mathbb{Z}$ la classe de k dans $\mathbb{Z}_n$ et en utilisant le théorème de division euclidienne, on vérifie que :

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\} = \left\{\overline{1}, \cdots, \overline{n}\right\}$$

est d'ordre n.

Pour tout couple (a, b) d'entiers relatifs, on note $a \wedge b$ le pgcd de a et b et $a \vee b$ leur ppcm.

La fonction indicatrice d'Euler est la fonction φ qui associe à tout entier naturel non nul n, le nombre $\varphi(n)$ d'entiers compris entre 1 et n qui sont premiers avec n (pour $n = 1$, on a $\varphi(1) = 1$).

Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}_n$.

– I – Généralités sur $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

1. Montrer qu'il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}_n$ telle que la surjection canonique π_n soit un morphisme d'anneaux.
   Plus généralement, pour tout idéal I d'un anneau commutatif unitaire $\mathbb{A}$, Il existe une unique structure d'anneau commutatif unitaire sur $\dfrac{\mathbb{A}}{I}$ telle que la surjection canonique $\pi_I : a \in \mathbb{A} \to \overline{a} = a + I \in \dfrac{\mathbb{A}}{I}$ soit un morphisme d'anneaux.
2. Montrer qu'un élément de $\mathbb{Z}_n \setminus \left\{\overline{0}\right\}$ est soit inversible, soit un diviseur de $\overline{0}$.
3. Quels sont les éléments nilpotents de l'anneau $\mathbb{Z}_n$?
4. Montrer que tous les sous-groupes de $\mathbb{Z}_n$ sont cycliques et que pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}_n$ d'ordre d.
5. Montrer que les idéaux de l'anneau $\mathbb{Z}_n$ sont ses sous-groupes additifs.
6. Déterminer tous les idéaux de $\mathbb{Z}_n$.
7. Quels sont les idéaux premiers, maximaux de $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $n \geq 2$?

– II – Morphismes de groupes, d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$. Le groupe $\mathrm{Aut}(\mathbb{Z}_n)$

Pour tout entier relatif k, on note respectivement $\overline{k}$ la classe de k modulo n et $\widehat{k}$ sa classe modulo m.

Un morphisme d'anneaux commutatifs unitaires $\varphi : \mathbb{A} \to \mathbb{B}$ est tel que $\varphi(1_\mathbb{A}) = 1_\mathbb{B}$.

On note $\mathrm{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}_m)$ [resp. $\mathrm{Hom}_{Ann}(\mathbb{Z}_n, \mathbb{Z}_m)$] l'ensemble des morphismes de groupes [resp. d'anneaux] de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$.

Pour tout entier $n \geq 2$, on note $\mathrm{Aut}(\mathbb{Z}_n)$ le groupe des automorphismes du groupe additif $\mathbb{Z}_n$.

1. Montrer que pour $n = m = 0$, on a :
$$\mathrm{Hom}_{gr}(\mathbb{Z}, \mathbb{Z}) \backsimeq \mathbb{Z} \text{ et } \mathrm{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}) = \{Id\}$$
2. Montrer que pour tout $n \in \mathbb{N}^*$, on a :
$$\mathrm{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}) = \{0\} \text{ et } \mathrm{Hom}_{Ann}(\mathbb{Z}_n, \mathbb{Z}) = \emptyset$$

3. Montrer que pour tout $m \in \mathbb{N}^*$, on a :

$$\mathrm{Hom}_{gr}(\mathbb{Z}, \mathbb{Z}_m) \backsimeq \mathbb{Z}_m \text{ et } \mathrm{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}_m) = \{\pi_m\}$$

4. Montrer que pour n, m premiers entre eux dans $\mathbb{N}^*$, on a :

$$\mathrm{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}_m) = \left\{\widehat{0}\right\} \text{ et } \mathrm{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}_m) = \emptyset$$

5. Montrer que pour n, m non premiers entre eux dans $\mathbb{N}^*$, on a :

$$\mathrm{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}_m) \backsimeq \mathbb{Z}_\delta = \mathbb{Z}_{n \wedge m}$$

et :

$$\mathrm{Hom}_{Ann}(\mathbb{Z}_n, \mathbb{Z}_m) = \begin{cases} \left\{\overline{k} \mapsto \widehat{k}\right\} \text{ si } m \text{ divise } n \\ \emptyset \text{ si } m \text{ ne divise pas } n \end{cases}$$

6. Montrer que pour tout $x \in \mathbb{Z}_n^\times$ l'application $\sigma(x)$ définie sur $\mathbb{Z}_n$ par :

$$\forall y \in \mathbb{Z}_n,\ \sigma(x)(y) = xy$$

est un automorphisme du groupe additif $\mathbb{Z}_n$, puis que l'application σ réalise un isomorphisme de $(\mathbb{Z}_n^\times, \cdot)$ sur $(\mathrm{Aut}(\mathbb{Z}_n), \circ)$.

7. Montrer que pour tout entier $n \geq 2$, les idéaux de l'anneau $\mathbb{Z}_n$ sont principaux. L'anneau $\mathbb{Z}_n$ est-il principal ? Quels sont les quotients de $\mathbb{Z}_n$?

– III – Le groupe multiplicatif $\mathbb{Z}_n^\times$, fonction indicatrice d'Euler

1. Soit a un entier relatif. Montrer que les propriétés suivantes sont équivalentes :
   (a) $\overline{a}$ est inversible dans $\mathbb{Z}_n$;
   (b) a est premier avec n ;
   (c) $\overline{a}$ est un générateur de $(\mathbb{Z}_n, +)$.
2. Montrer que pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1\ (n)$ (théorème d'Euler).
3. Soit p un entier naturel premier. Montrer que pour tout entier relatif a premier avec n, on a $a^{p-1} \equiv 1\ (p)$ et pour tout entier relatif a, on a $a^p \equiv a\ (p)$ (théorème de Fermat).
4. Montrer que pour tout entier $n \geq 3$, $\varphi(n)$ est un entier pair.
5. Soit $p \geq 2$ un nombre premier. Expliquer comment utiliser le théorème de Fermat pour simplifier le calcul du reste dans la division euclidienne par p d'un entier de la forme a^b, où a, b sont des entiers plus grands que p, l'entier p ne divisant pas a.
   Par exemple, calculer le reste dans la division euclidienne de 115^{2013} par 11.
6. Montrer que, pour tout entier $n \geq 2$, les assertions suivantes sont équivalentes :
   (a) n est premier ;
   (b) pour tout entier naturel non nul α, on a $\varphi(n^\alpha) = (n-1)\, n^{\alpha-1}$;
   (c) $\varphi(n) = n - 1$;
   (d) $\mathbb{Z}_n$ est un corps ;
   (e) $\mathbb{Z}_n$ est un intègre ;
   (f) $(n-1)! \equiv -1\ (n)$ (théorème de Wilson) ;
   (g) $(n-2)! \equiv 1\ (n)$;

(h) pour tout k compris entre 1 et n, on a $(n-k)!\,(k-1)! \equiv (-1)^k \pmod{n}$;

(i) pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$;

(j) pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$ et $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$.

7. Soit p un nombre premier impair.

(a) Montrer qu'il y a exactement $\dfrac{p-1}{2}$ carrés et $\dfrac{p-1}{2}$ non carrés dans $\mathbb{Z}_p^*$.

(b) Montrer que l'ensemble des carrés de $\mathbb{Z}_p^*$ est l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} - \overline{1}$ et que l'ensemble des non carrés de $\mathbb{Z}_p^*$ est l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} + \overline{1}$.

(c) Montrer que $-\overline{1}$ est un carré dans $\mathbb{Z}_p$ si, et seulement si, p est congru à 1 modulo 4. Dans ce cas, donner une racine carrée explicite de $-\overline{1}$.

8. On s'intéresse aux racines du polynôme $P(X) = X^2 - 1$ dans $\mathbb{Z}_n$ pour $n \geq 2$.

(a) Traiter le cas où $n = p^\alpha$ où $p \geq 3$ est premier et $\alpha \geq 1$.

(b) Traiter le cas où $n = 2^\alpha$ où $\alpha \geq 1$.

(c) Traiter le cas général $n \geq 2$.

9. Montrer que pour tout entier $n \geq 2$, on a :

$$n = \sum_{d \in \mathcal{D}_n} \varphi(d)$$

(formule de Möbius).

– IV – Le théorème chinois

1. Soient $(n_j)_{1 \leq j \leq r}$ une suite de $r \geq 2$ entiers naturels distincts de 0 et 1 et $n = \prod_{j=1}^{r} n_j$.

(a) Montrer que les entiers $n_1, \cdots, n_r$ sont deux à deux premiers entre eux si, et seulement si, les anneaux $\mathbb{Z}_n$ et $\prod_{j=1}^{r} \mathbb{Z}_{n_j}$ sont isomorphes.

(b) Pour $n_1, \cdots, n_r$ sont deux à deux premiers entre eux, montrer que l'application :

$$\begin{array}{rccc} \psi : & \mathbb{Z}_n & \to & \prod_{j=1}^{r} \mathbb{Z}_{n_j} \\ & \overline{k} & \mapsto & (\pi_1(k), \cdots, \pi_r(k)) \end{array}$$

est un isomorphisme d'anneaux d'inverse :

$$\begin{array}{rccc} \psi^{-1} : & \prod_{j=1}^{r} \mathbb{Z}_{n_j} & \to & \mathbb{Z}_n \\ & (\pi_1(a_1), \cdots, \pi_r(a_r)) & \mapsto & \overline{\sum_{i=1}^{r} a_i u_i m_i} \end{array}$$

où $(u_j)_{1 \leq j \leq r}$ est une suite d'entiers relatifs telle que $\sum_{j=1}^{r} u_j \dfrac{n}{n_j} = 1$.

2. Expliquer comment utiliser le théorème chinois pour étudier un système d'équations diophantiennes :
$$k \equiv a_j \pmod{n_j} \ (1 \leq j \leq r)$$
où $(a_j)_{1 \leq j \leq r}$ est une suite donnée d'entiers relatifs.
3. Résoudre le système d'équations diophantiennes :
$$\begin{cases} k \equiv 2 \pmod{4} \\ k \equiv 3 \pmod{5} \\ k \equiv 1 \pmod{9} \end{cases}$$
4. Montrer que si $\mathbb{A}, \mathbb{B}$ sont deux anneaux unitaires et φ est un isomorphisme d'anneaux de $\mathbb{A}$ sur $\mathbb{B}$, il réalise alors un isomorphisme de groupes de $\mathbb{A}^\times$ (groupe des éléments inversibles de $\mathbb{A}$) sur $\mathbb{B}^\times$.
5. Montrer que si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $2 \leq p_1 < \cdots < p_r$ premiers et les α_i entiers naturels non nuls, on a alors :
$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$
6. Soient p et q deux nombres premiers distincts et $n = pq$.
Montrer que si a et b sont deux entiers naturels tels que $ab \equiv 1 \pmod{\varphi(n)}$, alors pour tout entier relatif m, on a $m^{ab} \equiv m \pmod{n}$.
Ce résultat est à la base du système cryptographique R.S.A.

– V – $\mathbb{Z}_{p^\alpha}^\times$ est cyclique pour $p \geq 3$ premier et $\alpha \geq 1$

1. On se propose de montrer que, pour tout nombre premier p, le groupe $\mathbb{Z}_p^*$ est cyclique.
Ce résultat est un cas particulier du suivant : tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps commutatif $\mathbb{K}$ est cyclique.
Pour $\mathbb{Z}_p^*$, on peut en donner une démonstration directe basée sur des considérations arithmétiques relativement simples.
On peut aussi en donner une démonstration qui utilise la formule de Möbius.
   (a) Soient $(G, \cdot)$ un groupe commutatif, $r \geq 2$ un entier et $g_1, \cdots, g_r$ dans G des éléments d'ordres finis respectifs $n_1, \cdots, n_r$ deux à deux premiers entre eux. Montrer que $g = g_1 \cdot \cdots \cdot g_r$ est d'ordre $n = \prod_{k=1}^{r} n_k$.
   (b) Soient $p \geq 3$ un nombre premier impair et $p - 1 = \prod_{j=1}^{r} p_j^{\alpha_j}$ sa décomposition en facteurs premiers où $2 \leq p_1 < \cdots < p_r$ sont premiers et les α_j, pour j compris entre 1 et r, sont des entiers naturels non nuls.
      i. Soient j compris entre 1 et r, $q_j = \dfrac{p-1}{p_j^{\alpha_j}}$ et $x \in \mathbb{Z}_p^*$. Montrer que x^{q_j} est d'ordre $p_j^{r_{x,j}}$ où $0 \leq r_{x,j} \leq \alpha_j$.
      ii. Montrer que, pour j compris entre 1 et r, il existe dans $\mathbb{Z}_p^*$ un élément d'ordre $p_j^{\alpha_j}$.
      iii. En déduire que $\mathbb{Z}_p^*$ est cyclique.

(c) Soit p un nombre premier et $\mathcal{D}_{p-1}$ l'ensemble des diviseurs de $p-1$ dans $\mathbb{N}^*$.
Pour tout $d \in \mathcal{D}_{p-1}$, on note $\psi(d)$ le nombre d'éléments d'ordre d dans le groupe multiplicatif $\mathbb{Z}_p^*$.

i. Montrer que $p-1 = \sum_{d \in \mathcal{D}_{p-1}} \psi(d)$.

ii. Montrer que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_{p-1}$ tel que $\psi(d) \geq 1$.

iii. En utilisant la formule de Möbius, montrer que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_{p-1}$ et en déduire que $\mathbb{Z}_p^*$ est cyclique.

2. Montrer que si p est un nombre premier impair et α un entier supérieur ou égal à 2, alors le groupe multiplicatif $\mathbb{Z}_{p^\alpha}^\times$ est cyclique.

3. Montrer que $\mathbb{Z}_2^\times$ et $\mathbb{Z}_{2^2}^\times$ sont cycliques.

4. On s'intéresse au groupe multiplicatif $\mathbb{Z}_{2^\alpha}^\times$ pour $\alpha \geq 3$.

(a) Montrer qu'il existe une suite $(\lambda_k)_{k\in\mathbb{N}}$ d'entiers impairs tels que :

$$\forall k \in \mathbb{N},\ 5^{2^k} = 1 + \lambda_k 2^{k+2}$$

(b) Montrer que la classe résiduelle de 5 modulo 2^α est d'ordre $2^{\alpha-2}$ dans $\mathbb{Z}_{2^\alpha}^\times$.

(c) On désigne par ψ l'application qui à toute classe résiduelle modulo 2^α, $k + 2^\alpha\mathbb{Z}$, associe la classe résiduelle modulo 4, $k + 4\mathbb{Z}$. Montrer que cette application est bien définie, qu'elle induit un morphisme surjectif de groupes multiplicatifs de $\mathbb{Z}_{2^\alpha}^\times$ sur $\mathbb{Z}_4^\times$ et que son noyau est un groupe cyclique d'ordre $2^{\alpha-2}$.

(d) Montrer que l'application :

$$\begin{array}{rccc} \pi : & \mathbb{Z}_{2^\alpha}^\times & \to & \mathbb{Z}_4^\times \times \ker(\psi) \\ & x & \mapsto & (\psi(x), \psi(x)\, x) \end{array}$$

est un isomorphisme de groupes. En déduire que $\mathbb{Z}_{2^\alpha}^\times$ est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. Le groupe $\mathbb{Z}_{2^\alpha}^\times$ est-il cyclique ?

On peut montrer le résultat suivant.

