# Leçon 4 : Calcul modulaire

## 1. Objectifs

Il s'agit de :

- manipuler des calculs modulaires élémentaires.
- reconnaitre la notion d'inversible.
- résoudre des équations modulaires.
- découvrir la fonction d'Euler.

## 2. Un peu de cours

### 2.1. Congruences modulo $m$

**Définition 7 : congruence modulo $m$**

Soient $a$, $b$ et $m$ des entiers relatifs tels que $m \neq 0$.

$$\begin{aligned} a \equiv b\ [m] &\iff \text{Il existe } k \in \mathbb{Z} \text{ tel que } a = b + km \\ &\iff a - b \text{ est un multiple de } m \\ &\iff m \text{ divise } a - b \\ &\iff b \text{ est le reste de la division euclidienne de } a \text{ par } m \end{aligned}$$

On dit que $a$ ***est congru à*** $b$ ***modulo*** $m$.

**Exemple 10**

$17 \equiv 2\ [5]$ car $17 = 2 + 3 \times 5$
$17 \equiv 2\ [5]$ car $17 - 2 = 15$ est un multiple de 5.
$17 \equiv 2\ [5]$ car 5 divise $17 - 2$.
$17 \equiv 2\ [5]$ car 2 est le reste de la division euclidienne de 17 par 5.

**Propriété 4**

Soient $x$ et $m$ des entiers relatifs tels que $m \geqslant 2$.
Il existe un unique $\alpha \in [\![0\ ;\ m-1]\!]$ tel que $x \equiv \alpha\ [m]$

**Exemple 11**

$17 \equiv \mathbf{2}\ [5]$
Mais on a aussi $17 \equiv 7\ [5]$ et $17 \equiv 37\ [5]$ et $17 \equiv -3\ [5]$ (une infinité de possibilités).
Mais 2 est l'unique entier dans l'intervalle $[\![0\ ;\ 4]\!]$.

**Définition 8 : classe d'équivalence modulo $m$**

L'ensemble $\{y \in \mathbb{Z} / y \equiv x\ [m]\}$ est appelé ***la classe d'équivalence de*** $x$ ***modulo*** $m$.
On la note $[x]_m$.

**Exemple 12**

$[17]_5 = \{..., -8, -3, 2, 7, 12, 17, 22, ...\}$

**Définition 9 : $\mathbb{Z}/m\mathbb{Z}$**

On note $\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, [2]_m, ...., [m-1]_m\}$

**Remarque 2**

Par souci de simplification, nous écrirons $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, ...., m-1\}$

**Propriété 5 : règles de calculs**

Soient $a$, $a'$, $b$, $b'$ et $m$ des entiers tels que $m \neq 0$.
Si $a \equiv a'\ [m]$ et $b \equiv b'\ [m]$,
Alors :

- $a + b \equiv a' + b'\ [m]$
- $a \times b \equiv a' \times b'\ [m]$
- $a^p \equiv a'^p\ [m] \quad (p \geqslant 1)$

## 2.2. Inversibilité

**Définition 10 : inverse modulo $m$**

Soient $a$, $b$ et $m$ des entiers tels que $m \geqslant 2$.
On dit que $b$ ***est l'inverse de*** $a$ ***modulo*** $m$ ***si*** $a \times b \equiv 1\ [m]$. [a]

a. Cette égalité permet également de dire que $a$ ***est l'inverse de*** $b$ ***modulo*** $m$.

**Exemple 13**

$13 \times 7 \equiv 1\ [15]$ (car $13 \times 7 = 1 + 6 \times 15$), donc 7 est l'inverse de 13 modulo 15.
Mais cela nous indique aussi que 13 est l'inverse de 7 modulo 15.

**Théorème 2 : rappel du chapitre précédent - théorème de Bezout**

$$d = a \wedge b \quad \Leftrightarrow \quad \text{il existe } u \in \mathbb{Z} \text{ et } v \in \mathbb{Z} \text{ tels que } d = au + bv.$$

En particulier si $d = 1$, on a :

$$a \wedge b = 1 \quad \Leftrightarrow \quad \text{il existe } u \in \mathbb{Z} \text{ et } v \in \mathbb{Z} \text{ tels que } au + bv = 1.$$

**Exemple 14**

Si l'on reprend l'exemple 13, on a : $13 \times 7 - 6 \times 15 = 1 \leftarrow$ c'est l'**égalité de Bezout**.
L'égalité de Bezout va donc nous permettre de trouver des inverses modulaires.

**Propriété 6 : Critère d'inversibilité**

Soient $a$, $b$ et $m$ des entiers tels que $m \geqslant 2$.
$a$ est ***inversible*** modulo $m$ si et seulement si $a$ et $m$ sont premiers entre aux (autrement dit $a \wedge m = 1$).

### 2.3. Fonction d'Euler

**Définition 11 : fonction $\Phi$ d'Euler**

Soient $m$ un entier strictement positif.
On note $\Phi(m)$ le nombre d'éléments inversibles de $\mathbb{Z}/m\mathbb{Z}$ .

**Exemple 15**

$\mathbb{Z}/16\mathbb{Z} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$
Les éléments inversibles sont ceux qui sont premiers avec 16.
Donc $\mathbb{Z}/16\mathbb{Z}^* = \{1,3,5,7,9,11,13,15\}$
Et $\Phi(16) = 8$.

