Systèmes de congruences (II)

Jean-François Burnol, 11 avril

Dans

http://jf.burnol.free.fr/agreg180405chinoiseries.pdf

on s'est intéressé au système (avec des $A_i > 0$) :

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

qui possède au plus une solution modulo

$$M = \operatorname{ppcm}(A_1, \ldots, A_n) \tag{1}$$

et l'on a établi :

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

Je donne ici une deuxième preuve qui ne passe pas par les nombres premiers.

Preuve. Les gens vont être contents, je fais par récurrence. Le cas S_2 a été traité préalablement et est considéré connu.

Donc supposons $n \geqslant 2$, et le théorème établi pour les systèmes du type S_n et montrons qu'il vaut pour $n + 1$ congruences.

La nécessité étant une conséquence du cas S_2 admis en pré-requis, montrons la suffisance.

Par l'hypothèse de récurrence il existe un x_0 (dépendant des a_j et des A_j) tel que l'on puisse remplacer les n premières équations par une seule qui leur est équivalente :

$$x \equiv x_0 \pmod{\operatorname{ppcm}(A_1, \ldots, A_n)} \tag{2}$$

Pour conclure il s'agit de vérifier que $x_0 - a_{n+1}$ est divisible par

$$D = \operatorname{pgcd}(\operatorname{ppcm}(A_1, \ldots, A_n), A_{n+1}) \tag{3}$$

Or, par un Lemme que nous espérons établir après coup

$$D = \mathrm{ppcm}(\mathrm{pgcd}(A_1, A_{n+1}), \mathrm{pgcd}(A_2, A_{n+1}), \ldots, \mathrm{pgcd}(A_n, A_{n+1})) \tag{4}$$

Donc, il suffit d'établir que $x_0 - a_{n+1}$ est divisible par $d_j = \mathrm{pgcd}(A_j, A_{n+1})$, pour chaque $1 \leqslant j \leqslant n$. Mais modulo A_j donc aussi modulo d_j on a $x_0 \equiv a_j$ par définition de x_0. Et $a_j - a_{n+1}$ est divisible par d_j par hypothèse.

Ce qui conclut la preuve (modulo le Lemme qui suit). □

Lemme 1. *Soit* $n \geqslant 1$ *et* $A_1, \ldots, A_n$ *des entiers relatifs. Alors, pour tout* $A \in \mathbb{Z}$ *:*

$$\mathrm{pgcd}(\mathrm{ppcm}(A_1, \ldots, A_n), A) = \mathrm{ppcm}(\mathrm{pgcd}(A_1, A), \mathrm{pgcd}(A_2, A), \ldots, \mathrm{pgcd}(A_n, A)) \tag{5}$$

Preuve. D'abord je rappelle à tout hasard que $\mathrm{pgcd}(0, a) = |a|$ (y-compris pour $a = 0$) car dans tous les cas on prend $\mathrm{pgcd}(a, b)$ comme le générateur positif de l'idéal $a\mathbb{Z} + b\mathbb{Z}$). Par ailleurs $\mathrm{ppcm}(0, a) = 0$ pour tout $a \in \mathbb{Z}$ car dans tous les cas $\mathrm{ppcm}(a, b)$ est défini comme le générateur positif de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$.

De plus on convient que $\mathrm{ppcm}(x)$ est simplement $|x|$ (y-compris si $x = 0$) et de même pour $\mathrm{pgcd}(x)$ (mais on n'en a pas besoin ici, sauf si on avait voulu faire l'énoncé pour $n = 0$...)

L'énoncé est donc vrai pour $n = 1$. Supposons qu'il est vrai pour $n = 2$ et montrons le par récurrence pour $n + 1$. Avec

$$M_n = \mathrm{ppcm}(A_1, \ldots, A_n) \tag{6}$$

$$M_{n+1} = \mathrm{ppcm}(A_1, \ldots, A_n, A_{n+1}) \tag{7}$$

On calcule

$$\begin{aligned}
\mathrm{pgcd}(M_{n+1}, A) &= \mathrm{pgcd}(\mathrm{ppcm}(M_n, A_{n+1}), A) && (8)\\
&= \mathrm{ppcm}(\mathrm{pgcd}(M_n, A), \mathrm{pgcd}(A_{n+1}, A)) \quad (\text{cas } n = 2) && (9)\\
&= \mathrm{ppcm}(\mathrm{ppcm}(\mathrm{pgcd}(A_1, A), \ldots, \mathrm{pgcd}(A_n, A)), \mathrm{pgcd}(A_{n+1}, A)) \quad (\text{réc.}) && (10)\\
&= \mathrm{ppcm}(\mathrm{pgcd}(A_1, A), \ldots, \mathrm{pgcd}(A_n, A), \mathrm{pgcd}(A_{n+1}, A)) && (11)
\end{aligned}$$

Tout sera donc fini lorsqu'on aura fait le cas $n = 2$!

