Théorème chinois et applications

↪ **Refs :** Rombaldi p249-250 (dém) + Ulmer p 57-59 (appli)

Théorème : (des restes chinois) Soit A un anneau principal. Soit $a_1, \dots, a_r$ $(r \geq 2)$ des éléments non nuls et non inversibles de A, deux à deux premiers entre eux. Alors l'application $A \xrightarrow{\varphi} A/\langle a_1\rangle \times \dots \times A/\langle a_r\rangle$, $x \mapsto (x \bmod a_1, \dots, x \bmod a_r)$ est un morphisme d'anneaux surjectif de noyau $\operatorname{Ker}(\varphi) = \langle \prod_{j=1}^{r} a_j \rangle$, et φ induit un isomorphisme d'anneaux

$$\overline{\varphi} : A/\langle \prod_{j=1}^{r} a_j \rangle \longrightarrow A/\langle a_1\rangle \times \dots \times A/\langle a_r\rangle$$
$$x \bmod \prod_{j=1}^{r} a_j \longmapsto (x \bmod a_1, \dots, x \bmod a_r).$$

<u>Preuve du théorème</u> : Pour tout $j \in [\![1, r]\!]$, on note π_j la surjection canonique $\pi_j : A \to A/\langle a_j \rangle$, $x \mapsto x \bmod a_j$. Toutes les π_j sont des morphismes d'anneaux, donc φ est un morphisme d'anneaux également. De plus, $\operatorname{Ker}(\varphi) = \{x \in A \mid \forall j \in [\![1, r]\!], a_j \mid x\} = \langle \prod_{j=1}^{r} a_j \rangle$ puisque les $(a_j)_{1 \leq j \leq r}$ sont premiers entre eux deux à deux.

Il nous reste à montrer la surjectivité de φ. Pour cela, on définit pour tout $i \in [\![1, r]\!]$, $b_i = \prod_{j \neq i} a_j$. Alors les $(b_i)_{1 \leq i \leq r}$ sont premiers entre eux dans leur ensemble. En effet, supposons (par l'absurde) que les $(b_i)_{1 \leq i \leq r}$ ne sont pas premiers entre dans leur ensemble : alors il existe p premier dans A qui divise tous les b_i (A est principal donc factoriel). Puisque p divise $b_1 = \prod_{j=2}^{r} a_j$, il existe, d'après le lemme d'Euclide, un $i_0 \in [\![2, r]\!]$ tel que $p \mid a_{i_0}$. Mais p divise également $b_{i_0} = \prod_{j \neq i_0} a_j$, donc toujours par le lemme d'Euclide, il existe $i_1 \neq i_0$ tel que $p \mid a_{i_1}$. Donc p divise a_{i_0} et a_{i_1} ↯ absurde puisque $a_{i_0} \wedge a_{i_1} = 1$.

Ainsi, d'après le théorème de Bezout, il existe $(u_i)_{1 \leq i \leq r}$ des éléments de A tels que $\sum_{i=1}^{r} u_i b_i = 1$.

Alors pour tout $j \in [\![1, r]\!]$, $\pi_j(u_j b_j) = \pi_j(1 - \underbrace{\sum_{i \neq j} u_i b_i}_{\text{divisible par } a_j}) = \pi_j(1) = 1$,
et si $i \neq j$, $\pi_i(u_j \underbrace{b_j}_{\text{divisible par } a_i}) = 0$. Ainsi $u_j b_j$ est l'antécédent par φ de $(0, \dots, 0, \underset{j}{1}, 0, \dots, 0)$.

Ainsi, si l'on se donne $(\pi_1(x_1), \dots, \pi_r(x_r)) \in A/\langle a_1 \rangle \times \dots \times A/\langle a_r \rangle$, on définit $x = \sum_{i=1}^{r} x_i u_i b_i$ et alors pour tout $j \in [\![1, r]\!]$, $\pi_j(x) = \sum_{i=1}^{r} \pi_j(x_i) \times \pi_j(u_i b_i) = \pi_j(x_j)$.
et donc $\varphi(x) = (\pi_1(x_1), \dots, \pi_r(x_r))$.