Théorème 1 *Le groupe multiplicatif $\mathbb{Z}_n^\times$ est cyclique si, et seulement si, $n = 2$, 4, p^α ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.*

– VI – Nombres de Carmichaël

On appelle nombre de Carmichaël tout entier $n \geq 2$ non premier tel que :

$$\forall x \in \mathbb{Z}_n^\times,\ x^{n-1} = \overline{1}$$

1. Montrer qu'un nombre de Carmichaël est impair.

2. Montrer que 561 est un nombre de Carmichaël.

3. Soit $n \geq 3$ un entier admettant un facteur carré, c'est-à-dire qu'il existe un nombre premier $p \geq 2$ et un entier $q \geq 1$ tels que $n = p^2 q$.
Montrer que n n'est pas un nombre de Carmichaël.

4. Soit $n \geq 3$ un entier. Montrer que les propriétés suivantes sont équivalentes :

(a) il existe un entier $r \geq 3$ et des nombres premiers $3 \leq p_1 < \cdots < p_r$ tels que $n = \prod_{j=1}^{r} p_j$ et, pour tout indice j compris entre 1 et r, $p_j - 1$ divise $n-1$;

(b) n est non premier et :

$$\forall x \in \mathbb{Z}_n,\ x^n = x$$

(c) n est un nombre de Carmichaël.

5. Soit $a \in \mathbb{N}^*$ tel que les entiers $p_1 = 6a+1$, $p_2 = 12a+1$ et $p_3 = 18a+1$ soient premiers. Montrer que $n = p_1 p_2 p_3$ est un nombre de Carmichaël.

– VII – Le théorème de Frobénius-Zolotarev

Pour cette partie, $p \geq 3$ est un nombre premier impair et $n \geq 2$ est un entier.
Pour tout entier relatif a, on note $\overline{a} \in \mathbb{Z}_p$ la classe résiduelle de a modulo p.
On dit qu'un entier a non multiple de p est un résidu quadratique modulo p si il existe un entier k tel que $k^2 \equiv a \pmod{p}$, ce qui signifie que $\overline{a}$ est un carré dans $\mathbb{Z}_p^*$.
Pour tout $\lambda \in \mathbb{Z}_p^*$, on définit le symbole de Legendre $\left(\frac{\lambda}{p}\right)$ par :

$$\left(\frac{\lambda}{p}\right) = \begin{cases} 1 \text{ si } \lambda \text{ est un carré dans } \mathbb{Z}_p^* \\ -1 \text{ sinon} \end{cases}$$

1. Soit $\varphi : \mathbb{Z}_p^* \to \{-1, 1\}$ un morphisme de groupes non trivial.
Montrer que :

$$\forall \lambda \in \mathbb{Z}_p^*,\ \varphi(\lambda) = \left(\frac{\lambda}{p}\right)$$

2. Soit $\gamma : GL_n(\mathbb{Z}_p) \to \{-1, 1\}$ un morphisme de groupes non trivial.

(a) Montrer que $\gamma(A) = 1$ pour toute matrice de transvection A.

(b) Montrer que $\gamma(A) = \left(\frac{\det(A)}{p}\right)$ pour toute matrice de dilatation A.

(c) Montrer que $\gamma(A) = \left(\frac{\det(A)}{p}\right)$ pour toute matrice $A \in GL_n(\mathbb{Z}_p)$.

3. Une matrice $A \in GL_n(\mathbb{Z}_p)$ peut être identifiée à un automorphisme de $\mathbb{Z}_p^n$ qui est une permutation particulière de l'ensemble fini $\mathbb{Z}_p^n$, donc la restriction de la signature des permutations à $GL\left(\mathbb{Z}_p^n\right)$ permet de définir une morphisme de groupes ε de $GL_n(\mathbb{Z}_p)$ dans $\{-1, 1\}$.
Montrer que :

$$\forall A \in GL_n(\mathbb{Z}_p),\ \varepsilon(A) = \left(\frac{\det(A)}{p}\right)$$

– VIII – Groupes abéliens finis

On note $\theta(g)$ l'ordre d'un élément g d'un groupe G.
Pour un groupe fini G, l'entier $e(G) = \max_{g \in G} \theta(g)$ est l'exposant du groupe.
Un caractère d'un groupe G est un morphisme de groupes de G dans $\mathbb{C}^*$.
Pour tout entier $m \geq 2$, on note Γ_m le groupe cyclique des racines m-èmes de l'unité dans $\mathbb{C}^*$.

1. Soient $(G, \cdot)$ un groupe commutatif, $r \geq 2$ un entier et $g_1, g_2, \cdots, g_r$ des éléments deux à deux distincts de G d'ordres respectifs $m_1, m_2, \cdots, m_r$.
Montrer qu'il existe dans G un élément g_0 d'ordre égal au ppcm de ces ordres.

2. Soit $(G,\cdot)$ un groupe commutatif fini. Montrer que :
$$e(G)=\max_{g\in G}\theta(g)=\text{ppcm}\{\theta(g)\mid g\in G\}$$
3. Soit $(G,\cdot)$ un groupe commutatif fini d'ordre $n\geq 2$. Montrer que n et son exposant $m=\max_{g\in G}\theta(g)$ ont les mêmes facteurs premiers.
4. Montrer qu'un groupe de cardinal $p\geq 2$ premier est cyclique (donc commutatif et isomorphe à $\mathbb{Z}_p$).
5. Montrer qu'un groupe commutatif d'ordre pq, où p et q sont deux nombres premiers distincts, est cyclique. Il est donc commutatif et isomorphe à $\mathbb{Z}_{pq}$.
6. Montrer que si $n\geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique.
7. Montrer que si $n\geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe d'ordre n est cyclique.
8. Montrer que si $n\geq 2$ est un entier non premier avec $\varphi(n)$, il existe alors un groupe non cyclique d'ordre n.
   On a donc montré qu'un entier $n\geq 2$ est premier avec $\varphi(n)$ si, et seulement si, tout groupe d'ordre n est cyclique.
9. Soit G un groupe commutatif d'ordre $n\geq 2$.
   (a) Soit H un sous-groupe de G. Montrer que tout caractère $\varphi: H\to\mathbb{C}^*$ peut se prolonger en un caractère sur G.
   (b) Montrer qu'il existe une unique suite d'entiers $(n_k)_{1\leq k\leq r}$ telle que $n_1\geq 2$, n_2 est multiple de n_1, ..., n_k est multiple de n_{k-1} et G est isomorphe au groupe produit $\Gamma=\prod_{k=1}^{r}\Gamma_{n_k}$.
10. Soit G un groupe commutatif d'ordre $n\geq 2$.
    (a) Soient H un sous-groupe de G distinct de G, $\varphi: H\to\mathbb{C}^*$ un caractère et g un élément de $G\setminus H$.
       i. Justifier la définition de l'entier :
       $$r=\min\left\{k\in\mathbb{N}^*\mid g^k\in H\right\}$$
       ainsi que l'existence d'un nombre complexe $\alpha\in\mathbb{C}^*$ tel que $\varphi(g^r)=\alpha^r$.
       ii. Montrer que le caractère $\varphi: H\to\mathbb{C}^*$ peut se prolonger en un caractère sur le groupe $\langle g,H\rangle$ engendré par g et H.
       iii. Déduire de ce qui précède que le caractère $\varphi: H\to\mathbb{C}^*$ peut se prolonger en un caractère sur G.
    (b) On se donne un élément g_0 de G d'ordre égal à l'exposant de G, soit :
    $$m=\theta(g_0)=\max_{g\in G}\theta(g)=\text{ppcm}\{\theta(g)\mid g\in G\}$$
    En supposant que $m\leq n-1$, on note $K=\langle g_0\rangle$ le sous groupe cyclique de G engendré par g_0.
       i. Montrer qu'il existe un unique caractère $\varphi_0: K\to\mathbb{C}^*$ tel que $\varphi_0(g_0)=\omega=e^{\frac{2i\pi}{m}}$.
       ii. En prolongeant le caractère φ_0 en un caractère φ de G, montrer que l'application :
       $$\begin{array}{rccc}\theta: & \langle g_0\rangle\times\ker(\varphi) & \to & G\\ & \left(g_0^k,h\right) & \mapsto & g_0^k h\end{array}$$
       est un isomorphisme de groupes.

(c) Déduire de ce qui précède, qu'il existe une suite d'entiers $(n_k)_{1\leq k\leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de n_1, ..., n_k est multiple de n_{k-1} et G est isomorphe au groupe produit $\Gamma = \prod_{k=1}^{r} \Gamma_{n_k}$.

(d) Soient $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ deux suites d'entiers telles que $r \geq 2$, $s \geq 2$, $n_1 \geq 2$, $m_1 \geq 2$, n_{k-1} divise n_k et m_{j-1} divise m_j pour k compris entre 2 et r et j compris entre 2 et s. Montrer que ces suites sont identiques si, et seulement si, on a :

$$\forall m \in \mathbb{N}^*,\ \prod_{k=1}^{r} \operatorname{pgcd}(m, n_k) = \prod_{j=1}^{s} \operatorname{pgcd}(m, m_j)$$

(e) En utilisant le résultat précédent, montrer qu'il existe une unique suite d'entiers $(n_k)_{1\leq k\leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de n_1, ..., n_k est multiple de n_{k-1} et G est isomorphe au groupe produit $\Gamma = \prod_{k=1}^{r} \Gamma_{n_k}$ (théorème de Kronecker).
La suite $(n_k)_{1\leq k\leq r}$ est la suite des invariants de G et elle caractérise G à isomorphisme près.

2 Solution

– I – Généralités sur $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

1. On vérifie tout d'abord qu'on définit deux opérations internes sur $\mathbb{Z}_n$ avec :

$$\forall (x, y) \in \mathbb{Z}_n^2,\ \begin{cases} x + y = \overline{a + b} \\ xy = \overline{ab} \end{cases}$$

où $a \in \mathbb{Z}$ est un représentant de x et $b \in \mathbb{Z}$ est un représentant de y.
En effet, si a' est un autre représentant de x et b' un autre représentant de y, on a alors $a \equiv a'$ et $b \equiv b'$ modulo n, ce qui entraîne $a + b \equiv a' + b'$ et $ab \equiv a'b'$ modulo n, soit $\overline{a + b} = \overline{a' + b'}$ et $\overline{ab} = \overline{a'b'}$, ce qui prouve que ces définitions de $x + y$ et xy ne dépendent pas des choix des représentants de x et y.
On vérifie ensuite facilement que ces deux lois confèrent à $\mathbb{Z}_n$ une structure d'anneau commutatif unitaire et que π_n est bien un morphisme d'anneaux.
Réciproquement s'il existe une structure d'anneau commutatif unitaire sur $\mathbb{Z}_n$ qui fait de π_n un morphisme d'anneaux, on a alors pour tous $x = \pi_n(a), y = \pi_n(b)$ dans $\mathbb{Z}_n$:

$$\begin{cases} x + y = \pi_n(a) + \pi_n(b) = \pi_n(a + b) = \overline{a + b} \\ xy = \pi_n(a)\,\pi_n(b) = \pi_n(ab) = \overline{ab} \end{cases}$$

ce qui prouve l'unicité.

2. Ce résultat est en fait valable pour tout anneau $\mathbb{A}$ commutatif unitaire qui est fini avec au moins deux éléments (on suppose que $0 \neq 1$).
Pour $a \in \mathbb{A} \setminus \{0\}$, l'application $\mu_a : x \mapsto ax$ est un morphisme du groupe additif $(\mathbb{A}, +)$ et on a deux possibilités.
   – Soit μ_a est surjectif et dans ce cas le neutre 1 pour le produit a un antécédent a', donc $aa' = 1$ et a est inversible dans $\mathbb{A}$.
   – Soit μ_a est non surjectif et dans ce cas il est non injectif puisque $\mathbb{A}$ est fini, donc $\ker(\mu_a) \neq \{0\}$ et il existe $b \in \mathbb{A} \setminus \{0\}$ tel que $ab = 0$, ce qui signifie que a est un diviseur de 0.

3. On rappelle que si $\mathbb{A}$ est un anneau commutatif unitaire, l'ensemble :

$$\mathrm{Nil}\,(\mathbb{A}) = \{a \in \mathbb{A} \mid \exists q \in \mathbb{N}^* \ ; \ a^q = 0\}$$

est un idéal de $\mathbb{A}$. Les éléments de $\mathrm{Nil}\,(\mathbb{A})$ sont dits nilpotents et $\mathrm{Nil}\,(\mathbb{A})$ est le nilradical de $\mathbb{A}$.
Soient $n = \prod_{k=0}^{r} p_k^{\alpha_k}$ la décomposition de $n \geq 2$ en facteurs premiers et $m = \prod_{k=0}^{r} p_k$.
Pour $q = \max_{1\leq k\leq r} \alpha_k$, l'entier m^q est divisible par n, donc $\overline{m}^q = \overline{0}$ et $\overline{m}$ est nilpotent. On a donc $(\overline{m}) \subset \mathrm{Nil}\,(\mathbb{Z}_n)$.
Réciproquement si $\overline{a}$ est nilpotent, il existe alors un entier $q \in \mathbb{N}^*$ tel que $\overline{a}^q = \overline{0}$, ce qui signifie que a^q est divisible par n, donc par tous les p_k et a est divisible par tous les p_k, donc par le produit $m = \prod_{k=0}^{r} p_k$ (les p_k sont premiers deux à deux distincts). Il en résulte que $\overline{a} \in (\overline{m})$.
En définitive, $\mathrm{Nil}\left(\dfrac{\mathbb{Z}}{\prod_{k=0}^{r} p_k^{\alpha_k}\mathbb{Z}}\right) = \left(\overline{\prod_{k=0}^{r} p_k}\right)$. Cet idéal étant réduit à $\left\{\overline{0}\right\}$ si, et seulement si, tous les α_k sont égaux à 1.

4. Soit H un sous-groupe de $\mathbb{Z}_n$. Le théorème de Lagrange nous dit que son ordre d est un diviseur de n.
On note $q = \dfrac{n}{d}$.
Pour tout $\overline{a}$ dans H, on a $d\overline{a} = \overline{0}$, soit $da = kn$, ou encore $a = kq$, c'est-à-dire que $\overline{a} = k\overline{q}$ est dans le sous-groupe $\langle\overline{q}\rangle$ de $\mathbb{Z}_n$ engendré par $\overline{q}$.
On a donc $H \subset \langle\overline{q}\rangle$ et $\mathrm{card}\,(\langle\overline{q}\rangle) \geq d$.
Mais $d\overline{q} = \overline{n} = \overline{0}$ nous dit que $\overline{q}$ est d'ordre au plus égal à d. En définitive, $\langle\overline{q}\rangle$ est de cardinal d, donc égal à H.
Un sous-groupe d'ordre d de $\mathbb{Z}_n$, s'il existe, est donc unique.
Réciproquement, soit d un diviseur de n, $q = \dfrac{n}{d}$ et $H = \langle\overline{q}\rangle$ le sous-groupe de $\mathbb{Z}_n$ engendré par $\overline{q}$.
Si δ est l'ordre de H, on a $\delta\overline{q} = \overline{0}$, soit $\delta q = kn = kqd$ et $\delta = kd \geq d$. Mais on a aussi $d\overline{q} = \overline{0}$, ce qui entraîne $\delta \leq d$ et donc $\delta = d$.
Il existe donc un unique sous-groupe d'ordre d de $\mathbb{Z}_n$, c'est $\langle\overline{q}\rangle$.

5. Si I est un idéal de $\mathbb{Z}_n$, c'est en particulier un sous-groupe additif.
Réciproquement si I est un sous-groupe additif de $\mathbb{Z}_n$, pour $\left(\overline{a}, \overline{b}\right) \in I \times \mathbb{Z}_n$, on a :

$$\overline{a} \cdot \overline{b} = \pm\overline{|b|\,a} = \pm\,|b|\,\overline{a} = \pm\,(\overline{a} + \cdots + \overline{a}) \in I$$

et I est un idéal de $\mathbb{Z}_n$.

