# La fonction indicatrice d'Euler

## Rappels et notations

Soit $n$ un entier strictement positif.

- Pour tous $x, y$ de $\mathbb{Z}$, on note $x \equiv y\ [n]$ (et on dit que "$x$ est congru à $y$ modulo $n$") si l'une des conditions équivalentes suivantes est réalisée :
  - L'entier $n$ divise la différence $x - y$.
  - Il existe $k$ dans $\mathbb{Z}$ tel que $y = x + kn$.
  - Les entiers $x$ et $y$ ont le même reste dans la division par $n$.
- La relation $x \equiv y\ [n]$ est une relation d'équivalence sur $\mathbb{Z}$.
  On note $\overline{x} = \{x + kn,\ k \in \mathbb{Z}\}$ la classe d'équivalence d'un élément $x$ de $\mathbb{Z}$.
  On note $\mathbb{Z}_n$ l'ensemble de toutes les classes d'équivalence.
  L'ensemble $\mathbb{Z}_n$ est de cardinal $n$. Plus précisément $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.
- On définit deux lois sur $\mathbb{Z}_n$ en posant : $\forall\,(x, y) \in \mathbb{Z},\ \overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x}\,\overline{y} = \overline{xy}$.
  Muni de ces deux lois, $\mathbb{Z}_n$ possède une structure d'anneau commutatif.
  On note $U_n$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}$.
- On note $\varphi(n)$ le nombre d'entiers de $\{1, \ldots, n\}$ qui sont premiers avec $n$.
  L'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est appelée indicateur d'Euler.
- On note $m \wedge n$ (resp. $m \vee n$) le *plus grand commun diviseur* (resp. *le plus petit commun multiple*) de deux entiers $m$ et $n$.

## Énoncé

1. Soit $p$ un nombre premier.
   (a) Préciser la valeur de $\varphi(p)$.
   (b) Pour tout entier $m \geqslant 1$, montrer que $\varphi(p^m) = p^m - p^{m-1}$.
2. (a) Soit $a$ un entier relatif. Montrer que $\overline{a} \in U_n \Leftrightarrow a \wedge n = 1$.
   Il en résulte que $\varphi(n)$ est l'ordre (le cardinal) du groupe $U_n$.
   (b) Soit $a$ un entier relatif, premier avec $n$. Montrer que $a^{\varphi(n)} \equiv 1\ [n]$.
   On donnera deux démonstrations de ce résultat :
   — La première en utilisant l'ordre de $\overline{a}$ dans la groupe $U_n$.
   — La seconde en justifiant que l'application $\overline{x} \mapsto \overline{a}\,\overline{x}$ est une bijection de $U_n$.
   Quel résultat obtient-on quand $n$ est un entier premier ?
   (c) Montrer que pour tout $n \geqslant 3$, $\varphi(n)$ est un entier pair.
3. On suppose $n \geqslant 2$. Montrer que les trois conditions suivantes sont équivalentes :
   L'entier $n$ est premier ; L'anneau $\mathbb{Z}_n$ est un corps ; L'anneau $\mathbb{Z}_n$ est intègre.

4. On se donne deux entiers $a$ et $b$ au hasard dans $\{1,\dots,n\}$.

   Montrer que la probabilité pour que $a\wedge b=1$ est $p_n=\frac{1}{n^2}\left(2\sum_{k=1}^{n}\varphi(k)-1\right)$.

   On admet que $\lim\limits_{n\to+\infty}p_n=\frac{6}{\pi^2}$. On peut interpréter ce résultat en disant que la probabilité pour que deux entiers $a,b$ choisis au hasard soient premiers entre eux est $\frac{6}{\pi^2}$.

