Système de congruences

[CALDERO-PERRONIER, p]

ÉNONCÉ :

Théorème : Soient $n, m \in \mathbb{Z}$. Notons $\delta := pgcd(m,n)$ et $\mu := ppcm(m,n)$. On considère le morphisme d'anneaux défini par :

$$\begin{array}{rccc} \tilde{\varphi} : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & x & \longmapsto & ([x]_m, [x]_n) \end{array}$$

Alors il existe des morphismes $\varphi : \mathbb{Z}/\mu\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ injectif et $\Psi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$ surjectif tels que $Im(\varphi) = Ker(\Psi)$.

Applications :

1. Le système de congruences défini par :

$$(S) \quad \begin{cases} x \equiv 2 \quad [21] \\ x \equiv 11 \quad [35] \end{cases}$$

   n'admet pas de solutions.

2. Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b \ [\delta]$. En posant $x_0 = \frac{1}{\delta}(avn + bum)$ où $um + vn = \delta$, on a $\mathcal{S} = x_0 + \mu x$.

DÉVELOPPEMENT :

LEMMES : **Propriété universelle du quotient** : Soient G un groupe, $H \triangleleft G$, $f : G \longrightarrow G'$ tels que $H \subset Ker(f)$. Alors il existe un unique morphisme $\varphi : G/H \longrightarrow G'$ tel que $\varphi \circ \pi = f$.

Démonstration. Il suffit de considérer l'application :

$$\begin{array}{rccc} \varphi : & G/H & \longrightarrow & G' \\ & [x]_H & \longmapsto & f(x) \end{array}$$

et vérifions les différents points du théorème.

- φ est bien définie : Soient $x, y \in G$ tels que $[x]_H = [y]_H$. Alors $xy^{-1} \in H$ si bien que, comme $H \subset Ker(f)$, on a :

$$f(xy^{-1}) = 1_G \Rightarrow f(x) = f(y)$$

- φ est un morphisme : Soient $[x]_H, [y]_H$, on a :

$$\begin{aligned} \varphi([x]_H[y]_H) = \varphi([xy]_H) &= f(xy) \\ &= f(x)f(y) \\ &= \varphi([x]_H)\varphi([y]_H) \end{aligned}$$

- φ est unique : Considérons $\varphi' : G/H \longrightarrow G'$ tel que $\varphi' \circ \pi = f$. Alors pour tout $[x]_H$, on a :

$$\varphi([x]_H) = f(x) = \varphi'([x]_H)$$

  d'où $\varphi = \varphi'$.

De plus, on remarque que pour tout $x \in G$, $\varphi([x]_H) = \varphi(\pi(x)) = f(x)$, où $\pi : G \to G/H$ désigne la projection canonique, d'où le résultat. □

Démonstration. (*théorème*) : D'une part, on remarque que $Ker(\tilde{\varphi}) = \mu\mathbb{Z}$. Ainsi, par le lemme, on dispose d'un unique morphisme injectif $\varphi : \mathbb{Z}/\mu\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En posant $G = \mathbb{Z}$ et $G' = \mathbb{Z}/\delta\mathbb{Z}$ et comme $\delta \mid n$, $H = n\mathbb{Z}$ est inclus dans $Ker(f) = \delta\mathbb{Z}$, où

$$\begin{array}{rccc} f : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/\delta\mathbb{Z} \\ & x & \longmapsto & [x]_\delta \end{array}$$

Par passage au quotient, on dispose d'un morphisme $\Psi_1 : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$. De la même façon, il existe un morphisme $\Psi_2 : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$.
Ainsi, on définit Ψ par :

$$\begin{array}{rccc} \Psi : & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/\delta\mathbb{Z} \\ & ([x]_m, [x]_n) & \longmapsto & \Psi_1(x) - \Psi_2(y) \end{array}$$

qui est bien défini et est un morphisme de groupes additifs. De plus, il est surjectif car f l'est.
Vérifions que $Im(\varphi) = Ker(\Psi)$. Comme un élément de $Im(\varphi)$ est de la forme $([x]_m, [x]_n)$, on a : $\Psi(([x]_m, [x]_n)) = [x]_\delta - [x]_\delta = 0$, d'où l'inclusion $Im(\varphi) \subset Ker(\Psi)$. Enfin, par injectivité de φ, on a que

$$|Im(\varphi)| = \mu = \frac{mn}{\delta} = \frac{|\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|}{|Im(\Psi)|} = |Ker(\Psi)|$$

Ainsi, $Im(\varphi) = Ker(\Psi)$. □

Démonstration. (*Applications*) :

1. Supposons qu'il existe une solution $x \in \mathbb{Z}$, alors $\tilde{\varphi}(x) = ([2]_{21}, [11]_{35}) \in Ker(\Psi)$. Mais comme $\delta = 7$, on aurait $[2]_7 - [11]_7 = [-9]_7 = [0]_7$, ce qui est absurde, d'où l'assertion.
2. Par hypothèse, il existe $k \in \mathbb{Z}$ tel que $a = b + k\delta$.
   On a d'une part :
   $$x_0 = \frac{1}{\delta}(b(vn + um) + k\delta vn) = b + kvn \equiv b\ [n]$$
   et d'autre part :
   $$x_0 = a - kum \equiv a\ [m]$$
   Ainsi, si x est solution du système, $\tilde{\varphi}(x) = \tilde{\varphi}(x_0)$ et donc $x - x_0 \in Ker(\tilde{\varphi}) = \mu\mathbb{Z}$. Ainsi, $\mathcal{S} = x_0 + \mu\mathbb{Z}$.

□

Remarques :

- On a en particulier montrer qu'un système
  $$(\tilde{S}) \quad \begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$$
  admet une solution si et seulement si $a \equiv b\ [\delta]$.
- Il faut savoir illustrer ceci avec un exemple : prendre par exemple le système
  $$(\hat{S}) \quad \begin{cases} x \equiv 2\ [21] \\ x \equiv 9\ [35] \end{cases}$$
  de sorte que $2 \equiv 9\ [7]$.