

Master 1 Informatique 2023–2024 Compléments de maths

Compléments sur la résolution de systèmes de congruence.

Le théorème des restes chinois (Théorème 9 du poly) affirme l'existence de solutions entières pour un système de congruence, lorsque les modules sont deux à deux premiers entre eux. Lorsque ce n'est pas le cas, un système peut, ou non avoir des solutions. La proposition suivante donne une condition nécessaire et suffisante à l'existence de solutions dans le cas général.

Proposition. Soit $r \geq 1$. Soient a_1, \dots, a_r des entiers relatifs et n_1, \dots, n_r tels que $n_i \geq 1$ pour tout $i \in \{1, \dots, r\}$. On considère le système suivant d'inconnue $x \in \mathbb{Z}$.

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_r \pmod{n_r}. \end{cases} \quad (1)$$

Le système (1) admet des solutions si et seulement si les conditions suivantes sont vérifiées :

$$\forall i, j \in \{1, \dots, r\}, i \neq j, a_i \equiv a_j \pmod{\text{pgcd}(a_i, a_j)}.$$

Dans le cas où le système admet des solutions, celles-ci sont en nombre infini. Néanmoins, modulo $\text{ppcm}(n_1, \dots, n_r)$, la solution est unique.

Remarque. Ce résultat généralise le cas des entiers premiers entre eux car dans ce cas, les pgcd entre modules sont égaux à 1 et une équation $a_i \equiv a_j \pmod{1}$ est toujours vérifiée. En effet, dire que a_i est équivalent à a_j modulo 1, c'est dire que a_i peut s'écrire sous la forme $a_j + 1 \times k$ et en effet : $a_i = a_j + 1 \times (a_i - a_j)$. La condition d'unicité modulo le ppcm généralise aussi le théorème 9 car dans le cas où n et m sont premiers entre eux $\text{ppcm}(n, m) = nm$.

Dans la suite est présentée une résolution d'un système de congruence. On y montre comment se ramener à la résolution de systèmes à deux équations, et comment résoudre un système lorsque les modules ne sont pas premiers entre eux.

Exercice 26 question 3.

On considère le système suivant et cherche à le résoudre dans \mathbb{Z} .

$$\begin{cases} x \equiv 2 \pmod{8} \\ x \equiv 7 \pmod{9} \\ x \equiv 8 \pmod{14}. \end{cases} \quad (2)$$

Commençons par vérifier l'existence ou non de solutions. Tout d'abord, on observe que 8 et 9 sont premiers entre eux. C'est aussi le cas pour 9 et 14. Il n'y a donc pas de condition supplémentaire à vérifier pour ces couples. En revanche 8 et 14 ne sont pas premiers entre eux puisque $\text{pgcd}(8, 14) = 2$. Néanmoins, $2 \equiv 0 \pmod{2}$ et $8 \equiv 0 \pmod{2}$, on en déduit donc que le système (2) admet des solutions entières.

Nous avons vu en TD comment résoudre un système à deux équations lorsque les modules sont premiers entre eux. On est donc en mesure de prouver que le sous-système formé des deux premières équations vérifie l'équivalence suivante :

$$\begin{cases} x \equiv 2 \pmod{8} \\ x \equiv 7 \pmod{9} \end{cases} \iff x \equiv 34 \pmod{72} \quad (3)$$

Remarque. Il est **vivement conseillé** de vous exercer en remontrant comment la valeur 34 a été trouvée. Ceci étant dit, on peut tout de même vérifier que $34 \equiv 2 \pmod{8}$ et $34 \equiv 7 \pmod{9}$, donc 34 est bien une solution entière du sous-système et invoquer le théorème des restes chinois pour garantir que l'ensemble des solutions est $S = \{34 + 72k, k \in \mathbb{Z}\}$ (infinité de solutions entières, mais unicité de la solution modulo 72).

D'après l'équivalence (3), nous déduisons l'équivalence suivante :

$$\begin{cases} x \equiv 2 \pmod{8} \\ x \equiv 7 \pmod{9} \\ x \equiv 8 \pmod{14} \end{cases} \iff \begin{cases} x \equiv 34 \pmod{72} \\ x \equiv 8 \pmod{14} \end{cases} \quad (4)$$

Il ne reste donc qu'à résoudre ce système à deux équations. Deux options s'offrent à nous :

Option 1 : On cherche la solution pas à pas (analyse puis synthèse)

Soit $x \in \mathbb{Z}$ une solution du système (4). Puisque x est solution, x vérifie en particulier $x \equiv 34 \pmod{72}$ donc il existe $k \in \mathbb{Z}$ tel que $x = 34 + 72k$. On peut alors remplacer x dans la deuxième équation et obtenir :

$$34 + 72k \equiv 8 \pmod{14}.$$

De cette égalité, on déduit en réduisant modulo 14, $72k \equiv -26 \equiv 2 \pmod{14}$, et même, $2k \equiv 2 \pmod{14}$ (car $72 \equiv 2 \pmod{14}$). Ainsi, il existe $\ell \in \mathbb{Z}$ tel que $2k = 2 + 14\ell$, autrement dit, $k = 1 + 7\ell$. En remplaçant dans $x = 34 + 72k$ par la valeur de k trouvée, on obtient $x = 34 + 72 + 504\ell = 106 + 504\ell$.

