MULTIPLICATIVITÉ DE LA FONCTION D'EULER

Pour tout $n \in \mathbb{N}^*$ notons $I(n)$ l'ensemble des inversibles de $\mathbb{Z}_n$. On rappelle que $\left|I(n)\right| = \varphi(n)$.

Remarque préliminaire. Si $x \in I(n)$ et si d divise n, alors le reste r de x mod d appartient à $I(d)$. En effet, si r n'était pas inversible modulo d, il existerait un premier p divisant r et d. Or x peut s'écrire $x = dq + r$ (division euclidienne) ce qui montre que p diviserait également x et d et donc x et n, ce qui contredit l'inversibilité de x modulo n.

Théorème

Soient n_1 et n_2 des entiers ≥ 1, premiers entre eux, et $n = n_1 n_2$. L'application f définie comme suit est ***bijective***.

$$f : I(n) \to I(n_1) \times I(n_2)$$
$$x \mapsto (r_1 , r_2)$$

où r_1 (resp. r_2) désigne le reste modulo n_1 (resp. n_2) de x.

Preuve

1) L'application f est bien définie en vertu de la *remarque préliminaire*.

2) f est injective : Soient x et x' tels que $f(x) = f(x')$ c'est-à-dire tels que $x \equiv x'$ mod n_1 et $x \equiv x'$ mod n_2. On a donc $x - x' \equiv 0$ mod n_1 et $x - x' \equiv 0$ mod n_2. Il existe donc des entiers s et t tels que $x - x' = sn_1 = tn_2$, ce qui montre que $x - x'$ est un multiple du ppcm de n_1 et n_2, soit de $n = n_1 n_2$ puisque n_1 et n_2 sont premiers entre eux. Ainsi $x - x' \equiv 0$ mod n et, par suite, $x = x'$.

3) f est surjective : Soit (r_1 , r_2) dans $I(n_1) \times I(n_2)$. Cherchons x dans $I(n)$ tel que x mod n_1 = r_1 et x mod n_2 = r_2. On doit donc trouver des entiers s et t vérifiant $r_1 + sn_1 = r_2 + tn_2$, qui équivaut à $sn_1 - tn_2 = r_2 - r_1$. Comme n_1 et n_2 sont premiers entre eux, Bézout fournit s et t. On pose donc $x = r_1 + sn_1 = r_2 + tn_2$ mod n, et il ne reste plus qu'à montrer que x est inversible modulo n. S'il ne l'était pas, il existerait un premier p divisant x et n. p diviserait donc aussi n_1 ou n_2, disons n_1 pour fixer les idées. Si p divise x et n_1, il divise aussi x et r_1 puisque $x \equiv r_1 + sn_1$ mod n. Cela contredit l'inversibilité de r_1 modulo n_1.

Corollaire. Si les entiers ≥ 1 n_1 et n_2 sont premiers entre eux,

$$\boxed{\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)}$$

Preuve. La bijection f nous assure que $\left|I(n)\right| = \left|I(n_1) \times I(n_2)\right|$. D'où :

$$\varphi(n_1 n_2) = \varphi(n) = \left|I(n)\right| = \left|I(n_1) \times I(n_2)\right| = \left|I(n_1)\right| \cdot \left|I(n_2)\right| = \varphi(n_1)\varphi(n_2)$$