6. Les idéaux de $\mathbb{Z}_n$ sont ses sous-groupes, donc les $(\overline{q})$ où $q \in \{1, \cdots, n\}$ est un diviseur de n.
On peut vérifier que $\dfrac{\mathbb{Z}_n}{(\overline{q})} = \dfrac{\frac{\mathbb{Z}}{n\mathbb{Z}}}{q\frac{\mathbb{Z}}{n\mathbb{Z}}} \backsimeq \dfrac{\mathbb{Z}}{q\mathbb{Z}}$.

7. Pour $n \geq 2$, dans $\mathbb{Z}_n$ qui est fini, il y a équivalence entre idéal premier et maximal.
Pour $n \geq 2$, les idéaux de $\mathbb{Z}_n$ sont de la forme $I = (\overline{q})$ où $q = 0$ ou $q \neq 0$ est un diviseur de n.
Pour n premier, $\mathbb{Z}_n$ est un corps et ses seuls idéaux sont $\mathbb{Z}_n$ et $\left\{\overline{0}\right\}$, seul $\left\{\overline{0}\right\}$ est maximal.
Pour $n \geq 2$ non premier, on a deux possibilités, soit $I = (\overline{p})$ où $2 \leq p \leq n-1$ est un diviseur premier de n et dans ce cas I est maximal (on a $I \neq \mathbb{Z}_n$ puisque $\overline{p}$ qui divise $\overline{0}$ n'est pas inversible et si $(\overline{p}) \subset J = (\overline{q})$ avec q qui divise n, on a alors $\overline{p} = \overline{aq}$, soit $p = aq + kn = aq + kjq$ et q divise p, donc $q = 1$ ou $q = p$, soit $J = \mathbb{Z}_n$ ou $J = I$), soit $I = (\overline{q})$ où q est un diviseur non premier de n et I n'est pas maximal (pour $q = 1$, on a $I = \mathbb{Z}_n$ et pour $q \geq 2$, on a $q = ab$ avec

$2 \leq a, b \leq q-1$ et $I = \left(\overline{ab}\right) \subsetneqq (\overline{a}) \subsetneqq \mathbb{Z}_n$).
En définitive, les idéaux maximaux de $\mathbb{Z}_n$ sont les $(\overline{q})$ où q est un diviseur premier de n.

– II – Morphismes de groupes, d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$. Le groupe $\mathrm{Aut}(\mathbb{Z}_n)$

1. Pour $n = m = 0$, l'anneau $\mathbb{Z}_0$ est isomorphe à $\mathbb{Z}$ et il s'agit d'étudier les morphismes de groupes et d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}$.
   Un morphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{Z}$ est en particulier un morphisme de groupes, donc on a $\varphi(0) = 0$ et $\varphi(-k) = -\varphi(k)$ pour tout $k \in \mathbb{Z}$.
   En notant $a = \varphi(1)$, on vérifie facilement par récurrence que $\varphi(k) = ka$ pour tout entier naturel k et en conséquence $\varphi(k) = ka$ pour tout entier relatif k.
   Réciproquement, pour entier relatif a, l'application $\varphi : k \mapsto ka$ est un morphisme de groupes et c'est un morphisme d'anneaux si, et seulement si, $a = \varphi(1) = 1$. Donc :
   $$\mathrm{Hom}_{gr}(\mathbb{Z}, \mathbb{Z}) \backsimeq \mathbb{Z} \text{ et } \mathrm{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}) = \{Id\}$$

2. Soient $n \in \mathbb{N}^*$, $\varphi : \mathbb{Z}_n \to \mathbb{Z}$ un morphisme de groupes et $a = \varphi\left(\overline{1}\right) \in \mathbb{Z}$. De :
   $$0 = \varphi\left(\overline{0}\right) = \varphi(\overline{n}) = \varphi\left(n\overline{1}\right) = na$$
   on déduit que $a = 0$. On a donc, pour $n \in \mathbb{N}^*$:
   $$\mathrm{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}) = \{0\} \text{ et } \mathrm{Hom}_{Ann}(\mathbb{Z}_n, \mathbb{Z}) = \emptyset$$

3. Soient $m \in \mathbb{N}^*$, $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ un morphisme de groupes et $\widehat{a} = \varphi(1) \in \mathbb{Z}_m$ avec $a \in \{0, 1, \cdots, m-1\}$. Pour tout $k \in \mathbb{Z}$, on a :
   $$\varphi(k) = k\varphi(1) = k\widehat{a} = \widehat{ka}$$
   Réciproquement une telle application est un morphisme de groupes et c'est un morphisme d'anneaux si, et seulement si, $a = 1$, ce qui signifie que φ est la surjection canonique $\pi_m : k \mapsto \widehat{k}$. Donc :
   $$\mathrm{Hom}_{gr}(\mathbb{Z}, \mathbb{Z}_m) \backsimeq \mathbb{Z}_m \text{ et } \mathrm{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}_m) = \{\pi_m\}$$

4. Soient $n \in \mathbb{N}^*$, $m \in \mathbb{N}^*$, $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ un morphisme de groupes et $\widehat{a} = \varphi\left(\overline{1}\right) \in \mathbb{Z}_m$ avec $a \in \{1, \cdots, m\}$. De :
   $$\widehat{0} = \varphi\left(\overline{0}\right) = \varphi(\overline{n}) = \varphi\left(n\overline{1}\right) = n\widehat{a} = \widehat{na}$$
   on déduit que m divise na et comme il est premier avec n, il divise a, ce qui signifie que $a = m$. On a donc :
   $$\mathrm{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}_m) = \left\{\widehat{0}\right\} \text{ et } \mathrm{Hom}_{Ann}(\mathbb{Z}_n, \mathbb{Z}_m) = \emptyset$$

5. On suppose que $\delta = n \wedge m \geq 2$ et on se donne un morphisme de groupes $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$. En notant $\widehat{a} = \varphi\left(\overline{1}\right) \in \mathbb{Z}_m$ avec $a \in \{1, \cdots, m\}$, on a :
   $$\widehat{0} = \varphi\left(\overline{0}\right) = \varphi(\overline{n}) = \varphi\left(n\overline{1}\right) = n\widehat{a}$$
   dans $\mathbb{Z}_m$, donc $\theta(\widehat{a})$ divise n et comme $\theta(\widehat{a})$ divise aussi m (théorème de Lagrange), il divise $\delta = n \wedge m$, donc $\widehat{a}$ est dans le groupe cyclique $H = \left\langle \dfrac{\widehat{m}}{\delta} \right\rangle$ des éléments de $\mathbb{Z}_m$ d'ordre divisant δ.
   Réciproquement, pour tout $\widehat{a} \in \left\langle \dfrac{\widehat{m}}{\delta} \right\rangle$, l'application $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ définie par $\varphi\left(\overline{k}\right) = k\widehat{a}$ est bien définie (si $j \equiv k \bmod(n)$, on a alors $j = k + pn = k + p'\delta$ et $p'\delta\widehat{a} = \widehat{0}$ puisque $\widehat{a}$ est d'ordre

divisant δ, donc $k\widehat{a} = j\widehat{a}$) et c'est un morphisme de groupes.
On a donc :

$$\mathrm{Hom}_{gr}\left(\mathbb{Z}_n, \mathbb{Z}_m\right) \backsimeq \mathbb{Z}_\delta = \mathbb{Z}_{n \wedge m}$$

Si φ est un morphisme d'anneaux, on a alors $\widehat{a} = \varphi\left(\overline{1}\right) = \widehat{1}$ qui est d'ordre m divisant $\delta = n \wedge m$, ce qui revient à dire que $\delta = m$ ou encore que m divise n et dans ce cas $\varphi\left(\overline{k}\right) = k\widehat{1} = \widehat{k} = \pi_m\left(k\right)$.
Il y a donc un seul morphisme d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$.
On a donc :

$$\mathrm{Hom}_{Ann}\left(\mathbb{Z}_n, \mathbb{Z}_m\right) = \begin{cases} \left\{\overline{k} \mapsto \widehat{k}\right\} \text{ si } m \text{ divise } n \\ \emptyset \text{ si } m \text{ ne divise pas } n \end{cases}$$

6. Pour y, z dans $\mathbb{Z}_n$, on a :

$$\sigma\left(x\right)\left(y+z\right) = x\left(y+z\right) = xy + xz = \sigma\left(x\right)\left(y\right) + \sigma\left(x\right)\left(z\right)$$

c'est-à-dire que $\sigma\left(x\right)$ est un morphisme de groupes additifs.
Si $y \in \ker\left(\sigma\left(x\right)\right)$, alors $xy = \overline{0}$ et $y = x^{-1}xy = \overline{0}$, c'est-à-dire que $\sigma\left(x\right)$ est injectif et donc bijectif puisque $\mathbb{Z}_n$ est fini. On a donc bien $\sigma\left(x\right) \in \mathrm{Aut}\left(\mathbb{Z}_n\right)$.
Pour x, x' dans $\mathbb{Z}_n^\times$ et y dans $\mathbb{Z}_n$, on a :

$$\sigma\left(xx'\right)\left(y\right) = x\left(x'y\right) = \left(\sigma\left(x\right) \circ \sigma\left(x'\right)\right)\left(y\right)$$

On a donc $\sigma\left(xx'\right) = \sigma\left(x\right) \circ \sigma\left(x'\right)$ et σ est un morphisme de groupes.
Si $\sigma\left(x\right) = I_d$, on a $\sigma\left(x\right)\left(\overline{1}\right) = \overline{1}$, soit $x = x\overline{1} = \overline{1}$, donc σ est injective.
Si $u \in \mathrm{Aut}\left(\mathbb{Z}_n\right)$ et $\overline{k} = u\left(\overline{1}\right)$, alors pour tout $\overline{j} \in \mathbb{Z}_n$, on a :

$$u\left(\overline{j}\right) = u\left(j\overline{1}\right) = ju\left(\overline{1}\right) = j\overline{k} = \overline{jk} = \sigma\left(\overline{k}\right)\overline{j}$$

L'application σ est donc surjective. En définitive σ réalise un isomorphisme de groupes de $\left(\mathbb{Z}_n^\times, \cdot\right)$ sur $\left(\mathrm{Aut}\left(\mathbb{Z}_n\right), \circ\right)$.
On en déduit que :

$$\mathrm{card}\left(\mathrm{Aut}\left(\mathbb{Z}_n\right)\right) = \mathrm{card}\left(\mathbb{Z}_n^\times\right) = \varphi\left(n\right)$$

Comme $\mathrm{Hom}_{Ann}\left(\mathbb{Z}_n, \mathbb{Z}_n\right) = \left\{Id\right\}$, on a un seul automorphisme d'anneaux.

7. Pour $n = 0$, l'anneau $\mathbb{Z}_0 = \mathbb{Z}$ est principal et pour $n = 1$, on a $\mathbb{Z}_1 = \left\{\overline{0}\right\}$.
On peut remarquer que les idéaux de l'anneau $\mathbb{Z}_n$ sont ses sous-groupes additifs.
Si I est un idéal de $\mathbb{Z}_n$, c'est en particulier un sous-groupe additif.
Réciproquement si I est un sous-groupe additif de $\mathbb{Z}_n$, pour $\left(\overline{a}, \overline{b}\right) \in I \times \mathbb{Z}_n$, on a :

$$\overline{a} \cdot \overline{b} = \pm\overline{|b|\,a} = \pm\,|b|\,\overline{a} = \pm\left(\overline{a} + \cdots + \overline{a}\right) \in I$$

et I est un idéal de $\mathbb{Z}_n$.
Si I est un idéal de $\mathbb{Z}_n$, c'est en particulier un sous-groupe additif, donc il est cyclique, soit $I = \langle\overline{q}\rangle$, ce qui signifie qu'il est principal.
L'anneau $\mathbb{Z}_n$ est principal si, et seulement si, il est intègre, ce qui revient à dire que n est premier.
Comme q divise n, il y a un unique morphisme d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_q$, c'est :

$$\varphi : \overline{k} \in \mathbb{Z}_n \mapsto \widehat{k} \in \mathbb{Z}_q$$

Ce morphisme est surjectif de noyau :

$$\ker\left(\varphi\right) = \left\{\overline{k} \in \mathbb{Z}_n \mid q \text{ divise } k\right\} = \left\{\overline{jq} = j\overline{q} \mid j \in \mathbb{Z}\right\} = \left(\overline{q}\right)$$

donc $\dfrac{\mathbb{Z}_n}{\left(\overline{q}\right)}$ est isomorphe à $\mathbb{Z}_q$.

– III – Le groupe multiplicatif $\mathbb{Z}_n^\times$, fonction indicatrice d'Euler

1. Dire que $\overline{a}$ est inversible dans $\mathbb{Z}_n$ équivaut à dire qu'il existe $\overline{b}$ dans $\mathbb{Z}_n$ tel que $\overline{a}\overline{b} = \overline{1}$, encore équivalent à dire qu'il existe b, q dans $\mathbb{Z}$ tels que $ab + qn = 1$, ce qui équivaut à dire que a et n sont premiers entre eux (théorème de Bézout).
   En traduisant le fait que $\overline{a}$ est inversible dans $\mathbb{Z}_n$ par l'existence d'un entier relatif b tel que $\overline{a}\overline{b} = b\overline{a} = \overline{1}$, on déduit que cela équivaut à dire que $\overline{1}$ est dans le groupe engendré par $\overline{a}$ et donc que ce groupe est $\mathbb{Z}_n$.
2. Si a est premier avec n, alors $\overline{a}$ appartient à $\mathbb{Z}_n^\times$ qui est un groupe d'ordre $\varphi(n)$ et en conséquence son ordre divise $\varphi(n)$ (théorème de Lagrange), ce qui entraîne $\overline{a}^{\varphi(n)} = \overline{1}$, ou encore $a^{\varphi(n)} \equiv 1\ (n)$.
3. $\varphi(p) = p - 1$.
4. Pour $n \geq 3$, on a $\overline{(-1)} \neq \overline{1}$ et $\overline{(-1)}^2 = \overline{(-1)^2} = \overline{1}$, donc $\overline{(-1)}$ est d'ordre 2 qui va diviser l'ordre du groupe $\mathbb{Z}_n^\times$, soit $\varphi(n)$.
   Pour $n = 2$, on a $\mathbb{Z}_2 = \left\{\overline{0}, \overline{1}\right\}$, $\mathbb{Z}_2^\times = \left\{\overline{1}\right\}$ et $\varphi(2) = 1$.
5. Si p divise a, il divise aussi a^b et le reste cherché est nul.
   On suppose donc que p ne divise pas a.
   Tout d'abord, en vue de diminuer b, on effectue la division euclidienne de b par $p-1$, soit $b = q(p-1) + r$ avec $0 \leq r \leq p-2$ et on a $a^b = (a^{p-1})^q a^r$ avec $a^{p-1} \equiv 1\ (p)$ puisque p ne divise pas a, ce qui donne $a^b \equiv a^r\ (p)$.
   Ensuite, en vue de diminuer a, on effectue la division euclidienne de a par p, soit $a = q'p + s$ avec $1 \leq s \leq p-1$ et on a $a^b \equiv s^r\ (p)$.
   Le reste cherché est donc celui de la division de s^r par p avec $1 \leq s \leq p-1$ et $0 \leq r \leq p-2$.
   Pour $m = 115^{2013}$ et $p = 11$, on a $2013 \equiv 3\ (10)$ et $115 \equiv 5\ (11)$, donc $115^{2013} \equiv 5^3\ (11)$ et avec $5^2 \equiv 3$, $5^3 \equiv 4$ modulo 11, on déduit que $115^{2013} \equiv 4$ modulo 11, ce qui signifie que 4 est le reste dans la division euclidienne de 115^{2013} par 11.Comme 11 est premier le théorème de Fermat nous dit que 5^{10} est congru à 1 modulo 11. On effectue alors la division euclidienne de 2008 par 10, soit $2008 = 200 \times 10 + 8$ et on déduit que 5^{2008} est congru à 5^8 modulo 11. Enfin avec $5^2 \equiv 3$, $5^4 \equiv 9 \equiv -2$, $5^8 \equiv 4$ modulo 11, on déduit que $5^{2008} \equiv 4$ modulo 11, ce qui signifie que 4 est le reste dans la division euclidienne de 5^{2008} par 11.
6.

