Rombaldi p249 / p285+291

THÉORÈME DES RESTES CHINOIS & UNE APPLICATION

122, 142

120

Thm (des restes chinois): Soit A un anneau principal. Soit $(a_1, \dots, a_r) \in (A \setminus (A^\times \cup \{0\}))^r$ $(r \geq 2)$.
Posons $a = a_1 \cdots a_r$ et $\forall i \in [\![1,r]\!]$, $b_i = \frac{a}{a_i}$. Si les $a_1, \dots, a_r$ sont deux à deux premiers entre eux, alors

$$\overline{\varphi} : \frac{A}{\langle a_1 \cdots a_r \rangle} \longrightarrow \frac{A}{\langle a_1 \rangle} \times \cdots \times \frac{A}{\langle a_r \rangle}$$

$$x \bmod a_1 \cdots a_r \longmapsto (x \bmod a_1, \dots, x \bmod a_r)$$

est un isomorphisme d'anneaux ; de plus, il existe $(u_1, \dots, u_r) \in A^r$ tel que $\sum_{i=1}^{r} u_i b_i = 1$, et :

$$\overline{\varphi}^{-1} : (x_1 \bmod a_1, \dots, x_r \bmod a_r) \longmapsto \sum_{i=1}^{r} x_i u_i b_i \bmod a_1 \cdots a_r$$

▶ Soit $\varphi : A \longrightarrow \frac{A}{\langle a_1 \rangle} \times \cdots \times \frac{A}{\langle a_r \rangle}$ où $x \bmod a_i$ désigne l'image de x par la surjection canonique modulo a_i. Ces r dernières étant des morphismes d'anneaux, φ en est un également.
$x \longmapsto (x \bmod a_1, \dots, x \bmod a_r)$
De là, $\ker(\varphi) = \{x \in A \mid \forall j \in [\![1,r]\!], x \equiv 0 \bmod a_i\} = \{x \in A \mid \forall j \in [\![1,r]\!], a_j \mid x\} = \bigcap_{j=1}^{r} a_j A$. Or les a_i sont deux à deux premiers entre eux, donc d'après Prop 3 et Prop 8 du plan, et par une récurrence immédiate, $\ker(\varphi) = (a_1 \vee \cdots \vee a_r)A = a_1 \cdots a_r A$. D'après le théorème de factorisation des morphismes, $\overline{\varphi}$ est donc bien défini, et injectif.

▶ Montrons que $\overline{\varphi}$ est surjectif, donc bijectif, en exhibant sa réciproque : soit $(x_1 \bmod a_1, \dots, x_r \bmod a_r) \in \frac{A}{\langle a_1 \rangle} \times \cdots \times \frac{A}{\langle a_r \rangle}$.

▷ Les éléments $b_1, \dots, b_r$ sont premiers entre eux (dans leur ensemble) : par l'absurde, supposons le contraire. Alors il existe $p \in \mathcal{P}$ premier tel que $\forall i \in [\![1,r]\!]$, $p \mid b_i$. Donc $p \mid b_1 = a_2 \cdots a_r$, donc d'après le lemme d'Euclide, il existe $i_0 \in [\![2,r]\!]$ tel que $p \mid a_{i_0}$. Or $p \mid b_{i_0}$, donc il existe $i_1 \in [\![1,r]\!] \setminus \{i_0\}$ tel que $p \mid a_1$. Donc $p \mid a_{i_0} \wedge a_{i_1} = 1$, donc p est inversible : c'est absurde. □

▷ D'après le théorème de Bézout, il existe donc $(u_1, \dots, u_r) \in A^r$ tel que $\sum_{i=1}^{r} u_i b_i = 1$.

Posons $x := \sum_{i=1}^{r} u_i b_i x_i$. Soit $j \in [\![1,r]\!]$. Remarquons que pour $i \neq j$, $a_i \mid b_j$, donc $u_i b_i x_i \equiv 0 \bmod a_j$, et $u_i b_i \equiv 0 \bmod a_j$. De là, $1 = \sum_{i=1}^{r} u_i b_i \equiv u_j b_j \bmod a_j$, et $x \equiv u_j b_j x_j \equiv x_j \bmod a_j$.
Finalement, $\overline{\varphi}(x \bmod a_1 \cdots a_r) = \varphi(x) = (x_1 \bmod a_1, \dots, x_r \bmod a_r)$, CQFD ■

Application 1 : Cherchons $P \in \mathbb{Z}/5\mathbb{Z}[X]$ de degré minimal tel que $P(\bar{0}) = \bar{2}$, $P(\bar{1}) = \bar{0}$ et $P(\bar{2}) = \bar{1}$.
Cela revient à résoudre le système de congruence $\begin{cases} P \equiv \bar{2} \bmod X - \bar{0} \\ P \equiv \bar{0} \bmod X - \bar{1} \\ P \equiv \bar{1} \bmod X - \bar{2} \end{cases}$ dans $\mathbb{Z}/5\mathbb{Z}[X]$. Ce dernier étant principal, X, $X-\bar{1}$ et $X-\bar{2}$ étant deux à deux premiers entre eux (et non nuls, non inversibles), le théorème des restes chinois affirme l'existence d'une solution de la forme $P = \bar{2}U_0(X-\bar{1})(X-\bar{2}) + \bar{0}X(X-\bar{2})U_1 + \bar{1}U_2X(X-\bar{1})$

Or $P \equiv \bar{2} \bmod X$ donc $\bar{2} \equiv \bar{2}\,U_0\,\bar{2} \bmod X$, donc $U_0 \equiv \bar{3} \bmod X$ (rq : $\bar{2}^{-1} = \bar{3}$).
De même, $P \equiv \bar{1} \bmod X-\bar{2}$ donc $\bar{1} \equiv U_2\,X(X-\bar{1}) \bmod X-\bar{2}$. Or $X(X-\bar{1}) = (X-\bar{1})(X-\bar{2}) + \bar{2}$
donc $X(X-\bar{1}) \equiv \bar{2} \bmod X-\bar{2}$, donc $\bar{1} \equiv U_2\,\bar{2} \bmod X-\bar{2}$ puis $U_2 \equiv \bar{3} \bmod X-\bar{2}$.
On vérifie que pour $U_0 = U_2 = \bar{3}$, $P = (X-\bar{1})(X-\bar{2}) + \bar{3}\,X(X-\bar{1})$ est un polynôme d'interpolation, et qui plus est de degré minimal puisque de degré 2.

Application 2 : Résolvons $\begin{cases} k \equiv 2 & [4] \\ k \equiv 3 & [5] \\ k \equiv 1 & [9] \end{cases}$. Nous sommes bien dans les hypothèses du théorème des restes chinois : il suffit alors d'expliciter une relation de Bézout pour 4x5, 4x9 et 5x9.
Déjà, $20 \wedge 36 = 4 = 36 \times (-1) + 20 \times (2)$. Ensuite, $1 = 20 \wedge 36 \wedge 45 = 4 \wedge 45 = 45 \times (1) + 4 \times (-11)$,
donc $1 = 45 \times (1) + 36 \times (11) + 20 \times (-22)$. Posons $k_0 = 45 \times 1 \times 2 + 36 \times 11 \times 3 - 20 \times 22 \times 1 = 838$
D'après le théorème des restes chinois, en remarquant que $838 \equiv 118$ [4x5x9=180], l'ensemble des solutions est $118 + 180\,\mathbb{Z}$.