2

ETUDES

L'indicateur d'Euler

par Jean de BIASI, Université Paul Sabatier, Toulouse

n étant un naturel non nul, l'indicateur d'Euler de n, noté $\varphi(n)$, est le nombre des naturels inférieurs ou égaux à n et premiers avec n [par exemple : $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(10) = 4$...] P. Anglès, dans le Bulletin 302 (p. 145), détermine sa valeur en utilisant la formule du crible et une propriété de la fonction partie entière. Nous proposons ici deux autres méthodes de détermination de $\varphi(n)$, l'une probabiliste, l'autre basée sur un théorème d'isomorphisme dit *Théorème Chinois*. Nous donnons ensuite quelques propriétés de $\varphi(n)$.

Données :

$n \in \mathbf{N}_*$

$\mathcal{P}_n = \{p_1, p_2, \dots p_k\}$ = ensemble des facteurs premiers de n

$n = \prod_{p_i \in \mathcal{P}_n} p_i^{\alpha_i}$, $\alpha_i \in \mathbf{N}_*$

I) Détermination probabiliste de $\varphi(n)$

En munissant l'univers $\Omega = \{1,2,\dots, n\}$ de l'équiprobabilité [pour tout $j \in \Omega$, $P(j) = \frac{1}{n}$], $\frac{\varphi(n)}{n}$ représente la probabilité de tirer au hasard un naturel de Ω premier avec n. Soit E l'événement des naturels de Ω premiers avec n. Alors :

$E = \bigcap_{p_i \in \mathcal{P}_n} \overline{A_{p_i}}$ où $\overline{A_{p_i}} = \Omega \setminus A_{p_i}$ avec $A_{p_i} = \{ \lambda p_i / \lambda \in \mathbf{N}, \lambda p_i \in \Omega \}$

Si $n = hp_i$, on a $P(A_{p_i}) = \frac{h}{n}$ puisqu'il y a dans Ω h multiples de p_i inférieurs ou égaux à n ($1p_i$, $2p_i$, $3p_i$,... hp_i),d'où $P(A_{p_i}) = \frac{1}{p_i}$

Comme $A_{p_i} \cap A_{p_j}$ est l'ensemble des multiples de p_i et de p_j, donc de $p_i \cdot p_j$, on a

$$A_{p_i} \cap A_{p_j} = A_{p_i p_j}$$

et

$$P(A_{p_i} \cap A_{p_j}) = P(A_{p_i p_j})$$

$$= \frac{1}{p_i} \cdot \frac{1}{p_j} = P(A_{p_i}).P(A_{p_j})$$

(calcul analogue à celui de $P(A_{p_i})$)

Les événements A_{p_i} et A_{p_j} sont donc indépendants ; il en est alors de même pour leurs complémentaires (*) et par suite, de proche en proche, il vient ,

$$P(E) = \prod_{p_i \in \mathfrak{T}_n} P(\overline{A_{p_i}}) = \prod_{p_i \in \mathfrak{T}_n} [1 - P(A_{p_i})] = \prod_{p_i \in \mathfrak{T}_n} \left(1 - \frac{1}{p_i}\right)$$

d'où

$$\boxed{\varphi(n) = n \prod_{p_i \in \mathfrak{T}_n} \left(1 - \frac{1}{p_i}\right)} \qquad (1)$$

II) Détermination de $\varphi(n)$ à l'aide du Théorème Chinois

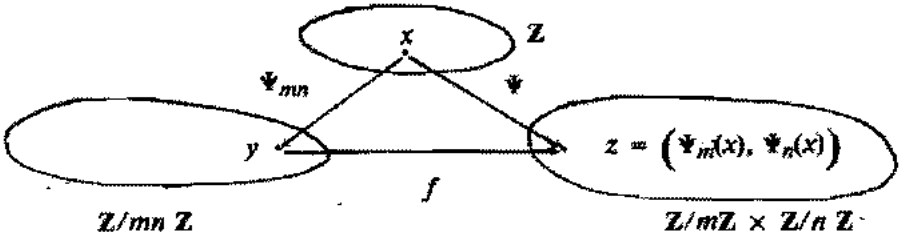
1) *Le Théorème Chinois*

Rappelons que, si n est un naturel quelconque non nul, l'ensemble $\mathbf{Z}/n\mathbf{Z}$ des classes résiduelles modulo n, muni de l'addition et de la multiplication induites par celles de $\mathbf{Z}$, est un anneau commutatif unitaire.

