Le Chinois en une fois

Jean-François Burnol, 6 avril 2017

Soient $n_1, \ldots, n_k$ des entiers strictement positifs premiers entre eux deux à deux. On veut résoudre le Problème Chinois :

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\cdots \qquad\quad \cdots\cdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Je dis pour ne pas y revenir que bien sûr une fois trouvée une solution particulière x les autres sont de la forme $x + tn_1 \ldots n_k$, avec $t \in \mathbf{Z}$.

Il y a de nombreuses approches pour trouver une solution particulière.

Tout d'abord il est extrêmement naturel d'exploiter l'aspect « linéaire » de ce problème et donc de rechercher une solution de la forme

$$x = a_1 x_1 + \cdots + a_k x_k$$

chaque x_j résolvant son problème avec 1 dans la j^{e} équation et 0 ailleurs. On sait bien que cela se résout en formant, par l'algorithme d'Euclide, une identité de Bézout,

$$\underbrace{Un_j + V\prod_{i\neq j} n_i = 1}_{\text{ceci donne un } x_j \text{ convenable !}}$$

Donc on aura dû appliquer k fois l'algorithme d'Euclide étendu !

Une autre approche est fort naturelle également et procéde itérativement en résolvant d'abord le système avec les deux premières équations, que l'on transforme en une seule équation modulo $n_1 n_2$, puis on recommence, etc…

Le système des deux premières équations se résout en un seul Bézout

$$Un_1 + Vn_2 = 1$$

car $a_1 Vn_2 + a_2 Un_1$ sera notre solution particulière. On l'utilise alors comme second membre pour le module $n_1 n_2$ et on résout le système avec n_3, et ainsi de suite… Cette approche nous demande $k-1$ Bézout, et les entiers sont plutôt plus petits que dans l'approche précédente. Donc ça va plus vite.

Encore une autre méthode consiste à trouver par n'importe quel moyen une écriture

$$\frac{1}{n_1 \dots n_k} = \frac{u_1}{n_1} + \cdots + \frac{u_k}{n_k}$$

Vous voyez que $x_1 = u_1 n_2 \dots n_k$, $x_2 = u_2 n_1 n_3 \dots n_k$, … serviront comme les x_j de tout à l'heure, et donc une solution particulière est

$$x = a_1 u_1 n_2 \dots n_k + \cdots + a_k u_k n_1 \dots n_{k-1}$$

ce qui, de manière plus mémorable, s'écrit :

$$\frac{x}{n_1 \dots n_k} = \frac{u_1 a_1}{n_1} + \cdots + \frac{u_k a_k}{n_k}$$

Le problème est de trouver la décomposition de $1/(n_1 \dots n_k)$. Si l'on fait par récurrence en maintenant à chaque étape une forme complètement décomposée, on aura besoin de $1 + 2 + 3 + \cdots + (k-1) = k(k-1)/2$ Bézout, c'est la catastrophe ! [1]

Non, bien sûr ce qu'il faut faire c'est de d'abord décomposer par exemple

$$\frac{1}{n_1 \dots n_k} = \frac{u}{n_1 \dots n_{k-1}} + \frac{v}{n_k}$$

pour nous débarrasser de n_k et ensuite on itère. Bon, en fait c'est un peu comme notre deuxième méthode. On aura besoin de $k-1$ identités de Bézout.

Ah, mais ne peut-on approcher ça par un découpage dyadique familier des méthodes « rapides » en algorithmique ? Par exemple imaginons qu'on a 8 entiers, on les sépare en deux groupes de 4, par un Bézout. Ensuite le premier groupe de 4 est séparé en deux de deux par un Bézout. On a besoin d'un Bézout pour l'autre groupe de 4. Ça fait 3 Bézout pour le moment, et il nous reste 4 groupes de 2 : ben non, au final on a encore eu à faire 7 Bézout ! On s'est cru malin(igne) et c'est tombé à plat !

Alors c'est là où normalement vous devriez être épaté(e)s par ce que je vais raconter. J'ai une solution sans calculs ! Il y a un léger caveat, mais bon voilà ma solution :

$$x = \frac{\dfrac{a_1}{n_1} + \cdots + \dfrac{a_k}{n_k}}{\dfrac{1}{n_1} + \cdots + \dfrac{1}{n_k}}$$

1. C'est en fait un peu plus subtil. Car lorsqu'on fait un Bézout avec l'un des n_i et un nombre même très grand, dès la première étape de l'algorithme d'Euclide, on a un reste plus petit que n_i, donc il y a peu d'effet lié à un coût de manipuler de « grands entiers », à part bien sûr faire explicitement tous les produits. Cependant faire les produits $n_1 n_2$, $n_1 n_2 n_3$, …, $n_1 \dots n_k$ aura aussi un coût en k^2, donc ça pourrait, se dit-on, être aussi coûteux que nos nombreux $k(k-1)/2$ Bézout. Cependant, pour exprimer la solution nous avons besoin de tous les produits $\prod_{i \neq k} n_i$, donc, non, je crois qu'on ne peut pas sauver la méthode avec les $k(k-1)/2$ Bézout…

Qu'est-ce que c'est que ce truc ?

