Théorème chinois généralisé

Perrine Jouteur

Je trouve ce développement assez sympathique, il s'apprend facilement et peut s'illustrer de plein de façons (les exemples, c'est le nerf de la guerre !). Je l'ai placé dans les leçons 120, 122, 126 et 142.

1 Contexte et prérequis

Définition 1.1 Un anneau est principal lorsqu'il est intègre et que tous ses idéaux sont principaux.

Proposition 1.1
Un anneau principal est factoriel.
De plus, dans un anneau principal, la relation de Bézout est vraie, et le théorème de Bézout aussi.

2 Théorème chinois classique

Soit A un anneau principal.

Dans toute cette section, on fixe des éléments $(m_1, \cdots, m_r)$ de A, et $(c_1, \cdots, c_r) \in A^r$. On considère le système suivant :

$$\begin{cases} x \equiv c_1 \ [m_1] \\ \cdots \\ x \equiv c_r \ [m_r] \end{cases} (*).$$

Théorème 2.1
On suppose que les m_i sont sont premiers entre eux deux à deux. Alors l'application $\beta : A \to A/(m_1) \times \cdots \times A/(m_r)$, $x \mapsto ([x]_{m_1}, \cdots, [x]_{m_r})$ est un morphisme d'anneaux, surjectif, de noyau $(m_1 \cdots m_r)$.
L'isomorphisme induit entre $A/(m_1 \cdots m_r)$ et $A/(m_1) \times \cdots \times A/(m_r)$ est d'inverse

$$\tilde{\beta}^{-1}([c_1]_{m_1}, \cdots, [c_r]_{m_r}) = [c_1 u_1 n_1 + \cdots c_r u_r n_r]_{m_1 \cdots m_r}$$

où pour tout i, on a posé $n_i = \frac{m_1 \cdots m_r}{m_i}$, de telle sorte que les n_i sont premiers entre eux dans leur ensemble, donc qu'il existe $u_1, \cdots, u_r$ tels que $u_1 n_1 + \cdots + u_r n_r = 1$.

Démonstration (du théorème)
• Le fait que β soit un morphisme d'anneaux surjectif est immédiat, car les projections de passage au quotient $A \to A/(m)$ sont des morphismes d'anneaux surjectifs.

• Montrons que le noyau de β est $(m_1 m_2)$.
Si x est multiple de $m_1 m_2$, alors sa classe modulo m_1 et nulle et sa classe modulo m_2 est nulle aussi donc $\beta(x) = 0$.
Inversement, si x est dans le noyau de β, alors m_1 divise x et m_2 divise x, et comme m_1 et m_2 sont premiers entre eux, on a $m_1 m_2$ qui divise x (valable car A est principal donc factoriel).

• Il suffit de le vérifier. ■

Corollaire 2.1 Le système $(*)$ possède des solutions, et possède une unique solution modulo $m_1 m_2$.

3 Le développement

Théorème 3.1
Soit A un anneau principal. Soient $(m_1, \cdots, m_r)$, et $(c_1, \cdots, c_r)$ des éléments de A. Alors le système $(*)$ possède des solutions ssi pour tout $i \neq j$, $c_i \equiv c_j \ [d_{ij}]$ où $d_{ij} = \text{pgcd}(m_i, m_j)$.

Démonstration
• La condition nécessaire est immédiate.

• Pour le sens direct, si $r = 1$, c'est immédiat.
Pour les $r \geq 2$, on va procéder par récurrence. La propriété que l'on va démontrer est

$$\mathcal{P}(r) : \text{"pour tout } (m_1, \cdots, m_r) \in A^r, \text{ pour tout } (c_1, \cdots, c_r) \in A^r, \text{ tels que pour tout } i \neq j,$$
$$c_i \equiv c_j \ [\text{pgcd}(m_i, m_j)], \text{ le système de congruences associé possède une solution."}$$

⋆ Initialisation à $r = 2$: soit $(m_1, m_2) \in A^2$, soit $(c_1, c_2) \in A^2$, tels que $c_1 \equiv c_2[d]$, où on a noté $d = \text{pgcd}(m_1, m_2)$. Notons $m_1 = dn_1$, $m_2 = dn_2$, avec n_1 et n_2 premiers entre eux. Il existe donc u, v tels que $n_1 u + n_2 v = 1$. On pose alors

$$x_0 = c_1 v n_2 + c_2 u n_1.$$

Vérifions que cela convient. La première équation est satisfaite de manière immédiate. Pour la deuxième, on remarque que

$$\begin{aligned} x_0 &= c_1 + \frac{c_2 - c_1}{d} u d n_1 \\ &= c_1 + (c_2 - c_1)(1 - v n_2) \\ &= c_2 - (c_2 - c_1) v n_2 \\ &= c_2 - \frac{c_2 - c_1}{d} v m_2 \\ &\equiv c_2 \ \ [m_2] \end{aligned}$$