$(a) \Rightarrow (b)$ Si n est premier, alors un entier k compris entre 1 et n^α n'est pas premier avec n^α si, et seulement si, il est divisible par n, ce qui équivaut à dire qu'il existe un entier q compris entre 1 et $n^{\alpha-1}$ tel que $k = qn$ et cela nous donne $n^{\alpha-1}$ possibilités. Il en résulte que :

$$\varphi(n^\alpha) = n^\alpha - n^{\alpha-1} = (n-1)\, n^{\alpha-1}$$

$(b) \Rightarrow (c)$ Il suffit de prendre $\alpha = 1$.

$(c) \Rightarrow (d)$ Si $\varphi(n) = n - 1$, on a alors $\mathbb{Z}_n^\times = \mathbb{Z}_n \setminus \left\{\overline{0}\right\}$ et $\mathbb{Z}_n$ est un corps.

$(d) \Rightarrow (e)$ Résulte du fait qu'un corps est en particulier un anneau intègre.

$(e) \Rightarrow (a)$ Supposons que $\mathbb{Z}_n$ soit intègre. Si d est un diviseur de n différent de n dans $\mathbb{N}$, il existe alors un entier q compris entre 2 et n tel que $n = qd$ et dans l'anneau intègre $\mathbb{Z}_n$ on a $\overline{q}\overline{d} = \overline{0}$ avec $\overline{d} \neq \overline{0}$, ce qui impose $\overline{q} = \overline{0}$, soit $q = n$ et $d = 1$. L'entier n est donc premier.

$(a) \Rightarrow (f)$ Si n est premier, l'anneau $\mathbb{Z}_n$ est alors un corps et tout élément $\overline{k}$ de $\mathbb{Z}_n^*$ est racine du polynôme $X^{n-1} - \overline{1}$, donc $X^{n-1} - \overline{1} = \prod_{k=1}^{n-1} \left(X - \overline{k}\right)$ dans $\mathbb{Z}_n[X]$ et en évaluant ce polynôme en $\overline{0}$, il vient $-\overline{1} = \prod_{k=1}^{n-1} \left(-\overline{k}\right) = (-1)^{n-1}\, \overline{(n-1)!} = \overline{(n-1)!}$ (pour $n = 2$, on a $(-1)^{n-1} = -\overline{1} = \overline{1}$ et $n \geq 3$ premier est impair, donc $(-1)^{n-1} = \overline{1}$).

$(f) \Rightarrow (a)$ Si $n \geq 2$ est tel que $\overline{(n-1)!} = -\overline{1}$ dans $\mathbb{Z}_n$, alors tout diviseur d de n compris entre 1 et $n-1$ divisant $(n-1)! = -1 + kn$ va diviser -1, ce qui impose $d = 1$ et l'entier n est premier.

$(f) \Leftrightarrow (g)$ Pour $n \geq 2$, on a $(n-1)! = (n-1)(n-2)! \equiv -(n-2)!$ modulo n.

$(f) \Leftrightarrow (h)$ L'implication $(h) \Rightarrow (f)$ est évidente (prendre $k = 1$).
Supposons que $(n-1)! \equiv -1 \ (n)$. Dans ce cas, n est premier.
Si $n = 2$, on a alors, pour $k = 1$ et $k = 2$:

$$(n-k)!(k-1)! = 1 \equiv (-1)^k \pmod 2$$

Pour $n \geq 3$ qui est premier impair, on procède par récurrence finie sur k.
Le résultat est acquis pour $k = 1$ et pour $k = n$ (puisque $(-1)^n = -1$).
En supposant le résultat acquis pour $k \in \{1, \cdots, n-2\}$, on a :

$$(n-(k+1))!k! = \frac{k}{n-k}(n-k)!(k-1)!$$

avec $\overline{n-k} = -\overline{k}$ qui est inversible dans le corps $\mathbb{Z}_n$ puisque $\overline{k} \neq \overline{0}$, ce qui nous donne l'égalité dans $\mathbb{Z}_n$:

$$\overline{(n-(k+1))!k!} = \frac{\overline{k}}{\overline{-k}}\overline{(n-k)!(k-1)!} = -\overline{(-1)^k} = \overline{(-1)^{k+1}}$$

soit $(n-(k+1))!k! \equiv (-1)^{k+1} \pmod n$.

$(a) \Rightarrow (i)$ Si $n \geq 2$ est premier, comme il divise $n! = k!(n-k)!\binom{n}{k}$ et est premier avec $k!(n-k)!$ (sinon il diviserait ce produit et donc l'un des entiers j compris entre 1 et $n-1$, ce qui est impossible), il divise $\binom{n}{k}$ (théorème de Gauss), ce qui revient à dire que $\binom{n}{k} \equiv 0 \pmod n$.

$(i) \Rightarrow (j)$ Supposons que $\binom{n}{k} \equiv 0 \pmod n$ pour tout entier k compris entre 1 et $n-1$.
Pour tout entier k compris entre 1 et $n-1$, on a :

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

(triangle de Pascal), donc $\binom{n-1}{k} \equiv -\binom{n-1}{k-1}$ modulo p et par récurrence finie sur k compris entre 0 et $n-1$, on déduit que $\binom{n-1}{k}$ est congru à $(-1)^k$ modulo n. En effet, pour $k = 0$, on a $\binom{n-1}{0} = 1 \equiv (-1)^0$ modulo n ; pour $k = 1$, on a $\binom{n-1}{1} = n-1 \equiv -1$ modulo n ; puis en supposant le résultat acquis pour $k-1$ compris entre 0 et $n-2$, on a $\binom{n-1}{k} \equiv -\binom{n-1}{k-1} \equiv -(-1)^{n-1} = (-1)^k$ modulo n.

$(j) \Rightarrow (a)$ Supposons que $\binom{n}{k} \equiv 0 \pmod n$ et $\binom{n-1}{k} \equiv (-1)^k \pmod n$ pour tout entier k compris entre 1 et $n-1$.
Pour tout diviseur k de n compris entre 1 et $n-1$, on a :

$$0 \equiv \binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} \equiv \frac{n}{k}(-1)^{k-1} \pmod n$$

(pour $k=1$, on a bien $\binom{n-1}{0}=1\equiv(-1)^0$ modulo n), ce qui impose $k=1$ (sinon n divise $\dfrac{n}{k}\in\{2,\cdots,n-1\}$, ce qui est impossible), donc n est premier.

7. Pour $p=2$, $\mathbb{Z}_2^*=\left\{\overline{1}\right\}$ et $\overline{1}$ est le un seul carré.
Pour $p\geq 3$ premier, on note $C_p=\left\{x^2\mid x\in\mathbb{Z}_p^*\right\}$ l'ensemble des carrés de $\mathbb{Z}_p^*$.

   (a) L'ensemble C_p est l'image du morphisme de groupes :

$$\begin{array}{cccc}\varphi_p & \mathbb{Z}_p^* & \to & \mathbb{Z}_p^* \\ & x & \mapsto & x^2\end{array}$$

   et le noyau de ce morphisme est :

$$\ker(\varphi_p)=\left\{x\in\mathbb{Z}_p^*\mid\left(x-\overline{1}\right)\left(x+\overline{1}\right)=\overline{0}\right\}=\left\{-\overline{1},\overline{1}\right\}$$

   avec $-\overline{1}\neq\overline{1}$ dans le corps $\mathbb{Z}_p$ pour $p\geq 3$ premier, donc $C_p=\mathrm{Im}(\varphi_p)$ est isomorphe à $\dfrac{\mathbb{Z}_p^*}{\left\{-\overline{1},\overline{1}\right\}}$ et :

$$\mathrm{card}(C_p)=\mathrm{card}\left(\frac{\mathbb{Z}_p^*}{\left\{-\overline{1},\overline{1}\right\}}\right)=\frac{p-1}{2}$$

   ce qui signifie qu'il y a exactement $\dfrac{p-1}{2}$ carrés et $\dfrac{p-1}{2}$ non carrés dans $\mathbb{Z}_p^*$.

   (b) Si $y\in C_p$, il existe alors $x\in\mathbb{Z}_p^*$ tel que $y=x^2$ et $y^{\frac{p-1}{2}}=x^{p-1}=\overline{1}$ (Fermat ou Lagrange). Donc C_p est contenu dans l'ensemble des racines du polynôme $P(X)=X^{\frac{p-1}{2}}-\overline{1}$ et comme ce polynôme a au plus $\dfrac{p-1}{2}=\mathrm{card}(C_p)$ éléments, C_p est l'ensemble de ces racines.
   Si $y\in\mathbb{Z}_p^*\setminus C_p$, on a alors $y^{\frac{p-1}{2}}\neq\overline{1}$ et $\left(y^{\frac{p-1}{2}}\right)^2=y^{p-1}=\overline{1}$, donc $y^{\frac{p-1}{2}}=-\overline{1}$. Donc $\mathbb{Z}_p^*\setminus C_p$ est contenu dans l'ensemble des racines du polynôme $Q(X)=X^{\frac{p-1}{2}}+\overline{1}$ et comme ce polynôme a au plus $\dfrac{p-1}{2}=\mathrm{card}\left(\mathbb{Z}_p^*\setminus C_p\right)$ éléments, $\mathbb{Z}_p^*\setminus C_p$ est l'ensemble de ces racines.

   (c) On a :

$$\begin{aligned}\left(-\overline{1}\in C_p\right)&\Leftrightarrow\left(\left(-1\right)^{\frac{p-1}{2}}\overline{1}=\overline{1}\right)\Leftrightarrow\left(\frac{p-1}{2}\equiv 0\pmod 2\right)\\&\Leftrightarrow\left(p\equiv 1\pmod 4\right)\end{aligned}$$

   Si $p\geq 3$ est un nombre premier congru à 1 modulo 4, il s'écrit $p=4q+1$ avec $q\geq 1$ et $m=\dfrac{p-1}{2}$ est un entier pair non nul.
   Tout entier k compris entre $m+1=\dfrac{p+1}{2}$ et $p-1$ s'écrit $k=p-j$ avec $1\leq j\leq m=\dfrac{p-1}{2}$, donc $k\equiv -j \bmod p$ et :

$$\begin{aligned}(p-1)!&=1\cdot 2\cdot\cdots\cdot m\cdot(m+1)\cdots(p-1)\\&\equiv(-1)^m(m!)^2\equiv(m!)^2\bmod p\end{aligned}$$

   puisque m est pair.
   D'autre part, comme p est premier, le théorème de Wilson nous dit que $(p-1)!\equiv -1 \bmod p$, donc $(m!)^2\equiv -1 \bmod(p)$.

8.

(a) Pour $n = p \geq 3$ premier impair, $\mathbb{Z}_n$ est intègre avec $-\overline{1} \neq \overline{1}$ et $-\overline{1}, \overline{1}$ sont les deux seules solutions ($x^2 - \overline{1} = \left(x - \overline{1}\right)\left(x + \overline{1}\right) = \overline{0}$ si, et seulement si, $x = -\overline{1}$ ou $x = \overline{1}$).
Soit $n = p^\alpha$ où $p \geq 3$ est premier et $\alpha \geq 2$.
On a déjà deux solutions distinctes $-\overline{1}$ et $\overline{1}$.
Si $x = \overline{k} \in \mathbb{Z}_{p^\alpha} \setminus \left\{-\overline{1}, \overline{1}\right\}$ est une solution, p^α divise $\left(x - \overline{1}\right)\left(x + \overline{1}\right)$, ce qui équivaut à dire qu'il existe des entiers relatifs non nuls u, v premiers avec p et des entiers naturels r, s tels que $r + s \geq \alpha$ et $k = 1 + up^r = -1 + vp^s$ (on a $(k-1)(k+1) = wp^\beta$ avec $\beta \geq \alpha$ et w non nul premier avec p).
Si $r \geq 1$ et $s \geq 1$, on a alors $2 = vp^s - up^r$ qui est divisible par $p \geq 3$, ce qui est impossible.
On a donc $r = 0$ ou $s = 0$, donc $s \geq \alpha$ ou $r \geq \alpha$, soit $\overline{k} = -\overline{1}$ ou $\overline{k} = \overline{1}$, ce qui est exclu.
En définitive, $-\overline{1}$ et $\overline{1}$ sont les deux seules solutions.

(b) Pour $n = 2$, on a $\mathbb{Z}_2 = \left\{\overline{0}, \overline{1}\right\}$ et $\overline{1}$ est l'unique solution.
Soit $n = 2^\alpha$ où $\alpha \geq 2$.
On a déjà deux solutions distinctes $-\overline{1}$ et $\overline{1}$.
Reprenant les notations et le raisonnement précédent, on a $k = 1 + u2^r = -1 + v2^s$ avec u, v impairs non nuls et $r + s \geq \alpha$, donc $2 = v \cdot 2^s - u \cdot 2^r$.
Si $r = 0$ [resp. $s = 0$], on a alors $s \geq \alpha$ et $u = 2\left(2^{s-1} - 1\right)$ [resp. $r \geq \alpha$ et $v = 2\left(2^{r-1} + 1\right)$] avec u [resp. v] impair, ce qui est impossible.
Donc $r \geq 1$, $s \geq 1$ et $1 = v \cdot 2^{s-1} - u \cdot 2^{r-1}$, ce qui impose $s = 1$ ou $r = 1$ (sinon le théorème de Bézout nous dit que 2^{s-1} et 2^{r-1} sont premiers entre eux, ce qui n'est pas pour $r \geq 2$ et $r \geq 2$), soit $r \geq \alpha - 1$ ou $s \geq \alpha - 1$, donc $r = \alpha - 1$ ou $s = \alpha - 1$ (sinon $\overline{k} = \overline{1}$ ou $\overline{k} = -\overline{1}$, ce qui est exclu), soit $\overline{k} = \overline{1 + u2^{\alpha-1}} = \overline{1 + 2^{\alpha-1}}$ ou $\overline{k} = \overline{-1 + v2^{\alpha-1}} = \overline{-1 + 2^{\alpha-1}}$puisque u et v sont impairs. On vérifie que réciproquement, ces deux éléments sont bien solutions distinctes.
En définitive, on a quatre solutions :

$$-\overline{1},\ \overline{1},\ \overline{1 + 2^{\alpha-1}},\ \overline{-1 + 2^{\alpha-1}}$$

pour $\alpha \geq 3$ et 2 solutions :

$$-\overline{1} = \overline{1 + 2},\ \overline{1} = \overline{-1 + 2}$$

pour $\alpha = 2$.

