Théorème chinois "traditionnel"

Soient $(m_i)_{1\leqslant i\leqslant r}\in\mathbb{Z}^r$ des entiers premiers entre eux deux-à-deux : $\forall i\neq j,\ \mathrm{pgcd}(m_i,m_j)=1$. Alors

$$\forall (a_i)_{1\leqslant i\leqslant r}\in\mathbb{Z}^r,\quad \exists x\in\mathbb{Z},\ \exists (k_i)_{1\leqslant i\leqslant r}\in\mathbb{Z}^r\quad :\quad \{\ x=a_i+k_i\,m_i\ \ \forall i\in[\![1,r]\!]$$

et toute autre solution est de la forme $x'=x+k\prod_{i=1}^r m_i$ avec $k\in\mathbb{Z}$.

De façon moins verbeuse,

$$\forall (a_i)_{1\leqslant i\leqslant r}\in\mathbb{Z}^r,\quad \exists x\in\mathbb{Z}\quad :\quad \{\ x\equiv a_i\ \mathrm{mod}\ m_i\ \ \forall i\in[\![1,r]\!]$$

c'est à dire qu'il existe une solution au système linéaire de congruence $\{\ x\equiv a_i\ \mathrm{mod}\ m_i\ \ \forall i$.

Preuve effective efficace : Soit $i\in[\![1,r]\!]$, posons

$$\hat{m}_i\ :=\ \prod_{\substack{1\leqslant j\leqslant r\\ j\neq i}} m_j$$

Alors, point crucial, $\mathrm{pgcd}(m_i,\hat{m}_i)=1$. On peut donc trouver r relations de Bezout :

$$\forall i\in[\![1,r]\!],\quad \exists u_i,v_i\in\mathbb{Z}\quad :\quad u_i\,m_i+v_i\,\hat{m}_i=1$$

Posons $e_i:=v_i\,\hat{m}_i$. On observe alors que

$$\begin{aligned} e_i\ &=\ 1-u_i\,m_i\ \equiv\ 1 \mod m_i\\ \forall j\neq i,\quad e_i\ &=\ v_i\,\hat{m}_i\ \equiv\ 0 \mod m_j \quad \text{car}\quad m_j\,\mathrm{div}\,\hat{m}_i\\ \text{donc}\ \forall j,\quad e_i\ &\equiv\ \mathbb{1}_{i=j} \mod m_j \end{aligned}$$

Ainsi, $(e_i)_{1\leqslant i\leqslant r}$ forme une « base de solutions » du système : on vérifie que

$$x\ :=\ \sum_{i=1}^r a_i\,e_i\ \equiv\ \sum_{i=1}^r a_i\,\mathbb{1}_{i=j}\ =\ a_j \mod m_j$$

est bien une solution du système.

Résolution pour $r=2$:

$$\forall x,k,\ell\in\mathbb{Z},\quad \begin{cases} x=a+k\,n\\ x=b+\ell\,m\end{cases}\quad\Longleftrightarrow\quad\begin{cases} x=a+k\,n\\ k\,n-\ell\,m=b-a=:c\end{cases}$$

Puisque $\mathrm{pgcd}(a,b)=1$, donnons-nous une relation de Bezout

$$n\,u+m\,v=1\quad\text{qui donne alors}\quad n\,u\,c+m\,v\,c=c$$

donc si l'on prend $k=u\,c=u\,(b-a)$ et $\ell=v\,c=v\,(b-a)$, on voit que $(x=a+k\,n,\ k,\ \ell)$ est solution particulière du système.

Autre solution particulière du système, plus simple à mémoriser :

$$x=n\,u\,b+m\,v\,a$$

en effet, la relation de Bezout donne $n\,u\,b=b-m\,v\,b$ et $m\,v\,a=a-n\,u\,a$ donc

$$\begin{cases} x=a+n\,u\,(b-a)\equiv a \mod n\\ x=b+m\,v\,(a-b)\equiv b \mod m\end{cases}$$

Maintenant, si (x',k',ℓ') est une autre solution, on a

$$\begin{aligned}\delta x:=x-x'\ &=\ (a+k\,n)-(a+k'\,n)\ =\ (k-k')\,n\\ &=\ (b+\ell\,m)-(b+\ell'\,m)\ =\ (\ell-\ell')\,m\end{aligned}$$

donc $m\,\mathrm{div}\,\delta x$ et $n\,\mathrm{div}\,\delta x$ donc, par le lemme de Gauss, $m\,n\,\mathrm{div}\,\delta x$ donc $x=x'+n\,m\,r$ avec $r\in\mathbb{Z}$.

Théorème chinois de $\mathbb{Z}/n\mathbb{Z}$

Soient $(m_i)_{1\leqslant i\leqslant r}\in\mathbb{Z}^r$ des entiers premiers entre eux deux-à-deux. $\forall i\in[\![1,r]\!]$, posons

$$\pi_i : \mathbb{Z} \xrightarrow{\text{can}} \mathbb{Z}/m_i\mathbb{Z} \quad \text{la projection canonique dans } \mathbb{Z}/m_i\mathbb{Z}$$

Alors on a une *surjection*

$$\pi_\times = \bigtimes_{i=1}^{r}\pi_i : x\longmapsto\big(\pi_i(x)\big)_{1\leqslant i\leqslant r} \quad \text{de} \quad \mathbb{Z}\twoheadrightarrow\bigtimes_{i=1}^{r}\mathbb{Z}/m_i\mathbb{Z}$$

qui se factorise en un unique *isomorphisme d'anneaux*

$$\mathbb{Z}/\left(\prod_{i=1}^{r}m_i\right)\mathbb{Z} \longleftrightarrow \bigtimes_{i=1}^{r}\mathbb{Z}/m_i\mathbb{Z}$$

Lien avec la formulation traditionnelle :

surjectivité $\Leftrightarrow$ existence de solutions, injectivité $\Leftrightarrow$ unicité modulo $\prod_{i=1}^{r}m_i$

Mais c'est un énoncé plus fort : on a une bijection, linéarité, ...

Et plus fort encore qu'une simple isomorphisme d'anneau, cet isomorphisme descend de $\pi_\times$!

Théorème chinois dans un anneau A commutatif

Théorème de Bezout : soient $a,b\in A$,

- Si $d\in\mathrm{PGCD}(a,b)$ est un PGCD, $aA+bA=dA$
  Et si A est *principal*, il existe toujours un PGCD.
- Si $m\in\mathrm{PPCM}(a,b)$ est un PPCM, $aA\cap bA=mA$

Théorème chinois général :

Soient $(I_i)_{1\leqslant i\leqslant r}$ des idéaux de A *comaximaux* deux-à-deux : $\forall i\neq j,\ I_i+I_j=A$ (c'est à dire que si $I_i=m_iA$ et $I_j=m_jA$, ce qui est toujours le cas dans un anneau principal, on ait $m_iA+m_jA=1A$, c'est à dire 1 est un PGCD, c'est à dire m_i *premier* avec m_j).

Alors on a une *surjection*

$$\pi_\times = \bigtimes_{i=1}^{r}\pi_i : x\longmapsto\big(\pi_i(x)\big)_{1\leqslant i\leqslant r} \quad \text{de} \quad A\twoheadrightarrow\bigtimes_{i=1}^{r}A/I_i \quad \text{avec} \quad \pi_i : A\xrightarrow{\text{can}}A/I_i$$

qui se factorise en un unique *isomorphisme d'anneaux*

$$A/\bigcap_{i=1}^{r}I_i \longleftrightarrow \bigtimes_{i=1}^{r}A/I_i$$