Indicatrice d'Euler

Pour tout $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers entre 1 et n et qui sont premiers avec n :

$$\varphi(n) = \text{Card}\{k \in [\![1, n]\!] \mid k \wedge n = 1\}$$

a) Soit $(a, b) \in \mathbb{N}^{*2}$ tq $a \wedge b = 1$, montrer que les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes

b) En déduire $\forall (a,b) \in (\mathbb{N}^*)^2 \quad (a \wedge b = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b))$

on dit que φ est une fonction arithmétique multiplicative

c) Soit p premier, montrer que

$$\forall r \in \mathbb{N}^* \quad \varphi(p^r) = p^r - p^{r-1}$$

d) En déduire que si $n \in \mathbb{N}^*$ admet une décomposition en facteurs premiers $n = \prod_{i=1}^{N} p_i^{r_i}$ alors $\varphi(n) = \prod_{i=1}^{N} (p_i^{r_i} - p_i^{r_i - 1}) = n \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right)$

Pour résoudre ce problème, on a besoin du théorème chinois

Soit $n \in \mathbb{N}^*$ $a_1, \dots a_n \in \mathbb{N}^*$ premiers entre eux 2 à 2.

$$a = \prod_{i=1}^{n} a_i$$

a) Démontrer que pour tout $(b_1, \dots b_n) \in \mathbb{Z}^n$, il existe $\beta \in \mathbb{Z}$ tq

$$\forall x \in \mathbb{Z} \left(\forall i \in [\![1, n]\!] \; x \equiv b_i (a_i) \Leftrightarrow x \equiv \beta (a) \right)$$

b) Pour tout $m \in \mathbb{N}^*$ et $x \in \mathbb{Z}$ on note $\text{cl}_m(x)$ la classe de x modulo m.

$$\text{cl}_m(x) = \{y \in \mathbb{Z} \mid m | y - x\} = x + m\mathbb{Z}$$

En déduire qu'il existe un isomorphisme de groupes

$$\Theta : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$$

$$\forall x \in \mathbb{Z} \quad \Theta(\text{cl}_a(x)) = (\text{cl}_{a_1}(x), \dots, \text{cl}_{a_n}(x))$$

preuve : a) Notons pour $i \in [\![1, n]\!]$ $A_i = \frac{a}{a_i}$

Pour $i \in [\![1, n]\!]$ comme $A_i \wedge a_i = 1$, d'après le th de Bézout

il existe $c_i \in \mathbb{Z}$ tq $A_i c_i = 1 \ (a_i)$

Notons $\beta = \sum_{i=1}^{n} A_i b_i c_i$

on a $\forall i \in [\![1, n]\!]$ $\beta \equiv A_i b_i c_i \ (a_i) \equiv b_i \ (a_i)$

b) Soit $\xi \in \mathbb{Z}/a\mathbb{Z}$. Il existe $x \in \mathbb{Z}$ tq $\xi = cl_a(x)$

posons $\theta(\xi) = (cl_{a_1}(x), \dots, cl_{a_n}(x))$

cette définition ne dépend pas de x car (rappelons-le)

$\forall (x,y) \in \mathbb{Z}^2$ $cl_a(x) = cl_a(y) \Rightarrow a \mid x-y$

$\Rightarrow \forall i \in [\![1, n]\!]$ $a_i \mid x-y$

$\Rightarrow \forall i \in [\![1, n]\!]$ $cl_{a_i}(x) = cl_{a_i}(y)$

- θ est un morphisme de groupes.

$\forall (x,y) \in \mathbb{Z}^2$ $\theta(cl_a(x) + cl_a(y)) = \theta(cl_a(x+y))$

$= \theta(cl_{a_1}(x+y), \dots, cl_{a_n}(x+y))$

$= \theta(cl_{a_1}(x) + cl_{a_1}(y), \dots, cl_{a_n}(x) + cl_{a_n}(y))$

$= \theta(cl_a(x)) + \theta(cl_a(y))$

- θ est injective

$\forall x \in \mathbb{Z}$ $\theta(cl_a(x)) = 0 \Rightarrow cl_{a_1}(x) = \dots = cl_{a_n}(x)$

$\Rightarrow \forall i \in [\![1, n]\!]$ $a_i \mid x$

$\Rightarrow a \mid x$

$\Rightarrow cl_a(x) = 0$

- θ est surjective.

