dév : Théorème chinois

Leçons : 120, 122, 142.
réf : TL1 p449.

Thm :
Soient $m_1, \dots, m_r \geq 2$ des entiers premiers entre eux 2 à 2. (donc $r \geq 2$). $M := \prod_{i=1}^{r} m_i$.
Soient $a_1, \dots, a_r \in \mathbb{Z}$. Considérons le système :

$$(S) \Leftrightarrow \begin{cases} x \equiv a_1 \ [m_1] \\ \vdots \\ x \equiv a_r \ [m_r]. \end{cases}$$

Ce système possède une solution $x \in \mathbb{Z}$ qui est unique modulo M

dem : réf : fournit méthode pour résolution
L122/142 : ici demo pour $A = \mathbb{Z}$. (A principal) ex idéaux principaux
Jacobson → unique décomp

① Unicité :
Soient $x, y \in \overset{A}{\mathbb{Z}}$ deux solution de (S).

$$\forall i \in [\![1, r]\!] \quad \begin{matrix} x \equiv a_i \equiv y \ [m_i] \\ \hline m_i \mid x - y \end{matrix}$$

Comme les m_i sont premiers entre eux deux à deux : $M \mid x - y$ ← de A principal
D'où $x \equiv y \ [M]$ ce qui donne bien unicité modulo M.

② Existence :
Montrons l'existence par récurrence sur $r \geq 2$:

$$P(r) : \text{"(S) possède une solution } x \in \mathbb{Z}\text{"}.$$

* Ini : $r = 2$.

Par le théorème de Bezout ($m_1 \wedge m_2 = 1$) : ok pour anneau principal.

$$\exists u, v \in \mathbb{Z}, \quad \underbrace{u m_1}_{:= x_1} + \underbrace{v m_2}_{:= x_2} = 1.$$

On a : $\begin{cases} x_1 \equiv 0 \ [m_1] \\ x_1 \equiv 1 \ [m_2] \end{cases}$ et $\begin{cases} x_2 \equiv 1 \ [m_1] \\ x_2 \equiv 0 \ [m_2]. \end{cases}$

On pose alors : $x := a_1 x_2 + a_2 x_1 \in \underset{\in A}{\mathbb{Z}}$ et $\begin{cases} x \equiv a_1 \ [m_1] \\ x \equiv a_2 \ [m_2]. \end{cases}$

x est donc solution.

* Hér : Soit $r \geq 3$. Supposons $P(r-1)$ vraie
Posons $P := m_1 \times \cdots \times m_{r-1}$.

Par HR. : $\exists y \in \mathbb{Z}$, $\forall i \in [\![1, r-1]\!]$, $y \equiv a_i \ [m_i]$.

De plus $P \wedge m_r = 1$ donc par le cas 2 :

$$\exists x \in \mathbb{Z}, \quad \begin{cases} x \equiv y \ [P] \\ x \equiv a_r \ [m_r] \end{cases}$$

$$x \equiv y \ [P] \overset{(*)}{\Leftrightarrow} \forall i \in [\![1, r-1]\!] \quad x \equiv y \ [m_i].$$
$$\Leftrightarrow \text{---------} \quad x \equiv a_i \ [m_i]$$

(*) détail : $m \wedge n = 1 \Rightarrow \left(\begin{cases} a \equiv b \ [m] \\ a \equiv b \ [n] \end{cases} \Leftrightarrow a \equiv b \ [mn] \right)$
$\Leftarrow$: Si $a = b \ [mn]$, $a - b = q\,mn$ donc $a \equiv b \ [m]$ et $a \equiv b \ [n]$.
$\Rightarrow$: Si $a - b = k_1 m = k_2 n$, $m \mid k_2 n \Rightarrow m \mid k_2$ car $m \wedge n = 1$ (Gauss)
donc $a - b = k\,mn$ d'où résultat.

Donc x est solution de (S).

* on conclut par principe de récurrence l'existence de x.

Thm: Soient $m_1, \dots, m_r \geq 2$ premiers entre eux deux à deux. ($r \geq 2$). $M = \prod_{i=1}^{r} m_i$

$$\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z} \simeq \mathbb{Z}/M\mathbb{Z}$$

dem:
On notera : * $B := \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$.
* $\pi : \mathbb{Z} \to \mathbb{Z}/M\mathbb{Z}$
* $\pi_i : \mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$ pour $i \in [\![1, r]\!]$ } morphismes canoniques.

On définit : $F : \begin{array}{ccc} \mathbb{Z}/M\mathbb{Z} & \longrightarrow & B \\ \overline{k} & \longmapsto & (\pi_1(k), \dots, \pi_r(k)) \end{array}$

① **Bien définie :**
Soient $k, l \in \mathbb{Z}$ tq $k \equiv l \ [M]$. i.e $\exists$ représentant d'1 m classe.
$\forall i \in [\![1, r]\!]$ $m_i \mid k - l$
$\pi_i(k) = \pi_i(l)$
donc $F(\overline{k}) = F(\overline{l})$. et F est bien défini.

② **Morphisme :**
Soient $\overline{x}, \overline{y} \in \mathbb{Z}/m\mathbb{Z}$.
* $F(\overline{x} + \overline{y}) = F(\overline{x+y}) = (\pi_i(x+y))_{1 \leq i \leq r} = (\pi_i(x) + \pi_i(y))_{1 \leq i \leq r} = F(\overline{x}) + F(\overline{y})$
* $F(\overline{x} \times \overline{y}) = F(\overline{xy}) = (\pi_i(xy))_{1 \leq i \leq r} = (\pi_i(x)\pi_i(y))_{1 \leq i \leq r} = F(\overline{x}) \times F(\overline{y})$

③ **Bijectivité :**
* inj ($\ker = \{0\}$) :
Soit $\overline{k} \in \ker(F)$.
$\forall i \in [\![1, r]\!]$, $\pi_i(k) = 0$.
$m_i \mid k$.
Ainsi $M \mid k$ (car les m_i sont 1 à 1 entre eux) puis $\overline{k} = \overline{0}$.
* De plus $|\mathbb{Z}/M\mathbb{Z}| = \prod_{i=1}^{r} m_i = |B|$., d'où F est bijective.