Théorème chinois et système d'équation diophantienne :

Ref : Rombaldi 1.10 1.1.2 1.1.2

Théorème : Soit A un anneau principal. Soient $(a_j)_{1\leq j\leq n}$ et $r \geqslant 2$ des éléments non nuls et non inversibles.

$\forall j \in [\![1,r]\!]$, π_j désigne la surjection canonique de A sur $A/(a_j)$

Si les (a_j) sont premiers entre eux 2-à-2. $\varphi : A \longrightarrow \prod_{j=1}^{r} A/(a_j)$ est un

$x \longmapsto (\pi_j(x))_{1\leq j\leq r}$

morphisme d'anneaux surjectif de noyau $\ker(\varphi) = (\prod_{j=1}^{r} a_j)$

et φ induit un isomorphisme d'anneaux $\overline{\varphi} : A/(\prod_{j=1}^{r} a_j) \longrightarrow \prod_{j=1}^{r} A/(a_j)$

$\pi(x) \longmapsto (\pi_j(x))_{1\leq j\leq r}$

d'inverse $\overline{\varphi}^{-1} : (\pi_j(x_j))_{1\leq j\leq r} \longmapsto \sum_{i=1}^{r} x_i u_i b_i$ où $\sum_{j=1}^{r} u_j b_j = 1$ et $b_j = \prod_{\substack{i=1 \\ i\neq j}}^{r} a_i$.

φ est un morphisme d'anneaux : Noble part, Noble pour $\times$ et $\varphi(1) = 1$.

$\ker(\varphi)$ est formé des multiples de tous les a_j ~~tous~~

Puisque les a_j sont premiers entre eux 2-à-2 alors ppcm $a = \prod_{j=1}^{r} a_j$ aussi

Les $b_i = \frac{a}{a_i}$ sont premiers entre eux dans leur ensemble :

sinon $\exists p \in A$ tq $p \mid b_j$ $\forall j \in [\![1,r]\!]$ car A factoriel.

donc $p \mid b_1 = \prod_{i=2}^{r} a_i$ donc $p \mid a_i$ pour un $i \in [\![2,r]\!]$

or $p \mid b_i$ donc un a_k pour $k \neq i$

donc $a_i \wedge a_k \neq 1$ absurde.

D'après le théorème de Bézout (A principal), on trouve $(u_i)_{1\leq i\leq r} \in A$ tq $\sum_{i=1}^{r} u_i b_i = 1$.

$\forall j \in [\![1,r]\!]$, $\pi_j(b_i) = \pi_j(0)$ pour $i \neq j$ car b_i est multiple de a_j

donc $\pi_j(1) = \pi_j\left(\sum_{i=1}^{r} u_i b_i\right) = \pi_j(u_j)\,\pi_j(b_j)$.

donc $\pi_j(b_j)$ est inversible dans $A/(a_j)$ d'inverse $\pi_j(u_j)$

Pour $(\pi_j(x_j))_{1\leq j\leq r}$ donné dans $\prod_{j=1}^{r} A/(a_j)$, en posant $x = \sum_{i=1}^{r} x_i u_i b_i$, on a $\forall j \in [\![1,r]\!]$,

$\pi_j(x) = \pi_j(x_j)\,\pi_j(u_j)\,\pi_j(b_j) = \pi_j(x_j)$

soit $\varphi(x) = (\pi_j(x_j))_{1\leq j\leq r}$

Le morphisme φ est donc surjectif et il se factorise en un isomorphisme :

$$\overline{\varphi} : A/(\prod_{j=1}^{r} a_j) = A/\ker\varphi \longrightarrow \prod_{j=1}^{r} A/(a_j)$$

$$\pi(x) \longmapsto (\pi_j(x))_{1\leq j\leq r}$$

Avec la surjectivité on a bien l'inverse voulue.

Théorème : Soit $n \geq 2$, $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$. On considère l'éq dans $\mathbb{Z}$: $(E) : ax \equiv b\ [n]$

On note $\delta = \text{pgcd}(a,n)$, $a = \delta a'$ et $n = \delta n'$ avec $a' \wedge n' = 1$

L'équation (E) a des solutions ssi $\delta \mid b$.

Dans ce cas, $S = \{ b' x_0' + k n' \mid k \in \mathbb{Z} \}$ où x_0' est une sol particulière de $a'x \equiv 1\ [n']$.

Si (E) a une solution $x \in \mathbb{Z}$, alors $\delta n' \mid \delta a' - b$ et $\delta \mid b$.

Si b est un multiple de δ, $b = \delta b'$ et toute sol de $a'x \equiv b'\ [n']$ est sol de E.

Les sols de $a'x \equiv b'\ (n')$ sont de la forme $x = b' x_0' + k n'$ où x_0' est sol de $a'x \equiv 1\ [n']$ et $k \in \mathbb{Z}$.

Réciproquement : $\forall k \in \mathbb{Z}$, on vérifie que $x = b' x_0' + k n'$ est sol de (E).

Le théorème chinois peut être utilisé pour étudier un système d'équations diophantiennes : $k \equiv a_j\ (n_j)$

Dans le cas où $n_1, \dots, n_r$ sont premiers entre eux 2-à-2, cela revient à trouver l'antécédent dans $\mathbb{Z}/n\mathbb{Z}$ de $(\pi_1(a_1), \dots, \pi_r(a_r))$ par l'isomorphisme $\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z}$

$\pi_n(k) \mapsto (\pi_1(k), \dots, \pi_r(k))$

cet antécédent est $\overline{k_0}$ où $k_0 = \sum_{i=1}^{r} a_i u_i m_i$ en désignant pour u_j une suite de $\sum_{j=1}^{r} u_j \frac{n}{n_j} = 1$.

On a donc ainsi une sol particulière et les autres sols sont les $k = k_0 + q \cdot n$ où $q \in \mathbb{Z}$.

Ex Considérons le système d'équations diophantiennes : $\begin{cases} k \equiv 2\ [4] \\ k \equiv 3\ [5] \\ k \equiv 1\ [9] \end{cases}$

$n_1 = 4$, $n_2 = 5$, $n_3 = 9$

Comme n_1, n_2, n_3 sont deux à deux premiers entre eux, ce système a des solutions données en déterminant les coefficients dans une relation de Bézout

$u_1 m_1 + u_2 m_2 + u_3 m_3 = 1$ où $m_1 = n_2 n_3 = 45$
$m_2 = n_1 n_3 = 36$
$m_3 = n_1 n_2 = 20$

Pour ce faire on utilise l'associativité des pgcd en écrivant que :

$$\begin{cases} n_2 \wedge n_3 = 4 = (-1) \times 36 + 2 \times 20 \\ 1 = n_1 \wedge (n_2 \wedge n_3) = 1 \times 45 + (-11) \times 4 \\ 1 = 1 \times 45 + 11 \times 36 + (-22) \times 20 \end{cases}$$

ce qui donne la solution particulière : $k_0 = 2 \times 45 + 33 \times 36 - 22 \times 20$
$= 838$

et la solution générale : $k = 838 + 180q$
$= 118 + 180q'$ $(q' \in \mathbb{Z})$

(on a effectué la D.E. de 838 par 180)