Soient alors :

- m, n deux naturels non nuls premiers entre eux.
- Ψ_m, Ψ_n, Ψ_{mn} les applications canoniques de $\mathbf{Z}$ respectivement dans $\mathbf{Z}/m\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Z}/mn\mathbf{Z}$.
- Ψ l'application canonique de $\mathbf{Z}$ dans l'anneau produit $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ (ensemble des couples de classes résiduelles respectivement modulo m et modulo n muni des lois induites par celles de $\mathbf{Z}/m\mathbf{Z}$ et de $\mathbf{Z}/n\mathbf{Z}$) c'est-à-dire l'application définie par

$$(\forall x)\left[x \in \mathbf{Z} \Rightarrow \Psi(x) = \left(\Psi_m(x), \Psi_n(x)\right)\right]$$



(*) Si $P(E_1 \cap E_2) = P(E_1) \times P(E_2)$, on a $P(\overline{E_1} \cap \overline{E_2}) = P(\overline{E_1 \cup E_2})$
$= 1 - P(E_1 \cup E_2) = 1 - [P(E_1) + P(E_2) - P(E_1 \cap E_2)] = [1 - P(E_1)][1 - P(E_2)]$
$= P(\overline{E_1}) \times P(\overline{E_2})$

Définissons une application f de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ en posant :

$$(\forall y)\left(y \in \mathbb{Z}/mn\mathbb{Z} \Rightarrow f(y) = \left(\psi_m(x), \psi_n(x)\right) \text{ avec } x \in \psi_{mn}^{-1}(y)\right)$$

f est bien une *application* car

si $\quad y = \psi_{mn}(x_1)$ et $y = \psi_{mn}(x_2)$, alors $x_1 - x_2 \in mn\mathbb{Z}$

d'où $\quad x_1 - x_2 \in m\mathbb{Z}$ et $x_1 - x_2 \in n\mathbb{Z}$

donc $\quad \psi_m(x_1) = \psi_m(x_2)$ et $\psi_n(x_1) = \psi_n(x_2)$.

f est un *morphisme de* $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (démonstration immédiate en revenant à la définition).

f est *injective* car

si $\quad f(y) = (0, 0)$, alors $y = \psi_{mn}(x)$ avec $\psi_m(x) = 0$ et $\psi_n(x) = 0$

d'où $\quad x \in m\mathbb{Z}$ et $x \in n\mathbb{Z}$

d'où $\quad x \in mn\mathbb{Z}$ (car $m \wedge n = 1$) et $\psi_{mn}(x) = 0 = y$. *

Comme de plus les ensembles $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont équipotents, f est aussi *surjective* et par suite est un *isomorphisme* entre ces deux anneaux.

D'où le

Théorème Chinois : Si m et n sont deux naturels non nuls premiers entre eux, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.

Remarque. Ce résultat s'étend à plus de 2 nombres premiers entre eux deux à deux.

2) *Détermination de* $\varphi(n)$

• $\varphi(n)$ est le nombre des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ puisque $\Psi_n(x)$ inversible dans $\mathbb{Z}/n\mathbb{Z}$ équivaut à l'existence de $x' \in \mathbb{Z}$ tel que

$\Psi_n(x)\,\Psi_n(x') = 1$ ou $\Psi_n(xx') = 1$ ou $xx' = 1 + \lambda n$ ou $x \wedge n = 1$

(d'après le théorème de Bezout).

• Par ailleurs, (u, v) inversible dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ équivaut à l'existence de (u', v') de cet anneau tel que $(uu', vv') = (1,1)$ c'est-à-dire $uu' = 1$ et $vv' = 1$ ou encore u et v inversibles (respectivement dans $\mathbb{Z}/m\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z}$).

• Grâce alors à l'isomorphisme défini par le Théorème Chinois, il vient

si $\quad m \wedge n = 1$ alors $\varphi(mn) = \varphi(m) \cdot \varphi(n)$

---

* $m \wedge n$ désigne ici le pgcd de m et n.