Ainsi le morphisme φ est surjectif et se factorise en un isomorphisme

$\overline{\varphi} : A/\langle \prod_{i=1}^{r} a_i \rangle \longrightarrow A/\langle a_1\rangle \times \dots \times A\langle a_r\rangle$, dont l'inverse

$x \bmod \prod_{i=1}^{r} a_i \mapsto (a \bmod a_1, \dots, a \bmod a_r)$

est donnée par $\overline{\varphi}^{-1} : A/\langle a_1\rangle \times \dots \times A/\langle a_r\rangle \longrightarrow A/\langle \prod_{i=1}^{r} a_i\rangle$

$$(\pi_1(x_1), \dots \pi_r(x_r)) \mapsto \sum_{i=1}^{r} x_i u_i b_i .$$

$$\begin{tikzcd} \varphi : A \arrow[r, two heads] \arrow[d] & \prod_{i=1}^{r} A/\langle a_i\rangle \arrow[l, bend right, dashed, "\varphi^{-1}"'] \arrow[dl, bend left, dashed, "\overline{\varphi}^{-1}"] \\ A/\langle a\rangle \arrow[ur, dashed, "\overline{\varphi}"'] & \end{tikzcd}$$

<u>Application à la résolution de systèmes de congruence :</u> Nous allons voir une méthode qui permet de rajouter des équations sans devoir tout modifier (contrairement à la méthode sous entendue dans la preuve, qui est tout de même très bien aussi !) On cherche une solution à $\begin{cases} x \equiv x_1 \bmod a_1 \\ \vdots \\ x \equiv x_r \bmod a_r \end{cases}$ de la forme $x = \gamma_1 + \gamma_2 a_1 + \gamma_3 a_1 a_2 + \dots + \gamma_r (a_1 a_2 \dots a_{r-1})$

avec $\nu(\gamma_i) < \nu(a_i)$ (on se place dans A euclidien !)

* On initialise avec $\gamma_1 = x_1$ afin de vérifier la première condition $(i \geq 2)$
* Supposons que l'on ait déterminé $\gamma_1, \dots \gamma_{i-1}$ à l'aide des $i-1$ premières équations, calculons γ_i à l'aide de $x \equiv x_i \bmod a_i$. Cette équation équivaut à $\gamma_1 + \gamma_2 a_1 + \dots + \gamma_i (a_1 \dots a_{i-1}) \equiv x_i \bmod a_i$, ou encore

$$\gamma_i (a_1 \dots a_{i-1}) \equiv x_i - (\gamma_1 + \gamma_2 a_1 + \dots + \gamma_{i-1}(a_1 \dots a_{i-2})) \bmod a_i .$$

Puisque $a_1 \dots a_{i-1}$ et a_i sont premiers entre eux, on en déduit que $a_1 \dots a_{i-1}$ est inversible dans $A/\langle a_i\rangle$, d'inverse δ_{i-1} que l'on peut obtenir grâce à l'algorithme d'Euclide étendu. Alors

$$\gamma_i = \delta_{i-1} (x_i - (\gamma_1 + \gamma_2 a_1 + \dots + \gamma_{i-1}(a_1 \dots a_{i-2})) \bmod a_i .$$

Par récurrence, nous avons alors obtenu $\gamma_1, \dots \gamma_r$ tel que x vérifie les r équations.

<u>Exemple 1 :</u> On veut résoudre dans $\mathbb{Z}$: $\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 0 \bmod 7 \end{cases}$ On pose donc $x = \gamma_1 + \gamma_2 \times 3 + \gamma_3 \times 15$

1) Comme $x \equiv 1 \bmod 3$, on a $\gamma_1 = 1$.
2) Comme $x \equiv 3 \bmod 5$, on a $1 + 3\gamma_2 \equiv 3 \bmod 5$, donc $\gamma_2 \equiv 2 \times 3^{-1} \bmod 5$. Or l'algo d'Euclide étendu nous donne $3 \times 2 - 1 \times 5 = 1$, donc l'inverse de 3 dans $\mathbb{Z}/5\mathbb{Z}$ est 2, d'où $\gamma_2 = 4$.
3) Comme $x \equiv 0 \bmod 7$, on a $1 + 3 \times 4 + 15\gamma_3 = 13 + 15\gamma_3 \equiv 0 \bmod 7$, donc $\gamma_3 = -13 \bmod 7 \equiv 1 \bmod 7$ (car $15 \equiv 1 \bmod 7$ ^^), donc $\gamma_3 = 1$, d'où $x = 13 + 15 = 28$. Ainsi les solutions du système dans $\mathbb{Z}$ sont de la forme $28 + 105k$ avec k dans $\mathbb{Z}$.

Exemple 2 : On veut résoudre dans $\mathbb{F}_5[X]$: $\begin{cases} f \equiv \bar{2} \bmod (X-\bar{0}) \\ f \equiv \bar{0} \bmod (X-\bar{1}) \\ f \equiv \bar{1} \bmod (X-\bar{2}) \end{cases}$, ce qui

(grâce au degré 1, à chaque étape il suffit d'évaluer :)

revient à chercher $f \in \mathbb{F}_5[X]$ tel que $f(\bar{0}) = \bar{2}$, $f(\bar{1}) = \bar{0}$ et $f(\bar{2}) = 1$

On pose donc $f = \gamma_1 + \gamma_2 X + \gamma_3 X(X-1) = \gamma_1 + \gamma_2 X + \gamma_3 (X^2 - X)$.

