Corrigé du DM 20

Arithmétique modulaire

Partie A - Étude de l'anneau $\mathbb{Z}/n\mathbb{Z}$

1. Il convient de vérifier que ces opération ne dépendent pas des représentants de la classe utilisés.
Soit $x, y \in \mathbb{Z}$ et $j, k \in \mathbb{Z}$ avec $x' = x + jn$ et $y' = y + kn$ c'est-à-dire $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{x'}$:

- $x' + y' \equiv (x + jn) + (y + kn) \equiv x + y + (j + k)n \equiv x + y \ [n]$
- $(x + jn) \times (y + kn) \equiv xy + xkn + yjn + jkn^2 \equiv xy + (xk + yj + jkn)n \equiv xy \ [n]$

Ainsi, $\overline{x + y} = \overline{x' + y'}$ et $\overline{xy} = \overline{x'y'}$; $\boxed{+ \text{ et } \times \text{ sont deux LCI pour } \mathbb{Z}/n\mathbb{Z}.}$

2. Nous ne connaissons pas d'ensemble usuel qui contienne $\mathbb{Z}/n\mathbb{Z}$, nous allons devoir revenir à la définition d'un anneau commutatif :

⇛ $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif :

- $+$ est une LCI
- $+$ est associative

  Soit $x, y, z \in \mathbb{Z}$, $(\overline{x} + \overline{y}) + \overline{z} = \overline{x + y} + \overline{z} = \overline{x + y + z} = \overline{x} + \overline{y + z} = \overline{x} + (\overline{y} + \overline{z})$
- $+$ est commutative
- $\overline{0} \in \mathbb{Z}/n\mathbb{Z}$ est élément neutre pour $+$
- pour $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ alors $\overline{-x}$ ou $\overline{n - x}$ est son opposé (inverse pour $+$)

⇛ $(\mathbb{Z}/n\mathbb{Z}, \times)$ est un magma associatif, commutatif et possédant un élément neutre :

- $\times$ est une LCI
- $\times$ est associative
- $\times$ est commutative
- $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ est élément neutre pour $\times$

⇛ $\times$ est distributive par rapport à $+$.

  Soit $x, y, z \in \mathbb{Z}$, $\overline{x} \times (\overline{y} + \overline{z}) = \overline{x} \times \overline{y + z} = \overline{x(y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \overline{x} \times \overline{y} + \overline{x} \times \overline{z}$
  Idem à droite.

Ainsi, $\boxed{\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right) \text{ est un anneau commutatif.}}$

3. Soit $x \in \mathbb{Z}$,

$$\begin{aligned}
\overline{x} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow \exists y \in \mathbb{Z}; \overline{x} \times \overline{y} = \overline{1} \\
&\Leftrightarrow \exists y \in \mathbb{Z}; \overline{xy} = \overline{1} \\
&\Leftrightarrow \exists y \in \mathbb{Z}; xy \equiv 1 \ [n] \\
&\Leftrightarrow \exists y, k \in \mathbb{Z}; xy + kn = 1 \\
&\Leftrightarrow x \wedge n = 1 \text{ d'après le théorème de Bezout}
\end{aligned}$$

Ainsi, $\boxed{\text{pour } x \in \mathbb{Z}, \overline{x} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} \text{ si et seulement si } x \wedge n = 1.}$

4. Soit $x \in \mathbb{Z}$, tel que $x \wedge n = 1$, alors d'après 3), $\overline{x}$ est inversible : il existe $y \in \mathbb{Z}$ tel que $\overline{xy} = \overline{1}$.
Donc pour tout $z \in \mathbb{Z}$, $\overline{z} = \overline{z}\overline{1} = \overline{zxy} = zy\overline{x} \in \langle x \rangle$.
Donc $\mathbb{Z}/n\mathbb{Z} = \langle x \rangle$; $\overline{x}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ qui est de cardinal n.
Ainsi, $\boxed{\text{pour } x \in \mathbb{Z}, \text{ si } x \wedge n = 1 \text{ alors } \overline{x} \text{ est d'ordre } n.}$

