25

Les anneaux $\mathbb{Z}/n\mathbb{Z}$

25.1 Congruences dans $\mathbb{Z}$. Anneaux $\mathbb{Z}/n\mathbb{Z}$

On rappelle que si n est un entier naturel et a, b deux entiers relatifs, on dit que a et b sont congrus modulo n, si $b - a$ est un multiple de n, ce qui se note $a \equiv b \ \ (n)$ (voir le paragraphe 23.2).

Cette relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ et pour tout entier relatif a, on note :

$$\begin{aligned}\overline{a} &= \{b \in \mathbb{Z} \mid b \equiv a \ \ (n)\} = \{b \in \mathbb{Z} \mid n \text{ divise } b - a\} \\ &= \{b = a + qn \mid q \in \mathbb{Z}\} = a + n\mathbb{Z}\end{aligned}$$

sa classe d'équivalence modulo n.

L'ensemble de toutes ces classes d'équivalence modulo n est noté $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. C'est l'ensemble quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$. On dit aussi que c'est l'ensemble des classes résiduelles modulo n.

Pour simplifier, on note :

$$\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{a} \mid a \in \mathbb{Z}\}.$$

Dans le cas particulier où $n = 0$, la congruence modulo 0 est tout simplement la relation d'égalité et pour tout entier relatif a, on a :

$$\overline{a} = a + 0\mathbb{Z} = \{a\}$$

de sorte que :

$$\mathbb{Z}_0 = \{\{a\} \mid a \in \mathbb{Z}\}$$

est en bijection avec $\mathbb{Z}$. On identifie alors $\mathbb{Z}_0$ à $\mathbb{Z}$.

Dans le cas particulier où $n = 1$, deux entiers relatifs quelconques sont toujours congrus modulo 1 et pour tout entier relatif a, on a :

$$\overline{a} = a + \mathbb{Z} = \mathbb{Z}$$

de sorte que :

$$\mathbb{Z}_0 = \{\mathbb{Z}\} = \{\overline{0}\}$$

est identifié à $\{0\}$.

Théorème 25.1 *Pour tout entier naturel non nul n, on a :*

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

Cet ensemble est donc de cardinal égal à n et il est en bijection avec l'ensemble de tous les restes modulo n.

Démonstration. Le théorème de division euclidienne nous permet d'écrire tout entier relatif a sous la forme $a = qn + r$ avec $0 \leq r \leq n-1$, ce qui entraîne que $\overline{a} = \overline{r}$. On a donc $\mathbb{Z}_n = \left\{ \overline{0}, \overline{1}, \cdots, \overline{n-1} \right\}$. Pour montrer que cet ensemble est de cardinal égal à n, il nous reste à montrer que tous ses éléments sont distincts. Si $\overline{r} = \overline{s}$ avec r et s compris entre 0 et $n-1$, on a alors $s - r = qn$ avec $q \in \mathbb{Z}$ et l'encadrement $0 \leq |s-r| = |q| \, n \leq n-1$ dans $\mathbb{N}$ impose $q = 0$, ce qui équivaut à $r = s$. ■

Considérant qu'un anneau a au moins deux éléments et que $\mathbb{Z}_1 = \left\{ \overline{0} \right\}$, on suppose dans ce qui suit que $n \geq 2$.

La compatibilité de la relation de congruence modulo n avec l'addition et la multiplication sur $\mathbb{Z}$ (voir le paragraphe 23.2) va nous permettre de transporter la structure d'anneau de $\mathbb{Z}$ à $\mathbb{Z}_n$, un tel prolongement étant unique.

On désigne par π_n la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}_n$, c'est l'application qui associe à tout entier relatif sa classe modulo n.

Tout antécédent par π_n d'un élément x de $\mathbb{Z}_n$ est appelé un représentant de x.

Théorème 25.2 *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.*

Démonstration. 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 $b \in \mathbb{Z}$ un représentant de b. En effet, si a' est un autre représentant de x et b' un 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. ■

25.2 Groupes cycliques

L'entier n est toujours supposé au moins égal à 2.

Si G est un groupe ayant un nombre fini d'éléments son cardinal est appelé l'ordre de G.

On rappelle que si G est un groupe et a un élément de G, on définit alors le sous-groupe de G engendré par a par :

$$\langle a \rangle = \left\{ a^k \mid k \in \mathbb{Z} \right\}$$

dans le cas où la loi est notée multiplicativement ou :

$$\langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$$

dans le cas où la loi est notée additivement.

On dit que a est d'ordre fini dans G si ce groupe $\langle a \rangle$ est fini et l'ordre de a est alors l'ordre de $\langle a \rangle$ (voir le paragraphe 23.5.1).