(c) En dehors des cas déjà traités, l'entier n s'écrit $n = 2^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ avec $p_1 = 2 < p_2 < \cdots < p_r$ premiers, $\alpha_1 \geq 0$, $\alpha_k \geq 1$ pour k compris entre 1 et r.
En notant, pour tout j compris entre 1 et r, $\overline{k}^{(j)}$ la classe de k modulo $p_j^{\alpha_j}$, le théorème chinois nous dit que l'application :

$$\varphi : \overline{k} \in \mathbb{Z}_n \mapsto \left(\overline{k}^{(1)}, \cdots, \overline{k}^{(r)}\right)$$

est un isomorphisme d'anneaux (pour $\alpha_1 = 0$, on se contente de $\overline{k} \in \mathbb{Z}_n \mapsto \left(\overline{k}^{(2)}, \cdots, \overline{k}^{(r)}\right)$)
et l'équation $\overline{k}^2 = \overline{1}$ équivaut à $\left(\overline{k}^{(j)}\right)^2 = \overline{1}^{(j)}$ pour tout j.
Le nombre de solutions est donc :

$$\begin{cases} 2^{r-1} \text{ pour } \alpha_1 = 0 \text{ ou } 1 \\ 2^r \text{ pour } \alpha_1 = 2 \\ 2^{r+1} \text{ pour } \alpha_1 \geq 3 \end{cases}$$

9. Pour tout entier $n \geq 2$, on note $\mathcal{D}_n$ l'ensemble des diviseurs positifs de n et pour tout $d \in \mathcal{D}_n$, on note :

$$S_d = \left\{k \in \{1, \cdots, n\} \mid k \wedge n = \frac{n}{d}\right\}$$

Pour $d = n$, S_n est l'ensemble des entiers k compris entre 1 et n premier avec n.
On vérifie que les S_d, pour d décrivant $\mathcal{D}_n$, forment une partition de $\{1, \cdots, n\}$ et pour tout $d \in \mathcal{D}_n$ on a $\text{card}\,(S_d) = \varphi(d)$.
En effet, il est clair que $S_d \cap S_{d'} = \emptyset$ pour $d \neq d'$ dans $\mathcal{D}_n$.
Si k est un entier compris entre 1 et n, en notant δ le pgcd de k et n, $k = \delta k'$ et $n = \delta d$ avec k' et d premiers entre eux, on a $k \wedge n = \delta = \dfrac{n}{d}$ et $k \in S_d$ avec $d \in \mathcal{D}_n$.
On a donc la partition :

$$\{1, \cdots, n\} = \bigcup_{d \in \mathcal{D}_n} S_d$$

Un entier k compris entre 1 et n est dans S_d si et seulement si il s'écrit $k = \dfrac{n}{d}k'$ avec k' compris entre 1 et d qui est premier avec d.
On a donc :

$$\text{card}\,(S_d) = \text{card}\,\{k' \in \{1, \cdots, d\} \mid k' \wedge d = 1\} = \varphi(d)$$

et la formule de Möbius s'en déduit.

– IV – Le théorème chinois

1. Pour tout entier relatif k, on note $\overline{k}$ sa classe modulo n et, pour tout indice j compris entre 1 et r, $\pi_j(k)$ sa classe modulo n_j.
Le produit cartésien $\prod_{j=1}^{r} \mathbb{Z}_{n_j}$ est naturellement muni d'une structure d'anneau commutatif unitaire avec les lois $+$ et $\cdot$ définies par :

$$\begin{cases} (\pi_1(j), \cdots, \pi_r(j)) + (\pi_1(k), \cdots, \pi_r(k)) = (\pi_1(j+k), \cdots, \pi_r(j+k)) \\ (\pi_1(j), \cdots, \pi_r(j)) \cdot (\pi_1(k), \cdots, \pi_r(k)) = (\pi_1(j \cdot k), \cdots, \pi_r(j \cdot k)) \end{cases}$$

   (a) Supposons les entiers $n_1, \cdots, n_r$ deux à deux premiers entre eux.
   L'application :

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \prod_{j=1}^{r} \mathbb{Z}_{n_j} \\ & k & \mapsto & (\pi_1(k), \cdots, \pi_r(k)) \end{array}$$

   est un morphisme d'anneaux et son noyau est formé des entiers multiples de tous les n_j, donc de leur ppcm $n = \prod_{j=1}^{r} n_j$ puisque ces entiers sont deux à deux premiers entre eux, il se factorise donc en un morphisme d'anneaux injectif :

$$\begin{array}{rccc} \psi: & \mathbb{Z}_n & \to & \prod_{j=1}^{r} \mathbb{Z}_{n_j} \\ & \overline{k} & \mapsto & (\pi_1(k), \cdots, \pi_r(k)) \end{array}$$

   Ces deux anneaux ayant même cardinal n, l'application ψ réalise en fait un isomorphisme d'anneaux de $\mathbb{Z}_n$ sur $\prod_{j=1}^{r} \mathbb{Z}_{n_j}$.
   Si les entiers $n_1, \cdots, n_r$ ne sont pas deux à deux premiers entre eux les groupes additifs $\mathbb{Z}_n$ et $\prod_{j=1}^{r} \mathbb{Z}_{n_j}$ ne peuvent être isomorphes puisque $\overline{1}$ est d'ordre n dans $\mathbb{Z}_n$ et tous les éléments de $\prod_{j=1}^{r} \mathbb{Z}_{n_j}$ ont un ordre qui divise le ppcm de $n_1, \cdots, n_r$ qui est strictement inférieur à n.

(b) On désigne par $(m_j)_{1\leq j\leq r}$ la suite d'entiers définie par :

$$m_j = \frac{n}{n_j} = \prod_{\substack{i=1\\ i\neq j}}^{r} n_i \ (1 \leq j \leq r)$$

Ces entiers sont premiers entre eux dans leur ensemble (sinon, il existe un nombre premier p qui divise tous les m_j, divisant $m_1 = \prod_{i=2}^{r} n_i$, il divise un n_i pour $2 \leq i \leq r$, mais divisant m_i, il divise un n_k pour $1 \leq k \neq i \leq r$, ce qui contredit le fait que n_i et n_k sont premiers entre eux) et le théorème de Bézout nous dit qu'il existe une suite $(u_j)_{1\leq j\leq r}$ d'entiers relatifs telle que $\sum_{j=1}^{r} u_j m_j = 1$.
Pour tout j compris entre 1 et r, on a :

$$\pi_j(1) = \pi_j\left(\sum_{i=1}^{r} u_i m_i\right) = \pi_j(u_j)\,\pi_j(m_j)$$

($\pi_j(m_j)$ est inversible dans $\mathbb{Z}_{n_j}$ d'inverse $\pi_j(u_j)$) et posant :

$$k = \sum_{i=1}^{r} a_i u_i m_i$$

on a $\pi_j(k) = \pi_j(a_j)\,\pi_j(u_j)\,\pi_j(m_j) = \pi_j(a_j)$, donc :

$$\psi\left(\overline{k}\right) = (\pi_1(k), \cdots, \pi_r(k)) = (\pi_1(a_1), \cdots, \pi_r(a_r))$$

L'inverse de ψ est donc défini par :

$$\psi^{-1}(\pi_1(a_1), \cdots, \pi_r(a_r)) = \overline{\sum_{i=1}^{r} a_i u_i m_i}$$

2.

(a) Dans le cas où les entiers $n_1, \cdots, n_r$ sont deux à deux premiers entre eux, cela revient à trouver l'antécédent dans $\mathbb{Z}_n$ de $(\pi_1(a_1), \cdots, \pi_r(a_r))$ par l'isomorphisme φ.
Cet antécédent est $\overline{k_0}$, où $k_0 = \sum_{i=1}^{r} a_i u_i m_i$, en désignant par $(u_j)_{1\leq j\leq r}$ une suite d'entiers relatifs telle que $\sum_{j=1}^{r} u_j \frac{n}{n_j} = 1$.
On a donc ainsi une solution particulière et les autres solutions sont les entiers $k = k_0 + q\cdot n$, où q est un entier relatif.

(b) Dans le cas où les entiers $n_1, \cdots, n_r$ ne sont pas deux à deux premiers entre eux, c'est un plus délicat.
Considérons tout d'abord le cas de deux équations :

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

avec $\delta = n_1 \wedge n_2 \geq 2$.
On a $n_1 = \delta n_1'$, $n_2 = \delta n_2'$ avec $n_1' \wedge n_2' = 1$ et il existe $(u_1, u_2) \in \mathbb{Z}^2$ tel que $u_1 n_1' + u_2 n_2' = 1$.

Montrons que ce système a des solutions si, et seulement si, $a_2 - a_1$ est multiple de δ.
Si $k \in \mathbb{Z}$ est une solution, δ qui divise n_1 et n_2 va alors diviser $k - a_1$ et $k - a_2$ et aussi la différence $a_2 - a_1$.
Réciproquement, supposons $a_2 - a_1$ multiple de δ, soit $a_2 - a_1 = q\delta$.
En posant :

$$k_0 = a_2 u_1 n_1' + a_1 u_2 n_2'$$

on a :

$$\begin{aligned} k_0 &= a_2 \left(1 - u_2 n_2'\right) + a_1 u_2 n_2' \\ &= a_2 + \left(a_1 - a_2\right) u_2 n_2' = a_2 + q\delta u_2 n_2' \\ &= a_2 + q u_2 n_2 \equiv a_2 \pmod{n_2} \end{aligned}$$

et de manière analogue on voit que $k_0 \equiv a_1 \pmod{n_1}$. L'entier k_0 est donc une solution de notre système.
Si $k \in \mathbb{Z}$ est une autre solution de notre système, cet entier est alors congru à k_0 modulo n_1 et modulo n_2, soit :

$$\begin{aligned} k - k_0 &= q_1 n_1 = q_1 \delta n_1' \\ &= q_2 n_2 = q_2 \delta n_2' \end{aligned}$$

donc :

$$\frac{k - k_0}{\delta} = q_1 n_1' = q_2 n_2'$$

et comme $n_1' \wedge n_2' = 1$, le théorème de Gauss nous dit que n_2' divise q_1, donc :

$$\frac{k - k_0}{\delta} = q_3 n_1' n_2'$$

avec $q_3 \in \mathbb{Z}$, ce qui peut aussi s'écrire :

$$k - k_0 = q_3 \delta n_1' n_2' = q_3 \frac{n_1 n_2}{\delta} = q_3 n_1 \vee n_2$$

Réciproquement on vérifie facilement que pour tout entier relatif q_3, $k_0 + q_3 n_1 \vee n_2$ est solution de notre système.
En définitive, l'ensemble des solutions est :

$$S = \{k_0 + q_3 n_1 \vee n_2 \mid q_3 \in \mathbb{Z}\}$$

où k_0 est une solution particulière.

3. Comme $n_1 = 4$, $n_2 = 5$, $n_3 = 9$ sont deux à deux premiers entre eux, ce système a des solutions données en déterminant des coefficients dans une relation de Bézout $u_1 m_1 + u_2 m_2 + u_3 m_3 = 1$, où $m_1 = n_2 n_3 = 45$, $m_2 = n_1 n_3 = 36$, $m_3 = n_1 n_2 = 20$.
Pour ce faire, on utilise l'associativité du ppcm en écrivant que :

$$\begin{cases} m_2 \wedge m_3 = 4 = (-1) \cdot 36 + 2 \cdot 20 \\ 1 = m_1 \wedge (m_2 \wedge m_3) = 1 \cdot 45 + (-11) \cdot 4 \\ 1 = 1 \cdot 45 + 11 \cdot 36 + (-22) \cdot 20 \end{cases}$$

ce qui donne la solution particulière :

$$k_0 = 2 \cdot 45 + 33 \cdot 36 - 22 \cdot 20 = 838$$

et la solution générale :

$$k = 838 + 180q = 118 + 180q' \ \ (q' \in \mathbb{Z})$$

(on a effectué la division euclidienne de 838 par $n = 180$).

4. On a $\varphi(1_{\mathbb{A}}) = 1_{\mathbb{B}}$ et pour $a \in \mathbb{A}^\times$, de $1_{\mathbb{B}} = \varphi(1_{\mathbb{A}}) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$, on déduit que $\varphi(a) \in \mathbb{B}^\times$.
Donc φ est un morphisme de groupes de $\mathbb{A}^\times$ dans $\mathbb{B}^\times$.
Comme φ est injectif, il en est de même de sa restriction à $\mathbb{A}^\times$.
Pour tout $b = \varphi(a) \in \mathbb{B}^\times$, il existe $c = \varphi(a') \in \mathbb{B}^\times$ tel que $1_{\mathbb{B}} = bc = \varphi(aa') = \varphi(1_{\mathbb{A}})$, donc $aa' = 1_{\mathbb{A}}$ et $a \in \mathbb{A}^\times$.
La restriction de φ à $\mathbb{A}^\times$ est donc surjective sur $\mathbb{B}^\times$ et elle réalise un isomorphisme de $\mathbb{A}^\times$ sur $\mathbb{B}^\times$.

5. En utilisant la décomposition en facteurs premiers $n = \prod_{j=1}^{r} p_j^{\alpha_j}$ d'un entier $n \geq 2$, on a :

$$\mathbb{Z}_n \underset{\to}{\backsim} \prod_{j=1}^{r} \mathbb{Z}_{p_j^{\alpha_j}}$$

et en conséquence :

$$\mathbb{Z}_n^\times \underset{\to}{\backsim} \left(\prod_{j=1}^{r} \mathbb{Z}_{p_j^{\alpha_j}}\right)^\times = \prod_{j=1}^{r} \left(\mathbb{Z}_{p_j^{\alpha_j}}\right)^\times$$

ce qui nous donne :

$$\varphi(n) = \prod_{i=1}^{r} \varphi\left(p_j^{\alpha_j}\right)$$

Le calcul de $\varphi(n)$ est alors ramené à celui de $\varphi(p^\alpha)$ où p est un nombre premier et α un entier naturel non nul.
Si p est premier, alors un entier k compris entre 1 et p^α n'est pas premier avec p^α si et seulement si il est divisible par p, ce qui équivaut à $k = mp$ avec $1 \leq m \leq p^{\alpha-1}$, il y a donc $p^{\alpha-1}$ possibilités.
On en déduit alors que :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)\,p^{\alpha-1}$$

Avec ce résultat on retrouve le fait que, pour tout $n \geq 3$ l'entier $\varphi(n)$ est pair.
En effet, pour $n = 2^\alpha$ avec $\alpha \geq 2$, on a $\varphi(n) = 2^{\alpha-1}$ qui est pair et pour $n = 2^\alpha \prod_{i=1}^{r} p_i^{\alpha_i} = p_1^{\alpha_1} m$ avec $\alpha \geq 0$, $r \geq 1$, tous les p_i étant premiers impairs, on a $\varphi(n) = (p_1 - 1)\,p_i^{\alpha_1 - 1}\varphi(m)$ qui est pair.
On déduit également que $\varphi(n)$ est compris entre 1 et $n-1$ (ce qui se voit aussi avec la définition).
En fait on a le résultat plus précis suivant :

$$\forall n \geq 2,\ \sqrt{n} - 1 < \varphi(n) \leq n - 1$$

(exercice, pas si simple).

6. Si $ab \equiv 1 \pmod{\varphi(n)}$, il existe alors un entier relatif k tel que :

$$ab = 1 + k\varphi(n) = 1 + k\,(p-1)\,(q-1)$$

Si m est un entier relatif premier avec p, on a alors $m^{p-1} \equiv 1 \pmod{p}$ (théorème de Fermat) et :

$$m^{ab} = m m^{k(p-1)(q-1)} \equiv m \pmod{p}$$

Si l'entier relatif m n'est pas premier avec p, c'est nécessairement un multiple de p (qui est premier) et :

$$m^{ab} \equiv 0 \equiv m \pmod{p}$$

De manière analogue, on a $m^{ab} \equiv m \pmod{q}$ et avec p et q premiers entre eux il en résulte que $m^{ab} \equiv m \pmod{pq}$.
Le principe du système R.S.A. est le suivant.
On se donne un ensemble $\{P_1, \cdots, P_n\}$ de $n \geq 2$ personnes qui souhaitent communiquer entre elles de façon codée.
On attribue à chacune de ces personnes P_k un entier $n_k = p_k q_k$ produit de deux nombres premiers et un entier c_k premier avec $\varphi(n_k) = (p_k - 1)(q_k - 1)$.
Les entiers n_k sont choisis très grands (de l'ordre de 10^{100}) de façon à rendre improbable les décompositions en facteurs premiers $n_k = p_k q_k$.
On dispose d'un annuaire public où est associé à chacun des P_k le couple (n_k, c_k).
Comme c_k est premier avec $\varphi(n_k)$, il est inversible modulo $\varphi(n_k)$ et seul P_k qui connaît la factorisation de n_k est capable de calculer l'inverse d_k de c_k.
Un message est une succession d'entiers inférieurs aux n_k.
Si P_1 veut envoyer un message m codé à P_2, il lui envoie le plus petit entier positif m_2 congru à m^{c_2} modulo n_2. Il suffit alors à P_2 de calculer $m_2^{d_2}$ qui est congru à m modulo n_2 (de $c_2 d_2 \equiv 1 \pmod{\varphi(n_2)}$, on déduit que $m_2^{d_2} \equiv m^{c_2 d_2} \equiv m \pmod{n_2}$) pour décoder le message m_2.