Ceux qui lisent mes fiches (y-en-a-t-il ?) auront immédiatement reconnu mon approche à la décomposition de Dunford. Mais je n'insiste pas.

Tout d'abord, cette solution en est clairement une comme on voit en multipliant en haut et en bas par $n_1 \dots n_k$ et en réduisant modulo n_1 à la fois le numérateur et le dénominateur, ça donne $\frac{a_1 n_2 \dots n_k}{n_2 \dots n_k} = a_1$, et idem avec les autres...

Le petit couac, c'est que x est un nombre rationnel !

Pour moi, le problème est quasi résolu là, mais si vous insistez que je dois fournir un nombre entier, ce n'est pas un problème.

Théorème. *Il existe une identité de Bézout*

$$U \sum_j \prod_{i \neq j} n_i + V n_1 \dots n_k = 1$$

et le problème Chinois admet comme solution particulière

$$x = U \sum_j a_j \prod_{i \neq j} n_i$$

Preuve. Considérons un diviseur premier p de $n_1 \dots n_k$. Il divise l'un et uniquement l'un des n_j. Mais alors ce p divise *tous* les termes de la somme à gauche *sauf* $\prod_{i \neq j} n_i$. Donc il ne divise PAS la grosse somme. La grosse somme et le produit sont donc premiers entre eux et il existe une identité de Bézout.

Je laisse en exercice le fait que la formule pour x marche ![2] □

Nous pouvons donc résoudre le Chinois en une fois : un unique Bézout nous donne le U et c'est gagné !

Faisons un peu de pratique. Je prends $n_1 = 10$, $n_2 = 21$, et $n_3 = 13$. Je calcule $S = 10 * 21 + 10 * 13 + 21 * 13 = 613$, et $P = 10 * 21 * 13 = 2730$.

2. Et je m'aperçois que je laisse en exercice le lien entre ce Théorème et ma formule magique

$$x = \frac{\frac{a_1}{n_1} + \dots + \frac{a_k}{n_k}}{\frac{1}{n_1} + \dots + \frac{1}{n_k}}$$

Mais c'est que je ne peux pas tout faire !

Je fais l'algorithme d'Euclide étendu à ma façon, qui n'est pas très connue,[3] mais bon, comme j'ai une macro qui le fait automatiquement je ne peux pas rajouter de commentaires, mais vous pouvez faire comme vous voulez.

$$
\begin{aligned}
2730 &= 4\times 613 + 278\\
4 &= 4\times 1 + 0\\
1 &= 4\times 0 + 1
\end{aligned}
$$

$$
\begin{aligned}
613 &= 2\times 278 + 57\\
9 &= 2\times 4 + 1\\
2 &= 2\times 1 + 0
\end{aligned}
$$

$$
\begin{aligned}
278 &= 4\times 57 + 50\\
40 &= 4\times 9 + 4\\
9 &= 4\times 2 + 1
\end{aligned}
$$

$$
\begin{aligned}
57 &= 1\times 50 + 7\\
49 &= 1\times 40 + 9\\
11 &= 1\times 9 + 2
\end{aligned}
$$

$$
\begin{aligned}
50 &= 7\times 7 + 1\\
383 &= 7\times 49 + 40\\
86 &= 7\times 11 + 9
\end{aligned}
$$

$$
\begin{aligned}
7 &= 7\times 1 + 0\\
2730 &= 7\times 383 + 49\\
613 &= 7\times 86 + 11
\end{aligned}
$$

$$86\times 2730 - 383\times 613 = 1$$

Ça marche donc avec $U = -383$.