5. On vient de montrer le sens $\Leftarrow$. Montrons le sens $\Rightarrow$.
Soit $\overline{x}$ un générateur de $\mathbb{Z}/n\mathbb{Z}$. En particulier $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ et donc il existe $k \in \mathbb{N}$ tel que $k\overline{x} = \overline{k}\,\overline{x} = \overline{1}$, donc x est inversible.
Ainsi, $\boxed{\overline{x} \text{ est un générateur de } \mathbb{Z}/n\mathbb{Z} \text{ si et seulement si } \overline{x} \in U(\mathbb{Z}/n\mathbb{Z}).}$

6. Résolution d'équations :

• (E_1) : $\overline{6} \times x = \overline{7}$ dans $\mathbb{Z}/55\mathbb{Z}$. Travaillons directement dans $\mathbb{Z}/55\mathbb{Z}$.
Comme $6 \wedge 55 = 1$ avec l'identité de Bezout $55 \times 1 - 6 \times 9 = 1$, alors $\overline{6}$ est inversible d'inverse $\overline{-9}$.

$$\overline{6} \times x = \overline{7} \quad \Leftrightarrow \quad x = \overline{-9} \times \overline{7} = \overline{-63} = \overline{-8} = \overline{47}$$

Ainsi, $\boxed{\mathcal{S}_{E_1} = \{\overline{47}\} \text{ dans } \mathbb{Z}/55\mathbb{Z}.}$

• (E_2) : $\overline{6} \times x = \overline{11}$ dans $\mathbb{Z}/34\mathbb{Z}$. Travaillons dans $\mathbb{Z}$
Résoudre E_2 revient à rechercher les entiers $k \in \mathbb{Z}$ tel que

$$6k \equiv 11\ [34] \text{ ou encore tel que } 34 \text{ divise } 6k - 11$$

Or 2 divise 34 mais $6k - 11$ est impair, donc 2 ne divise pas $6k - 11$. Il n'y a pas de solution.
Ainsi, $\boxed{\mathcal{S}_{E_2} = \emptyset \text{ dans } \mathbb{Z}/34\mathbb{Z}.}$

• (E_3) : $\overline{6} \times x = \overline{15}$ dans $\mathbb{Z}/27\mathbb{Z}$.Travaillons dans $\mathbb{Z}$

$$6k \equiv 15\ [27] \quad \Leftrightarrow \quad 2k \equiv 5\ [9]$$

Or $2 \wedge 9 = 1$ avec $5 \times 2 - 1 \times 9 = 1$, alors $\overline{2}$ est inversible dans $\mathbb{Z}/9\mathbb{Z}$, d'inverse $\overline{5}$.

$$\begin{aligned} 6k \equiv 15\ [27] \quad &\Leftrightarrow \quad 5 \times 2k \equiv 5 \times 5\ [9] \\ &\Leftrightarrow \quad k \equiv 25 \equiv 7\ [9] \end{aligned}$$

Les solutions dans $\mathbb{Z}$ de $6k \equiv 15\ [27]$ sont $7 + 9\mathbb{Z}$.
Cela donne trois solutions dans $\mathbb{Z}/27\mathbb{Z}$: $\overline{7}, \overline{16}$ et $\overline{25}$.
Ainsi, $\boxed{\mathcal{S}_{E_3} = \{\overline{7}, \overline{16}, \overline{25}\} \text{ dans } \mathbb{Z}/27\mathbb{Z}.}$

7. Travaillons par implications successives :

• $(i) \quad \Rightarrow \quad (iii)$: Tout élément non nul est inversible (pour $\times$) et donc premier avec n d'après 3).
Ainsi n est premier avec tout entier de $[\![1, n-1]\!]$, donc n est premier.

• $(iii) \quad \Rightarrow \quad (ii)$: Soit $x, y \in \mathbb{Z}$ tel que $\overline{xy} = \overline{0}$, donc n divise xy. Procédons par disjonction sur la divisibilité de x par n.

- Soit n divise x ;
- Soit n ne divise pas x. Comme n est premier, $n \wedge x = 1$. Le théorème de Gauss donne que n divise y.