• Si p est premier, on a

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

car les nombres compris entre 1 et p^α et non premiers avec p sont p, $2p$, $3p$, ..., $p^{\alpha-1}p$. En appliquant alors de proche en proche le résultat précédent après avoir remarqué que si p_1, ..., p_k sont des nombres premiers deux à deux distincts, $p_1^{\alpha_1}$ est premier avec $\prod_2^k p_i^{\alpha_i}$ etc, on aboutit à

$$\varphi(n) = \varphi\left(\prod_1^k p_i^{\alpha_i}\right) = \prod_1^k p_i^{\alpha_i}\left(\prod_1^k\left(1 - \frac{1}{p_i}\right)\right) = n \prod_{p_i \in \mathcal{P}_n}\left(1 - \frac{1}{p_i}\right)$$

Remarque. Le résultat, $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ lorsque $m \wedge n = 1$, se généralise, en tenant compte, par exemple, de la valeur de $\varphi(n)$, sous la forme suivante :

$$\text{Si} \quad m \wedge n = d \quad \text{alors} \quad \varphi(mn) = \frac{d.\varphi(m).\varphi(n)}{\varphi(d)}$$

Quelques propriétés de $\varphi(n)$

1) *Somme des naturels inférieurs à n et premiers avec n*

Pour $n > 2$, $\varphi(n)$ est un nombre pair [dans l'expression précédente, il existe des facteurs du type $p_i - 1$ avec p_i premier impair si n n'est pas une puissance de 2; sinon, si $n = 2^\alpha$ ($\alpha > 1$) alors $\varphi(n) = 2^\alpha - 2^{\alpha-1} = 2^{\alpha-1}$] et par ailleurs,

$$\text{si} \quad k \wedge n = 1 \quad \text{et} \quad 1 \leqslant k < n,$$
$$\text{alors} \quad (n-k) \wedge n = 1 \quad \text{et} \quad 1 \leqslant n - k < n.$$

Par suite les nombres compris entre 1 et n et premiers avec n peuvent être regroupés en $\frac{\varphi(n)}{2}$ couples du type $(k, n-k)$. Leur somme vaut donc

$$(k + n - k)\frac{\varphi(n)}{2} = \frac{1}{2} n\,\varphi(n)$$

Proposition. *La somme des naturels inférieurs ou égaux à n et premiers avec n vaut $\frac{1}{2}n\varphi(n)$.*

2) *Somme des $\varphi(d)$ pour tous les d divisant n*

Soit $D(n) = \{d_1 = 1, d_2, \ldots, d_k, \ldots, d_n = n\}$ l'ensemble des diviseurs de n écrits dans l'ordre croissant. Effectuons une *partition* de l'intervalle de naturels $I_n = [1, n]$ en les sous-ensembles suivants :

$\{x \in I_n,\ x \wedge n = 1\}$ dont le cardinal est $\varphi(n)$

$\{x \in I_n,\ x \wedge n = d_2\}$ dont le cardinal est $\varphi\left(\frac{n}{d_2}\right)$ car à chaque x de ce type on

peut associer bijectivement $\frac{x}{d_2}$ tel que $\frac{x}{d_2} \wedge \frac{n}{d_2} = 1$

$\{x \in I_n,\ x \wedge n = d_k\}$ dont le cardinal est $\varphi\left(\frac{n}{d_k}\right)$

$\{x \in I_n,\ x \wedge n = n\}$ dont le cardinal est $1 = \varphi\left(\frac{n}{n}\right)$

Comme, lorsque d_k parcourt $D(n)$, $\frac{n}{d_k}$ le parcourt aussi (en sens inverse), on obtient la

Proposition. *La somme des $\varphi(d)$ étendue à tous les diviseurs d de n est égale à n.*

3) *Le théorème d'Euler*

Sachant que

- Si x est élément d'un groupe multiplicatif d'ordre r et d'élément unité 1, $x^r = 1$;
- un élément a de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a est premier avec n et que par suite le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre $\varphi(n)$, on obtient le

Théorème (d'Euler) *: Si a et n sont deux naturels premiers entre eux, alors*

$$a^{\varphi(n)} - 1 \equiv 0\ [n]$$

Remarque. Un cas particulier de ce résultat est le petit théorème de Fermat. En effet, si n est premier, $\varphi(n) = n - 1$ et dans ce cas :

$$a^{n-1} - 1 \equiv 0\ [n]$$