Le théorème mandarin

Xavier Caruso

Janvier 2009

Le théorème chinois est un énoncé classique sur les congruences, bien connu de tout agrégatif qui se respecte. Rappelons qu'il dit qu'un système de congruences de la forme $x \equiv a_i \pmod{N_i}$ avec les N_i premiers entre eux deux à deux admet toujours une solution (et, selon les versions, donne même une description explicite de celles-ci). Par contraste, la situation semble beaucoup plus confuse (au moins dans l'esprit des agrégatifs) lorsque les modulos N_i ne sont plus supposés premiers entre eux. Peut-on, dans ce cas, trouver des conditions simples à vérifier qui assurent l'existence d'une solution ? Peut-on, le cas échéant, décrire simplement l'ensemble des solutions ? Ce sont des questions qui, lors d'un oral, ont souvent du mal à trouver une réponse spontanée. Le but de cette note est de mener à bien cette étude, et notamment de répondre aux deux questions précédemment posées.

Théorème 1. *Soient $N_1, N_2, \dots, N_k$ des entiers strictement positifs, et $a_1, a_2, \dots, a_k$ des entiers quelconques. Alors le système suivant :*

$$(S) : \begin{cases} x & \equiv & a_1 & \pmod{N_1} \\ x & \equiv & a_2 & \pmod{N_2} \\ & \vdots & & \\ x & \equiv & a_k & \pmod{N_k} \end{cases}$$

admet une solution si, et seulement si pour tous i et j, on a $a_i \equiv a_j \pmod{d_{ij}}$ où $d_{ij} = \textsc{Pgcd}(N_i, N_j)$. Le cas échéant, il existe un entier a tel que (S) soit équivalent à la seule congruence $x \equiv a \pmod{\textsc{Ppcm}(N_1, \dots, N_k)}$.

Remarque. Lorsque les N_i sont premiers entre eux, on a $d_{ij} = 1$ pour tout couple (i, j) et donc les conditions $a_i \equiv a_j \pmod{d_{ij}}$ sont automatiquement satisfaites. On retrouve ainsi, dans ce cas, l'énoncé du théorème chinois. De plus, toujours dans ce cas, l'ensemble des solutions est décrit par la simple congruence $x \equiv a \pmod{N_1 \cdots N_k}$ puisque le plus petit commun multiple d'entiers premiers entre eux deux à deux n'est autre que leur produit.

Démonstration. La condition est clairement nécessaire. En effet, de $x \equiv a_i \pmod{N_i}$, on déduit $x \equiv a_i \pmod{d_{ij}}$ puisque d_{ij} divise N_i. De même, à partir de $x \equiv a_j \pmod{N_j}$, on obtient $x \equiv a_j \pmod{d_j}$. Il s'ensuit $a_i \equiv a_j \pmod{d_{ij}}$ comme voulu.

Pour la réciproque, on raisonne par récurrence. Le cas $k = 1$ est évident (on prend $a = a_1$), et on initialise la récurrence avec $k = 2$. Posons $d = d_{12}$. Le théorème de Bézout montre l'existence de deux entiers u et v tels que $uN_1 - vN_2 = d$. En multipliant cette égalité par $\frac{a_2 - a_1}{d}$ qui est entier par hypothèse, on obtient des entiers k_1 et k_2 tels que $k_1 N_1 - k_2 N_2 = a_2 - a_1$. Définissons $a = a_1 + k_1 N_1 = a_2 + k_2 N_2$. Il est clair que c'est une solution de (S). Il ne reste donc plus qu'à montrer que (S) est équivalent à $x \equiv a$

(mod $\textsc{Ppcm}(N_1, N_2)$). Or, en posant $y = x - a$, on voit tout de suite que x est solution de (S) si, et seulement si y est à la fois multiple de N_1 et N_2, *i.e* si, et seulement si y est multiple de $\textsc{Ppcm}(N_1, N_2)$. La conclusion en résulte.