Ainsi, $\mathbb{Z}/n\mathbb{Z}$ est intègre.

• $(ii) \quad \Rightarrow \quad (i)$: Soit $\overline{x} \neq \overline{0}$, alors une petite récurrence dans un anneau intègre donne que la suite $\left(\overline{x}^k\right)$ ne s'annule pas.
Or l'anneau $\mathbb{Z}/n\mathbb{Z}$ est fini donc les éléments de la suite ne sont pas deux à deux distincts : il existe $i, j \in \mathbb{N}$ avec $i < j$ tel que $\overline{x^i} = \overline{x^j}$, ce qui donne :

$$\begin{aligned} \overline{x^i} = \overline{x^j} \quad &\Leftrightarrow \quad \overline{x^i}\left(\overline{x^{j-i}} - \overline{1}\right) = \overline{0} \\ &\Leftrightarrow \quad \overline{x^{j-i}} - \overline{1} = \overline{0} \text{ car l'anneau est intègre et } \overline{x^i} \neq \overline{0} \\ &\Leftrightarrow \quad \overline{x} \times \overline{x^{j-i-1}} = \overline{1} \text{ donc } \overline{x} \text{ est inversible.} \end{aligned}$$

Ainsi, $U(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$ donc c'est un corps.
Ainsi, $\boxed{\mathbb{Z}/n\mathbb{Z} \text{ est un corps} \quad \Leftrightarrow \quad \mathbb{Z}/n\mathbb{Z} \text{ est intègre} \quad \Leftrightarrow \quad n \text{ est premier.}}$

8. Dans $\mathbb{Z}/15\mathbb{Z}$ on a $\overline{10}\times\overline{3}=\overline{30}=\overline{0}$: $\mathbb{Z}/15\mathbb{Z}$ n'est pas intègre.
9. Résolution de E_4 dans $\mathbb{Z}/19\mathbb{Z}$:

$$\begin{aligned}
x^2-\overline{6}x+\overline{12}=0 &\Leftrightarrow \left(x-\overline{3}\right)^2-\overline{9}+\overline{12}=0\\
&\Leftrightarrow \left(x-\overline{3}\right)^2+\overline{3}=0\\
&\Leftrightarrow \left(x-\overline{3}\right)^2-\overline{16}=0\\
&\Leftrightarrow \left(x-\overline{3}\right)^2-\overline{4}^2=0\\
&\Leftrightarrow \left(x-\overline{3}-\overline{4}\right)\left(x-\overline{3}+\overline{4}\right)=0\\
&\Leftrightarrow \left(x-\overline{7}\right)\left(x+\overline{1}\right)=0\\
&\Leftrightarrow x=\overline{7} \text{ ou } x=-\overline{1} \text{ car 19 étant premier, } \mathbb{Z}/19\mathbb{Z} \text{ est intègre}
\end{aligned}$$

Ainsi, $\boxed{\mathcal{S}_{E_3}=\{\overline{7},\overline{18}\} \text{ dans } \mathbb{Z}/19\mathbb{Z}.}$

Partie B - Étude de l'anneau $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$