Définition 25.1 *On dit qu'un groupe G est monogène s'il est engendré par l'un de ses éléments, c'est-à-dire s'il existe a dans G tel que $G = \langle a \rangle$. Un groupe monogène fini est dit cyclique.*

Remarque 25.1 *Un groupe cyclique est nécessairement commutatif.*

Remarque 25.2 *Un groupe cyclique engendré par un élément $a \neq 1$ (le neutre de G) a au moins deux élément, 1 et a.*

Exemple 25.1 *Tout élément x de $\mathbb{Z}_n$ s'écrivant :*

$$x = \overline{k} = \underbrace{\overline{1} + \cdots + \overline{1}}_{k \text{ fois}} = k\overline{1}$$

avec $\overline{k} = \overline{0}$ si, et seulement si, k est multiple de n. Il en résulte que $(\mathbb{Z}_n, +)$ est un groupe cyclique d'ordre (ou de cardinal) n. En fait, à isomorphisme près, c'est le seul.

Exemple 25.2 *Le groupe :*

$$\left\langle e^{\frac{2i\pi}{n}} \right\rangle = \left\{ e^{\frac{2ik\pi}{n}} \mid 0 \leq k \leq n-1 \right\}$$

des racines n-ièmes de l'unité est cyclique d'ordre n.

Exemple 25.3 *Si θ est un réel tel que $\dfrac{\theta}{2\pi}$ n'est pas rationnel, alors le groupe :*

$$\left\langle e^{i\theta} \right\rangle = \left\{ e^{ik\theta} \mid k \in \mathbb{Z} \right\}$$

est monogène infini puisque $e^{ik\theta} \neq 1$ pour tout $k \in \mathbb{Z}$.

Théorème 25.3 *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}_n$.*

Démonstration. Soit $G = \langle a \rangle = \{1, a, a^2, \cdots, a^{n-1}\}$ un groupe cyclique d'ordre n. L'application $\varphi_a : k \mapsto a^k$ réalise un morphisme surjectif de groupes de $(\mathbb{Z}, +)$ sur $(G, \cdot)$ de noyau $\ker(\varphi_a) = n\mathbb{Z}$ (par définition de l'ordre de a).

Si j, k sont deux entiers relatifs tels que $j \equiv k \ (n)$ on a alors $k - j = qn$ et $a^k = a^j a^{qn} = a^j$. On peut donc définir l'application $\overline{\varphi_a}$ de $\mathbb{Z}_n$ dans G par $\overline{\varphi_a} : \overline{k} \mapsto a^k$.

On vérifie facilement que $\overline{\varphi_a}$ est un morphisme de groupes surjectif de $(\mathbb{Z}_n, +)$ sur $(G, \cdot)$ de noyau $\ker(\overline{\varphi_a}) = \left\{\overline{0}\right\}$. Cette application réalise donc un isomorphisme de groupes de $(\mathbb{Z}_n, +)$ sur $(G, \cdot)$. ■

Dans le cas où n est premier, on a le résultat plus précis suivant qui est une conséquence du théorème de Lagrange (théorème 20.9).

Théorème 25.4 *Soit p un nombre premier. Tout groupe G d'ordre p est cyclique, donc isomorphe à $\mathbb{Z}_p$.*

Démonstration. Tout élément de $G \setminus \{1\}$ est d'ordre p (puisque son ordre divise p et est différent de 1), il en résulte que G est cyclique d'ordre p, donc isomorphe à $\mathbb{Z}_p$. ■

Le résultat qui suit nous dit que les sous groupes d'un groupe cyclique sont cycliques.

Théorème 25.5 *Tous les sous groupes de $\mathbb{Z}_n$ sont cycliques d'ordre qui divise n. Réciproquement pour tout diviseur d de n, il existe un unique sous groupe de G d'ordre d, c'est le groupe cyclique engendré par $q = \frac{n}{d}$:*

$$H = \langle \overline{q} \rangle = \left\{ \overline{0}, \overline{q}, \cdots, (d-1)\,\overline{q} \right\}.$$

Démonstration. 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 $q = \frac{n}{d}$.

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 $H \subset \langle \overline{q} \rangle$, ce qui entraîne 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 d'ordre 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, $q = \frac{n}{d}$ 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 $\langle \overline{q} \rangle$. ■

25.3 Fonction indicatrice d'Euler

Définition 25.2 *On dit qu'un élément $\overline{a}$ de $\mathbb{Z}_n$ est inversible s'il existe $\overline{b}$ dans $\mathbb{Z}_n$ tel que $\overline{a}\overline{b} = \overline{1}$.*

On note $\mathbb{Z}_n^*$ l'ensemble des éléments inversibles de $\mathbb{Z}_n$. C'est un groupe pour la loi multiplicative.