Ainsi on vient de montrer que **si** x est solution, **alors** x vérifie $x = 106 + 504\ell$. (D'après la proposition, on peut s'arrêter ici car on a trouvé une équation modulo $504 = \frac{72 \times 14}{\text{pgcd}(72, 14)} = \text{ppcm}(72, 14)$).

Réciproquement, soit $t \in \mathbb{Z}$, vérifions que $106 + 504t$ est solution du système (4). Modulo 72, on observe que $106 + 504t \equiv 106 \pmod{72}$ puisque $504 = 72 \times 7$. Enfin $106 \equiv 34 \pmod{72}$ donc $106 + 504t$ vérifie la première équation.

Modulo 14, on observe que $106 + 504t \equiv 106 \pmod{14}$ puisque $504 = 14 \times 36$. Enfin $106 \equiv 8 \pmod{14}$ donc $106 + 504t$ vérifie la seconde équation.

Ainsi $106 + 504t$ est solution du système et ce, quelque soit $t \in \mathbb{Z}$.

On a donc prouvé (par analyse/synthèse) que l'ensemble des solutions du système est

$$S = \{106 + 504t, t \in \mathbb{Z}\}.$$

Remarque. On note une nouvelle fois l'infinité de solutions entières, mais l'unicité de la solution modulo le ppcm.

Option 2 : méthode proche de celle vue en TD pour les modules premiers entre eux.

On part de nouveau du système suivant :

$$\begin{cases} x \equiv 34 \pmod{72} \\ x \equiv 8 \pmod{14} \end{cases}$$

On a déjà noté que $\text{pgcd}(72, 14) = 2$, l'algorithme d'Euclide étendu nous donne donc un couple $(u, v) \in \mathbb{Z}^2$ tel que $72u + 14v = 2$.

$$\begin{aligned}
72 &= 72 \times 1 + 14 \times 0 \\
14 &= 72 \times 0 + 14 \times 1 \\
2 &= 72 \times 1 + 14 \times (-5) \quad L_3 = L_1 - 5L_2
\end{aligned}$$

Ainsi $(u, v) = (1, -5)$ convient. En regardant l'égalité (dans \mathbb{Z}) $72u + 14v = 2$, modulo 72 et modulo 14 on obtient successivement : $14v = 2 \pmod{72}$ et $72u = 2 \pmod{14}$. En notant que $14v = -70$ et $72u = 72$, on a donc :

$$\begin{cases} -70 \equiv 2 \pmod{72} \\ -70 \equiv 0 \pmod{14} \end{cases} \quad \text{et} \quad \begin{cases} 72 \equiv 0 \pmod{72} \\ 72 \equiv 2 \pmod{14} \end{cases}$$

Ainsi, en multipliant -70 par $34/2 = 17$ et 72 par $8/2 = 4$, on obtient :

$$\begin{cases} 17 \times -70 \equiv 17 \times 2 \equiv 34 \pmod{72} \\ 17 \times -70 \equiv 17 \times 0 \equiv 0 \pmod{14} \end{cases} \quad \text{et} \quad \begin{cases} 4 \times 72 \equiv 4 \times 0 \equiv 0 \pmod{72} \\ 4 \times 72 \equiv 4 \times 2 \equiv 8 \pmod{14} \end{cases}$$

Enfin en additionnant les équations ci-dessus, on obtient alors :

$$\begin{cases} 17 \times -70 + 4 \times 72 \equiv 34 + 0 \equiv 34 \pmod{72} \\ 17 \times -70 + 4 \times 72 \equiv 0 + 8 \equiv 8 \pmod{14} \end{cases} .$$

Ainsi $17 \times -70 + 4 \times 72$ est une solution du système. D'après la généralisation du théorème des restes chinois, il s'agit de l'unique solution modulo $\text{ppcm}(72, 14) = 504$.

Notons que $17 \times -70 + 4 \times 72 = -1190 + 288 = -182 + 288 = 106 \pmod{504}$. On en déduit donc

$$S = \{106 + 504t, t \in \mathbb{Z}\}.$$