My Ismail Mamouni
http ://myismail.net

Td : Arithmétique dans Z

Les fonctions artihmétiques multiplicatives

Notations

On appelle **fonction arithmétique** toute fonction de $\mathbb{N}^*$ dans $\mathbb{R}$. L'objectif du problème est d'étudier deux fonctions arithmétiques célèbres : la fonction indicatrice d'Euler et la fonction μ de Möbius, puis d'étudier une opération sur les fonctions arithmétiques : le produit de convolution.

Si a et b sont deux entiers, on note $a \wedge b$ le plus grand commun diviseur de a et b. On notera bien que pour tout $a \geq 1$, $0 \wedge a = a$.

En l'absence de précisions supplémentaires, lorsque que l'on parle de décomposition de $n \in \mathbb{N}^*$ en facteurs premiers :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

il sera implicite que pour tout $i \in [\![1, r]\!]$, les α_i sont des entiers non nuls et les p_i des nombres premiers distincts.

On dit que $n \in \mathbb{N}^*$ a un facteur carré si et seulement s'il existe $k \in \mathbb{N}^*$ tel que k^2 divise n.

On rencontrera souvent le symbole $\sum_{d|n}$, cela signifiera que la somme porte sur les entiers $d \geq 1$ qui divisent n.

A-L'indicatrice d'Euler

Soit $n \in \mathbb{N}^*$, on définit **l'indicatrice d'Euler** par :

$$\varphi(n) = \text{Card}\{k \in [\![0, n-1]\!],\ k \wedge n = 1\}.$$

Autrement dit, $\varphi(n)$ est le nombre d'entiers naturels premiers avec n et inférieurs strictement à n.

1. Calculer $\varphi(n)$ pour $1 \leq n \leq 12$, on présentera les résultats sous forme de tableau et on détaillera le calcul uniquement pour $n = 12$.
2. Montrer que p est premier si et seulement si $\varphi(p) = p - 1$.
3. Soit p premier et $\alpha \in \mathbb{N}^*$.
   (a) Soit $k \in \mathbb{N}^*$, montrer que k et p^α ne sont pas premiers entre eux si et seulement si p divise k.
   (b) Dénombrer les multiples de p compris entre 0 et $p^\alpha - 1$.
   (c) En déduire $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
4. Dans la suite de cette partie, on souhaite trouver une formule pour calculer $\varphi(n)$ pour n quelconque sachant que d'après la question précédente, on connaît une expression de $\varphi(p^\alpha)$ pour p premier. Pour ce faire nous allons d'abord démontrer que φ est une fonction multiplicative, c'est-à-dire que pour $(m, n) \in (\mathbb{N}^*)^2$, on a :

$$m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

On définit pour tout $n \in \mathbb{N}^*$, l'ensemble :

$$\mathcal{A}(n) = \{k \in\ [\![0, n-1]\!],\ k \wedge n = 1\}.$$

On se donne désormais $(m, n) \in (\mathbb{N}^*)^2$ premiers entre eux et on définit l'application :

$$\begin{array}{rccc} f & : & \mathcal{A}(mn) & \to & \mathcal{A}(m) \times \mathcal{A}(n) \\ & & x & \mapsto & (r, s) \end{array}$$

où r est le reste de la division euclidienne de x par m et s est le reste de la division euclidienne de x par n.

(a) Justifier que f est bien définie.

(b) On veut montrer que f est injective, pour cela on suppose que $f(x) = f(y) = (r, s)$ avec $(x, y) \in \mathcal{A}(mn)^2$.

i. Ecrire les divisions euclidiennes de x puis y par m et n.

ii. En déduire que mn divise $x - y$.

iii. Démontrer que $|x - y| \leq mn - 1$.

iv. Justifier alors que f est injective.

(c) On veut montrer que f est surjective, pour cela on se donne $(r, s) \in \mathcal{A}(m) \times \mathcal{A}(n)$.

i. Justifier l'existence de deux entiers relatifs u et v tels que $um + vn = 1$.

ii. Vérifier que $a = sum + rvn$ satisfait : $a = r\ [m]$ et $a = s\ [n]$.

iii. En déduire que f est surjective.

(d) Démontrer que φ est multiplicative.

5. Soit $n \geq 2$ et $r \geq 1$, on suppose que la décomposition de n en facteurs premiers s'écrit : $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.

(a) Démontrer que :

$$\varphi(n) = n \prod_{i=1}^{r} \Big(1 - \frac{1}{p_i}\Big).$$

(b) Calculer $\varphi(105)$, $\varphi(120)$ et $\varphi(1000)$.

(c) Démontrer que pour tout $n \geq 3$, $\varphi(n)$ est pair.

6. Le but de cette question est de démontrer le théorème d'Euler qui s'énonce ainsi : soit $n \geq 2$ et $a \in \mathbb{N}$ tel que $a \wedge n = 1$ alors :

$$a^{\varphi(n)} = 1\ [n].$$

(a) Expliquer pourquoi le théorème d'Euler généralise le petit théorème de Fermat.

(b) Soit $a \in [\![0, n-1]\!]$, on dit que a est inversible modulo n si et seulement s'il existe $b \in [\![0, n-1]\!]$ tel que $ab = 1\ [n]$. Démontrer que a est inversible modulo n si et seulement si a est premier avec n.

(c) On note $U(n)$ l'ensemble des éléments inversibles modulo n. Démontrer que $U(n)$ muni de la multiplication modulo n est un groupe. Quel est son cardinal ?

(d) En déduire le théorème d'Euler.