**Propriété 7 : calcul de $\Phi(m)$**

- Si $m$ est premier, alors $\Phi(m) = m-1$
- Si $m = p^k$ où $p$ est premier, alors $\Phi(m) = p^{k-1}(p-1)$
- Si $m$ et $n$ sont premiers entre eux, alors $\Phi(mn) = \Phi(m)\Phi(n)$

**Exemple 16**

$\Phi(15) = \Phi(3) \times \Phi(5) = 2 \times 4 = 8$
$\Phi(16) = \Phi(2^4) = 2^{4-1}(2-1) = 8 \times 1 = 8$

**Théorème 3 : théorème d'Euler**

Si $x \wedge m = 1$, alors $x^{\Phi(m)} \equiv 1\ [m]$

**Exemple 17**

$2 \wedge 15 = 1$, donc $2^{\Phi(15)} \equiv 1\ [15]$, ie $2^8 \equiv 1\ [15]$

## 3. Pratique guidée - Exercices corrigés

**Exemple 18 : Trouver l'inverse d'un nombre**

Trouver l'inverse de 11 modulo 9.
$11 \wedge 9 = 1$, donc 11 est inversible modulo 9.

1re méthode : algorithme d'Euclide inversé.
On commence par dérouler l'algorithme d'Euclide :

$$11 = 9 \times 1 + \mathbf{2}$$

$$9 = 2 \times 4 + \mathbf{1}$$

$$2 = 1 \times 2 + 0$$

On isole le reste "1" de la deuxième ligne : $1 = 9 - 2 \times 4$ ✪
On isole le reste "2" de la première ligne : $2 = 11 - 9 \times 1$ et on l'injecte dans l'équation ✪
$1 = 9 - 2 \times 4$
$1 = 9 - (11 - 9 \times 1) \times 4$
$1 = 9 - 11 \times 4 + 9 \times 4$
$1 = 9 \times 5 - 11 \times 4$

On aboutit à l'identité de Bezout : $9\times5-11\times4=1$
Que l'on peut réécrire : $-11\times4=1-9\times5$
Autrement dit, par définition de la congruence, $11\times(-4)\equiv1\ [9]$
On vient de trouver que $-4$ est l'inverse de 11 modulo 9.
Ou encore 5 est l'inverse de 11 modulo 9.

2e méthode : algorithme de XGCD
Chaque étape de cet algorithme aboutit à un triplet $(d,u,v)$ qui vérifie : $d=11u+9v$

| $t_a$ | $t_b$ | div eucl | $t_r$ |
|---|---|---|---|
| $(11,1,0)$ | $(9,0,1)$ | $11 \mid 9$<br>$2 \mid 1$ | $(11,1,0)-1(9,0,1)=(2,1,-1)$ |
| $(9,0,1)$ | $(2,1,-1)$ | $9 \mid 2$<br>$1 \mid 4$ | $(9,0,1)-4(2,1,-1)=(1,-4,5)$ |
| $(2,1,-1)$ | $(1,-4,5)$ | $2 \mid 1$<br>$0 \mid 2$ | $(2,1,-1)-2(1,-4,5)=(0,9,-11)$ |
| **(1, -4, 5)** | $(0,9,-11)$ | | |

Le triplet $(1,-4,5)$, nous donne la relation : $1=11\times(-4)+9\times5$
Et donc, comme précédemment, $11\times(-4)\equiv1\ [9]$

**Exemple 19 : Résoudre une équation modulaire**

Résoudre l'équation $11x\equiv7\ [9]$.

On a vu précédemment que 11 est inversible modulo 9 et que son inverse est 5.
On multiplie donc les deux côtés de l'équation par 5 (l'opération de division n'existe pas lorsqu'on manipule des congruences).

$5\times11x\equiv7\times5\ [9]$
$x\equiv35\ [9]\equiv8\ [9]$

**Exemple 20 : Calculer $\Phi(m)$**

Calculer $\Phi(45)$.

On commence par décomposer 45 en produit de facteurs premiers : $45=3^2\times5$.
$3^2$ et 5 sont premiers entre eux, donc $\Phi(45)=\Phi(3^2)\times\Phi(5)$
$\Phi(3^2)=3^1(3-1)=6$ et $\Phi(5)=4$
Ainsi, $\Phi(45)=6\times4=24$.

**Exemple 21 : Puissance modulaire**

- Calculer $2^{24}\ [45]$
  On a vu dans l'exemple précédent que $\Phi(45)=24$.
  De plus $2\wedge45=1$
  Donc d'après le théorème d'Euler, $2^{24}\equiv1\ [45]$.
- Calculer $2^{78}\ [45]$
  L'idée ici est d'utiliser le théorème d'Euler pour faire baisser la puissance.
  On effectue la division euclidienne de 78 par 24 : $78=3\times24+6$
  Donc $2^{78}=2^{3\times24+6}=2^{3\times24}\times2^6=(2^{24})^3\times2^6$
  Puisque $2^{24}\equiv1\ [45]$, on a $(2^{24})^3\equiv1^3\ [45]\equiv1\ [45]$.
  Ainsi, $2^{78}\equiv2^6\ [45]\equiv64\ [45]\equiv19\ [45]$.
  Conclusion : $2^{78}\equiv19\ [45]$.