Conclusion :

Corollaire 1. *Une solution particulière au système*

$$
\begin{aligned}
x &\equiv a_1 \pmod{10}\\
x &\equiv a_2 \pmod{21}\\
x &\equiv a_3 \pmod{13}
\end{aligned}
$$

est donnée par

$$x = -383\cdot\left(273a_1 + 130a_2 + 210a_3\right)$$

3. Vous remarquez qu'il n'y a aucun signe négatif ? c'est pas la « remontée » vers Bézout usuelle…

Bon, peut-on encore simplifier ? Oui bien sûr. Si je mets le 383 à l'intérieur dans le produit $383 * 273$ je n'ai besoin que de le connaître modulo 10, car $10 * 273 = n_1 n_2 n_3$. Donc en fait, notre vériable solution eſt

$$x = -(3 * 273a_1 + 5 * 130a_2 + 6 * 210a_3)$$

Prenons plutôt des nombres positifs :

$$x = 7 * 273a_1 + 16 * 130a_2 + 7 * 210a_3$$

et comme par hasard avec $x_1 = 7 * 273 = 1911$, $x_2 = 16 * 130 = 2080$, $x_3 = 1470$ on a des « idempotents » comme dans notre toute première méthode.

On voit donc que l'on peut reformer plus commodément pour la pratique notre théorème :

Théorème. *Le problème Chinois admet comme solution particulière*

$$x = U \cdot \Big(\sum_j a_j \prod_{i \neq j} n_i \Big)$$

et plus commodément aussi

$$x = \sum_j U_j a_j \prod_{i \neq j} n_i$$

avec U_j le reſte de U dans la division euclidienne par n_j, où U eſt tout entier intervenant dans une identité de Bézout

$$U \sum_j \prod_{i \neq j} n_i + V n_1 \dots n_k = 1$$

Il eſt toujours possible de trouver une telle identité lorsque les n_j sont premiers entre eux deux à deux car les deux entiers $\sum_j \prod_{i \neq j} n_i$ et $n_1 \dots n_k$ sont alors premiers entre eux.

Comme U eſt unique modulo $n_1 \dots n_k$, les entiers $0 < U_j < n_j$ sont indépendants du choix de U. D'ailleurs, la classe de congruence de U modulo n_j eſt l'inverse multiplicatif de $\prod_{i \neq j} n_i$.

Terminons sur la remarque suivante : on peut fusionner le terme $V n_1 \dots n_k$ avec par exemple le terme $U \prod_{i \neq 1} n_i$ et ainsi obtenir une identité de Bézout prouvant que les $\prod_{i \neq j} n_i$ sont premiers entre eux dans leur ensemble.

Bien sûr, ceci peut s'acquérir en examinant quels nombres premiers peuvent diviser tous les termes et conclure qu'il n'y en a pas.

Mais il est plus fort de dire que les *deux* entiers $\sum_j \prod_{i\neq j} n_i$ et $n_1 \dots n_k$ sont premiers entre eux et de déduire comme conséquence que les $\prod_{i\neq j} n_i$ sont premiers entre eux dans leur ensemble.

~~C'est tout pour aujourd'hui !~~

Addendum. On peut choisir les signes arbitrairement $\epsilon_j = \pm 1$, $1 \leqslant j \leqslant m$ et obtenir une (pseudo) solution particulière aussi à partir de

$$x = \frac{\sum_j \epsilon_j \dfrac{a_j}{n_j}}{\sum_j \epsilon_j \dfrac{1}{n_j}},$$

car le dénominateur ne peut jamais s'annuler.

Lorsque l'on fait les calculs à la main, le fait d'alterner les signes conduira à un $\sum_j \epsilon_j \prod_{i\neq j} n_i$ plus petit. Ce qui peut accélérer un peu l'algorithme d'Euclide pour trouver le $U(\epsilon_1, \dots, \epsilon_k)$ via Bézout.

En fait on peut plus généralement obtenir une (pseudo, car pas entière) solution particulière de la forme

$$x = \frac{\sum_j \dfrac{a_j y_j}{n_j}}{\sum_j \dfrac{y_j}{n_j}},$$

avec un choix arbitraire des y_j du moment que pour tout j, la condition $(n_j, y_j) = 1$ est respectée.

Car le dénominateur ne peut alors pas s'annuler (si on le multiplie par $\prod_i n_i$ et que l'on réduit alors modulo n_1, la classe est non nulle). Il existera une identité de Bezout

$$1 = U(y_1, \dots, y_m) \sum_j y_j \prod_{i\neq j} n_i + V(y_1, \dots, y_m) \cdot n_1 \dots n_k$$

par le même raisonnement que celui-fait précédemment.

Ce qui donnera une (véritable) solution particulière

$$x = U(y_1, \dots, y_m) \sum_j a_j y_j \prod_{i\neq j} n_i$$

J'aurais peut-être dû écrire $U \cdot n_1 \dots n_k + V \cdot \sum_j \prod_{i\neq j} n_i = 1$ et non pas $V \cdot n_1 \dots n_k + U \cdot \sum_j \prod_{i\neq j} n_i = 1$ à cause de l'ordre alphabétique.