La fonction indicatrice d'Euler

Marc Lorenzi

26 décembre 2025

Définition 1. La *fonction indicatrice d'Euler* est la fonction $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ définie par $\varphi(n) = |\Phi(n)|$ où

$$\Phi(n) = \{a \in [\![0, n-1]\!] : a \wedge n = 1\}$$

Voici les premières valeurs de $\varphi(n)$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

Proposition 1. *Pour tout nombre premier p et tout entier non nul α,*

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

Démonstration. Soit p un nombre premier. Soit $\alpha \in \mathbb{N}^*$. Soit $a \in [\![0, p^\alpha - 1]\!]$. On a

$$\begin{aligned} a \in \Phi(p^\alpha) &\iff a \wedge p^\alpha = 1 \\ &\iff a \wedge p = 1 \\ &\iff a \text{ n'est pas multiple de } p \\ &\iff a \notin \{kp : k \in [\![0, p^{\alpha-1} - 1]\!]\} \end{aligned}$$

Le cardinal de ce dernier ensemble est $p^{\alpha-1}$, d'où le résultat. □

Soient $m, n \in \mathbb{N}^*$ deux entiers premiers entre eux. Soit $a \in \Phi(mn)$. L'entier a est premier avec mn, donc avec m et n. Comme a est premier avec m, le reste $a \bmod m$ de la division euclidienne de a par m est aussi premier avec m. De même, $a \bmod n$ est premier avec n.

Considérons la fonction $f : \Phi(mn) \longrightarrow \Phi(m) \times \Phi(n)$ définie par

$$f(a) = (a \bmod m, a \bmod n)$$

Proposition 2. *La fonction f est bijective.*

Démonstration. Soient $a, a' \in \Phi(mn)$. Supposons que $f(a) = f(a')$. On a $a \bmod m = a' \bmod m$ et $a \bmod n = a' \bmod n$. On en déduit que m et n divisent $a' - a$. Or, m et n sont premiers entre eux, donc mn divise $a' - a$. Remarquons que $|a' - a| < mn$ pour en déduire $a = a'$. Ainsi, f est injective.

Soient $x \in \Phi(m)$ et $y \in \Phi(n)$. Comme m et n sont premiers entre eux, le théorème de Bézout affirme l'existence de $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. Posons

$$a = (umy + vnx) \bmod mn$$

On a $a \equiv vnx \bmod m$. Or, $vn = 1 - um \equiv 1 \bmod m$, donc $a \equiv x \bmod m$. De même, $a \equiv y \bmod n$. Comme x est premier avec m, a l'est aussi. De même, a est premier avec n et donc a est premier avec mn. Ainsi, $a \in \Phi(mn)$ et $f(a) = (x, y)$. La fonction f est donc surjective. □

Proposition 3. *La fonction φ est* multiplicative *: pour tous $m, n \in \mathbb{N}^*$,*

$$m \wedge n = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$$

Démonstration. Soient $m, n \in \mathbb{N}^*$ premiers entre eux. La fonction $f : \Phi(mn) \longrightarrow \Phi(m) \times \Phi(n)$ de la proposition précédente est bijective, donc

$$\varphi(mn) = |\Phi(mn)| = |\Phi(m) \times \Phi(n)| = |\Phi(m)| \times |\Phi(n)| = \varphi(m)\varphi(n)$$

□

Corollaire 4. *Soit $r \in \mathbb{N}^*$. Soient $n_1, \ldots, n_r$ des entiers non nuls premiers entre eux deux à deux. On a*

$$\varphi\left(\prod_{k=1}^{r} n_k\right) = \prod_{k=1}^{r} \varphi(n_k)$$

Démonstration. Raisonnons par récurrence sur r. Le résultat est immédiat pour $r = 1$. Soit $r \in \mathbb{N}^*$. Supposons la propriété vérifiée par r. Soient $n_1, \ldots, n_{r+1}$ des entiers non nuls premiers entre eux deux à deux. L'entier n_{r+1} est premier avec $n_1, \ldots, n_r$ donc aussi avec leur produit. De là,

$$\varphi(n_1 \ldots n_{r+1}) = \varphi(n_1 \ldots n_r)\varphi(n_{r+1})$$

On termine avec l'hypothèse de récurrence. □

Proposition 5. *Soit $n \in \mathbb{N}^*$. Écrivons*

$$n = \prod_{k=1}^{r} p_k^{\alpha_k}$$

où $r \in \mathbb{N}$, les p_k sont des nombres premiers distincts et les α_k sont des entiers naturels non nuls. On a

$$\varphi(n) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$$

Démonstration. Les $p_k^{\alpha_k}$ sont premiers entre eux deux à deux. Par le corollaire 4,

$$\varphi(n) = \prod_{k=1}^{r} \varphi(p_k^{\alpha_k})$$

Appliquons maintenant la proposition 1.

$$\varphi(n) = \prod_{k=1}^{r} (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = \prod_{k=1}^{r} p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$$

□