– V – $\mathbb{Z}_{p^\alpha}^\times$ est cyclique pour $p \geq 3$ premier et $\alpha \geq 1$

1.

(a) On désigne par m l'ordre de $g = g_1 \cdot \cdots \cdot g_r$ et pour tout k compris entre 1 et r, on note $m_k = \dfrac{n}{n_k}$.
De $g^n = g_1^{n_1 m_1} \cdot \cdots \cdot g_r^{n_r m_r} = 1$, on déduit que l'ordre m de g divise n.
De $g^m = 1$, on déduit, pour tout k compris entre 1 et r, que $g^{m \cdot m_k} = g_k^{m \cdot m_k} = 1$, donc l'ordre n_k de g_k divise $m \cdot m_k$ et comme il est premier avec m_k, il divise m. L'entier m est donc multiple de $\bigvee_{k=1}^{r} n_k = \prod_{k=1}^{r} n_k = n$.
En définitive, $m = n$.

(b)

i. On a $(x^{q_k})^{p_k^{\alpha_k}} = x^{p-1} = \overline{1}$ (Fermat ou Lagrange), donc l'ordre $\theta(x^{q_k})$ de x^{q_k} est un diviseur de $p_k^{\alpha_k}$, soit $\theta(x^{q_k}) = p_k^{r_{x,k}}$ où $0 \leq r_{x,k} \leq \alpha_k$.

ii. En notant, pour k compris entre 1 et r, $r_k = \max_{x \in \mathbb{Z}_p^*} r_{x,k}$, on a $0 \leq r_k \leq \alpha_k$ et pour tout $x \in \mathbb{Z}_p^*$:

$$(x^{q_k})^{p_k^{r_k}} = 1$$

ce qui signifie que les $p-1$ éléments de $\mathbb{Z}_p^*$ sont racines du polynôme :

$$P(X) = X^{m_k} - 1$$

où $m_k = q_k p_k^{r_k} = \dfrac{p-1}{p_k^{\alpha_k - r_k}} \leq p-1$, ce qui impose que $m_k = p-1$, soit $r_k = \alpha_k$. Il existe donc $x_k \in \mathbb{Z}_p^*$ tel que $x_k^{q_k}$ soit d'ordre $p_k^{\alpha_k}$.

iii. Comme les $p_k^{\alpha_k}$ sont deux à deux premiers entres eux, l'élément $x = \prod_{k=1}^{r} x_k^{q_k}$ de $\mathbb{Z}_p^*$ est d'ordre $\prod_{j=1}^{r} p_k^{\alpha_k} = p-1$ et $\mathbb{Z}_p^*$ est cyclique d'ordre $p-1$.

(c)

i. Comme tout élément de $\mathbb{Z}_p^\times$ a un ordre qui divise $p-1$, on a $p-1=\sum_{d\in\mathcal{D}_{p-1}}\psi(d)$.

ii. Dire que $\psi(d)\geq 1$ équivaut à dire qu'il existe dans $\mathbb{Z}_p^\times$ au moins un élément x d'ordre d et le groupe $G=\left\{\overline{1},x,\cdots,x^{d-1}\right\}$ est alors formé de d solutions distinctes de l'équation $X^d-\overline{1}=\overline{0}$, or cette équation a au plus d solutions dans le corps commutatif $\mathbb{Z}_p$, donc G est exactement l'ensemble de toutes les solutions de cette équation.
Les éléments d'ordre d dans $\mathbb{Z}_p^\times$ sont donc les générateurs du groupe cyclique G et il y a $\varphi(d)$ tels générateurs, donc $\psi(d)=\varphi(d)$ si $\psi(d)>0$.

iii. Avec la formule de Möbius, on en déduit que :

$$\sum_{d\in\mathcal{D}_{p-1}}\psi(d)=\sum_{d\in\mathcal{D}_{p-1}}\varphi(d)$$

avec $\psi(d)=0$ ou $\psi(d)=\varphi(d)$, ce qui entraîne que $\psi(d)=\varphi(d)$ pour tout $d\in\mathcal{D}_{p-1}$.

2. Cela résulte des points suivants.

(a) Pour tout entier k compris entre 1 et $p-1$, $\binom{p}{k}$ est divisible par p.
En effet, pour k compris entre 1 et $p-1$, p divise $k!\,(p-k)!\binom{p}{k}=p!$ et tout entier j compris entre 1 et $p-1$ est premier avec p, donc p divise $\binom{p}{k}$ (théorème de Gauss).

(b) Il existe une suite d'entiers naturels non nuls $(\lambda_k)_{k\in\mathbb{N}}$ tous premiers avec p tels que :

$$\forall k\in\mathbb{N},\ (1+p)^{p^k}=1+\lambda_k p^{k+1}$$

On procède par récurrence sur $k\geq 0$.
Pour $k=0$, on prend $\lambda_0=1$.
Pour $k=1$, on a :

$$(1+p)^p=1+p^2+\sum_{k=2}^{p}\binom{p}{k}p^k$$

avec $\binom{p}{k}p^k$ divisible par p^3 pour k compris entre 2 et p si $p\geq 3$, ce qui donne :

$$(1+p)^p=1+p^2+\nu p^3=1+\lambda_1 p^2$$

avec $\lambda_1=1+\nu p$ premier avec p.
En supposant le résultat acquis pour $k\geq 1$, on a :

$$(1+p)^{p^{k+1}}=\left(1+\lambda_k p^{k+1}\right)^p=1+\lambda_k p^{k+2}+\sum_{j=2}^{p}\binom{p}{j}\lambda_k^j p^{j(k+1)}$$

avec $\binom{p}{j}\lambda_k^j p^{j(k+1)}$ divisible par p^{k+3}, pour j compris entre 2 et p, ce qui donne :

$$(1+p)^{p^{k+1}}=1+p^{k+2}\left(\lambda_k+\nu p\right)=1+\lambda_{k+1}p^{k+2}$$

avec $\lambda_{k+1}=\lambda_k+\nu p$ premier avec p si λ_k est premier avec p.

(c) La classe résiduelle modulo p^α, $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}_{p^\alpha}^\times$.
$1+p$ étant premier avec p^α, on a bien $\overline{1+p}\in\mathbb{Z}_{p^\alpha}^\times$ et avec :

$$\begin{cases}(1+p)^{p^{\alpha-1}}=1+\lambda_{\alpha-1}p^\alpha\equiv 1\ (\text{mod}\ p^\alpha)\\ (1+p)^{p^{\alpha-2}}=1+\lambda_{\alpha-2}p^{\alpha-1}\neq 1\ (\text{mod}\ p^\alpha)\end{cases}$$

($\lambda_{\alpha-2}$ est premier avec p, donc $\lambda_{\alpha-2}p^{\alpha-1}$ ne peut être divisible par p^α) on déduit que $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}_{p^\alpha}^\times$.

(d) Si $x = k + p\mathbb{Z}$ un générateur du groupe cyclique $\mathbb{Z}_p^\times$, alors $y = k^{p^{\alpha-1}} + p^\alpha\mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_{p^\alpha}^\times$.
La classe modulo p, $x = k + p\mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_p^\times$ et du fait que $p^{\alpha-1} - 1$ est divisible par $p-1$ pour $\alpha \geq 2$, on déduit que $k^{p^{\alpha-1}-1} \equiv 1 \pmod{p}$ et $k^{p^{\alpha-1}} \equiv k \pmod{p}$, ce qui entraîne que la classe modulo p de $j = k^{p^{\alpha-1}}$ est d'ordre $p-1$ dans $\mathbb{Z}_p^\times$. D'autre part avec :

$$j^{p-1} = k^{(p-1)p^{\alpha-1}} = k^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$$

on déduit que $y = j + p^\alpha\mathbb{Z} = k^{p^{\alpha-1}} + p^\alpha\mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_{p^\alpha}^\times$ (si $j^r \equiv 1 \pmod{p^\alpha}$ avec $r \geq 1$, alors p^α et donc p divise $j^r - 1$ ce qui entraîne $j^r \equiv 1 \pmod{p}$ et r est multiple de $p-1$).

(e) On en déduit que $\mathbb{Z}_{p^\alpha}^\times$ est cyclique.
Dans $\mathbb{Z}_{p^\alpha}^\times$ on a $x = \overline{1+p}$ d'ordre $p^{\alpha-1}$ et un élément y d'ordre $p-1$ avec $p-1$ et $p^{\alpha-1}$ premiers entre eux, il en résulte que $z = xy$ est d'ordre $\text{ppcm}\left(p-1, p^{\alpha-1}\right) = (p-1)\,p^{\alpha-1} = \varphi\left(p^\alpha\right)$ dans $\mathbb{Z}_{p^\alpha}^\times$. En conséquence $\mathbb{Z}_{p^\alpha}^*$ est cyclique d'ordre $\varphi\left(p^\alpha\right)$.

3. On a $\mathbb{Z}_2^\times = \left\{\overline{1}\right\}$ et $\mathbb{Z}_4^\times = \left\{\overline{1}, \overline{-1}\right\} \approx \mathbb{Z}_2$.

4.

(a) On procède par récurrence sur $k \geq 0$. Pour $k = 0$, on a $5 = 1 + 2^2$ et $\lambda_0 = 1$. Pour $k = 1$, on a $5^2 = 1 + 3 * 2^3$ et $\lambda_1 = 3$. En supposant le résultat acquis pour $k \geq 1$, on a :

$$5^{2^{k+1}} = \left(1 + \lambda_k 2^{k+2}\right)^2 = 1 + \lambda_{k+1} 2^{k+3}$$

avec $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1} = \lambda_k\left(1 + \lambda_k 2^{k+1}\right)$ impair si λ_k l'est.

(b) On a $5^{2^{\alpha-2}} = 1 + \lambda_{\alpha-2} 2^\alpha \equiv 1 \pmod{2^\alpha}$ et $5^{2^{\alpha-3}} = 1 + \lambda_{\alpha-3} 2^{\alpha-1} \neq 1 \pmod{2^\alpha}$ du fait que $\lambda_{\alpha-3} \equiv 1 \pmod{2}$. On a donc $5 + 2^\alpha\mathbb{Z}$ d'ordre $2^{\alpha-2}$ dans $\mathbb{Z}_{2^\alpha}^\times$ et $H = \langle 5 + 2^\alpha\mathbb{Z}\rangle$ est un sous-groupe cyclique d'ordre $2^{\alpha-2}$ de $\mathbb{Z}_{2^\alpha}^\times$, il est donc isomorphe à $\mathbb{Z}_{2^{\alpha-2}}$.

(c) Si $k \equiv k' \pmod{2^\alpha}$ alors 2^α divise $k - k'$ et $k \equiv k' \pmod{4}$ ($\alpha \geq 2$), donc l'application ψ est bien définie. Dire que $k + 2^\alpha\mathbb{Z}$ est inversible dans $\mathbb{Z}_{2^\alpha}$ équivaut à dire que k est premier avec 2^α et donc avec 4, c'est-à-dire que ψ envoie $\mathbb{Z}_{2^\alpha}^*$ dans $\mathbb{Z}_4^*$. Il est facile de vérifier que ψ est un morphisme de groupes multiplicatifs. Si $x = k + 4\mathbb{Z}$ est inversible dans $\mathbb{Z}_4$ alors $k \equiv 1 \pmod{4}$ ou $k \equiv -1 \pmod{4}$ et $x = \psi(y)$ avec $y = 1 + 2^\alpha\mathbb{Z}$ ou $y = -1 + 2^\alpha\mathbb{Z}$ dans $\mathbb{Z}_{2^\alpha}^\times$, c'est-à-dire que ψ est surjective. Par passage au quotient ψ induit alors un isomorphisme de $\dfrac{\mathbb{Z}_{2^\alpha}^\times}{\ker(\psi)}$ sur $\mathbb{Z}_4^\times$, il en résulte que :

$$\text{card}\left(\mathbb{Z}_{2^\alpha}^\times\right) = \text{card}\left(\ker(\psi)\right)\text{card}\left(\mathbb{Z}_4^\times\right) = 2\,\text{card}\left(\ker(\psi)\right)$$

et $\text{card}\left(\ker(\psi)\right) = 2^{\alpha-2}$. Avec $5 + 2^\alpha\mathbb{Z}$ d'ordre $2^{\alpha-2}$ dans $\ker(\psi)$ ($5 \equiv 1 \pmod{4}$) on déduit que $\ker(\psi)$ est cyclique d'ordre $2^{\alpha-2}$ engendré par $5 + 2^\alpha\mathbb{Z}$.

(d) Pour $x \in \mathbb{Z}_{2^\alpha}^\times$, on a $\psi(x) \in \mathbb{Z}_4^* = \left\{\overline{1}, \overline{-1}\right\}$. Si $\psi(x) = \overline{1}$, alors $\psi(x)\,x = x \in \ker(\psi)$ et si $\psi(x) = \overline{-1}$, alors $\psi(x)\,x = -x$ et $\psi(\psi(x)\,x) = -\psi(x) = \overline{1}$ et $\psi(x)\,x \in \ker(\psi)$. Du fait que ψ est un morphisme de groupes multiplicatifs, on déduit qu'il en est de même de π.
Si $x \in \ker(\pi)$, alors $\psi(x) = \overline{1}$ et $\psi(x)\,x = \overline{1}$, donc $x = \overline{1}$ et π est injectif. Ces deux groupes ayant même cardinal, on déduit que π est un isomorphisme. En résumé $\mathbb{Z}_{2^\alpha}^\times$ est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ pour $\alpha \geq 3$ et $\mathbb{Z}_{2^\alpha}^\times$ n'est pas cyclique puisqu'il n'y a pas d'élément d'ordre $2^{\alpha-1}$ dans $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$.

– VI – Nombres de Carmichaël

1. Si n est pair, alors $n-1$ est impair et $\left(\overline{-1}\right)^{n-1} = \overline{-1}$ ($n \neq 2$ puisqu'il est non premier) et n n'est pas un nombre de Carmichaël.

2. On a la décomposition en facteurs premiers $561 = 3 \cdot 11 \cdot 17 = \prod_{k=1}^{3} p_k$.
   Dire que a est premier avec 561 équivaut à dire qu'il est premier avec chaque p_k et le théorème de Fermat nous dit que $a^{p_k-1} \equiv 1 \bmod (p_k)$ et en remarquant que 560 est divisible par chaque $p_k - 1$ ($560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$), on en déduit que $a^{560} \equiv 1 \bmod (p_k)$ pour $k = 1, 2, 3$ et la question précédente nous dit que $a^{560} \equiv 1 \ (561)$.

