

Algèbre et Arithmétique Effectives - 10/01/26

cours 5

Def: Un élément $a \in \mathbb{Z}/n\mathbb{Z}$ est inversible, si il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab \equiv 1 \pmod{n}$

Exercice:

1) Calculer l'inverse de 20 modulo 63, si il existe.

20 est inversible modulo 63 parce que $\text{pgcd}(20, 63) = 1$

Pour le calculer:

$$63 = 3 \cdot 20 + 3$$

$$20 = 6 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1 \quad \leftarrow \text{pgcd}(20, 63)$$

$$2 = 2 \cdot 1 + 0$$

On calcule une identité de Bézout:

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (20 - 6 \cdot 3) = -20 + 7 \cdot 3 =$$

$$= -20 + 7(63 - 3 \cdot 20) = -22 \cdot 20 + 7 \cdot 63$$

↓

$$-22 \cdot 20 + 7 \cdot 63 = 1$$

↓ mod 63

$$-22 \cdot 20 \equiv 1 \pmod{63}$$

$$41 \cdot 20 \equiv 1 \pmod{63}$$

Donc l'inverse de 20 modulo 63 est 41.

2) Calculer l'inverse de 3 modulo 7.

C'est plus vite de procéder par "force brute"

$$3 \cdot 1 \equiv 3 \pmod{7}$$

$$3 \cdot 2 \equiv 6 \pmod{7}$$

$$3 \cdot 3 \equiv 9 \equiv 2 \pmod{7}$$

$$3 \cdot 4 \equiv 12 \equiv 5 \pmod{7}$$

$$3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$$

\Rightarrow 5 est l'inverse de 3 modulo 7.

Notations : L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^\times$

Remarque : $|(\mathbb{Z}/n\mathbb{Z})^\times| = |\{a \in \mathbb{Z} : 1 \leq a \leq n \text{ et } \text{pgcd}(a, n) = 1\}| = \varphi(n)$
function φ d'Euler.

Exemple : Soit p un premier :

$$\varphi(p) = p-1$$

$\forall a \in \mathbb{Z}/p\mathbb{Z}, a \neq 0, a$ est un élément inversible.

Proposition : Soit p un nombre premier. Alors tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles.
Cela implique que $\mathbb{Z}/p\mathbb{Z}$ est un corps (commutatif).

TD 3 - Exercice 2

$$\left(\frac{\mathbb{Z}}{20\mathbb{Z}}\right)^\times = \{ a \in \frac{\mathbb{Z}}{20\mathbb{Z}} : a \text{ est inversible} \} =$$
$$= \{ a \in \mathbb{Z} : 1 \leq a \leq 20 \text{ et } \text{pgcd}(a, 20) = 1 \} =$$
$$= \{ 1, 3, 7, 9, 11, 13, 17, 19 \}$$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

inverses 1 7 3 9 11 17 13 19

TD 3 - Exercice 3

$$n = 651$$

46 est inversible modulo 651 ?

↓ Euclide (651, 46)

$\text{pgcd}(46, 651) = 1 \Rightarrow$ oui, 46 est inversible

↓ Euclide Étendu (quelques calculs)

$$-13 \cdot 651 + 184 \cdot 46 = 1$$

↓ mod 651

$$184 \cdot 46 \equiv 1 \pmod{651}$$

modulo 651

Donc l'inverse de 46 l'est 184.

Résoudre des congruences linéaires

Soit $n \in \mathbb{N}_>0$ 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 :

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



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



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

a



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

b

n

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



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

$$\text{Sol} = \{7k + 3, k \in \mathbb{Z}\}$$

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

Exemple : $2z \equiv 3 \pmod{4}$.

On voit que $\forall z \in \mathbb{Z}/\mathbb{Z}$,

z n'est pas une solution

\Rightarrow La congruence n'admet pas de solutions en \mathbb{Z} .

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

$\forall b \in \mathbb{Z}$ la congruence

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

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

Démonstration

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

La congruence $az \equiv b \pmod{n}$ a une solution $z \in \mathbb{Z}$

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

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

$$\Leftrightarrow \text{pgcd}(a, n) | b \Leftrightarrow d | b.$$

↑

exercice en TD

Propositions

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

$$az \equiv az' \pmod{n} \Leftrightarrow z \equiv z' \pmod{n}$$

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

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

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

Par le théorème, (*) possède des solutions, car $\text{pgcd}(2, 8) = 2 | 6$.

$$\cancel{2z} = \cancel{2} \cdot 3 \pmod{\cancel{2} \cdot 4}$$

$$\Leftrightarrow z \equiv 3 \pmod{4}$$

on met en évidence le pgcd et on simplifie

Démo

1) Si $\text{pgcd}(a, n) = 1 \Rightarrow a$ est inversible modulo n
 $\Rightarrow \exists a^{-1} \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \cdot a^{-1} \equiv 1 \pmod{n}$.