5. Dans cette question, $m$ et $n$ sont deux éléments de $\mathbb{N}^*$, premiers entre eux.
   On note $u$ et $v$ deux entiers relatifs tels que $um+vn=1$.
   Pour tout $x$ de $\mathbb{Z}$, on note $\overline{x}$ la classe de $x$ modulo $mn$ (c'est-à-dire l'élément correspondant dans l'ensemble $\mathbb{Z}_{mn}$), $\widehat{x}$ la classe de $x$ modulo $m$, et $\widetilde{x}$ la classe de $x$ modulo $n$.

   (a) Montrer qu'on définit une application $\psi$ de $\mathbb{Z}_{mn}$ dans $\mathbb{Z}_m\times\mathbb{Z}_n$ en posant, pour tout entier relatif $x$, $\psi(\overline{x})=(\widehat{x},\widetilde{x})$.

   (b) Montrer que l'application $\psi$ est un isomorphisme d'anneaux.

   (c) Pour tout $(\widehat{y},\widetilde{z})$ de $U_m\times U_n$, montrer que $\psi^{-1}(\widehat{y},\widetilde{z})=\overline{x}$, avec $x=umz+vny$.

   (d) Montrer que la restriction de $\psi$ à $U_{mn}$ est une bijection de $U_{mn}$ sur $U_m\times U_n$.

   (e) En déduire l'égalité $\varphi(mn)=\varphi(m)\varphi(n)$.

6. Pour tout $n\geqslant 1$, on note $\mathbb{P}_n$ l'ensemble des diviseurs premiers de $n$ (en particulier $\mathbb{P}_1=\emptyset$).

   (a) Montrer que $\mathbb{P}_m\cap\mathbb{P}_n=\mathbb{P}_{m\wedge n}$ et $\mathbb{P}_m\cup\mathbb{P}_n=\mathbb{P}_{m\vee n}=\mathbb{P}_{mn}$.
   Que dire de $\mathbb{P}_m$ et $\mathbb{P}_n$ si $m$ et $n$ sont premiers entre eux ?

   (b) Pour tout $n\geqslant 1$, montrer que $\varphi(n)=n\prod\limits_{p\in\mathbb{P}_n}\left(1-\frac{1}{p}\right)$. Calculer $\varphi(10!)$.

   (c) Pour tous entiers $m,n\geqslant 1$, montrer que $\varphi(m)\varphi(n)\leqslant\varphi(mn)$, et qu'il n'y a égalité que lorsque $m$ et $n$ sont premiers entre eux.

7. Dans cette question, on se donne $m$ et $n$ dans $\mathbb{N}^*$.

   (a) Montrer que si $m$ divise $n$, alors $\varphi(m)$ divise $\varphi(n)$.

   (b) Montrer $\varphi(m)\vee\varphi(n)$ divise $\varphi(m\vee n)$ et que que $\varphi(m\wedge n)$ divise $\varphi(m)\wedge\varphi(n)$.

8. Dans cette question, on se donne $n$ dans $\mathbb{N}^*$. On note $\mathcal{D}_n$ l'ensemble des diviseurs de $n$.

   (a) On considère l'application $f:\{1,\dots,n\}\to\mathcal{D}_n$ définie par $f(k)=n\wedge k$.
   Montrer que chaque $d$ de $\mathcal{D}_n$ possède exactement $\varphi(\frac{n}{d})$ antécédents par $f$.

   (b) En déduire l'égalité $\sum\limits_{d\in\mathcal{D}_n}\varphi(d)=n$.

   (c) Pour tout $k$ de $\mathbb{N}^*$, on définit $\mu(k)$ de la façon suivante :

   — Si $k$ est divisible par le carré d'au moins un entier premier, alors $\mu(k)=0$.

   — Sinon $\mu(k)=(-1)^m$ où $m$ est le nombre de diviseurs premiers de $k$.

   Prouver l'égalité : $\varphi(n)=\sum\limits_{d\in\mathcal{D}_n}\mu(d)\frac{n}{d}$.

   Indication : raisonner par récurrence sur le nombre de diviseurs premiers de $n$.