1) Comme $f \equiv \bar{2} \bmod (X)$, on a $\gamma_1 = \bar{2}$ donc $f = \bar{2} + \gamma_2 X + \gamma_3 (X^2 - X)$

2) Comme $f \equiv \bar{0} \bmod (X - \bar{1})$, ie $f(\bar{1}) = 0$, alors $\bar{2} + \gamma_2 = 0$, et donc $\gamma_2 = -\bar{2} = \bar{3}$. Ainsi $f = \bar{2} + \bar{3}X + \gamma_3 (X^2 - X)$.

3) Comme $f \equiv \bar{1} \bmod (X - \bar{2})$, ie $f(\bar{2}) = \bar{1}$, alors $\bar{2} + \bar{3} \times \bar{2} + \gamma_3 \times \bar{2} = \bar{1}$, ie $\bar{2} \times \gamma_3 = \bar{3}$. On utilise de nouveau l'algorithme d'Euclide étendu : $3 \times 2 - 1 \times 5 = 1$, donc $\bar{2}^{-1} = \bar{3}$, d'où $\gamma_3 = \bar{4}$.

Ainsi $f = \bar{2} + \bar{3}X + \bar{4}(X^2 - X) = \bar{2} + \bar{4}X + \bar{4}X^2$ (solution de degré minimal)

Remarques : * On peut aussi utiliser la méthode de la preuve :

(ex du Rombaldi) On veut résoudre dans $\mathbb{Z}$ $\begin{cases} k \equiv 2 [4] \\ k \equiv 3 [5] \\ k \equiv 1 [9] \end{cases}$.

On essaie de trouver u_1, u_2, u_3 tels que $u_1 m_1 + u_2 m_2 + u_3 m_3 = 1$ où $m_1 = 5 \times 9 = 45$, $m_2 = 4 \times 9 = 36$ et $m_3 = 4 \times 5 = 20$. On utilise l'associativité du PGCD :

$m_2 \wedge m_3 = 4 = -1 \times 36 + 2 \times 20 \Rightarrow 1 = m_1 \wedge (m_2 \wedge m_3) = 1 \times 45 - 11 \times 4$

$\Rightarrow 1 = 1 \times 45 - 11 \times 4 = 1 \times 45 + 11 \times 36 - 22 \times 20$.

Et alors $k = 2 \times 45 + 33 \times 36 - 22 \times 20 = 838$ et les solutions sur $\mathbb{Z}$ sont de la forme $838 + 180q = 118 + 180q'$.

* L'algo présenté ici s'appelle algo de Garner ou principe des bases mixtes.

* Pour résoudre, on peut aussi faire les relations de Bezout entre a_i et b_i : $u_i a_i + v_i b_i = 1$, et alors la solution est donnée par $\sum_{i=1}^{r} x_i v_i b_i$ (mais tout ça c'est la même chose par associativité du pgcd).

* Le théorème chinois a évidemment beaucoup d'autres applications, typiquement pour étudier φ l'indicatrice d'Euler, et la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$, ou pour le système RSA.

* Rappel sur l'algo d'Euclide étendu : (par un exemple parce que c'est beaucoup plus parlant) on cherche les coeffs de Bezout u et v tels que $120u + 23v = 1$:

$\begin{array}{r|l} 120 & 23 \\ -115 & 5 \\ \hline 5 & \end{array}$ $\quad \begin{array}{r|l} 23 & 5 \\ -20 & 4 \\ \hline 3 & \end{array}$ $\quad \begin{array}{r|l} 5 & 3 \\ -1 & 1 \\ \hline 2 & \end{array}$ $\quad \begin{array}{r|l} 3 & 2 \\ -2 & 1 \\ \hline 1 & \end{array}$

$$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (5 - 3 \times 1) \times 1 = 2 \times 3 - 5 \\ &= 2 \times (23 - 4 \times 5) - 5 = 2 \times 23 - 9 \times 5 \\ &= 2 \times 23 - 9(120 - 5 \times 23) = 47 \times 23 - 9 \times 120 \end{aligned}$$