10. Les deux lois sont bien des lois de composition interne. Soit $(\widehat{x},\widetilde{y}),(\widehat{u},\widetilde{v}),(\widehat{a},\widetilde{b})\in\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$.
   - ▶ $\left(\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z},+\right)$ est un groupes commutatif.
   - • associativité de $+$: $\Big(\left(\widehat{x},\widetilde{y}\right)+\left(\widehat{u},\widetilde{v}\right)\Big)+\left(\widehat{a},\widetilde{b}\right) = \left(\widehat{x}+\widehat{u},\widetilde{y}+\widetilde{v}\right)+\left(\widehat{a},\widetilde{b}\right)=\left(\left(\widehat{x}+\widehat{u}\right)+\widehat{a},\left(\widetilde{y}+\widetilde{v}\right)+\widetilde{b}\right)$
     $+$ est associative dans les anneaux du type $\mathbb{Z}/p\mathbb{Z}$
     $=\left(\widehat{x}+\left(\widehat{u}+\widehat{a}\right),\widetilde{y}+\left(\widetilde{v}+\widetilde{b}\right)\right)=\left(\widehat{x},\widetilde{y}\right)+\left(\widehat{u}+\widehat{a},\widetilde{v}+\widetilde{b}\right)$
     $=\left(\widehat{x},\widetilde{y}\right)+\Big(\left(\widehat{u},\widetilde{v}\right)+\left(\widehat{a},\widetilde{b}\right)\Big)$
   - • $\left(\widehat{0},\widetilde{0}\right)$ élément neutre pour $+$
   - • $\left(\widehat{-x},\widetilde{-y}\right)$ est l'inverse de $\left(\widehat{x},\widetilde{y}\right)$ pour $+$
   - • commutativité de $+$: $\left(\widehat{x},\widetilde{y}\right)+\left(\widehat{u},\widetilde{v}\right)=\left(\widehat{x}+\widehat{u},\widetilde{y}+\widetilde{v}\right)=\left(\widehat{u}+\widehat{x},\widetilde{v}+\widetilde{y}\right)=\left(\widehat{u},\widetilde{v}\right)+\left(\widehat{x},\widetilde{y}\right)$
   - ▶ $\left(\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z},\times\right)$ est un magma associatif unitaire et $\times$ est distributive par rapport à $\times$.
   - • associativité de $\times$
   - • $\left(\widehat{1},\widetilde{1}\right)$ élément neutre pour $+$
   - • $\times$ est distributive par rapport à $+$.
11. Il s'agit de montrer que l'application est bien définie sur les classes, qu'elle ne dépend pas du représentant de la classe.
    Soit $x,y\in\mathbb{Z}$ tel que $\overline{x}=\overline{y}$ dans $\mathbb{Z}/nm\mathbb{Z}$. Alors il existe $k\in\mathbb{Z}$ tel que $x=y+knm$.
    Il vient $x\equiv y\ [n]$ et $x\equiv y\ [m]$ c'est-à- dire $\widehat{x}=\widehat{y}$ et $\widetilde{x}=\widetilde{y}$.
    Ainsi, $\boxed{\psi \text{ est bien définie.}}$
12. Montrons que ψ est un morphisme d'anneau. Soit $\overline{x},\overline{y}\in\mathbb{Z}/nm\mathbb{Z}$:
    - • $\psi\left(\overline{x}+\overline{y}\right)=\psi\left(\overline{x+y}\right)=\left(\widehat{x+y},\widetilde{x+y}\right)=\left(\widehat{x}+\widehat{y},\widetilde{x}+\widetilde{y}\right)=\left(\widehat{x},\widetilde{x}\right)+\left(\widehat{y},\widetilde{y}\right)=\psi\left(\overline{x}\right)+\psi\left(\overline{y}\right)$
    - • $\psi\left(\overline{x}\times\overline{y}\right)=\psi\left(\overline{x\times y}\right)=\left(\widehat{x\times y},\widetilde{x\times y}\right)=\left(\widehat{x}\times\widehat{y},\widetilde{x}\times\widetilde{y}\right)=\left(\widehat{x},\widetilde{x}\right)\times\left(\widehat{y},\widetilde{y}\right)=\psi\left(\overline{x}\right)\times\psi\left(\overline{y}\right)$
    - • $\psi\left(\overline{1}\right)=\left(\ \widehat{1}\ ,\ \widetilde{1}\ \right)$

    Ainsi, $\boxed{\psi \text{ est un morphisme d'anneau.}}$
13. La caractérisation de l'injectivité du morphisme ψ est $\mathrm{Ker}\left(\psi\right)=\{\overline{0}\}$. Soit $\overline{x}\in\mathbb{Z}/nm\mathbb{Z}$, alors

$$\psi(\overline{x})=\left(\ \widehat{0}\ ,\ \widetilde{0}\ \right) \quad\Rightarrow\quad \widehat{x}=\widehat{0} \text{ et } \widetilde{x}=\widetilde{0} \quad\Rightarrow\quad n|x \text{ et } m|x$$