3. Avec :
$$(1+pq)(1-pq) = 1 - p^2q^2 = 1 - qn \equiv 1 \pmod{n}$$
   on déduit que $x = \overline{1+pq} \in \mathbb{Z}_n$ est inversible d'inverse $\overline{1-pq}$.
   Comme $pq \not\equiv 0 \pmod{n}$ ($n = p^2q$ ne peut diviser pq), on a $x \neq \overline{1}$ et avec :
$$(1+pq)^p = 1 + p^2q + p^2q \sum_{j=2}^{p} \binom{p}{j} p^{j-2}q^{j-1} \equiv 1 \pmod{n}$$
   on déduit que x est d'ordre p dans $\mathbb{Z}_n^\times$.
   Si n est de Carmichaël, on a alors $x^{n-1} = \overline{1}$ et l'ordre p de x va diviser $n - 1 = p^2q - 1$, ce qui est impossible.

4. Soit $n = \prod_{j=1}^{r} p_j$, où $r \geq 3$, $3 \leq p_1 < \cdots < p_r$ sont premiers tels que chaque $p_j - 1$, pour j compris entre 1 et r, divise $n - 1$.
   Un tel entier, produit d'au moins trois nombres premiers est non premier.
   Soit $x = \overline{k} \in \mathbb{Z}_n$ avec $k \in \{1, \cdots, n\}$. Pour tout j compris entre 1 et r, on a deux possibilités :
   soit p_j divise k et dans ce cas, il divise aussi k^n, donc $k^n \equiv k \equiv 0 \pmod{p_j}$;
   soit p_j ne divise pas k et dans ce cas, il est premier avec k, donc $k^{p_j-1} \equiv 1 \pmod{p_j}$ (théorème de Fermat) et comme $n - 1$ est multiple de $p_j - 1$, on a aussi $k^{n-1} \equiv 1 \pmod{p_j}$ et $k^n \equiv k \pmod{p_j}$.
   On a donc, dans tous les cas, $k^n \equiv k \pmod{p_j}$ et de l'exercice **??** on déduit que $k^n \equiv k \pmod{n}$ puisque $n = \prod_{j=1}^{r} p_j = n = \bigvee_{j=1}^{r} p_j$.
   Supposons que n soit non premier et que $x^n = x$ pour tout $x \in \mathbb{Z}_n$. Pour $x \in \mathbb{Z}_n^\times$, on peut simplifier par x et on obtient $x^{n-1} = \overline{1}$. L'entier n est donc de Carmichaël.
   Si n est un nombre de Carmichaël, le lemme précédent nous dit alors qu'il est sans facteurs carrés et comme il est non premier, il s'écrit $n = \prod_{j=1}^{r} p_j$, avec $r \geq 2$ et $3 \leq p_1 < \cdots < p_r$ premiers.
   Pour tout j compris entre 1 et r le groupe multiplicatif $\mathbb{Z}_{p_j}^\times$ est cyclique d'ordre $p_j - 1$, donc il existe un élément x_j d'ordre $p_j - 1$ dans $\mathbb{Z}_{p_j}^\times$ et comme n est de Carmichaël, on a aussi $x_j^{n-1} = \overline{1}$, donc l'ordre $p_j - 1$ de x_j divise $n - 1$.
   Il reste enfin à montrer que $r \geq 3$.
   Supposons que $n = p_1p_2$ avec $3 \leq p_1 < p_2$ premiers tels que $p_i - 1$ divise $n - 1$ pour $i = 1, 2$. En écrivant que $n - 1 = (p_1 - 1) + p_1(p_2 - 1)$, on déduit que $n - 1$ ne peut être divisible par $p_2 - 1$, en effet si $p_2 - 1$ divise $n - 1$ il divise $p_1 - 1$ avec $p_1 < p_2$, ce qui est impossible. En conséquence un nombre de Carmichaël a au moins trois facteurs premiers.
   Les entiers $561 = 3 \times 11 \times 17$, $1105 = 5 \times 13 \times 17$ et $1729 = 7 \times 13 \times 19$ sont des nombres de Carmichaël puisque $560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$, $1104 = 4 \cdot 276 = 12 \cdot 92 = 16 \cdot 69$ et $1728 = 6 \cdot 288 = 12 \cdot 144 = 18 \cdot 96$.

5. L'entier n est non premier et on a $n \equiv 1 \pmod{6a}$, $n \equiv (6a+1)^2 \equiv 1 \pmod{12a}$, $n \equiv (6a+1)(12a+1) \equiv 1 \pmod{18a}$, ce qui signifie que $p_j - 1$ divise $n - 1$ pour $j = 1, 2, 3$. Donc

n est de Carmichaël.
Pour $a = 1$, on obtient $n = 7 \cdot 13 \cdot 19 = 1729$.

– VII – Le théorème de Frobénius-Zolotarev

Pour cette partie, $p \geq 3$ est un nombre premier impair et $n \geq 2$ est un entier.
Pour tout entier relatif a, on note $\overline{a} \in \mathbb{Z}_p$ la classe résiduelle de a modulo p.
On dit qu'un entier a non multiple de p est un résidu quadratique modulo p si il existe un entier k tel que $k^2 \equiv a \pmod{p}$, ce qui signifie que $\overline{a}$ est un carré dans $\mathbb{Z}_p^*$.
Pour tout $\lambda \in \mathbb{Z}_p^*$, on définit le symbole de Legendre $\left(\frac{\lambda}{p}\right)$ par :

$$\left(\frac{\lambda}{p}\right) = \begin{cases} 1 \text{ si } \lambda \text{ est un carré dans } \mathbb{Z}_p^* \\ -1 \text{ sinon} \end{cases}$$

1. Comme $\mathbb{Z}_p^*$ est cyclique d'ordre $p-1$, il existe $\mu \in \mathbb{F}_p^*$ tel que $\mathbb{F}_p^* = \langle \mu \rangle = \{1, \mu, \cdots, \mu^{p-2}\}$.
Donc pour tout élément λ de $\mathbb{Z}_p^*$, il existe un unique entier k compris entre 0 et $q-2$ tel que $\lambda = \mu^k$ et on a :
$$\varphi(\lambda) = (\varphi(\mu))^k$$
avec $\varphi(\mu) = \pm 1$.
Si $\varphi(\mu) = 1$, on a alors $\varphi(\lambda) = 1$ pour tout $\lambda \in \mathbb{Z}_p^*$ et φ est trivial contrairement à l'hypothèse.
On a donc $\varphi(\mu) = -1$ et $\varphi(\lambda) = (-1)^k$ pour tout $\lambda \in \mathbb{Z}_p^*$.
Si λ est un carré dans $\mathbb{Z}_p^*$, il s'écrit alors $\lambda = \nu^2$ et on a $\varphi(\lambda) = (\varphi(\nu))^2 = (\pm 1)^2 = 1$.
Si λ est un non carré dans $\mathbb{Z}_p^*$, il s'écrit alors $\lambda = \mu^k$ avec k impair et on a $\varphi(\lambda) = (-1)^k = -1$.
En conclusion, $\varphi(\lambda) = \left(\frac{\lambda}{p}\right)$ pour tout $\lambda \in \mathbb{Z}_p^*$.

2.

(a) Pour $1 \leq i \neq j \leq n$ fixés, l'application :
$$\varphi : \lambda \in \mathbb{Z}_p \mapsto \gamma(T_{ij}(\lambda)) \in \{-1, 1\}$$
est un morphisme de groupes de $(\mathbb{Z}_p, +)$ dans $(\{-1, 1\}, \cdot)$.
En effet, pour λ, μ dans $\mathbb{Z}_p$, on a $\varphi(\lambda + \mu) = \gamma(T_{ij}(\lambda + \mu))$ avec :
$$\begin{aligned} T_{ij}(\lambda + \mu) &= I_n + (\lambda + \mu) E_{ij} = (I_n + \lambda E_{ij})(I_n + \mu E_{ij}) \\ &= T_{ij}(\lambda) T_{ij}(\mu) \end{aligned}$$
puisque $E_{ij}^2 = 0$ pour $i \neq j$, donc :
$$\begin{aligned} \varphi(\lambda + \mu) &= \gamma(T_{ij}(\lambda) T_{ij}(\mu)) = \gamma(T_{ij}(\lambda)) \gamma(T_{ij}(\mu)) \\ &= \varphi(\lambda) \varphi(\mu) \end{aligned}$$
Ces groupes étant finis, on a :
$$\operatorname{card}(\mathbb{F}_q) = \operatorname{card}(\ker(\varphi)) \operatorname{card}(\operatorname{Im}(\varphi))$$
c'est-à-dire que $\operatorname{card}(\operatorname{Im}(\varphi))$ divise $p = \operatorname{card}(\mathbb{F}_p)$.
Mais $\operatorname{Im}(\varphi)$ étant un sous-groupe de $\{-1, 1\}$ est de cardinal égal à 1 ou 2 et nécessairement $\operatorname{card}(\operatorname{Im}(\varphi)) = 1$ puisque p est impair.
On a donc $\operatorname{Im}(\varphi) = \{\varphi(0)\} = \{1\}$, ce qui signifie que φ est la fonction constante égale à 1 ou encore que $\gamma(T_{ij}(\lambda)) = 1$ pour tout $\lambda \in \mathbb{Z}_p$.

(b) En notant $D_n(\lambda) = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$ une matrice de la dilatation avec $\lambda \in \mathbb{Z}_p^*$, l'application :

$$\varphi : \lambda \in \mathbb{Z}_p \mapsto \gamma(D_n(\lambda)) \in \{-1, 1\}$$

est un morphisme de groupes (puisque $D_n(\lambda\mu) = D_n(\lambda) D_n(\mu)$), donc $\gamma(D_n(\lambda)) = \left(\frac{\lambda}{p}\right) = \left(\frac{\det(A)}{p}\right)$.

(c) Résulte du fait que toute matrice $A \in GL_n(\mathbb{Z}_p)$ est produit de matrices de transvections (si elle est dans $SL_n(\mathbb{Z}_p)$) ou d'une matrice de dilatation de rapport $\det(A)$ et de matrices de transvections (si elle n'est pas dans $SL_n(\mathbb{Z}_p)$).

3. Il s'agit de montrer que le morphisme de groupes ε est non trivial, ce qui revient à trouver un automorphisme $u \in GL\left(\mathbb{Z}_p^n\right)$ de signature -1.
Un corps fini $\mathbb{F}_{p^n}$ à p^n éléments est aussi un $\mathbb{Z}_p$-espace vectoriel de dimension n, donc isomorphe à $\mathbb{Z}_p^n$.
Il nous suffit donc de trouver un $\mathbb{Z}_p$-automorphisme de $\mathbb{F}_{p^n}$ de signature -1.
Comme $\mathbb{F}_{p^n}^*$ est cyclique d'ordre $p^n - 1$, il est engendré par un élément g d'ordre $p^n - 1$.
On vérifie alors que le $\mathbb{Z}_p$-automorphisme $\sigma : x \mapsto gx$ est de signature -1.
En effet, c'est la permutation de $\mathbb{F}_{p^n}$:

$$\sigma = \begin{pmatrix} 0 & 1 & g & g^2 & \cdots & g^{p^n-2} \\ 0 & g & g^2 & g^3 & \cdots & 1 \end{pmatrix}$$

soit le $(p^n - 1)$-cycle $\begin{pmatrix} 1 & g & g^2 & \cdots & g^{p^n-2} \end{pmatrix}$ qui est de signature $(-1)^{p^n} = -1$ puisque p est impair.

– VIII – Groupes abéliens finis

1. On procède par récurrence sur $r \geq 2$.

(a) Pour $r = 2$, on procède comme suit.
Si $\theta(g_1)$ et $\theta(g_2)$ sont premiers entre eux, $g_0 = g_1 g_2$ est alors d'ordre $m_1 m_2 = \text{ppcm}(m_1, m_2)$.
En effet, comme G est commutatif, on a $g_0^{m_1 m_2} = (g_1^{m_1})^{m_2} (g_2^{m_2})^{m_1} = 1$ et $m_0 = \theta(g_0)$ divise $m_1 m_2$.
Avec $1 = g_0^{m_0} = g_1^{m_0} g_2^{m_0}$, on déduit que $g_1^{m_0} = (g_2^{m_0})^{-1} \in \langle g_1 \rangle \cap \langle g_2 \rangle = \{1\}$ ($\langle g_1 \rangle \cap \langle g_2 \rangle$ est contenu dans $\langle g_1 \rangle$ et dans $\langle g_2 \rangle$, donc son cardinal divise m_1 et m_2 et en conséquence il divise $m_1 \wedge m_2 = 1$, donc il vaut 1), soit $g_1^{m_0} = g_2^{m_0} = 1$ et m_0 est multiple de m_1 et m_2, donc de $\text{ppcm}(m_1, m_2) = m_1 m_2$.
En conclusion, on a l'égalité $m_0 = m_1 m_2$.
Pour le cas général, l'idée est de se ramener à ce cas de figure.
On écrit les décompositions en facteurs premiers de m_1 et m_2 sous la forme :

$$m_1 = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\alpha_i},\ m_2 = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{r} p_i^{\beta_i}$$

où les facteurs premiers p_i ont été regroupés de sorte que $\alpha_i > \beta_i$ pour $1 \leq i \leq k$ et $\alpha_i \leq \beta_i$ pour $k+1 \leq i \leq r$, les exposants α_i, β_i étant positifs ou nuls (si l'une des conditions $\alpha_i > \beta_i$ ou $\alpha_i \leq \beta_i$ n'est jamais vérifiée, alors le produit correspondant vaut 1).
Avec ces écritures, on a :

$$\text{ppcm}(m_1, m_2) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\beta_i} = q_1 q_2$$

où $q_1 = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $q_2 = \prod_{i=k+1}^{r} p_i^{\beta_i}$ sont premiers entre eux et $m_1 = q_1 r_1$, $m_2 = q_2 r_2$.
Les éléments $g_1' = g_1^{n_1}$ et $g_2' = g_2^{n_2}$ sont alors d'ordres respectifs q_1 et q_2 et $g_0 = g_1' g_2'$ est d'ordre $q_1 q_2 = \text{ppcm}(m_1, m_2)$.

(b) Supposons le résultat acquis pour $r \geq 2$ et soient $g_1, g_2, \cdots, g_{r+1}$ deux à deux distincts dans G d'ordres respectifs $m_1, m_2, \cdots, m_{r+1}$.
L'hypothèse de récurrence nous dit qu'il existe $g_0' \in G$ d'ordre $m_0' = \text{ppcm}(m_1, m_2, \cdots, m_r)$ et le cas $r = 2$ qu'il existe g_0 d'ordre :

$$\begin{aligned}\text{ppcm}(m_0', m_{r+1}) &= \text{ppcm}(\text{ppcm}(m_1, m_2, \cdots, m_r), m_{r+1}) \\ &= \text{ppcm}(m_1, m_2, \cdots, m_{r+1})\end{aligned}$$

(associativité du ppcm).

2. Comme G est commutatif fini, il existe $g_0 \in G$ tel que :

$$\theta(g_0) = \text{ppcm}\{\theta(g) \mid g \in G\}$$

En désignant par g_1 un élément de G tel que $\theta(g_1) = \max_{g \in G} \theta(g)$, on a $\theta(g_0) \leq \theta(g_1)$ ($\theta(g_1)$ est le plus grand) et $\theta(g_1)$ divise $\theta(g_0)$ ($\theta(g_0)$ est multiple de tous les ordres) donc $\theta(g_1) \leq \theta(g_0)$ et $\theta(g_0) = \theta(g_1)$.

