

Algèbre et Arithmétique Effectives - 13/10/26 Cours 6

Rappel du cours précédent

Déf : Un élément $a \in \mathbb{Z}/n\mathbb{Z}$ est invertible si il existe $b \in \mathbb{Z}/n\mathbb{Z}$ t.q. $ab=1$ ($ab \equiv 1 \pmod{n}$)

Exemple : 3 est invertible mod 7 car $3 \cdot 5 = 15 \equiv 1 \pmod{7}$ et son inverse est donc 5.

Proposition : Un élément $a \in \mathbb{Z}/n\mathbb{Z}$ est invertible si et seulement si $\text{pgcd}(a, n) = 1$.

Dém

$\Rightarrow$) Si $a \in \mathbb{Z}/n\mathbb{Z}$ est invertible $\Rightarrow \exists b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab \equiv 1 \pmod{n} \Rightarrow n \mid (ab-1)$
 $\Rightarrow \exists k \in \mathbb{Z}$ t.q. $ab-1 = nk \Rightarrow$
 $\Rightarrow ab - nk = 1 \Rightarrow \text{pgcd}(a, n) \mid 1 \Rightarrow$
 $\quad \quad \quad \uparrow$
 $\quad \quad \text{exo 6.1 TD1}$
 $\Rightarrow \text{pgcd}(a, n) = 1.$

$\Leftarrow$) Si $\text{pgcd}(a, n) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ tels que
 $au + nv = 1 \Rightarrow au - 1 = n(-v) \Rightarrow$
 $\Rightarrow au \equiv 1 \pmod{n}$

Donc a est invertible et u est l'inverse de a .

La démonstration nous suggère un algorithme d'inversion modulaire.

Algorithme : Inverse Mod (a, n)

Entrées : Deux entiers $a, n \neq 0$

Sortie : Un entier b , $0 < b < n$, tel que $ab \equiv 1 \pmod{n}$
S'il existe, une erreur sinon.

1. $(d, u, v) \leftarrow \text{EuclideEtendu}(a, n)$
2. Si $d \neq 1$. Renvoyer une erreur
« a n'est pas inversible modulo n »
3. Renvoyer $u \pmod{n}$.

Exemple : 1) Calculer l'inverse de 20 modulo 63.

$$63 = 3 \cdot 20 + 3 \quad \textcircled{3}$$

$$20 = 6 \cdot 3 + 2 \quad \textcircled{2}$$

$$3 = 1 \cdot 2 + 1 \quad \textcircled{1}$$

$$2 = 2 \cdot 1$$

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

$$\begin{aligned} 1 &\stackrel{\textcircled{1}}{=} 3 - 1 \cdot 2 \stackrel{\textcircled{2}}{=} 3 - (20 - 6 \cdot 3) = \\ &= -20 + 7 \cdot 3 = -20 + 7(63 - 3 \cdot 20) = \\ &= \underbrace{-22 \cdot 20}_{\textcircled{3}} + \underbrace{7 \cdot 63}_{\textcircled{3}} \end{aligned}$$

$$\Rightarrow 1 = -22 \cdot 20 + 7 \cdot 63 \quad (\text{identité de Bézout})$$

$$\Rightarrow -22 \equiv 41 \pmod{63} \text{ est l'inverse de } 20 \pmod{63}.$$

2) Calculer l'inverse de 3 modulo 7.
C'est plus rapide de procéder par "force brute"

$$3 \cdot 5 = 15 \equiv 1 \pmod{7} \Rightarrow 5 \text{ est l'inverse de } 3 \pmod{7}.$$

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

Exemple : $(\mathbb{Z}/36\mathbb{Z})^\times = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

Pour compter les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ on introduit la fonction indicatrice d'Euler.

Def : La fonction indicatrice d'Euler est la fonction $\varphi: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ définie par :

$$\varphi(n) := \left| \{a \in \mathbb{Z} : 1 \leq a \leq n \text{ et } \text{pgcd}(a, n) = 1\} \right|$$

↑
cardinalité

Exemples

1) $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4.$

2) Si p est un nombre premier, alors $\forall 1 \leq a \leq p-1$
on a $\text{pgcd}(a, p) = 1 \Rightarrow \varphi(p) = p-1.$

Donc on a :

$$\left| (\mathbb{Z}/n\mathbb{Z})^\times \right| = \left| \{a \in \mathbb{Z} : 1 \leq a \leq n, \text{ tel que } \text{pgcd}(a, n) = 1\} \right| = \varphi(n)$$

↑
proposition précédente

En particulier :

$$\left| (\mathbb{Z}/p\mathbb{Z})^\times \right| = \varphi(p) = p-1,$$

c'est-à-dire, tout élément non nul est inversible modulo p . On a donc la proposition suivante :

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

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

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

$$\Updownarrow$$

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

$$\Updownarrow$$

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

$\begin{matrix} \nearrow a & & \nwarrow b & & \nwarrow n \end{matrix}$

$$\Updownarrow$$

$\text{pgcd}(3, 7) = 1$
 $\Rightarrow 3$ 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 solution. Donc 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 $\underline{az} - \underline{nk} = b \iff$

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

$\downarrow$

$\text{pgcd}(a, n) \mid b \Rightarrow b = 2d, 2 \in \mathbb{Z}$

$au + bv = d \Rightarrow a \cdot \underbrace{2u}_z + b \cdot \underbrace{2v}_k = 2d = b$.

Proposition (voir démonstration plus en bas)

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 :

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

Remarque : Soient a, n, b tels que $d = \text{pgcd}(a, n) \mid b$.

$$\text{Alors : } az \equiv b \pmod{n} \iff \frac{a}{d}z \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

$\begin{matrix} \parallel & \parallel \\ d \cdot \frac{a}{d} & d \cdot \frac{b}{d} \end{matrix}$

Exemple : 1) $2z \equiv 6 \pmod{8}$

$\begin{matrix} \uparrow & \uparrow & \uparrow \\ a & b & n \end{matrix}$

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

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

$\Updownarrow$ proposition (2)

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

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

2) $6z \equiv 3 \pmod{15}$

Ici on a $\text{pgcd}(6, 15) = 3 \mid 3$, donc, d'après le théorème, la congruence a des solutions.

$$\frac{6}{3}z \equiv \frac{3}{3} \pmod{\frac{15}{3}}$$

$\Updownarrow$

$$2z \equiv 1 \pmod{5}$$

$\Updownarrow$

$$3 \cdot 2z \equiv 3 \cdot 1 \pmod{5}$$

$\Updownarrow$

$$z \equiv 3 \pmod{5}$$

on multiplie par l'inverse de 2 mod 5

L'ensemble des solutions est $S = \{5k+3 : k \in \mathbb{Z}\}$.

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} .

exo 3 d'TD1

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

Donc on a :

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

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

on divise
par d

$$\Leftrightarrow \frac{a}{d}z \equiv \frac{a}{d}z' \pmod{\frac{n}{d}} \Leftrightarrow z \equiv z' \pmod{\frac{n}{d}} \quad (+ \textcircled{1})$$

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 $d \mid b$.