Et maintenant sur des polynômes parce que c'est sympa de le savoir aussi : on cherche U et V tels que $fU+gV=1$ où $f(X)=X^4+2X^3+X+1$ et $g(X)=X^3+X-1$

$$\begin{array}{l|l} X^4+2X^3+X+1 & X^3+X-1 \\ \hline -\;X^4+X^2-X & X+2 \\ \hline \quad 2X^3-X^2+2X+1 & \\ -\;2X^3+2X-2 & \\ \hline \quad -X^2+3 & \end{array} \qquad \begin{array}{l|l} X^3+X-1 & -X^2+3 \\ \hline -\;X^3-3X & -X \\ \hline \quad 4X-1 & \end{array} \qquad \begin{array}{l|l} -X^2+3 & 4X-1 \\ \hline -\;-X^2+\frac{1}{4}X & -\frac{1}{4}X-\frac{1}{16} \\ \hline \quad -\frac{1}{4}X+3 & \\ -\;-\frac{1}{4}X+\frac{1}{16} & \\ \hline \quad \frac{47}{16} & \end{array}$$

$$\begin{aligned}
\frac{47}{16} &= (-X^2+3)+(4X-1)\times\left(\tfrac{1}{4}X+\tfrac{1}{16}\right) \\
&= (-X^2+3)+\left(\tfrac{1}{4}X+\tfrac{1}{16}\right)\left((X^3+X-1)+X(-X^2+3)\right) \\
&= (-X^2+3)\left(1+\tfrac{1}{4}X^2+\tfrac{1}{16}X\right)+\left(\tfrac{1}{4}X+\tfrac{1}{16}\right)(X^3+X-1) \\
&= \left(f-(X+2)g\right)\left(1+\tfrac{1}{4}X^2+\tfrac{1}{16}X\right)+\left(\tfrac{1}{4}X+\tfrac{1}{16}\right)g \\
&= \underbrace{\left(1+\tfrac{1}{16}X+\tfrac{1}{4}X^2\right)}_{P} f+\underbrace{\left[\left(\tfrac{1}{4}X+\tfrac{1}{16}\right)-(X+2)\left(1+\tfrac{1}{4}X^2+\tfrac{1}{16}X\right)\right]}_{Q}
\end{aligned}$$

et alors $U=\frac{16}{47}P$ et $V=\frac{16}{47}Q$ (Bref, c'est fastidieux)

⁂ On peut montrer dans le cas où n et m ne sont pas premiers entre eux qu'alors $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/\mathrm{ppcm}(n,m)\mathbb{Z}\times\mathbb{Z}/\mathrm{pgcd}(n,m)\mathbb{Z}$, et que le système $\begin{cases} x\equiv a[m] \\ x\equiv b[n]\end{cases}$ admet une solution ssi $a-b$ est divisible par $\mathrm{pgcd}(n,m)$ et alors les solut° sont de la forme $\underline{k_0}+k\,\mathrm{ppcm}(m,n)$

cf Rombaldi pour ⊕ de détails

⁂ Si $\mathbb{K}$ est un corps et $(\alpha_0,\dots,\alpha_n)$ sont des éléments distincts de $\mathbb{K}$, et $(\beta_0,\dots,\beta_n)$ des éléments quelconques de $\mathbb{K}$, le théorème chinois montre l'existence d'un polynôme d'interpolation ie un polynôme $P\in\mathbb{K}_n[X]$ tel que $P(\alpha_i)=\beta_i$ (et les solutions quelconques sont de la forme $P+Q\prod_{i=0}^{n}(X-\alpha_i)$)

En effet les α_i étant distincts, les $(X-\alpha_i)$ sont premiers entre eux, donc $\underset{\displaystyle\mathbb{K}_n[X]}{\underset{\wr\wr}{\mathbb{K}[X]/\langle\prod_{i=0}^{n}(X-\alpha_i)\rangle}}\simeq\prod_{i=0}^{n}\mathbb{K}[X]/\langle(X-\alpha_i)\rangle$.

De plus $P(\alpha_i)=\beta_i$ équivaut à la division euclidienne $P=Q(X-\alpha_i)+\beta_i$, ou encore à $P\equiv\beta_i \bmod (X-\alpha_i)$, ce qui conclut.

Autre exemple de cela : trouver P de degré minimal tel que $\begin{cases} f(-1)=-1 \\ f(0)=1 \\ f(1)=2 \\ f(2)=-2\end{cases}$, ça équivaut à $\begin{cases} f\equiv -1 \bmod X+1 \\ f\equiv 1 \bmod X \\ f\equiv 2 \bmod X-1 \\ f\equiv -2 \bmod X-2\end{cases}$, on cherche $f=\gamma_1+\gamma_2(X+1)+\gamma_3X(X+1)+\gamma_4X(X+1)(X-1)+\gamma_5X(X+1)(X-1)(X-2)$

et à chaque étape il suffit d'évaluer en