Système de Congruences

Carnet de Voyage p167

Théorème : Soient $(m,n) \in \mathbb{N}^*$ et δ leur pgcd et μ leur ppcm

Alors si $\overline{a}_\delta = \overline{b}_\delta$ (dans $\mathbb{Z}/\delta\mathbb{Z}$), le système (S) : $\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$ à pour ensemble de solution $\{x_0 + k\mu,\ k \in \mathbb{Z}\}$ où $x_0 = \frac{1}{\delta}(avn + bum)$ où $u, v \in \mathbb{Z}$ tel que $um + vn = \delta$

Démonstration :

* Soit le morphisme d'anneaux $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$x \longmapsto (\overline{x}_m, \overline{x}_n)$

On a $\ker(\varphi) = \mu\mathbb{Z}$

* On en déduit par passage au quotient, un morphisme injectif $\tilde{\varphi}$ par le Thm d'isomorphisme
$\tilde{\varphi} : \mathbb{Z}/\mu\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$\overline{x}_\mu \longmapsto (\overline{x}_m, \overline{x}_n) := \varphi(x)$

Le passage au quotient assure que le morphisme est bien défini (Ne dépend pas du choix du représentant $\overline{x}_\mu = \overline{y}_\mu \Rightarrow x = y + \mu k \quad \varphi(x) = \varphi(y) + \varphi(\mu k) = \varphi(y)$)

Le fait d'avoir quotienté par le noyau ne change pas l'image : $\mathrm{Im}(\varphi) = \mathrm{Im}(\tilde{\varphi})$

* Soient $r, s \in \mathbb{N}^*$ tel que $r \mid s$. Alors $\exists k \in \mathbb{N}$, tel que $s = kr$.
Soit $\psi : \mathbb{Z}/s\mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z}$ qui est un morphisme d'anneau
$\overline{x}_s \longmapsto \overline{x}_r$

Soient $x, x' \in \overline{x}_s$. Alors $x' = x + k's = x + k'kr$ donc $\overline{x'}_r = \overline{x}_r$
L'application est bien définie car ne dépend pas du choise de x et c'est bien un morphisme

* Comme $\delta \mid m$ et $\delta \mid n$, par le point précédent, $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/\delta\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/\delta\mathbb{Z}$ définissent bien des morphismes
$\overline{x}_m \mapsto \overline{x}_\delta$ et $\overline{x}_n \mapsto \overline{x}_\delta$

Ainsi, $\psi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$ définit bien un morphisme
$(\overline{x}_m, \overline{y}_n) \longmapsto \overline{x}_\delta - \overline{y}_\delta$

Soit $\overline{x}_\delta$ dans $\mathbb{Z}/\delta\mathbb{Z}$, et x un représentant, alors $\psi(\overline{x}_m, \overline{0}_n) = \overline{x}_\delta$

Donc ψ est surjectif.

* On a l'inclusion $Im(\tilde{\varphi}) \subset Ker(\psi)$: En effet, un élément de $Im(\tilde{\varphi})$ est de la forme $(\overline{x_m}, \overline{x_n})$, donc $\psi(\overline{x_m}, \overline{x_n}) = \overline{x}_\delta - \overline{x}_\delta = \overline{0}$

L'égalité se déduit par cardinalité :

L'injectivité de $\tilde{\varphi}$ implique que $|Im(\tilde{\varphi})| = |\mathbb{Z}/\mu\mathbb{Z}| = \mu$.

Donc $|Im(\tilde{\varphi})| = \mu = \frac{mn}{\delta} = \frac{|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|}{|\mathbb{Z}/\delta\mathbb{Z}|} = \frac{|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|}{|Im(\psi)|} = |Ker(\psi)|$ d'après le Thm d'isomorphisme

par surjectivité de ψ

Exemple : $\begin{cases} x \equiv 2 \ [21] \\ x \equiv 11 \ [35] \end{cases}$ n'a pas de solution.

$7 = pgcd(21, 35)$

Si une solution existait, on aurait, $x \in \mathbb{Z}$ tel que $\psi(x) = (\overline{x}_{21}, \overline{x}_{35}) = (\overline{2}_{21}, \overline{11}_{35})$ et donc $(\overline{2}_{11}, \overline{11}_{35})$ serait dans $Im(\tilde{\varphi}) = Ker(\psi)$. Or $\overline{2}_7 - \overline{11}_7 = -\overline{9}_7 \neq 0$ Absurde.

* Si $\overline{a}_\delta = \overline{b}_\delta$ alors $a = b + h\delta$ où $h \in \mathbb{Z}$, ainsi :

$$x_0 = \frac{1}{\delta}\left((b + h\delta)v_m + b u_m\right) = b \underbrace{\frac{v_m + u_m}{\delta}}_{=1} + h v_m$$

D'où $x_0 \equiv b \ [n]$ et de la même manière, $x_0 \equiv a \ [m]$ (en remplaçant $b = a - h\delta$)

Soit x une solution de (S), on a alors $\psi(x) = \psi(x_0)$ donc $x - x_0 \in Ker(\psi) = \mu\mathbb{Z}$.

Donc l'ensemble des solutions est $\{x_0 + h\mu, h \in \mathbb{Z}\}$