Théorème 25.6 *Soit a un entier relatif. Les propriétés suivantes sont équivalentes :*

1. *$\overline{a}$ est inversible dans $\mathbb{Z}_n$;*
2. *a est premier avec n ;*
3. *$\overline{a}$ est un générateur de $(\mathbb{Z}_n, +)$.*

Démonstration. 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 $\mathbb{Z}_n$. ■

Définition 25.3 *On appelle fonction indicatrice d'Euler la fonction qui associe à tout entier naturel non nul n, le nombre, noté $\varphi(n)$, d'entiers compris entre 1 et n qui sont premiers avec n.*

Le théorème précédent nous dit que pour tout entier $n \geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe cyclique $(\mathbb{Z}_n, +)$ (ou de n'importe quel groupe cyclique d'ordre n) ou encore que c'est le nombre d'éléments inversibles de $\mathbb{Z}_n$.

Du théorème de Lagrange, on déduit immédiatement le résultat suivant.

Théorème 25.7 (Euler) *Pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1 \ (n)$.*

Démonstration. Si a est premier avec n, alors $\overline{a}$ appartient à $\mathbb{Z}_n^*$ 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 $a^{\varphi(n)} \equiv 1 \ (n)$. ■

Si n est premier, alors tout entier compris entre 1 et $n-1$ est premier avec n, ce qui implique que $\varphi(n) = n - 1$ et le théorème d'Euler devient le petit théorème de Fermat.

Théorème 25.8 (Fermat) *Soit p un entier naturel premier. Pour tout entier relatif a on a :*

$$a^p \equiv a \ (p).$$

Démonstration. Le théorème d'Euler nous dit que $a^{p-1} \equiv 1 \ (p)$ si a est premier avec n, c'est-à-dire si a n'est pas multiple de p, ce qui entraîne $a^p \equiv a \ (p)$. Pour a multiple de p, on a $a^p \equiv a \equiv 0 \ (p)$. ■

La réciproque de ce théorème est fausse comme nous le montrera l'étude des nombres de Carmichaël au paragraphe **??**. Par exemple on a $a^{561} \equiv a \ (561)$ pour tout entier relatif a avec $561 = 3 \cdot 11 \cdot 17$ non premier.

Le théorème de Fermat peut être utilisé pour calculer des congruences avec des grands nombres. Si p est un nombre premier impair, n, m deux entiers naturels, l'entier n n'étant pas multiple de p, en effectuant les divisions euclidiennes par p et par $p-1$, on $n = qp + r$, $m = q'(p-1) + s$ avec $1 \leq r \leq p-1$, $0 \leq s \leq p-2$ et :

$$n^m \equiv r^s \ (p)$$

Par exemple on a $2003^{2003} \equiv 4 \ (5)$. En effet $2003 = 5 \cdot 400 + 3$ et $2003 = 4 \cdot 500 + 3$.

Dans le cas où n est premier tous les éléments de $\mathbb{Z}_n \setminus \{\overline{0}\}$ sont inversibles et en conséquence $\mathbb{Z}_n$ est un corps. En fait on a le résultat plus précis suivant.

Théorème 25.9 *Pour $n \geq 2$ il y équivalence entre :*

1. *n est premier ;*
2. *$\mathbb{Z}_n$ est un corps ;*
3. *$\mathbb{Z}_n$ est un intègre.*

Démonstration. On vient de voir que pour n premier $\mathbb{Z}_n$ est un corps.

De manière générale, tout corps est intègre.

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

Remarque 25.3 *L'implication* $(3) \Rightarrow (2)$ *est aussi conséquence du fait que tout anneau unitaire fini et intègre est un corps (théorème de Wedderburn). Si A est un anneau fini intègre, alors pour tout $a \in A \setminus \{0\}$ l'application $x \mapsto ax$ est injective de A dans A, donc bijective, ce qui entraîne l'existence de $a' \in A$ tel que $aa' = e$ (e est le neutre pour la multiplication).*

Ce résultat nous permet de retrouver le petit théorème de Fermat.

On peut également en déduire le théorème de Wilson.

Théorème 25.10 (Wilson) *Un entier n est premier si et seulement si* $(n-1)! \equiv -1 \ (n)$.