Or n et m sont premiers entre eux, donc, d'après le corollaire de Gauss $nm|x$ et donc $\overline{x}=\overline{0}$.
La réciproque est évidente. Ainsi, $\boxed{\psi \text{ est injectif.}}$

14. Soit $(\widehat{a},\widetilde{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. On cherche l'existence d'un $x \in \mathbb{Z}$ tel que $\psi(\overline{x}) = (\widehat{a},\widetilde{b})$.
Ainsi, la surjectivité de ψ se ramène à montrer l'existence d'une solution au lemme chinois suivant :

$$\begin{cases} x \equiv a\ [n] \\ x \equiv b\ [m] \end{cases}$$

Comme $n \wedge m = 1$, alors la relation de Bezout donne qu'il existe de $u, v \in \mathbb{Z}$ tel que $nu + mv = 1$.
Alors $x = amv + bnu$ est une solution et donc $\psi\big(\ \overline{amv + bnu}\ \big) = (\widehat{a},\widetilde{b})$.
Ainsi, $\boxed{\psi \text{ est surjectif}}$ et donc, d'après 13), ψ est un isomorphisme.

15. Montrons que $\psi\left(U(\mathbb{Z}/nm\mathbb{Z})\right) = U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$.
- Soit $\overline{x} \in U(\mathbb{Z}/nm\mathbb{Z})$ et $\overline{y}$ tel que $\overline{x} \times \overline{y} = \overline{1}$. Il vient :

$$(\widehat{1},\widetilde{1}) = \psi(\overline{1}) = \psi(\overline{x} \times \overline{y}) = \psi(\overline{x}) \times \psi(\overline{y}) \quad \Rightarrow \quad \psi(\overline{x}) \in U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$$

- Soit $(\widehat{a},\widetilde{b}) \in U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$ et $(\widehat{c},\widetilde{d})$ tel que $\widehat{a} \times \widehat{c} = \widehat{1}$ et $\widetilde{b} \times \widetilde{d} = \widetilde{1}$.
Par surjectivité de ψ, il existe $\overline{x}, \overline{y} \in \mathbb{Z}/nm\mathbb{Z}$ tel que $\psi(\overline{x}) = (\widehat{a},\widetilde{b})$ et $\psi(\overline{y}) = (\widehat{c},\widetilde{d})$.
Alors, $\psi(\overline{x} \times \overline{y}) = \psi(\overline{x}) \times \psi(\overline{y}) = (\widehat{a},\widetilde{b}) \times (\widehat{c},\widetilde{d}) = (\widehat{a} \times \widehat{c}, \widetilde{b} \times \widetilde{d}) = (\widehat{1},\widetilde{1})$.
Par injectivité de ψ, on a $\overline{x} \times \overline{y} = \overline{1}$ et donc $\overline{x} \in U(\mathbb{Z}/nm\mathbb{Z})$ donc $(\widehat{a},\widetilde{b}) \in \psi\left(U(\mathbb{Z}/nm\mathbb{Z})\right)$.

Comme ψ est bijective, il vient que $\boxed{U(\mathbb{Z}/nm\mathbb{Z}) \text{ et } U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z}) \text{ sont équipotents.}}$

Partie C - Indicatrice d'Euler et de Carmichael

16. Associons les entiers de $[\![1, n]\!]$ aux n éléments (classes d'équivalence) de $\mathbb{Z}/n\mathbb{Z}$: $\{\overline{1}, \overline{2}, \ldots, \overline{n}\}$.
On a vu en 3) que x est premier avec n si et seulement s'il est inversible (pour $\times$).
Ainsi, $\boxed{\varphi(n) = \text{Card}\big(U(\mathbb{Z}/n\mathbb{Z})\big).}$

17. D'après la question précédente, $\varphi(n)$ est l'ordre du groupe $\big(U(\mathbb{Z}/n\mathbb{Z}), \times\big)$.
Soit a premier avec avec n, alors $\overline{a} \in U(\mathbb{Z}/n\mathbb{Z})$. Notons k son ordre, c'est-à-dire le cardinal du sous-groupe qu'il engendre, alors : $\overline{a}^k = \overline{1}$ ou encore $a^k \equiv 1\ [n]$.
Le théorème de Lagrange donne que k divise $\varphi(n)$. Notant q le quotient de $\varphi(n)$ par k alors

$$a^k \equiv 1\ [n] \quad \Rightarrow \quad a^{qk} \equiv 1^q\ [n] \quad \Rightarrow \quad a^{\varphi(n)} \equiv 1\ [n]$$