Donc :

$$az \equiv az' \pmod{n} \Leftrightarrow \underbrace{a^{-1} \cdot az}_{\substack{1 \\ \parallel}} \equiv \underbrace{a^{-1} \cdot az'}_{\substack{1 \\ \parallel}} \pmod{n}$$

$$\Leftrightarrow z \equiv z' \pmod{n}$$

2) Soit $d = \text{pgcd}(a, n) \Rightarrow \boxed{\text{pgcd}\left(\frac{a}{d}, \frac{n}{d}\right) = 1}$.

Donc on a :

$$az \equiv az' \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } az - az' = nk$$

on divise
les deux
côtés par
 d

$$\Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } \frac{a}{d}z - \frac{a}{d}z' = \frac{n}{d}k \Leftrightarrow$$

$$\Leftrightarrow \frac{a}{d}z \equiv \frac{a}{d}z' \pmod{\frac{n}{d}} \xrightarrow{\text{partie 1}} z \equiv z' \pmod{\frac{n}{d}}$$

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 $\frac{n}{d}$, sinon.

Système de congruences linéaires

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:

$$(**) \left\{ \begin{array}{l} z \equiv a_1 \pmod{n_1} \\ z \equiv a_2 \pmod{n_2} \\ \vdots \\ z \equiv a_K \pmod{n_K} \end{array} \right.$$

Théorème (chinois)

L'ensemble des solutions dans \mathbb{Z} de $(**)$ est non vide et c'est une classe d'équivalence modulo $N = \prod_{i=1}^K n_i$.

Démonstration

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 les n_i sont à deux au plus premiers entre eux.

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

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

$$2. \quad \forall i=1, \dots, K : \quad N_i = \frac{N}{n_i} \quad (\text{division exacte})$$

$$3. \quad \forall i=1, \dots, K : \quad U_i \leftarrow \text{InverseMod}(N_i, n_i)$$

$$4. \quad \text{Résoudre } \sum_{i=1}^K a_i \cdot U_i \cdot N_i \pmod{N}$$

Vérification que $z = \sum_{i=1}^K a_i \cdot u_i \cdot N_i$ est bien une solution de (**).

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

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

$$\begin{aligned} \text{Donc } \sum_{i=1}^K a_i \cdot u_i \cdot N_i &= \sum_{j \neq i} a_j \cdot u_j \cdot N_j + a_i \cdot u_i \cdot N_i = \\ &= 0 + a_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i} \quad \forall i=1, \dots, K. \end{aligned}$$

Donc z est une solution de (**).

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

$$\begin{aligned} z' \equiv z \pmod{N} &\Leftrightarrow \exists k \in \mathbb{Z} \text{ t.q. } z' = z + kN = \\ &= z + kN_i \cdot n_i \Rightarrow z' \equiv z \equiv a_i \pmod{n_i}, \quad \forall i=1, \dots, K. \\ &\uparrow \\ N = N_i \cdot n_i & \quad z \text{ est solution de (**)} \end{aligned}$$

Réciiproquement, si z' est une solution du système, alors $z' \equiv a_i \equiv z \pmod{n_i} \Rightarrow n_i \mid z' - z$, $\forall i$

$$\Rightarrow \prod n_i = N \mid z' - z \Rightarrow z' \equiv z \pmod{N}.$$

\square

TD 3 - Exo 5

Résoudre :

$$z+4 \equiv 16z+13 \pmod{48}$$

$$2+4-16z \equiv 16z+13-4-16z \pmod{18}$$

$$-15z \equiv 9 \pmod{18}$$

$$3z \equiv 9 \pmod{18}$$

Est-ce qu'il y a des solutions? Oui, parce que
 $\text{pgcd}(3, 18) = 3 \mid 9$.

On met en évidence le pgcd:

$$\cancel{3} \cdot z \equiv \cancel{3} \cdot 3 \pmod{\cancel{3} \cdot 6}$$



$$z \equiv 3 \pmod{6}$$

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

$$\{6k+3, k \in \mathbb{Z}\}.$$