Soit $(\xi_1, \dots, \xi_n) \in \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$

il existe $(b_1, \dots, b_n) \in \mathbb{Z}^n$

$\forall i \in [\![1, n]\!]$ $\xi_i = cl_{a_i}(b_i)$

d'après a) $\exists\, p \in \mathbb{Z}$ tq $\forall\, i \in [\![1, n]\!]$ $p \equiv b_i\ (a_i)$

on a alors $\theta(\mathrm{cl}_b(p)) = (\mathrm{cl}_{a_1}(p), \dots, \mathrm{cl}_{a_n}(p))$

$= (\mathrm{cl}_{a_1}(b_1), \dots, \mathrm{cl}_{a_n}(b_n)) = (\xi_1, \dots, \xi_n)$

Autre solution : θ est injective de $\mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$ finis de même cardinal, θ est bijective.

Revenons à l'indicatrice d'Euler.

a) d'après le théorème chinois, l'application

$\theta : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est canonique définie par

$\mathrm{cl}_{ab}(x) \longmapsto (\mathrm{cl}_a(x), \mathrm{cl}_b(x))$

est un isomorphisme de groupes additifs.

Montrons que c'est un isomorphisme d'anneaux !

- $\forall (x, y) \in \mathbb{Z}^2$ $\theta(\mathrm{cl}_{ab}(x)\,\mathrm{cl}_{ab}(y)) = \theta(\mathrm{cl}_{ab}(xy))$

$= (\mathrm{cl}_a(xy), \mathrm{cl}_b(xy))$

$= (\mathrm{cl}_a(x)\,\mathrm{cl}_a(y), \mathrm{cl}_b(x)\,\mathrm{cl}_b(y))$

$= (\mathrm{cl}_a(x), \mathrm{cl}_b(x))\,(\mathrm{cl}_a(y), \mathrm{cl}_b(y))$

$= \theta(\mathrm{cl}_{ab}(x))\,\theta(\mathrm{cl}_{ab}(y))$

- Étant neuf

$\theta(\mathrm{cl}_{ab}(1)) = (\mathrm{cl}_a(1), \mathrm{cl}_b(1))$

donc θ est un isomorphisme d'anneaux.

b) $\forall\, n \in \mathbb{N}^*$, U_n l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$

Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ tq $k \wedge n = 1$

$\varphi(n) = \mathrm{Card}\, U_n$

Comme θ est un isomorphisme d'anneaux

θ transporte les inversibles, c'est-à-dire

$\forall\, x \in \mathbb{Z}$ $\mathrm{cl}_{ab}(x)$ est inversible dans $\mathbb{Z}/ab\mathbb{Z}$ ssi

$(cl_a(x), cl_b(x))$ est inversible dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

ou a immédiatement que $\begin{cases} cl_a(x) \text{ est inversible dans } \mathbb{Z}/a\mathbb{Z} \\ cl_b(x) \text{ — dans } \mathbb{Z}/b\mathbb{Z} \end{cases}$

donc $\varphi(ab) \cdot \text{Card}(U_{ab}) = \text{Card}(U_a \times U_b)$

$= \text{Card } U_a \times \text{Card } U_b$

$= \varphi(a)\varphi(b)$

c) Comme p est premier on a $\forall n$ de $\{1, p, \dots p^r\}$

$n \wedge p^r \neq 1 \Leftrightarrow n \wedge p \neq 1 \Leftrightarrow p \mid n$

$\Leftrightarrow n \in \{kp, 1 \leq k \leq p^{r-1}\}$

d'où $\varphi(p^r) = p^r - \text{Card}\{kp, 1 \leq k \leq p^{r-1}\} = p^r - p^{r-1}$

d) Avec b) et avec une récurrence directe

si $a_1, \dots a_N$ sont des entiers premiers entre eux 2 à 2.