La preuve est donc terminée modulo ce cas (qui est celui correspondant à la réduction d'un S_3 à un S_2, donc la remarque faite précédemment que toute la difficulté de S_n était déjà dans S_3 revient à ce propos à l'esprit). □

Lemme 2. *Soit* $A, B, C \in \mathbb{Z}$. *Alors :*

$$\mathrm{pgcd}(\mathrm{ppcm}(A, B), C) = \mathrm{ppcm}(\mathrm{pgcd}(A, C), \mathrm{pgcd}(B, C)) \tag{12}$$

Preuve. En termes d'idéaux il s'agit de prouver

$$(A\mathbb{Z} \cap B\mathbb{Z}) + C\mathbb{Z} = (A\mathbb{Z} + C\mathbb{Z}) \cap (B\mathbb{Z} + C\mathbb{Z}) \tag{13}$$

Si $C = 0$ c'est vrai (immédiat) ; si $A = 0$ aussi (quasi-immédiat). Donc si $B = 0$ aussi. On peut donc les supposer non nuls, et quitte à les remplacer par leurs valeurs absolues, dorénavant $A, B, C > 0$.

Si l'on s'autorise les nombres premiers, notre affirmation se ramène à établir pour des entiers naturels a, b, c :

$$\min(\max(a, b), c) = \max(\min(a, c), \min(b, c)) \tag{14}$$

ce qui est faisable (avec des nombres réels quelconques) en considérant tous les cas de figures : on peut sans perte de généralité supposer $a \leqslant b$, donc on examine $c \leqslant a \leqslant b$, $a \leqslant c \leqslant b$ et $a \leqslant b \leqslant c$. Ça marche !

Mais je cherche à éviter le recours aux nombres premiers dans la preuve de ce lemme !

Le terme de gauche est certainement inclus à la fois dans $A\mathbb{Z} + C\mathbb{Z}$ et dans $B\mathbb{Z} + C\mathbb{Z}$, donc dans leur intersection, qui est le terme de droite.

Ce qui est plus délicat c'est l'inclusion du terme de droite dans celui de gauche. Supposons donc que $x \in A\mathbb{Z} + C\mathbb{Z}$ et aussi $x \in B\mathbb{Z} + C\mathbb{Z}$. Posons $D = \mathrm{pgcd}(A, B)$. On a

$$\frac{B}{D}x \in \frac{B}{D}(A\mathbb{Z} + C\mathbb{Z}) \subset \frac{AB}{D}\mathbb{Z} + C\mathbb{Z} \tag{15}$$

$$\frac{A}{D}x \in \frac{A}{D}(B\mathbb{Z} + C\mathbb{Z}) \subset \frac{AB}{D}\mathbb{Z} + C\mathbb{Z} \tag{16}$$

Il existe une identité de Bézout $uA + vB = D$ et donc

$$x = u\frac{A}{D}x + v\frac{B}{D}x \in \frac{AB}{D}\mathbb{Z} + C\mathbb{Z} \tag{17}$$

Or AB/D est précisément $\mathrm{ppcm}(A, B)$ et la preuve est terminée. □

Seconde preuve. En fait c'est la même mais sans idéaux, et je suppose d'emblée $A, B, C > 0$.

$\mathrm{ppcm}(A, B)$ est un multiple de A donc de $\mathrm{pgcd}(A, C)$. Donc $\mathrm{pgcd}(A, C)$ divise à la fois C et $\mathrm{ppcm}(A, B)$ ainsi il divise $\mathrm{pgcd}(\mathrm{ppcm}(A, B), C)$.

De même pour pgcd(B, C) : il divise pgcd(ppcm(A, B), C). Les deux combinés on voit que ppcm(pgcd(A, C), pgcd(B, C)) divise pgcd(ppcm(A, B), C).

C'était la partie facile. Je rappelle que l'on veut en fait l'égalité :

$$\text{pgcd}(\text{ppcm}(A, B), C) = \text{ppcm}(\text{pgcd}(A, C), \text{pgcd}(B, C)) \tag{18}$$

Notons $D = \text{pgcd}(A, B)$, et $M = AB/D = \text{ppcm}(A, B)$.

Soit maintenant

$$x = \text{ppcm}(\text{pgcd}(A, C), \text{pgcd}(B, C)) \tag{19}$$

Comme x est divisible par pgcd(A, C), on peut, par BÉZOUT pour (A, C), écrire x sous la forme kA + lC donc le produit $\frac{B}{D}x$ est de la forme kM + l'C et est divisible par pgcd(M, C).

De même x étant divisible par pgcd(B, C) est de la forme mB + nC donc $\frac{A}{D}x$ est de la forme mM + n'C et est divisible par pgcd(M, C).

Mais il existe u, v avec uA + vB = D, donc $x = u\frac{A}{D}x + v\frac{B}{D}x$ est lui aussi divisible par pgcd(M, C).

On vient de montrer que ppcm(pgcd(A, C), pgcd(B, C)) était multiple de pgcd(M, C) et c'est qu'il restait à établir. □