Démonstration. Si n est premier alors $\mathbb{Z}_n$ est un corps commutatif et tout élément $\overline{k}$ de $\mathbb{Z}_n^*$ est racine du polynôme $X^{n-1}-\overline{1}$, on a 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 $-\overline{1}=\prod_{k=1}^{n-1}\left(-\overline{k}\right)=(-1)^{n-1}\overline{(n-1)!}$. Pour $n=2$, on a $-\overline{1}=\overline{1}$ et pour $n\geq 2$ premier on a n impair et $-\overline{1}=\overline{(n-1)!}$ dans $\mathbb{Z}_n$.

Réciproquement 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 donne $d=1$ et l'entier n est premier. ∎

Le calcul de $\varphi(n)$ pour $n\geq 2$ peut se faire en utilisant la décomposition de n en facteurs premiers grâce au théorème chinois.

Théorème 25.11 (chinois) *Les entiers n et m sont premiers entre eux si, et seulement si, les anneaux $\mathbb{Z}_{nm}$ et $\mathbb{Z}_n\times\mathbb{Z}_m$ sont isomorphes.*

Démonstration. Pour tout entier relatif k, on note $\overline{k}$ sa classe modulo nm, $\dot{k}$ sa classe modulo n et $\ddot{k}$ sa classe modulo m.

Le produit cartésien $\mathbb{Z}_n\times\mathbb{Z}_m$ est naturellement muni d'une structure d'anneau commutatif unitaire avec les lois $+$ et $\cdot$ définies par :

$$\left\{\begin{array}{l}\left(\dot{j},\ddot{k}\right)+\left(\dot{j'},\ddot{k'}\right)=\left(j\dot{+}j',k\ddot{+}k'\right)\\ \left(\dot{j},\ddot{k}\right)\cdot\left(\dot{j'},\ddot{k'}\right)=\left(j\dot{\cdot}j',k\ddot{\cdot}k'\right)\end{array}\right.$$

Supposons n et m premiers entre eux. L'application $\varphi:k\mapsto\left(\dot{k},\ddot{k}\right)$ est un morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}_n\times\mathbb{Z}_m$ et son noyau est formé des entiers divisibles par n et m donc par nm puisque ces entiers sont premiers entre eux, il se factorise donc en un morphisme injectif d'anneaux de $\mathbb{Z}_{nm}$ dans $\mathbb{Z}_n\times\mathbb{Z}_m$ par $\overline{\varphi}:\overline{k}\mapsto\left(\dot{k},\ddot{k}\right)$. Ces deux anneaux ayant même cardinal, l'application $\overline{\varphi}$ réalise en fait un isomorphisme d'anneaux de $\mathbb{Z}_{nm}$ dans $\mathbb{Z}_n\times\mathbb{Z}_m$.

Si n et m ne sont pas premiers entre eux les groupes additifs $\mathbb{Z}_{nm}$ et $\mathbb{Z}_n\times\mathbb{Z}_m$ ne peuvent être isomorphes puisque $\overline{1}$ est d'ordre nm dans $\mathbb{Z}_{nm}$ et tous les éléments de $\mathbb{Z}_n\times\mathbb{Z}_m$ ont un ordre qui divise le ppcm de n et m qui est strictement inférieur à nm. ∎

Corollaire 25.1 *Si n et m sont deux entiers naturels non nuls premiers entre eux, alors $\varphi(nm)=\varphi(n)\varphi(m)$.*

Démonstration. On utilise les notations de la démonstration précédente.

La restriction de l'isomorphisme $\overline{\varphi}$ à $\mathbb{Z}_{nm}^*$ réalise un isomorphisme de groupes multiplicatifs de $\mathbb{Z}_{nm}^*$ sur $\mathbb{Z}_n^*\times\mathbb{Z}_m^*$, ce qui entraîne :

$$\varphi(nm)=\operatorname{card}\left(\mathbb{Z}_{nm}^*\right)=\operatorname{card}\left(\mathbb{Z}_n^*\right)\operatorname{card}\left(\mathbb{Z}_m^*\right)=\varphi(n)\varphi(m).$$

∎

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.

Lemme 25.1 *Soient p un nombre premier et α un entier naturel non nul. On a :*

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

Démonstration. 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 :

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

■

Théorème 25.12 *Si $n \geq 1$ 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, alors :*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right).$$

Démonstration. En utilisant les résultats précédents, on a :

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} \varphi(p^{\alpha_i}) = \prod_{i=1}^{r} (p_i - 1)\, p_i^{\alpha_i - 1} = n \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right).$$

■

De ce résultat on déduit que pour tout $n \geq 3$, $\varphi(n)$ est un entier 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 (ce qui se voit aussi avec la définition). En fait on a le résultat plus précis suivant.

Théorème 25.13 *Pour tout entier $n \geq 2$, on a :*

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

Démonstration. L'inégalité $\varphi(n) < n$ est une conséquence immédiate de la définition.