Ainsi x_0 est bien solution du problème. De plus, on peut raffiner le résultat, en constatant que pour tout $t \in A$, l'élément $x_0 + t\,\text{ppcm}(m_1, m_2)$ est encore solution de $(*)$, et que ce sont les seules solutions.
En effet, si y est une solution, alors $x_0 - y \equiv 0[m_1]$ et $x_0 - y \equiv 0[m_2]$ donc $x_0 - y$ est un multiple commun de m_1 et m_2, et donc $x_0 - y$ est divisible par $\text{ppcm}(m_1, m_2)$.

On a donc démontré la proposition suivante :

$$\text{L'entier } x_0 \text{ est solution de } \begin{cases} x \equiv c_1[m_1] \\ x \equiv c_2[m_2] \end{cases}$$
$$\text{si et seulement si}$$
$$x_0 \equiv c_1 v n_2 + c_2 u n_1 [\text{ppcm}(m_1, m_2)]$$

⋆ Hérédité : soit $r \geq 2$ tel que $\mathcal{P}(r)$. Soient $(m_1, \cdots, m_{r+1}), (c_1, \cdots, c_{r+1}) \in A^{r+1}$, tels que pour tout $i \neq j$, on ait $c_i \equiv c_j \ [\text{pgcd}(m_i, m_j)]$.

D'après le cas $r = 2$, le système de deux équations $\begin{cases} x \equiv c_1[m_1] \\ x \equiv c_2[m_2] \end{cases}$ équivaut à la simple équation $x \equiv c_1 v n_2 + c_2 u n_1 \ [\text{ppcm}(m_1, m2)]$, où on a gardé les mêmes notations qu'avant.
Notons $c := c_1 v n_2 + c_2 u n_1$. Le système à $r+1$ équations que l'on cherche à résoudre équivaut au système à r équations suivant :

$$\begin{cases} x \equiv c \ \ [\text{ppcm}(m_1, m_2)] \\ x \equiv c_3 \ \ [m_3] \\ \cdots \\ x \equiv c_{r+1} \ \ [m_{r+1}] \end{cases}.$$

Vérifions que les hypothèses de $\mathcal{P}(r)$ sont vérifiées ici. Pour tout $i, j \geq 3$, on a bien $c_i \equiv c_j \ [\text{pgcd}(m_i, m_j)]$.
Soit $i \geq 3$. On veut montrer que $c \equiv c_i \ [\text{pgcd}(\text{ppcm}(m_1, m_2), m_i)]$.
Pour cela, on montre d'abord que $\text{pgcd}(\text{ppcm}(m_1, m_2), m_i) = \text{ppcm}(\text{pgcd}(m_1, m_i), \text{pgcd}(m_2, m_i))$. En effet, on regarde la décomposition en facteurs irréductibles de m_i, m_1 et m_2 et on a l'égalité.
Or on a $c_1 \equiv \alpha \ [\text{pgcd}(m_i, m_1)]$ et $c_2 \equiv \alpha \ [\text{pgcd}(m_i, m_2)]$, et aussi par hypothèse, $c_1 \equiv c_i \ [\text{pgcd}(m_i, m_1)]$ et $c_2 \equiv c_i \ [\text{pgcd}(m_i, m_2)]$ et donc par transitivité, $c_i \equiv \alpha \ [\text{pgcd}(m_i, m_1)]$ et $c_i \equiv \alpha \ [\text{pgcd}(m_i, m_2)]$. Donc $c_i \equiv \alpha [\text{ppcm}(\text{pgcd}(m_i, m_1), \text{pgcd}(m_i, m_2))]$ et on a ce qu'on voulait.

Par hypothèse de récurrence, on a donc une solution à notre système. ■

Remarque 3.1 Dans le cas où $A = \mathbb{Z}$, on peut estimer la complexité temporelle de la résolution du système. Supposons par exemple que $m_1 \leq m_2$.
Le calcul de d, u et v se fait via un algorithme d'Euclide étendu, en $O(\log(m_2))$ étapes, et à chaque étape on fait une division euclidienne et deux multiplications, donc en tout on a $O(\log(m_2)\log(m_1))$.
Pour le calcul de $\text{ppcm}(m_1, m_2)$, on peut faire $m_1 m_1/d$, donc c'est en $O(\log(m_1)\log(m_2))$.