Algèbre et Arithmétique Effectives — 07/10/25 Cours 5

Résoudre des congruences linéaires

Soit $n \in \mathbb{Z}_{>0}$ et soient $a, b \in \mathbb{Z}$.

On veut déterminer l'ensemble des entiers z qui satisfont la congruence

$$az \equiv b \pmod{n}$$

Exemple : Déterminer tous les entiers z tels que

$$3z + 4 \equiv 6 \pmod{7}$$

$$\Updownarrow$$

$$3z + 4 - 4 \equiv 6 - 4 \pmod{7}$$

$$\Updownarrow$$

$$3z \equiv 2 \pmod{7}$$

(a, b, n)

$$\Updownarrow$$

$\text{pgcd}(3,7) = 1$
$\Rightarrow$ 3 est inversible mod 7 et l'inverse est 5

$$5 \cdot 3z \equiv 5 \cdot 2 \pmod{7}$$

$$\Updownarrow$$

$$z \equiv 3 \pmod{7}$$

L'ensemble des solutions dans $\mathbb{Z}$ est

$$S = \{7k + 3 : k \in \mathbb{Z}\}.$$

Attention : Une congruence linéaire n'a pas toujours de solutions.

Exemple : $2z \equiv 3 \pmod 4$

On voit que $\forall\, z \in \mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$, z n'est pas une solution $\Rightarrow$ la congruence n'admet pas de solutions dans $\mathbb{Z}$.

Théorème : Soient $a, n \in \mathbb{Z}$, $n > 0$. Soit $d := \text{pgcd}(a,n)$. Alors $\forall\, b \in \mathbb{Z}$ la congruence

$$az \equiv b \pmod n$$

a une solution $z \in \mathbb{Z}$ si et seulement si $d \mid b$.

Dém

Soit $b \in \mathbb{Z}$.

La congruence $az \equiv b \pmod n$ admet une solution $z \in \mathbb{Z} \iff \exists\, z, k \in \mathbb{Z}$ tels que $az - b = nk$

$\iff \exists\, z, k \in \mathbb{Z}$ tels que $az - nk = b \iff$

$\iff \text{pgcd}(a,n) \mid b \iff d \mid b$.

$\downarrow$

$\text{pgcd}(a,n) \mid b \Rightarrow b = \lambda d,\ \lambda \in \mathbb{Z}$

$au + bv = d \Rightarrow a \cdot \underbrace{\lambda u}_{z} + b \cdot \underbrace{\lambda v}_{k} = \lambda d = b.$

Proposition :

1) Si $\text{pgcd}(a,n) = 1$, alors :

$$az \equiv az' \pmod n \iff z \equiv z' \pmod n.$$

2) Si $d = \text{pgcd}(a,n)$, alors :

$$az \equiv az' \pmod{n} \iff z \equiv z' \pmod{\frac{n}{d}}.$$

Exemple : $2z \equiv 6 \pmod{8}$

(a, b, n)

Ici on a $\text{pgcd}(2,8) = 2 \mid 6$, donc, d'après le théorème, la congruence a des solutions.

$2z \equiv 2 \cdot 3 \pmod{2 \cdot 4}$

$\Updownarrow$ proposition ②

$z \equiv 3 \pmod{4}$

L'ensemble des solutions est $S = \{4k+3 : k \in \mathbb{Z}\}$.

Dém (de la proposition)

① c'est trivial, car si $\text{pgcd}(a,n) = 1$, alors a est inversible et il suffit de multiplier les deux côtés par a^{-1}.

② Soit $d = \text{pgcd}(a,n) \implies \text{pgcd}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$ (exo 4 du TD 4)

Donc on a :

$az \equiv az' \pmod{n} \iff \exists k \in \mathbb{Z}$ t.q. $az - az' = nk$

$\iff \exists k \in \mathbb{Z}$ t.q. $\frac{a}{d}z - \frac{a}{d}z' = \frac{n}{d}k \iff$

(on divise par d) $\iff \frac{a}{d}z \equiv \frac{a}{d}z' \pmod{\frac{n}{d}} \overset{+①}{\iff} z \equiv z' \pmod{\frac{n}{d}}$

Corollaire : Soient $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ et $d = \text{pgcd}(a, n)$.
L'ensemble des solutions de l'équation

$$az \equiv b \pmod{n}$$

est :

- vide, si $d \nmid b$.
- une classe d'équivalence modulo $\frac{n}{d}$, si $d \mid b$.

Système de congruences linéaires

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

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

Théorème

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. $\forall i = 1, \dots, k$: $N_i = \frac{N}{n_i}$ (division exacte)
3. $\forall i = 1, \dots, k$: $U_i \leftarrow \text{InverseMod}(N_i, n_i)$

(cela existe car $\text{pgcd}(N_i, n_i) = 1$)

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

Exemple

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

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 je dois 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 :

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

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

Suite de la démonstration

On montre d'abord que

$$z = \sum_{i=1}^{k} a_i \cdot u_i \cdot N_i$$

est bien une solution du système (*).

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

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

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

$$z = \sum_{j=1}^{k} a_j u_j N_j = \sum_{\substack{j=1,\dots,k \\ j \neq i}} a_j u_j N_j + a_i u_i N_i \equiv$$

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

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

Donc z est une solution de (*).

On montre maintenant que tout élément z' dans la classe de z modulo N est aussi une solution du système.

$$z' \equiv z \pmod N \iff \exists\, k \in \mathbb{Z} \text{ t.q. } z' = z + Nk =$$

$$= z + \underbrace{N_i n_i}_{N} k \implies \forall i = 1, \dots, k,\ z' = z + N_i n_i k \equiv$$

$$\equiv z \pmod{n_i} \equiv a_i \pmod{n_i}$$

Il reste à montrer que si z' est une solution de (*) alors $z' \equiv z \pmod N$.

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

$z' \equiv a_i \pmod{n_i} \equiv z \pmod{n_i} \Rightarrow$

$\Rightarrow \forall i = 1, \dots, k \quad n_i \mid z' - z \Rightarrow \prod_{i=1}^{k} n_i \mid z' - z \Rightarrow$

$\operatorname{pgcd}(n_i, n_j) = 1$ si $i \neq j$

$\Rightarrow N \mid z' - z \Rightarrow z' \equiv z \pmod N.$

□