Système de congruences linéaires

Considérons le système de congruences suivantes

$$(*)\quad \begin{cases} x \equiv 2 \pmod 7 & ① \\ x \equiv 3 \pmod 5 & ② \end{cases}$$

Une première méthode pour résoudre ce système est la suivante :

$x \equiv 2 \pmod 7 \iff \exists\, K \in \mathbb{Z}$ tel que $x = 7K+2$.

Pour déterminer la classe de congruence de K, on utilise ② :

$$x \equiv 3 \pmod 5 \iff 7K+2 \equiv 3 \pmod 5 \iff$$
$$\iff 2K \equiv 1 \pmod 5 \iff K \equiv 3 \pmod 5 \iff$$
$$\iff \exists\, h \in \mathbb{Z} \text{ t. q. } K = 5h+3.$$

Donc x est solution du système $(*)$ si et seulement si $\exists\, h \in \mathbb{Z}$ t.q.

$$x = 7(5h+3)+2 = 35h+23.$$

Le système $(*)$ a donc une unique solution modulo 35.

Dans ce cours on va voir que cela est un exemple d'un résultat plus général : le théorème des restes chinois.

THÉORÈME DES RESTES CHINOIS

Soient $n_1, \dots, n_k$ des entiers premiers entre eux deux à deux, c'est à dire $\text{pgcd}(n_i, n_j) = 1$, $\forall\, i \neq j$.
Soient $a_1, \dots, a_k \in \mathbb{Z}$.
On considère le système de congruences linéaires

$$(**)\quad \begin{cases} z \equiv a_1 \pmod{n_1} \\ z \equiv a_2 \pmod{n_2} \\ \vdots \\ z \equiv a_k \pmod{n_k} \end{cases}$$

Alors l'ensemble des solutions dans $\mathbb{Z}$ de $(*)$ est non vide et c'est une classe d'équivalence modulo $N = n_1 \cdots n_k$.

Dém

L'existence d'au moins une solution est donnée par l'algorithme suivant, qui renvoie le représentant canonique de la classe d'équivalence modulo N.

Algorithme : RestesChinois $((a_1,\dots,a_k),(n_1,\dots,n_k))$

Entrées : deux k-uplets d'entiers $(a_1,\dots,a_k)$ et $(n_1,\dots,n_k)$ tels que $\text{pgcd}(n_i,n_j)=1$, $\forall i \neq j$.

Sortie : Un entier z, $0 \leq z < N$, où $N = \prod_{i=1}^{k} n_i$ tel que $z \equiv a_i \pmod{n_i}$ $\forall\ i = 1,\dots,k$.

1. $N \leftarrow \prod_{i=1}^{k} n_i$

2. $\forall\ i=1,\dots,k$: $N_i = \dfrac{N}{n_i}$ (division exacte)

3. $\forall\ i=1,\dots,k$: $U_i \leftarrow$ InverseMod(N_i, n_i)
   ↳ U_i est l'inverse de N_i mod n_i et cela existe, car $\text{pgcd}(n_i,N_i)=1$.

4. Renvoyer $\sum_{i=1}^{k} a_i \cdot U_i \cdot N_i \mod N$.

Montrons d'abord que l'algorithme est correcte. Pour cela on montrera que :

① l'entier $z_0 = \sum_{i=1}^{k} a_i U_i N_i$ est une solution du système $(**)$

② tout entier dans la classe de congruence modulo N de z_0 est une solution du système (**)

On montrera ensuite que la classe de z_0 est l'unique solution du système (**)

① Soit $z_0 = \sum_{i=1}^{N} a_i u_i N_i$.

Par construction $u_i \cdot N_i \equiv 1 \pmod{n_i}$, $\forall i = 1, \dots, K$.

De plus, $\forall j \neq i$, $n_i \mid N_j = \prod_{\ell \neq j} n_\ell$

Donc $\forall i = 1, \dots, K$ on a :

$$z_0 = \sum_{j=1}^{K} a_j u_j N_j = \left(\sum_{\substack{j=1,\dots,K \\ j \neq i}} a_j u_j N_j \right) + a_i u_i N_i \equiv$$

$$\equiv 0 + a_i \cdot 1 \pmod{n_i} \equiv a_i \pmod{n_i}$$

($j \neq i$, $n_i \mid N_j$; $u_i N_i \equiv 1 \pmod{n_i}$)

Donc z_0 est une solution de (*).

