Une caractérisation des diviseurs de 24

Jean-Yves Degos*

Décembre 1993

Théorème : *Les diviseurs positifs de 24 sont les entiers n tels que, dans l'anneau* $\mathbb{Z}/n\mathbb{Z}$*, tous les éléments inversibles sont involutifs, c'est-à-dire sont leur propre inverse, c'est-à-dire que* n *vérifie la propriété suivante :*

$$\forall (x,y) \in (\mathbb{Z}/n\mathbb{Z})^2, xy = 1 \Longrightarrow x = y \tag{1}$$

PREUVE : Si n est un diviseur positif de 24 (i.e. $n \in \{1,2,3,4,6,8,12,24\}$), on a vite fait de s'assurer que la propriété (1) est vraie.

Réciproquement, soit n un entier satisfaisant la propriété (1), montrons que c'est un diviseur de 24.

1) Si on note $U_n = (\mathbb{Z}/n\mathbb{Z})^*$, alors U_n est commutatif, et la propriété (1) s'interprète ainsi : $\forall x \in U_n, x^2 = 1$. On en déduit que l'ordre de U_n est une puissance de 2. Or son ordre n'est autre que $\phi(n)$, l'indicateur d'Euler de n. Ainsi, si :

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

est la décomposition de n en facteurs premiers, on sait qu'on a :

$$\phi(n) = \prod_{i=1}^{r} p_i^{r_i - 1}(p_i - 1) \tag{2}$$

Mais maintenant, $\phi(n)$ étant une puissance de 2, chaque facteur du produit de la formule (2) est une puissance de 2. C'est-à-dire :

a) les p_i sont des nombres premiers de la forme $2^{k_i} + 1$

b) si de plus $k_i \neq 0$, alors $r_i = 1$

Il en résulte que n s'écrit forcément $n = 2^k p_1 p_2 \dots p_r$ où les p_i sont des nombres premiers deux à deux non associés de la forme décrite en a) et b)

2) Grâce au Théorème des Chinois, on a alors l'isomorphisme :

$$U_n \simeq (\mathbb{Z}/2^k\mathbb{Z})^* \times (\mathbb{Z}/p_1\mathbb{Z})^* \times (\mathbb{Z}/p_2\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_r\mathbb{Z})^* \tag{3}$$

*jydegos **chez** protonmail **point** com

3) Supposons alors que dans l'expression (3), l'un des p_i soit tel que $k_i \geq 2$. Alors, grâce à l'identité :

$$(2^{k_i} - 1)^2 = (2^{k_i} + 1)(2^{k_i} - 3) + 4$$

on en déduit que dans $(\mathbb{Z}/p_i\mathbb{Z})^*$, la classe de $2^{k_i} - 1$ modulo $2^{k_i} + 1$ n'est pas d'ordre 2, car on a $4 < 2^{k_i} + 1$. À cause de l'isomorphisme (3), on trouve alors un élément dans U_n, différent de l'élément neutre, qui n'est pas d'ordre 2, ce qui contredit l'hypothèse (1).

Ainsi $k_i \in \{0, 1\}$ et donc n s'écrit : $n = 2^k 3^j$, avec $j \in \{0, 1\}, k \geq 0$.

4) Supposons alors $k \geq 4$. L'entier $2^k - 3$ est inversible modulo 2^k, et on a l'identité :

$$(2^k - 3)^2 = 2^{2k} - 6.2^k + 9$$

dont on déduit que la classe de $2^k - 3$ modulo 2^k n'est pas d'ordre 2 car son carré est congru à 9, et pour $k \geq 4, 9 < 2^k$. On a alors, à nouveau à cause de l'isomorphisme (3), un élément de U_n qui n'est pas d'ordre 2, ce qui contredit l'hypothèse (1).

On conclut de tout ce qui précède que $n = 2^j 3^k, k \in \{0, 1, 2, 3\}, j \in \{0, 1\}$.

Ainsi $n \in \{1, 2, 3, 4, 6, 8, 12, 24\}$, et c'est donc bien un diviseur de 24. ■