Le théorème des restes chinois

Marc Lorenzi

24 décembre 2025

Pour tout entier $n \geq 1$, on note $\mathbb{Z}_n$ l'anneau des entiers modulo n.

On se donne deux entiers naturels non nuls a et b. Considérons l'application $f : \mathbb{Z}_{ab} \longrightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ définie pour tout $x \in \mathbb{Z}$ par

$$f(x + ab\mathbb{Z}) = (x + a\mathbb{Z}, x + b\mathbb{Z})$$

Cette application est bien définie parce que si $x \equiv x' \bmod ab$ alors $x \equiv x' \bmod a$ et $x \equiv x' \bmod b$.

Proposition 1. *L'application f est un morphisme d'anneaux.*

Démonstration. Soient $x, y \in \mathbb{Z}$. On a

$$\begin{aligned} f((x + ab\mathbb{Z}) + (y + ab\mathbb{Z})) &= f((x + y) + ab\mathbb{Z}) \\ &= (x + y + a\mathbb{Z}, x + y + b\mathbb{Z}) \\ &= ((x + a\mathbb{Z}) + (y + a\mathbb{Z}), (x + b\mathbb{Z}) + (y + b\mathbb{Z})) \\ &= (x + a\mathbb{Z}, x + b\mathbb{Z}) + (y + a\mathbb{Z}, y + b\mathbb{Z}) \\ &= f(x + ab\mathbb{Z}) + f(y + ab\mathbb{Z}) \end{aligned}$$

De même,

$$\begin{aligned} f((x + ab\mathbb{Z}) \times (y + ab\mathbb{Z})) &= f((xy) + ab\mathbb{Z}) \\ &= (xy + a\mathbb{Z}, xy + b\mathbb{Z}) \\ &= ((x + a\mathbb{Z}) \times (y + a\mathbb{Z}), (x + b\mathbb{Z}) \times (y + b\mathbb{Z})) \\ &= (x + a\mathbb{Z}, x + b\mathbb{Z}) \times (y + a\mathbb{Z}, y + b\mathbb{Z}) \\ &= f(x + ab\mathbb{Z}) \times f(y + ab\mathbb{Z}) \end{aligned}$$

Enfin, $f(1 + ab\mathbb{Z}) = (1 + a\mathbb{Z}, 1 + b\mathbb{Z})$. □

Proposition 2. *Si $a \wedge b = 1$, alors f est un isomorphisme.*

Démonstration. Supposons $a \wedge b = 1$. Soit $x \in \mathbb{Z}$. Supposons que $x + ab\mathbb{Z} \in \ker f$. On a alors $x + a\mathbb{Z} = a\mathbb{Z}$ et $x + b\mathbb{Z} = b\mathbb{Z}$, c'est à dire a divise x et b divise x. Comme a et b sont premiers entre eux, ab divise x donc $x + ab\mathbb{Z} = ab\mathbb{Z}$. Ainsi, f est injective. De plus,

$$|\mathbb{Z}_{ab}| = |\mathbb{Z}_a \times \mathbb{Z}_b| = ab$$

donc f est bijective. $\square$

On généralise facilement à un produit d'un nombre d'entiers quelconque. Si $n \geq 1$ et $a_1, \ldots, a_n$ sont n entiers naturels non nuls premiers entre eux deux à deux, alors l'application $f : \mathbb{Z}_{a_1 \ldots a_n} \longrightarrow \mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_n}$ définie par

$$f(x + a_1 \ldots a_n \mathbb{Z}) = (x + a_1\mathbb{Z}, \ldots, x + a_n\mathbb{Z})$$

est un isomorphisme d'anneaux.

Il est possible d'obtenir une expression explicite de f^{-1}. Soit $n \geq 1$. Soient $a_1, \ldots, a_n$ des entiers naturels non nuls premiers entre eux deux à deux. Pour tout $i \in [\![1, n]\!]$, soit

$$\widehat{a}_i = \prod_{j \neq i} a_j$$

Proposition 3. *Les entiers $\widehat{a}_1, \ldots, \widehat{a}_n$ sont premiers entre eux dans leur ensemble.*

Démonstration. Supposons le contraire. Soit p un nombre premier qui divise les $\widehat{a}_i$. Comme p divise $\widehat{a}_n = a_1 \ldots a_{n-1}$, il existe par le lemme d'Euclide $j \in [\![1, n-1]\!]$ tels que p divise a_j. Les a_i étant premiers entre eux deux à deux, a_j est premier avec $\widehat{a}_j$. Contradiction, puisqu'on a supposé que p divise $\widehat{a}_j$. $\square$

Les $\widehat{a}_i$ étant premiers entre eux dans leur ensemble, il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que

$$\sum_{i=1}^{n} u_i \widehat{a}_i = 1$$

Soit

$$z = \sum_{i=1}^{n} u_i \widehat{a}_i x_i$$

Pour tout $j \in [\![1, n]\!]$ et tout $i \neq j$, $\widehat{a}_i \equiv 0 \bmod a_j$. On a donc

$$z \equiv u_j \widehat{a}_j x_j \bmod a_j$$

Or,

$$u_j \widehat{a}_j = 1 - \sum_{i \neq j} u_i \widehat{a}_i \equiv 1 \bmod a_j$$

d'où $z \equiv x_j \bmod a_j$.

Ainsi, $f^{-1} : \mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_n} \longrightarrow \mathbb{Z}_{a_1 \ldots a_n}$ est définie pour tous $x_1, \ldots, x_n \in \mathbb{Z}$ par

$$f^{-1}(x_1 + a_1\mathbb{Z}, \ldots, x_n + a_n\mathbb{Z}) = \sum_{i=1}^{n} u_i \widehat{a}_i x_i + a_1 \ldots a_n \mathbb{Z}$$