Systèmes de congruences

Jean-François Burnol, 5 avril 2018, typo corrigée 10 avril

On s'intéresse au système (avec des $A_i > 0$) :

$$\begin{aligned} x &\equiv a_1 \pmod{A_1} \\ x &\equiv a_2 \pmod{A_2} \\ &\vdots \\ x &\equiv a_n \pmod{A_n} \end{aligned} \tag{S_n}$$

Lorsque les modules A_i sont premiers entre eux le Théorème Chinois dit qu'il y a une unique solution modulo $\prod_i A_i$. En général la différence de deux solutions est divisible par chaque A_i donc par leur PPCM.

$$M = \mathrm{PPCM}(A_1, \ldots, A_n) \tag{1}$$

Il y a donc **au plus** une solution modulo M.

Le cas n = 2. Le système S_2 est résoluble si et seulement si $a_1 - a_2$ est divisible par $d = \mathrm{PGCD}(A_1, A_2)$:

- si x est solution alors x est congru modulo d à la fois à a_1 et a_2 d'où la nécessité,
- pour la suffisance, partons d'une identité de Bézout $u_1A_1 + u_2A_2 = d$, que je mets sous forme $u_1\frac{A_1}{d} + u_2\frac{A_2}{d} = 1$. On pose alors :

$$y = a_2u_1\frac{A_1}{d} + a_1u_2\frac{A_2}{d} \tag{2}$$

ATTENTION aux indices !
Modulo A_1 on peut remplacer dans y le a_2 par a_1 puisque la différence est divisible par d et d fois A_1/d fait A_1. Donc

$$y \equiv a_1u_1\frac{A_1}{d} + a_1u_2\frac{A_2}{d} = a_1 \pmod{A_1} \tag{3}$$

et de même modulo A_2, d'où la solution unique

$$x \equiv a_2u_1\frac{A_1}{d} + a_1u_2\frac{A_2}{d} \pmod{\mathrm{PPCM}(A_1, A_2)} \tag{4}$$

Le cas n = 3. S_3 contient déjà toute la difficulté du cas général ! Inutile de le traiter séparément. On anticipe un problème en regardant l'équation (2), car est-ce que c'est a_2 ou a_3 qui serait associé à un $\frac{A_1}{D}$, $D = \mathrm{PGCD}(A_1, A_2, A_3)$? En fait la question est mal posée car ce D ne va pas intervenir. On reviendra plus tard sur ce qui peut remplacer (2).

Le cas général. La théorie (on reviendra sur la pratique) se traduit par le théorème suivant :

Théorème 1. *Le système* S_n *possède une solution si et seulement si les conditions de compatibilité* $a_i - a_j \equiv 0 \pmod{\mathrm{PGCD}(A_i, A_j)}$ *sont satisfaites pour* ***tous*** *les couples* $(i, j), i < j$.

Preuve. La nécessité est immédiate, montrons la suffisance.

Soit M le PPCM. Soit p un diviseur premier de M. Définissons x_p de la manière suivante : [1]

— $x_p = a_1$ si $v_p(a_1) = v_p(M)$,
— sinon, $x_p = a_2$ si $v_p(a_2) = v_p(M)$,
— sinon, $x_p = a_3$ si $v_p(a_3) = v_p(M)$,
— ...
— sinon $x_p = a_n$. On a alors $v_p(a_n) = v_p(M)$.

Considérons maintenant le système des congruences :

$$\forall p \mid M \quad y \equiv x_p \pmod{p^{v_p(M)}} \tag{5}$$

Les modules étant premiers entre eux deux-à-deux, le Théorème Chinois spécial nous dit que ce système a une solution y. On peut normaliser y par $0 \leqslant y < M$, ce qui le rend unique.

Montrons que ce y résout notre S_n.

Pour établir $y \equiv a_1 \pmod{A_1}$ il suffit de vérifier

$$\forall p \mid M \quad y \equiv a_1 \pmod{p^{v_p(A_1)}} \tag{6}$$

car en tout cas tous les diviseurs premiers de A_1 sont parmi ceux de M (et une équation de congruence modulo 1 n'impose aucune contrainte). En effet, ces équations toutes ensemble disent que $y - a_1$ est divisible par A_1.

Or, *par la condition de compatibilité*, on a certainement

$$x_p \equiv a_1 \pmod{p^{v_p(A_1)}} \tag{7}$$

1. Je rappelle que $v_p(x)$ est l'exposant de p dans la factorisation de x. On peut aussi l'étendre aux fractions. Par convention $+\infty$ si $x = 0$.

car il existe un indice j avec $v_p(A_j) = v_p(M)$ et tel que $x_p = a_j$. Or on a par hypothèse que $\mathrm{PGCD}(A_1, A_j)$ divise $a_1 - a_j$. Mais $p^{v_p(A_1)}$ divise $\mathrm{PGCD}(A_1, A_j)$, donc il divise $a_1 - a_j$ c'est-à-dire il divise $a_1 - x_p$ ce qu'il fallait vérifier pour (7).

