Le théorème chinois

Un exemple détaillé

On veut résoudre le système $x = x_i \mod n_i$ défini par

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 5 \\ x \equiv 4 \mod 7 \\ x \equiv 5 \mod 11 \\ x \equiv 9 \mod 13 \end{cases}$$

On remarque tout d'abord que 3, 5, 7, 11 et 13 sont premiers entre eux. On va remplir le tableau suivant au fur et à mesure en rajoutant les équations une à une.

i	n_i	x_i	N	u	v	x	$x \mod n_i$
1	3	1	3	$\times$	$\times$	1	1
2	5	2	–	–	–	–	–
3	7	4	–	–	–	–	–
4	11	5	–	–	–	–	–
5	13	9	–	–	–	–	–

On commence par remplir la ligne 2 : u et v sont les coefficients de Bézout de n_2 et de N (qu'on lit à la ligne 1). L'algorithme d'Euclide étendu permet de trouver la relation $(-1)n_2 + 2N = 1$. On peut donc remplir les cases u et v de la ligne 2. On a $x \leftarrow un_2x + vNx_2 = 7 \mod 15$ et $N \leftarrow Nn_2 = 15$. On finit ensuite de remplir la ligne 2 du tableau :

i	n_i	x_i	N	u	v	x	$x \mod n_i$
1	3	1	3	$\times$	$\times$	1	1
2	5	2	15	-1	2	7	2
3	7	4	–	–	–	–	–
4	11	5	–	–	–	–	–
5	13	9	–	–	–	–	–

On s'occupe ensuite de la ligne 3 : u et v sont les coefficients de Bézout de n_3 et de N (qu'on lit à la ligne 2). L'algorithme d'Euclide étendu permet de trouver la relation $(-2)n_3 + 1N = 1$. On peut donc remplir les cases u et v de la ligne 3. On a ensuite $x \leftarrow un_3x + vNx_3 = 67 \mod 105$ et $N \leftarrow Nn_3 = 105$. On finit de remplir la ligne 3 du tableau :

i	n_i	x_i	N	u	v	x	$x \mod n_i$
1	3	1	3	$\times$	$\times$	1	1
2	5	2	15	-1	2	7	2
3	7	4	105	-2	1	67	4
4	11	5	–	–	–	–	–
5	13	9	–	–	–	–	–

On continue ainsi jusqu'à remplir complètement le tableau.

i	n_i	x_i	N	u	v	x	$x \mod n_i$
1	3	1	3	$\times$	$\times$	1	1
2	5	2	15	-1	2	7	2
3	7	4	105	-2	1	67	4
4	11	5	1155	-19	2	907	5
5	13	9	15015	-533	6	8992	9

Finalement $x = 8992 \mod 15015$.

Pseudocode

Algorithme 1 Théorème chinois

Entrée : $n_1, \ldots, n_k$ des entiers premiers entre eux deux à deux et $x_1, \ldots, x_k$ des entiers.
Sortie : Un entier x tel que $x \equiv x_i \mod n_i$.

1: $N \leftarrow n_i$
2: $x \leftarrow x_1$
3: **pour** i de 2 à k **faire**
4: calculer à l'aide de l'algorithme d'Euclide étendu les coefficients de Bézout u et v tels que $un_i + vN = 1$.
5: $x \leftarrow un_i x + uNx_i$
6: $N \leftarrow Nn_i$
7: $x \leftarrow x \mod N$
8: **fin pour**
9: **retourner** x