$$\varphi\left(\prod_{i=1}^{N} a_i\right) = \prod_{i=1}^{N} \varphi(a_i) = \prod_{i=1}^{N} \varphi(p_i^{r_i}) = \prod_{i=1}^{N} (p_i^{r_i} - p_i^{r_i-1})$$

$$= \prod_{i=1}^{N} p_i^{r_i}\left(1 - \frac{1}{p_i}\right)$$

$$= \prod_{i=1}^{N} p_i^{r_i} \prod_{i=1}^{N}\left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{N}\left(1 - \frac{1}{p_i}\right)$$

Théorème d'Euler

$$\forall n \in \mathbb{N}^* \quad \forall a \in \mathbb{Z}^* \quad \left(a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \ (n)\right)$$

Preuve : L'ensemble U_n des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un groupe multiplicatif de cardinal $\varphi(n)$

$$\forall \bar{y} \in \mathbb{Z}/n\mathbb{Z} \quad \bar{y}^{\varphi(n)} = \bar{1} \quad (*)$$

$$\forall a \in \mathbb{Z}^* \quad \left(a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \ (n)\right)$$

$\Leftarrow$ l'ordre de $\bar{a}$ divise $\varphi(n)$ donc $(\bar{a})^{\varphi(n)} = \bar{1}$ soit $a^{\varphi(n)} \equiv 1 \ (n)$

Quelques résultats

1) Montrer que $\forall (n,k) \in (\mathbb{N}^*)^2 \quad \varphi(n^k) = n^{k-1}\varphi(n)$

Sol Soit $n = \prod_{i=1}^{N} p_i^{r_i}$ décomposition en facteurs premiers de n.

$$\varphi(n^k) = \varphi\left(\prod_{i=1}^{N} p_i^{r_i k}\right) = \prod_{i=1}^{N}\left(p_i^{r_i k} - p_i^{r_i k - 1}\right)$$

$$= \left(\prod_{i=1}^{N} p_i^{r_i(k-1)}\right)\left(\prod_{i=1}^{N}\left(p_i^{r_i} - p_i^{r_i-1}\right)\right)$$

$$= n^{k-1}\varphi(n)$$

2) a) $\forall n \in \mathbb{N}^* \quad \sum_{d \mid n} \varphi(d) = n$

b) en déduire $\forall n \in \mathbb{N}^* \quad \sum_{k=1}^{n} \varepsilon\left(\frac{n}{k}\right)\varphi(k) = \frac{n(n+1)}{2}$

Sol : Soit $\mathrm{Div}(n)$ l'ensemble des diviseurs ≥ 1 de n.

Soit la relation $\mathcal{R}$ définie dans $\{1, \dots, n\}$ par

$$i \mathcal{R} j \iff i \wedge n = j \wedge n$$

c'est une relation d'équivalence.

Chaque classe modulo $\mathcal{R}$ contient un diviseur de n et un seul.

(la classe i contient $i \wedge n$)

D'où $n = \mathrm{card}(\{1, \dots, n\}) = \sum_{d \in \mathrm{Div}(n)} \mathrm{card}\left(cl_{\mathcal{R}}(d)\right)$

D'autre part, pour tout $d \in \mathrm{Div}(n)$, l'application

$k \longmapsto kd$ est une bijection de $\left\{k \in \{1, \dots, \frac{n}{d}\} \mid k \wedge \frac{n}{d} = 1\right\}$

sur $cl_{\mathcal{R}}(d)$

d'où $\mathrm{card}\left(cl_{\mathcal{R}}(d)\right) = \varphi\left(\frac{n}{d}\right)$

Ainsi : $n = \sum_{d \in \mathrm{Div}(n)} \varphi\left(\frac{n}{d}\right) = \sum_{d \in \mathrm{Div}(n)} \varphi(d)$ car l'application

$\mathrm{Div}(n) \longrightarrow \mathrm{Div}(n)$ est une permutation.