Ainsi, $\boxed{\text{pour tout } n \in \mathbb{N}^* \text{ et tout } a \text{ premier avec } n, \text{ alors } a^{\varphi(n)} \equiv 1\ [n].}$

18. On vient de voir que pour tout a premier avec n, l'ordre de $\overline{a}$ divise $\varphi(n)$ et donc $\varphi(n)$ est un multiple commun des ordres des éléments de $U(\mathbb{Z}/n\mathbb{Z})$.
- Montrons que $\lambda(n)$ est aussi un multiple commun de ces ordres.
Soit a premier avec n, et k l'ordre de $\overline{a}$ dans $(U(\mathbb{Z}/n\mathbb{Z}), \times)$. La division euclidienne de $\lambda(n)$ par k donc qu'il existe $(q, r) \in \mathbb{N}^2$ tel que

$$\lambda(n) = qk + r \text{ et } r \in [\![0, k-1]\!]$$

Or $a^r \equiv a^r \times \big(\underbrace{a^k}_{\equiv 1\ [n]}\big)^q \equiv a^{kq+r} \equiv q^{\lambda(n)} \equiv 1\ [n]$.
Par définition de k, il vient que $r = 0$ et donc que k divise $\lambda(n)$.
- Par définition, $\lambda(n)$ est donc aussi le plus petit multiple commun des ordres des éléments inversibles.

Ainsi, $\boxed{\lambda(n) \text{ divise } \varphi(n).}$

19. Calcul de $\varphi(8)$ et $\lambda(8)$:
- Les nombres premiers avec 8 dans $[\![1, 8]\!]$ sont $\{1, 3, 5, 7\}$ donc $\boxed{\varphi(8) = 4.}$

• Calculons les ordres des éléments précédent : 1 est d'ordre 1 ; 3,4 et 5 sont d'ordre 2, en effet $3^2 \equiv 1$ [8] etc.. Ainsi, $\boxed{\lambda(8) = 2.}$

20. Soit $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$.

• Sur $[\![1, p]\!]$, tous les nombres, excepté p, sont premiers avec p, donc $\varphi(p) = p - 1$.

• Sur $[\![1, p^\alpha]\!]$, les nombres premiers avec p sont ceux qui ne sont pas divisible par p puisque p est premier. Or il y a $\left\lfloor \dfrac{p^\alpha}{p} \right\rfloor = p^{\alpha-1}$ nombres divisibles par p. Donc, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Ainsi, $\boxed{\text{pour tout } p \in \mathbb{P} \text{ et } \alpha \in \mathbb{N}^*, \quad \varphi(p^\alpha) = p^{\alpha-1}(p-1).}$

21. Soit $n, m \in \mathbb{N}^*$ premiers entre eux. D'après 15), $U(\mathbb{Z}/nm\mathbb{Z})$ et $U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$ sont équipotents donc

$$\mathrm{Card}\big(U(\mathbb{Z}/nm\mathbb{Z})\big) = \mathrm{Card}\big(U(\mathbb{Z}/n\mathbb{Z})\big) \times \mathrm{Card}\big(U(\mathbb{Z}/m\mathbb{Z})\big) \text{ et donc } \varphi(nm) = \varphi(n)\varphi(m)$$

Ainsi, $\boxed{\varphi \text{ est } \textbf{multiplicative}.}$

22. Considérant la décomposition en facteurs premiers de n, il vient :

$$\boxed{n = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \Rightarrow \quad \varphi(n) = \prod_{i=1}^{k} \varphi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)}$$

Remarque – En particulier, dans le schéma RSA, $n = pq$ est le produit de deux nombres premiers. Alors $\varphi(n) = (p-1)(q-1)$.