Passons maintenant à l'hérédité. Supposons le théorème connu pour $k-1$ et donnons-nous un système (S) comme dans l'énoncé avec les conditions $a_i \equiv a_j \pmod{d_{ij}}$. D'après le cas que l'on vient de traiter, il existe un entier a' tel que les deux dernières congruences de (S) soient équivalentes à $x \equiv a' \pmod{N'}$ avec $N' = \textsc{Ppcm}(N_k, N_{k-1})$. Pour pouvoir appliquer l'hypothèse de récurrence, il s'agit de vérifier que le système de $(k-1)$ congruences

$$(S') : \begin{cases} x \equiv a_1 \pmod{N_1} \\ x \equiv a_2 \pmod{N_2} \\ \quad \vdots \\ x \equiv a_{k-2} \pmod{N_{k-2}} \\ x \equiv a' \pmod{N'} \end{cases}$$

satisfait les hypothèses du théorème. Il est déjà clair que si i et j sont compris entre 0 et $k-2$, on a $a_i \equiv a_j \pmod{d_{ij}}$. Il ne reste donc qu'à montrer que, pour tout $i \in \{1, \ldots, k-2\}$, on a $a_i \equiv a' \pmod{d'_i}$ avec $d'_i = \textsc{Pgcd}(N_i, N')$. Or, en décomposant N_i, N_{k-1} et N_k en facteurs premiers, on montre directement que $d'_i = \textsc{Ppcm}(d_{i,k-1}, d_{i,k})$. Ainsi la congruence souhaitée découle directement des hypothèses $a_i \equiv a_{k-1} \equiv a' \pmod{d_{k-1}}$ et $a_i \equiv a_k \equiv a' \pmod{d_k}$. L'hypothèse de récurrence nous assure qu'il existe un entier a tel que (S') — et donc (S) — soit équivalent à $x \equiv a \pmod{\textsc{Ppcm}(N_1, \ldots, N_{k-2}, N')}$. Comme il est clair que $\textsc{Ppcm}(N_1, \ldots, N_{k-2}, N') = \textsc{Ppcm}(N_1, \ldots, N_k)$, le théorème est démontré. □

Le théorème implique directement que (S) a une solution si, et seulement si chaque sous-système formé de deux équations de (S) en a une. En effet, si (S) a une solution, il est clair que chaque sous-système en a également une puisque la même convient. Réciproquement, le fait que le sous-système

$$\begin{cases} x \equiv a_i \pmod{N_i} \\ x \equiv a_j \pmod{N_j} \end{cases}$$

ait une solution implique, en appliquant le théorème avec $k = 2$, que $a_i \equiv a_j \pmod{d_{ij}}$. Mais comme ceci est vrai pour tous i et j, une nouvelle application du théorème montre que (S) a une solution.

Cette propriété peut se reformuler comme suit. Définissons pour commencer un sous-ensemble arithmétique[1] de $\mathbb{Z}$ comme un ensemble de la forme $a + n\mathbb{Z}$ pour certains entiers a et n (pas nécessairement premiers entre eux, bien entendu). On a alors

Théorème 2. *Soient $C_1, \ldots, C_k$ des sous-ensembles arithmétiques de $\mathbb{Z}$. Alors $C_1 \cap \cdots \cap C_k \neq \emptyset$ si, et seulement si $C_i \cap C_j \neq \emptyset$ pour tous indices i et j dans $\{1, \ldots, k\}$.*

Sous cette forme, l'énoncé précédent peut être rapproché du théorème de Helly suivant.