$d \longmapsto \frac{n}{d}$

A-t-on solution TEO ITP p41

Soit $A = \left\{ \frac{p}{n} , p \in [\![1, n]\!] \right\}$ ensemble de cardinal n

Ses éléments admettent une forme irréductible $\frac{k}{d}$ avec $k \wedge d = 1$

et $d \mid n$

On a donc $A = \bigcup_{d \mid n} A_d$ où $A_d = \left\{ \frac{k}{d}, k \wedge d = 1 \text{ et } k \in [\![1, d]\!] \right\}$

Cette réunion est disjointe par unicité de l'écriture d'un nombre rationnel irréductible.

donc $n = \operatorname{Card} A = \sum_{d \mid n} \operatorname{Card} A_d = \sum_{d \mid n} \varphi(d)$

b) $\forall n \in [\![1, n]\!] \quad \sum_{d \mid n} \varphi(d) = n$

Pour chaque k de $[\![1, n]\!]$ $\varphi(k)$ apparaît exactement $E\left(\frac{n}{k}\right)$ fois

dans les sommes précédentes $\sum_{d \mid n} \varphi(d)$ $(1 \leq n \leq n)$

d'où $\sum_{k=1}^{n} E\left(\frac{n}{k}\right) \varphi(k) = \sum_{m=1}^{n} \left(\sum_{d \mid m} \varphi(d) \right) = \sum_{m=1}^{n} (m) = \frac{n(n+1)}{2}$

cf Monier ITPS p 116 -

pour d'autres résultats.

Suite sympa : Soient $u \in \mathbb{N}^*$ et $(u_\ell)_{\ell \in \mathbb{N}}$ la suite définie par $u_0 = u$

et $\forall \ell \in \mathbb{N} \quad u_{\ell+1} = \varphi(u_\ell)$. Montrer $\exists r \in \mathbb{N}, u_r = 1$

Il est clair que $\forall n \in \mathbb{N}^* \begin{cases} \varphi(n) \leq n-1 \text{ si } n \geq 2 \\ \varphi(n) = 1 \text{ si } n = 1 \end{cases}$

En particulier $\forall n \in \mathbb{N}^* \quad \varphi(n) \leq n$ de (u_ℓ) est décroissante.

Comme $\forall \ell \in \mathbb{N} \quad u_\ell \in \mathbb{N}$, on en déduit que $(u_\ell)_{\ell \in \mathbb{N}}$ est stationnaire

$\exists r \in \mathbb{N}$ tq $u_{r+1} = u_r$. Puisque $\forall n \geq 2 \quad \varphi(n) < n$, on a

nécessairement $u_r = 1$.

compléments

La fonction indicatrice d'Euler est la fonction

$$\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$$
$$n \longmapsto \{k \text{ entier} \mid 1 \leq k \leq n \text{ et } k \wedge n = 1\}$$

φ peut être aussi définie comme :

- le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
- le nombre d'éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$
- le nombre de racines $n^{ièmes}$ primitives de l'unité dans $\mathbb{C}$

A propos du théorème d'Euler :

Soit $(n, a) \in \mathbb{N}^{*2}$ tq $n \wedge a = 1$ alors $a^{\varphi(n)} \equiv 1 \ (n)$

Si n est premier $a^n \equiv a \ (n)$ (petit théorème de Fermat)

démo : Soit $a \in (\mathbb{Z}/n\mathbb{Z}, \times)$ est un inversible ssi $a \wedge n = 1$

Notons $U(\mathbb{Z}/n\mathbb{Z}, \times)$ le groupe multiplicatif formé par les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$.

$$\text{Card}\left(U(\mathbb{Z}/n\mathbb{Z}, \times)\right) = \varphi(n)$$

Comme $a \in U(\mathbb{Z}/n\mathbb{Z}, \times)$, son ordre (ie le plus petit entier k tq $a^k = 1$)

est, selon le théorème de Lagrange un diviseur de l'ordre de $\varphi(n)$ de $U(\mathbb{Z}/n\mathbb{Z}, \times)$. D'où $a^{\varphi(n)} \equiv 1 \ (n)$ dans $(\mathbb{Z}/n\mathbb{Z}, \times)$

Si n est premier, $\varphi(n) = n - 1$ et si a est un multiple de n, alors $a \equiv 0 \ (n)$ et la formule est vraie.

Rq $\varphi(n)$ est pair pour $n \geq 2$

Si $n = 2^r$ avec $1 < r$, $\varphi(n) = 2^{r-1}(2-1)$ est pair

Sinon n comprend au moins un facteur premier impair et $\varphi(n)$

en multiple de $p-1$