3. Soit $G = \{g_1, \cdots, g_n\}$ un groupe commutatif fini d'ordre $n \geq 2$.
Comme il existe $i \in \{1, \cdots, n\}$ tel que $m = \theta(g_i)$, cet entier m divise l'ordre n de G et l'ensemble des facteurs premiers de m est contenu dans l'ensemble des facteurs premiers de n.
En utilisant l'application φ du groupe produit $H = \prod_{k=1}^{n} \langle g_k \rangle$ dans G définie par :

$$\forall h = (h_1, \cdots, h_n) \in H,\ \varphi(h) = \prod_{i=1}^{n} h_i$$

on vérifie d'abord que n divise le produit des ordres $\prod_{k=1}^{n} \theta(g_k)$.
L'application φ est surjective et comme G est commutatif, c'est un morphisme de groupes.
Ce morphisme φ induit alors un isomorphisme du groupe quotient $H/\ker(\varphi)$ sur G, ce qui entraîne que $\text{card}(H) = \text{card}(\ker(\psi))\,\text{card}(G)$ et $n = \text{card}(G)$ divise $\text{card}(H) = \prod_{k=1}^{n} \theta(g_k)$.
Sachant que m est aussi le ppcm des ordres des éléments de G, il est multiple de chaque $\theta(g_k)$ et m^n est multiple de $\prod_{k=1}^{n} \theta(g_k)$ donc de n.
Donc l'ensemble des facteurs premiers de n est contenu dans l'ensemble des facteurs premiers de m.
En définitive m et n ont les mêmes facteurs premiers.

4. Soit $(G, \cdot)$ un groupe de cardinal premier $p \geq 2$. Si $g \in G \setminus \{1\}$, il est d'ordre différent de 1 qui divise p, donc cet ordre est p et G est cyclique engendré par g.

5. On peut le montrer en utilisant le théorème de Cauchy qui nous dit qu'il existe dans G un groupe d'ordre p et un d'ordre q, ces groupes sont cycliques et on a ainsi un élément g d'ordre p et un élément h d'ordre q. L'élément gh est alors d'ordre pq (pour G commutatif) et G est cyclique.
On peut se passer du théorème de Cauchy en procédant comme suit.
S'il existe dans G un élément g d'ordre p et un élément h d'ordre q, alors gh est d'ordre pq et G est cyclique.

Sinon les éléments de $G \setminus \{1\}$ sont tous d'ordre p ou tous d'ordre q. Supposons les tous d'ordre p. Si $g \in G$ est d'ordre p, alors le groupe quotient $G/\langle g \rangle$ est d'ordre q premier, donc cyclique engendré par $\overline{g_0}$ d'ordre q dans $G/\langle g \rangle$, ce qui entraîne que $\theta(g_0) = p$ divise q (puisque $\overline{g_0}^p = \overline{g_0^p} = \overline{1}$), ce qui est impossible pour $p \neq q$ premiers.

6. Comme $m = \text{ppcm}\{\theta(g) \mid g \in G\} = \theta(g_0)$ et n ont les mêmes facteurs premiers, on a les décompositions en facteurs premiers $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ et $m = \prod_{k=1}^{r} p_k^{\beta_k}$, où les p_k sont premiers deux à deux distincts et $1 \leq \beta_k \leq \alpha_k$ pour tout k compris entre 1 et n.
Sachant que :
$$\varphi(n) = \prod_{k=1}^{r} p_k^{\alpha_k - 1}(p_k - 1)$$
on déduit que si $\varphi(n)$ est premier avec n, alors tous les α_k valent 1 (sinon p_k divise $\varphi(n)$ et n) et les β_k valent aussi 1, ce qui donne $n = m$ et G est cyclique puisque g_0 est d'ordre $n = \text{card}(G)$.
On peut aussi utiliser le théorème de Cauchy.
Si n est premier avec $\varphi(n)$, on a alors $n = \prod_{k=1}^{r} p_k$, où les p_k sont premiers deux à deux distincts.
Le théorème de Cauchy nous assure l'existence, pour tout entier k compris entre 1 et n, d'un élément g_k d'ordre p_k dans G. Comme G est commutatif, le produit $g = \prod_{k=1}^{r} g_k$ est d'ordre n.

7. Voir FGN agrégation, p. 30.

8. Dire que $n \geq 2$ est premier avec $\varphi(n)$ équivaut à dire que $n = \prod_{k=1}^{r} p_k$, où les p_k sont premiers deux à deux distincts tels que p_k ne divise pas $p_j - 1$ pour $1 \leq j, k \leq r$.
Si n est non premier avec $\varphi(n)$, on a alors deux possibilités.
Soit n a un facteur carré et il s'écrit $n = p^2 q$ avec $p \geq 2$ premier et $q \geq 1$, soit n est sans facteur carré de la forme $n = \prod_{k=1}^{r} p_k$, où les p_k sont premiers deux à deux distincts, l'un des p_k divisant l'un des $p_j - 1$ pour $1 \leq j, k \leq r$.
Dans le premier cas, le groupe commutatif $G = \dfrac{\mathbb{Z}}{p\mathbb{Z}} \times \dfrac{\mathbb{Z}}{pq\mathbb{Z}}$ est d'ordre n non cyclique (théorème chinois).
Dans le deuxième cas, Voir FGN agrégation, p. 30.

9.

(a)

i. Comme $g^{\theta(g)} = 1 \in H$ (ou $g^n = 1 \in H$), on peut définir l'entier :
$$r = \min\left\{k \in \mathbb{N}^* \mid g^k \in H\right\}$$
et comme $\mathbb{C}$ est algébriquement clos, il existe $\alpha \in \mathbb{C}^*$ tel que $\varphi(g^r) = \alpha^r$.

ii. On note :
$$K = \left\{g^k h \mid k \in \mathbb{Z},\ h \in H\right\}$$
le sous-groupe de G engendré par g et H et on vérifie que l'application :
$$\begin{array}{rccc} \varphi_K : & K & \to & \mathbb{C}^* \\ & g^k h & \mapsto & \alpha^k \varphi(h) \end{array}$$
est bien définie, puis que c'est un morphisme de groupes.
Si $g^k h = g^{k'} h'$ avec $k \geq k'$ dans $\mathbb{Z}$ et h, h' dans H, on a alors $g^{k-k'} = h' h^{-1} \in H$ et $k - k' = qr$ (la division euclidienne par r nous donne $k - k' = qr + s$ avec $0 \leq s \leq r - 1$,

donc $h'h^{-1} = g^{k-k'} = (g^r)^q g^s$ et $g^s = ((g^r)^q)^{-1} h'h^{-1} \in H$, ce qui impose $s = 0$ par le caractère minimal de r), donc :

$$\varphi\left(h'h^{-1}\right) = \varphi\left(g^{k-k'}\right) = \varphi\left(g^r\right)^q = \left(\alpha^r\right)^q = \alpha^{k-k'}$$

et $\alpha^k \varphi(h) = \alpha^{k'} \varphi(h')$.
Donc l'application φ_K est bien définie.
On vérifie facilement que c'est un morphisme de groupes.
En effet, pour $g^k h$ et $g^{k'} h'$ dans K, on a :

$$\begin{aligned}\varphi_K\left(\left(g^k h\right)\left(g^{k'} h'\right)\right) &= \varphi_K\left(g^{k+k'} hh'\right) = \alpha^{k+k'} \varphi(hh') \\ &= \alpha^k \varphi(h)\, \alpha^{k'} \varphi(h') = \varphi_K\left(g^k h\right) \varphi_K\left(g^{k'} h'\right)\end{aligned}$$

iii. Avec la construction précédente, si $K = G$, on a bien prolongé φ à G. Sinon on reprend cette construction à partir de K.
Comme le groupe G est fini, on aura pronlongé φ à G par ces itérations.

(b) Soit $g_0 \in G$ tel que :

$$m = \theta(g_0) = \max_{g \in G} \theta(g) = \text{ppcm}\{\theta(g) \mid g \in G\}$$

Comme G n'est pas réduit à $\{1\}$, on a $2 \leq m \leq n-1$ en supposant que $m \neq n$.

i. On vérifie qu'il existe un unique caractère $\varphi_0 : K \to \mathbb{C}^*$ tel que $\varphi_0(g_0) = \omega = e^{\frac{2i\pi}{m}}$.
Si un tel caractère existe, on a alors pour tout entier relatif k, $\varphi_0\left(g_0^k\right) = \omega^k$, ce qui prouve son unicité.
Définissant l'application φ_0 de la sorte, on vérifie que c'est un caractère de K.
D'une part cette application est bien définie puisque l'égalité $g_0^k = g_0^{k'}$ dans G équivaut à $k \equiv k' \pmod{m}$, ce qui donne $\omega^k = \omega^{k'}$ et d'autre part, on vérifie facilement que c'est un morphisme de groupes.

ii. On prolonge ce caractère en un caractère φ de G et on vérifie que l'application :

$$\begin{array}{rccc}\theta : & \langle g_0 \rangle \times \ker(\varphi) & \to & G \\ & \left(g_0^k, h\right) & \mapsto & g_0^k h\end{array}$$

est un isomorphisme de groupes.
Comme le groupe G est commutatif, l'application θ est bien un morphisme de groupes.
Si $\left(g_0^k, h\right) \in \ker(\theta)$, on a alors $g_0^k h = 1$ et $\varphi\left(g_0^k h\right) = \omega^k = 1$, donc $k \equiv 0 \pmod{m}$, ce qui nous donne $g_0^k = 1$ et $h = 1$.
Donc θ est injective.
Pour tout $g \in G$, on a $g^m = 1$, donc $\varphi(g^m) = (\varphi(g))^m = 1$ et $\varphi(g) \in \Gamma_m$, soit $\varphi(g) = \omega^k = \varphi\left(g_0^k\right)$ pour un entier k et $h = g\left(g_0^k\right)^{-1} \in \ker(\varphi)$, ce qui nous donne $g = g_0^k h = \theta\left(g_0^k, h\right)$.
Donc θ est surjective et θ est un isomorphisme.

(c) On prouve tout d'abord l'existence d'une telle suite d'entiers par récurrence sur l'ordre $n \geq 2$ du groupe commutatif G.
Pour $n = 2$, le groupe G est cyclique isomorphe à $\Gamma_2 = \{-1, 1\}$.
Supposons le résultat acquis pour les groupes commutatifs d'ordre au plus égal à $n-1 \geq 2$ et soit G un groupe commutatif d'ordre $n \geq 3$.
Si, avec les notations précédentes, on a $m = n$, le groupe G est alors cyclique d'ordre n isomorphe à Γ_n.

Supposons que $2 \leq m \leq n-1$.
On a alors $\text{card}(\ker(\varphi)) = \dfrac{\text{card}(G)}{\text{card}(\langle g_0 \rangle)} = \dfrac{n}{m} \in \{2, \cdots, n-1\}$ et par hypothèse de récurrence, $\ker(\varphi)$ est isomorphe à un groupe produit $\Gamma = \prod_{k=1}^{r} \Gamma_{n_k}$ avec $n_1 \geq 2$ qui divise n_2, ..., n_{k-1} qui divise n_k.
Le groupe cyclique $\langle g_0 \rangle$ étant isomorphe à $\Gamma_m = \Gamma_{n_{r+1}}$, on en déduit un isomorphisme de $\prod_{k=1}^{r+1} \Gamma_{n_k}$ sur G.
Comme m est le ppcm des ordres des éléments de G, c'est aussi le ppcm des ordres des éléments du groupe produit $\Gamma = \prod_{k=1}^{r+1} \Gamma_{n_k}$ et en particulier, il multiple de n_k qui est l'ordre de $\left(1, \cdots, e^{\frac{2i\pi}{n_k}}, 1\right)$.

(d) La condition nécessaire est évidente.
Supposons que :

$$\forall m \in \mathbb{N}^*, \ \prod_{k=1}^{r} \text{pgcd}(m, n_k) = \prod_{j=1}^{s} \text{pgcd}(m, m_j)$$

Prenant $m = \prod_{k=1}^{r} n_k \prod_{j=1}^{j} m_j$, on a $\text{pgcd}(m, n_k) = n_k$ pour tout k compris entre 1 et r et $\text{pgcd}(m, m_j) = m_j$ pour tout j compris entre 1 et s, donc :

$$\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} m_j$$

Prenant $m = n_r$ qui est multiple de tous les n_k, on a $\text{pgcd}(m, n_k) = n_k$ pour tout k compris entre 1 et r et :

$$\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} \text{pgcd}(n_r, m_j)$$

donc :

$$\prod_{j=1}^{j} m_j = \prod_{j=1}^{j} \text{pgcd}(n_r, m_j)$$

ou encore :

$$\prod_{j=1}^{s} \frac{m_j}{\text{pgcd}(n_r, m_j)} = 1 \text{ dans } \mathbb{N}^*$$

ce qui équivaut à dire que :

$$\text{pgcd}(n_r, m_j) = m_j \ \ (1 \leq j \leq s)$$

En particulier, on a $m_s = \text{pgcd}(n_r, m_s)$ divise n_r.
Comme les suites $(n_k)_{1 \leq k \leq r}$ et $(m_j)_{1 \leq j \leq s}$ jouent des rôles symétriques, on a aussi n_r qui divise m_s et l'égalité $n_r = m_s$.
Par récurrence, on en déduit que $r = s$ et $n_k = m_k$ pour tout k compris entre 1 et r.

(e) On remarque que l'exposant d'un groupe $\Gamma = \prod_{k=1}^{r} \Gamma_{n_k}$ est n_r. En effet, comme n_r est multiple de tous les n_k, on a $(z_1, \cdots, z_r)^{n_r} = (z_1^{n_r}, \cdots, z_r^{n_r}) = (1, \cdots, 1)$, donc les éléments de Γ sont d'ordre au plus égal à n_r et comme $(1, \cdots 1, , \omega_{n_r})$ est d'ordre n_r, cet entier n_r est bien l'exposant de Γ.

Supposons qu'il existe deux suites d'entiers $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ avec les propriétés voulues.
Si $r=1$, on a alors $n=n_1=e(G)=m_s$ et nécessairement $s=1$ (sinon $n=\text{card}(\Gamma)=m_1\cdots m_s\geq 2m_s=2n$, ce qui n'est pas).
Si $r\geq 2$, on a alors $s\geq 2$.
Pour tout entier $m\geq 1$ l'image du groupe $\prod_{k=1}^{r}\Gamma_{n_k}\backsimeq\prod_{j=1}^{s}\Gamma_{m_j}$ par le morphisme de groupe $\varphi_m : x\mapsto x^m$ est le groupe :

$$\prod_{k=1}^{r}\left\langle\omega_{n_k}^m\right\rangle\backsimeq\prod_{j=1}^{s}\left\langle\omega_{m_j}^m\right\rangle$$

On utilise alors le fait que si dans un groupe un élément ω est d'ordre p, l'élément ω^m est d'ordre $p'=\dfrac{p}{\text{pgcd}(m,p)}$ (en effet, en notant $\delta=\text{pgcd}(m,p)$, on a $p=\delta p'$, $m=\delta m'$, avec $\text{pgcd}(m',p')=1$ et pour tout entier k, l'égalité $(\omega^m)^k=1$ équivaut à $km=\alpha p$, soit à $km'=\alpha p'$ ce qui revient à dire que p' divise k puisque $\text{pgcd}(m',p')=1$, donc $p'=\theta(\omega^m)$).
On a donc l'égalité des cardinaux :

$$\prod_{k=1}^{r}\frac{n_k}{\text{pgcd}(m,n_k)}=\prod_{j=1}^{s}\frac{m_j}{\text{pgcd}(m,m_j)}$$

pour tout entier $m\geq 1$.
De l'égalité $\prod_{k=1}^{r}n_k=\prod_{j=1}^{s}m_j$, on déduit les égalités $\prod_{k=1}^{r}\text{pgcd}(m,n_k)=\prod_{j=1}^{s}\text{pgcd}(m,m_j)$ pour tout $m\geq 1$, ce qui équivaut à l'unicité de la suite $(n_k)_{1\leq k\leq r}$.