② Soit z' un entier dans la classe de z_0. Alors on a :

$$z' \equiv z_0 \pmod{N} \iff \exists K \in \mathbb{Z} \text{ t.q. } z' = z_0 + NK =$$

$$= z_0 + N_i n_i K \Rightarrow \forall i = 1, \dots, K, \quad z' = z_0 + N_i n_i K \equiv$$

($N = \frac{N}{n_i} \cdot n_i = N_i \cdot n_i$)

$$\equiv z_0 + 0 \pmod{n_i} \equiv a_i \pmod{n_i}.$$

Comme évoqué plus en haut, il reste à montrer que si $z' \in \mathbb{Z}$ est une solution de (**), alors $z' \equiv z_0 \pmod{N}$

Si z' est une solution de (**), alors $\forall i = 1, \dots, K$ on a

$$z' \equiv a_i \pmod{n_i} \equiv z_0 \pmod{n_i} \Rightarrow \forall i = 1, \dots, K \quad n_i \mid (z' - z_0)$$

$$\Rightarrow \prod_{i=1}^{K} n_i \mid (z' - z_0) \Rightarrow N \mid (z' - z_0) \Rightarrow z' \equiv z_0 \pmod{N}$$

($\text{pgcd}(n_i, n_j) = 1$, $\forall i \neq j$)

Exemple 1

$$\begin{cases} z \equiv 4 \mod 7 \\ z \equiv 5 \mod 11 \\ z \equiv 3 \mod 5 \end{cases}$$

On a $\text{pgcd}(7,11) = \text{pgcd}(7,5) = \text{pgcd}(11,5) = 1$.

D'après le théorème il existe une unique solution modulo $N = 5 \cdot 7 \cdot 11 = 385$.

$N_1 = N/7 = 55$

$N_2 = N/11 = 35$

$N_3 = N/5 = 77$

Maintenant on doit résoudre :

$U_1 \cdot 55 \equiv 1 \pmod 7 \iff U_1 \cdot 6 \equiv 1 \pmod 7 \iff U_1 = 6$

$U_2 \cdot 35 \equiv 1 \pmod{11} \iff U_2 \cdot 2 \equiv 1 \pmod{11} \iff U_2 = 6$

$U_3 \cdot 77 \equiv 1 \pmod 5 \iff U_3 \cdot 2 \equiv 1 \pmod 5 \iff U_3 = 3$

On calcule :

$$4 \cdot 6 \cdot 55 + 5 \cdot 6 \cdot 35 + 3 \cdot 3 \cdot 77 = 3063 \mod 385$$

$$= \boxed{368 \pmod{385}}$$

Exemple 2

$$\begin{cases} 3x \equiv 1 \pmod 4 \\ 2x \equiv 5 \pmod 7 \\ 6x \equiv 3 \pmod 9 \end{cases}$$

Il faut d'abord mettre, si possible, le système sous la forme (**). Dans notre cas, cela donne :

$$\begin{cases} 3\cdot 3x \equiv 3\cdot 1 \pmod 4 \\ 4\cdot 2x \equiv 4\cdot 5 \pmod 7 \\ \frac{6x}{3} \equiv \frac{3}{3} \pmod{\frac{9}{3}} \end{cases} \iff \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 6 \pmod 7 \\ 2x \equiv 1 \pmod 3 \end{cases} \iff$$

$$\iff \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 6 \pmod 7 \\ x \equiv 2 \pmod 3 \end{cases}$$

Maintenant le système est de la forme (**) et on peut appliquer l'algorithme des restes chinois.

1) $N = 4\cdot 7\cdot 3 = 84$

2) $N_1 = \frac{84}{4} = 21$, $N_2 = \frac{84}{7} = 12$, $N_3 = \frac{84}{3} = 28$.

3) $21U_1 \equiv 1 \pmod 4 \iff U_1 \equiv 1 \pmod 4$

$12U_2 \equiv 1 \pmod 7 \iff 5U_2 \equiv 1 \pmod 7 \iff U_2 \equiv 3 \pmod 7$

$28U_3 \equiv 1 \pmod 3 \iff U_3 \equiv 1 \pmod 3$

4) $z_0 = 3\cdot 1\cdot 21 + 6\cdot 3\cdot 12 + 2\cdot 1\cdot 28 = 63 + 216 + 56 = 335 \equiv$

$\equiv -1 \mod 84 \equiv \boxed{83 \mod 84}$

Donc l'unique solution du système modulo 84 est 83. Cela aurait pu être trouvée rapidement, en remarquant que le système est équivalent au suivant.

$$\begin{cases} x \equiv -1 \pmod 4 \\ x \equiv -1 \pmod 7 \\ x \equiv -1 \pmod 3 \end{cases}$$