On a donc obtenu (6) et on fait de même pour les autres congruences. Ce qui conclut la démonstration. □

Remarque. Je laisse en exercice le fait qu'il faut vraiment exiger les compatibilités pour tous les couples. On peut, quel que soit n, faire un exemple où toutes les paires d'équations de S_n sont compatibles entre elles sauf les deux dernières.

Pratique. Le plus simple est d'appliquer itérativement la méthode pour $n = 2$. On remplace les deux premières équations par une seule équivalente, découvrant au passage si la compatibilité est vérifiée. Et ainsi de suite...

On peut faire une fois pour toutes le calcul des identités de Bézout pour A_1 et A_2 puis $\mathrm{PPCM}(A_1, A_2)$ et A_3 puis $\mathrm{PPCM}(A_1, A_2, A_3)$ et A_4 etc... au cas où il s'agit de résoudre encore et encore S_n mais avec des a_i variables.

Existe-t-il un analogue de (2)? Oui. En fait, (2) nous dit grosso modo que dans le cas $n = 2$ on applique formellement la formule pour résoudre le Chinois spécial, et si le système est compatible le y est bien une solution de S_2. Il se trouve que cela marche aussi pour tout n si on s'y prend bien.

Une formule pour la solution. Le lemme suivant est bien connu :

Lemme 1. *Si* $M = \mathrm{PPCM}(A_1, \ldots, A_n)$ *alors les* M/A_i *sont premiers entre eux dans leur ensemble.*

Preuve. Si p premier les divise tous il est en tout cas un diviseur de M. Mais il existe j avec $v_p(A_j) = v_p(M)$ donc p ne peut pas diviser M/A_j contradiction. □

Il existe donc une identité de Bézout

$$v_1 \frac{M}{A_1} + v_2 \frac{M}{A_2} + \cdots + v_n \frac{M}{A_n} = 1 \tag{8}$$

et l'analogue valable pour tout n de (2) est

$$y = a_1 v_1 \frac{M}{A_1} + a_2 v_2 \frac{M}{A_2} + \cdots + a_n v_n \frac{M}{A_n} \tag{9}$$

En effet **si une solution x à S_n existe** alors ce y vérifie

$$y \equiv x v_1 \frac{M}{A_1} + x v_2 \frac{M}{A_2} + \cdots + x v_n \frac{M}{A_n} = x \pmod{M} \tag{10}$$

puisque la différence $(a_j - x)$ est divisible par A_j donc $(a_j - x)M/A_j$ est divisible par M...

Donc (9) résout S_n **si** S_n **admet une solution !**

Finalement comment obtenir une équation de Bézout (8) ? Elle revient à trouver une écriture avec des entiers relatifs

$$\frac{1}{\mathrm{PPCM}(A_1, \ldots, A_n)} = \sum_j \frac{v_j}{A_j} \tag{11}$$

Il suffit de faire étape par étape $\mathrm{PPCM}(A_1, A_2)$ puis $\mathrm{PPCM}(\mathrm{PPCM}(A_1, A_2), A_3)$ etc... donc ce sont exactement les mêmes Bézout deux par deux qui interviennent dans ce que je décrivais plus haut.

Remarque. On peut montrer en effet qu'un y défini par (9) est solution de S_n si les conditions de compatibilité sont satisfaites, donnant ainsi une autre preuve du Théorème principal. Mais pour ce faire je n'ai pas pour le moment de méthode essentiellement différente que de considérer à nouveau les nombres premiers p et le genre de raisonnement déjà fait pour la preuve du Théorème.

La même remarque s'applique pour la méthode qui consiste à remplacer les équations $x \equiv a_j \pmod{A_j}$ par

$$\forall j \qquad x \equiv a_j \pmod{A'_j} \tag{12}$$

où les A'_j sont choisis de sorte que

1. pour chaque j, A'_j divise A_j,
2. les A'_j sont premiers entre eux deux-à-deux,
3. $\prod_j A'_j = \mathrm{PPCM}(A_1, \ldots, A_n)$.

Pour montrer que la solution (qui existe toujours) du nouveau système est une solution de S_n lorsque les relations de compatibilité sont vérifiées, je dois passer à nouveau par un raisonnement avec les nombres premiers du style de celui déjà fait pour le Théorème principal. Donc l'intérêt de cette méthode semble faible sur le plan théorique, et aussi très discutable sur le plan pratique car il n'est pas facile d'obtenir les A'_j et en plus il faudra aussi faire des Bézout avec eux pour résoudre concrètement le système qu'ils définissent.