Théorème chinois et applications

Rombaldi, page 244

Ulmer Anneaux, corps page 58

Théorème chinois Soient A un anneau et des éléments $a_1, \dots, a_r \in A$ premiers entre eux deux à deux.

Alors $\varphi : A \longrightarrow A/(a_1) \times \dots \times A/(a_r)$, $x \longmapsto (\pi_j(x))_{1 \leq j \leq r}$ est un morphisme d'anneaux surjectif de noyau $\ker \varphi = \left(\prod_{j=1}^{r} a_j\right) =: (a)$.

De plus, φ induit un isomorphisme $\overline{\varphi} : A/(a) \longrightarrow A/(a_1) \times \dots \times A/(a_r)$, $\overline{\pi}(x) \longmapsto (\pi_j(x))_j$ d'inverse $\overline{\varphi}^{-1} : (\pi_j(x_j))_{1 \leq j \leq r} \longmapsto \sum_{i=1}^{r} x_i u_i b_i$ avec $\sum_{i=1}^{r} u_i b_i = 1$.

Il est clair que :

$\varphi : A \longrightarrow A/(a_1) \times \dots \times A/(a_r)$, $x \longmapsto (\pi_j(x))_{1 \leq j \leq r}$ est un morphisme d'anneaux.

Son noyau est formé des multiples de tous les a_j, donc de leur ppcm $a = a_1 \cdots a_r$ puisque les a_j sont premiers entre eux deux à deux.

On pose pour $j \in [\![1, r]\!]$, $b_j = \frac{a}{a_j}$. Supposons que les b_j ne sont pas premiers entre eux dans leur ensemble. Il existe alors un élément premier p de A tel que :

$\forall j \in [\![1, r]\!]$, $p \mid b_j$ car A est principal donc factoriel

On obtient :

$p \mid b_1 = a_2 \cdots a_r$ donc il existe $i \in [\![2, r]\!]$ tel que $p \mid a_i$

$p \mid b_i = \prod_{j \neq i} a_j$ donc il existe $j \neq i$ tel que $p \mid a_j$

Absurde, donc les $(b_j)_{1 \leq j \leq r}$ sont premiers entre eux dans leur ensemble et par Bézout, il existe $u_1, \dots, u_r \in A$ tels que :

$$\sum_{i=1}^{r} u_i b_i = 1$$

On obtient alors pour tout $j \in [\![1, r]\!]$,

$\pi_j(1) = \pi_j\left(\sum u_i b_i\right) = \pi_j(u_j)\,\pi_j(b_j)$ donc $\pi_j(b_j) \in (A/(a_j))^*$ d'inverse $\pi_j(u_j)$.

Soit $(\pi_j(x_j))_{1 \leq j \leq r} \in A/(a_1) \times \dots \times A/(a_r)$ donné.

En posant $x = \sum_{i=1}^{r} x_i u_i b_i$, on a :

$\forall j \in [\![1, r]\!]$, $\pi_j(x) = \pi_j(x_j)\,\pi_j(u_j)\,\pi_j(b_j) = \pi_j(x_j)$

Par conséquent, φ est surjectif et se factorise en un isomorphisme $\overline{\varphi} : A/(a) \longrightarrow A/(a_1) \times \dots \times A/(a_r)$ d'inverse $\overline{\varphi}^{-1} : (\pi_j(x_j))_{1 \leq j \leq r} \longmapsto \sum_{i=1}^{r} x_i u_i b_i$.

Application Considérons le système $\begin{cases} u \equiv 1 \mod 3 \\ u \equiv 3 \mod 5 \\ u \equiv 0 \mod 7 \end{cases}$

Les solutions dans $\mathbb{Z}$ sont de la forme $28 + 105k$, $k \in \mathbb{Z}$.

Posons $u = u_1 + 3u_2 + 3 \times 5 u_3$.

On a :

- $u \equiv 1 \mod 3$ donc $u_1 \equiv 1 \mod 3$. Ainsi, $u_1 = 1$ et $u = 1 + 3u_2 + 3 \times 5 u_3$.
- $u \equiv 3 \mod 5$ donc $1 + 3u_2 \equiv 3 \mod 5$. Ainsi, $u_2 \equiv 2 \times 3^{-1} \mod 5$, or $\overline{3}^{-1} = \overline{2}$ donc $u_2 \equiv 4 \mod 5$.

On a donc $u_2 = 4$ et $u = 1 + 3 \times 4 + 3 \times 5 u_3 = 13 + 15 u_3$

- $u \equiv 0 \mod 7$ i.e. $13 + 15 u_3 \equiv 0 \mod 7$. On obtient donc : $u_3 \equiv +1 \mod 7$. On obtient alors $u = 13 + 15 = 28$.

Réciproquement $u = 28$ est bien solution du système.

Or :

$3 \times 5 \times 7 = 105$

Donc toutes les solutions sont de la forme $28 + 105k$, $k \in \mathbb{Z}$.

Application Considérons le système $\begin{cases} f(\bar{0}) = \bar{2} \\ f(\bar{1}) = \bar{0} \\ f(\bar{2}) = \bar{1} \end{cases}$ dans $\mathbb{Z}_5$.

La solution de degré minimal est $f = \bar{2} + \bar{4}X + \bar{4}X^2$.

Ce système se réécrit : $\begin{cases} f \equiv \bar{2} \mod X \\ f \equiv \bar{0} \mod X - \bar{1} \\ f \equiv \bar{1} \mod X - \bar{2} \end{cases}$

Posons $f = f_1 + f_2 X + f_3 X(X - \bar{1})$

On a :

- $f \equiv \bar{2} \mod X$ donc $f_1 = \bar{2}$. On a alors $f = \bar{2} + f_2 X + f_3 X(X - \bar{1})$.
- $f \equiv \bar{0} \mod X - \bar{1}$ i.e. $f(\bar{1}) = \bar{0}$, donc $\bar{2} + f_2 = \bar{0}$ i.e. $f_2 = -\bar{2} = \bar{3}$. Ainsi, $f = \bar{2} + \bar{3}X + f_3 X(X - \bar{1})$
- $f \equiv \bar{1} \mod X - \bar{2}$ i.e. $f(\bar{2}) = \bar{1}$. Donc : $\bar{2} + \bar{3} \times \bar{2} + \bar{2} f_3 = \bar{1}$, i.e. $f_3 = \bar{2}^{-1}\bar{3} = \bar{3} \times \bar{3} = \bar{4}$.

Par conséquent, la solution minimale est :

$f = \bar{2} + \bar{3}X + \bar{4}X(X - \bar{1}) = \bar{2} + \bar{4}X + \bar{4}X^2$.