Pour montrer l'autre inégalité on procède en plusieurs étapes.

On s'intéresse d'abord aux valeurs n comprises entre 2 et 7. Pour ces valeurs, on a $\varphi(2) = 1 > \sqrt{2} - 1$, $\varphi(5) = 4 > \sqrt{5} - 1$ et $\varphi(3) = \varphi(4) = \varphi(6) = 2 > \sqrt{k} - 1$ pour $k = 3, 4, 6$.

On s'intéresse ensuite aux entiers de la forme $n = \prod_{i=1}^{r} p_i$ avec $3 \leq p_1 < \cdots < p_r$ premiers. Dans ce cas, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = \prod_{i=1}^{r} \frac{p_i - 1}{\sqrt{p_i}}.$$

Pour $p \geq 3$, on a $p(p-3) \geq 0$, soit $p^2 - 3p + 1 > 0$ ou encore $(p-1)^2 p$, c'est-à-dire $p - 1 > \sqrt{p}$. On en déduit donc que $\varphi(n) > \sqrt{n}$.

Considérons le cas de n impair supérieur ou égal à 7. Il s'écrit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $3 \leq p_1 < \cdots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r. En posant $m = \prod_{i=1}^{r} p_i$, on a :

$$\varphi(n) = \frac{n}{m} \prod_{i=1}^{r} \varphi(p_i) = \frac{n}{m}\varphi(m)$$

et :

$$\frac{\varphi(n)}{\sqrt{n}} = \sqrt{\frac{n}{m}}\frac{\varphi(m)}{\sqrt{m}} \geq \frac{\varphi(m)}{\sqrt{m}} > 1,$$

ce qui donne $\varphi(n) > \sqrt{n}$.

Pour $n = 2^\alpha$ avec $\alpha \geq 3$, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = 2^{\frac{\alpha}{2}-1} = \left(\sqrt{2}\right)^{\alpha-2} > 1$$

et $\varphi(n) > \sqrt{n}$.

Pour $n = 2^\alpha 3^\beta$ avec $\alpha \geq 1$, $\beta \geq 1$ et $(\alpha, \beta) \neq (1, 1)$, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = 2^{\frac{\alpha}{2}} 3^{\frac{\beta}{2}-1} = \left(\sqrt{2}\right)^{\alpha} \left(\sqrt{3}\right)^{\beta-2} > 1$$

(pour $\beta \geq 2$ il n'y a pas de problème et pour $\beta = 1$ on a $\alpha \geq 2$ et $\left(\sqrt{2}\right)^{\alpha} \left(\sqrt{3}\right)^{-1} \geq \dfrac{2}{\sqrt{3}} > 1$), ce qui donne $\varphi(n) > \sqrt{n}$.

Enfin, si n est pair supérieur ou égal à 7, il s'écrit $n = 2^{\alpha_1} \prod\limits_{i=2}^{r} p_i^{\alpha_i}$ avec $3 \leq p_2 < \cdots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r. En posant $m = 2 \prod\limits_{i=2}^{r} p_i$, on a : :

$$\frac{\varphi(n)}{\sqrt{n}} = \sqrt{\frac{n}{m}}\frac{\varphi(m)}{\sqrt{m}} \geq \frac{\varphi(m)}{\sqrt{m}},$$

avec :

$$\frac{\varphi(m)}{\sqrt{m}} = \frac{1}{\sqrt{2}} \prod_{i=2}^{r} \frac{p_i - 1}{\sqrt{p_i}}.$$

Pour $p \geq 3$, on a $\dfrac{p-1}{\sqrt{p}} > 1$, donc $\dfrac{\varphi(m)}{\sqrt{m}} > \dfrac{p_2 - 1}{\sqrt{2}\sqrt{p_2}}$ et pour $p_2 \geq 5$, on a $\dfrac{p_2 - 1}{\sqrt{2}\sqrt{p_2}} > 1$. Il reste à étudier le cas $p_2 = 3$, soit $n = 2^{\alpha_1} 3^{\alpha_2} r$, avec $r = \prod\limits_{i=3}^{r} p_i^{\alpha_i}$ où $5 \leq p_3 < \cdots < p_r$ sont premiers. Dans ce cas, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = \frac{\varphi\left(2^{\alpha_1} 3^{\alpha_2}\right)}{\sqrt{2^{\alpha_1} 3^{\alpha_2}}} \frac{\varphi(r)}{\sqrt{r}} > 1$$

d'après ce qui précède.

On a donc ainsi montré que $\varphi(n) > \sqrt{n}$ pour tout $n \geq 7$. ∎