La fonction ϕ d'Euler

christina.boura@uvsq.fr

6 mars 2020

1 La fonction ϕ d'Euler

Un sous-ensemble important de $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des éléments qui ont un inverse multiplicatif modulo n. Ce sous-ensemble, qui forme un groupe, est noté $(\mathbb{Z}/n\mathbb{Z})^*$.

Définition 1.1. *Soit n un entier positif. Alors,*

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \text{pgcd}(a, n) = 1\}.$$

Théorème 1.2. *Soit p un nombre premier. Alors, $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots p-1\}$.*

Démonstration. Tous les entiers inférieurs à p sont relativement premiers avec lui. □

On s'intéresse au nombre d'éléments dans $(\mathbb{Z}/n\mathbb{Z})^* = \{0, 1, \ldots, n-1\}$, or cherche le nombre d'entiers qui sont premiers avec n. Comment peut-on determiner cela ?

Première approche : On peut calculer

$$\begin{aligned}
\text{pgcd}(0, n) &= n \\
\text{pgcd}(0, n) &= 1 \\
\ldots & \quad \ldots \\
\text{pgcd}(n-1, n) &= 1
\end{aligned}$$

et compter le nombre de résultats égaux à 1. On peut alors donner la définition suivante :

Définition 1.3 (La fonction ϕ d'Euler)**.** *Le nombre d'entiers de $\mathbb{Z}/n\mathbb{Z}$ qui sont relativement premiers avec n est noté $\phi(n)$.*

Exemple 1.4. *Soit $n = 6$ et $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Calculer $\phi(6)$.*

On calcule :

$$\begin{aligned}
\text{pgcd}(0, 6) &= 6 \\
\text{pgcd}(1, 6) &= 1 \\
\text{pgcd}(2, 6) &= 2 \\
\text{pgcd}(3, 6) &= 3 \\
\text{pgcd}(4, 6) &= 2 \\
\text{pgcd}(5, 6) &= 1
\end{aligned}$$

Donc $\phi(6) = 2$.

La problème de cette approche est qu'on ne peut pas appliquer cela a des nombres très grands.

Question : Comment calculer $\phi(n)$ pour n grand ?

Il existe une formule très simple pour calculer $\phi(n)$ qui nécessite la connaissance de la factorisation de n en nombres premiers.

Factorisation de n en nombres premiers Chaque entier peut etre ecrit comme le produit de nombres premiers :

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k},$$

$p_1, p_2, \ldots p_k$ sont des nombres premiers distincts. Cette décomposition est unique.

Exemple Soit $n = 280 = 4 \cdot 70 = 4 \cdot 2 \cdot 35 = 2^3 \cdot 5 \cdot 7 = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3}$.

Proposition 1.5. *Si $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, où p_i sont des nombres premiers distincts, nous avons*

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}).$$

En particulier, la fonction ϕ d'Euler vérifie les propriétés suivantes :

1. $\varphi(1) = 1$
2. *Pour tout p premier, et tout $e \geq 1$, $\phi(p^e) = p^e - p^{e-1}$.*
3. *Pour tout m, n tels que $\mathrm{pgcd}(m, n) = 1$, $\phi(mn) = \varphi(m)\varphi(n)$.*

Exemple 1.6. *Calculer :*

1. $\phi(7)$
2. $\phi(2583)$ *sachant que* $2583 = 3^2 \cdot 7 \cdot 41$.

Solution :

1. $\phi(7) = 7 - 1 = 6$
2. $\phi(m) = (3^2 - 3^1)(7^1 - 7^0)(41^1 - 41^0) = 6 \cdot 6 \cdot 40 = 1440$.