Théorème 3 (Helly)**.** *Soient $C_1, \ldots, C_k$ des parties convexes de $\mathbb{R}^2$. Alors $C_1 \cap \cdots \cap C_k \neq \emptyset$ si, et seulement si $C_a \cap C_b \cap C_c \neq \emptyset$ pour tous indices a, b et c dans $\{1, \ldots, k\}$.*

Remarque. On pourra objecter que le théorème de Helly fait intervenir des intersections trois à trois, et non deux à deux comme c'est le cas dans le théorème 2. Il se trouve que cette objection n'est pas vraiment pertinente car le théorème de Helly admet en fait une

[1] La terminologie n'est sans doute pas très bonne ; elle vient de la notion de suite arithmétique.

généralisation à toute dimension d qui fait intervenir des intersections $(d+1)$ à $(d+1)$ et qui s'énonce précisément comme suit : soient $C_1, \ldots, C_k$ des parties convexes de $\mathbb{R}^d$. Alors $C_1 \cap \cdots \cap C_k \neq \emptyset$ si, et seulement si $C_{i_0} \cap \cdots \cap C_{i_d} \neq \emptyset$ pour tous indices $i_0, \ldots, i_d$ dans $\{1, \ldots, k\}$. La situation que nous avons envisagée ici dans le théorème 2 correspondrait donc plutôt à un cas unidimensionnel (ce qui semble raisonnable vu que nos ensembles arithmétiques sont des sous-ensembles de $\mathbb{Z} = \mathbb{Z}^1$). Nous avons toutefois préféré énoncer le théorème de Helly en dimension 2 car celui-ci est évident et, en tout cas beaucoup moins frappant en dimension 1.

Pour terminer cette note, on donne la démonstration du théorème de Helly dans le cas de la dimension 2. D'aucuns pourront remarquer que la trame de la preuve donnée ci-dessous est tout à fait similaire à celle de la démonstration du théorème 1.

Démonstration du théorème de Helly dans le cas du plan. On procède par récurrence sur n. Évidemment, il n'y a rien à faire si $k \leqslant 3$. On initialise la récurrence avec $k = 4$. Soit A_1 (resp. A_2, resp. A , resp. A) un élément de $C_2 \cap C \cap C$ (resp. $C_1 \cap C \cap C$, resp. $C_1 \cap C_2 \cap C$, resp. $C_1 \cap C_2 \cap C$). On considère l'enveloppe convexe C des quatre points précédents. Si c'est un triangle (éventuellement aplati), disons pour fixer les idées de sommets A_1, A_2 et A , il suffit de remarquer que C est entièrement inclus dans C puisque ce dernier est convexe et que les points extrémaux de C appartiennent à C . En particulier A est dans C et donc dans l'intersection de tous les C_i. Supposons maintenant que C soit un quadrilatère. Ses sommets sont évidemment A_1, A_2, A et A et supposons, quitte à changer les indices, qu'il sont parcourus dans ce sens. Par le même argument que précédemment, le segment $[A_1A\,]$ (resp. $[A_2A\,]$) est entièrement contenu dans $C_2 \cap C$ (resp. $C_1 \cap C$) ; leur intersection, qui existe d'après l'hypothèse sur l'ordre de parcours, est donc dans tous les C_i.

Passons à l'hérédité. Supposons le théorème de Helly démontré lorsqu'il y a $k-1$ convexes, et donnons-nous k convexes vérifiant les bonnes hypothèses. Posons $C' = C_{k-1} \cap C_k$ et montrons que la famille de convexes $(C_1, \ldots, C_{k-2}, C')$ vérifie encore les hypothèses du théorème de Helly. On a bien sûr $C_a \cap C_b \cap C_c \neq \emptyset$ si a, b et c sont dans $\{1, \ldots, k-2\}$. Il suffit donc de montrer que $C_a \cap C_b \cap C'$ est non vide pour tous a et b dans $\{1, \ldots, k-2\}$. Mais $C_a \cap C_b \cap C' = C_a \cap C_b \cap C_{k-1} \cap C_k$, et il suffit, pour montrer la non-vacuité de cette intersection, d'invoquer le théorème de Helly dans le cas $k = 4$ (que l'on a démontré dans le premier alinéa). L'hypothèse de récurrence nous dit alors que $C_1 \cap \cdots \cap C_{k-2} \cap C'$ est non vide, ce qui est exactement ce que l'on désirait. □