# Fiche de Révision : Arithmétique Modulaire

## Division Euclidienne dans $\mathbb{Z}$

- **Définition :** Pour tout entier $a$ et entier positif $b$, il existe deux entiers $q$ (quotient) et $r$ (reste) tels que
  $a = bq + r$ avec $0 \leq r < b$.
- Exemple : $23 \div 5 = 4$ (quotient), reste $3$ car $23 = 5 \times 4 + 3$.

## Congruences

- **Définition :** Deux entiers $a$ et $b$ sont congruents modulo $n$ si $n$ divise $a - b$.
  On écrit :
  $a \equiv b[n]$ si et seulement si $n|(a - b)$.
- Intuition : $a$ et $b$ laissent le même reste lorsqu'on les divise par $n$.
- Exemple : $23 \equiv 3(mod 5)$ car $23 - 3 = 20$ est divisible par 5.

## Classes d'Équivalence et Z/nZ

- Une classe d'équivalence modulo $n$ regroupe tous les entiers ayant le même reste après division par $n$.
- On note $[a]$ la classe d'équivalence de $a$ modulo $n$.
- **Z/nZ :** L'ensemble des classes d'équivalence modulo $n$ est noté $\mathbb{Z}/n\mathbb{Z}$ et contient $n$ éléments :
  $\mathbb{Z}/n\mathbb{Z} = [0], [1], [2], ..., [n - 1]$.

## Opérations sur les Congruences

- Si $a \equiv b[n]$ et $c \equiv d[n]$, alors :
  - Addition : $a + c \equiv b + d[n]$
  - Soustraction : $a - c \equiv b - d[n]$
  - Multiplication : $a * c \equiv b * d[n]$
- Puissance : Si $a \equiv b[n]$, alors $a^k \equiv b^k[n]$ pour tout entier positif $k$.

- Division : On ne divise que par un entier invertible modulo $n$. Un entier $a$ admet un inverse modulo $n$ si $gcd(a, n) = 1$.

# Algorithme d'Euclide & Étendu

- **Algorithme d'Euclide :**
  Permet de calculer $gcd(a, b)$.
- **Algorithme d'Euclide Étendu :**
  Donne, en plus du $gcd(a, b)$, des entiers $u$ et $v$ tels que $gcd(a, b) = au + bv$.
- Cet algorithme est utilisé pour trouver l'inverse d'un entier modulo $n$ (quand $gcd(a, n) = 1$).
  - $u_i = u_{i-2} - q_i * u_{i-1}$
  - $v_i = v_{i-2} - q_i * v_{i-1}$
  - Les étapes 1 et 2 sont toujours les mêmes.

## Exemple

On cherche l'inverse de 15 modulo 26, donc:

$$15k \equiv 1[26]$$

| Etape n°k | Dividende | Diviseur | Reste $r_k$ | Quotient $q_k$ | $u_k$ | $v_k$ |
|---|---|---|---|---|---|---|
| 1 | | | | | 1 | 0 |
| 2 | | | | | 0 | 1 |
| 3 | 15 | 26 | 15 | 0 | 1 | 0 |
| 4 | 26 | 15 | 11 | 1 | -1 | 1 |
| 5 | 15 | 11 | 4 | 1 | 2 | -1 |
| 6 | 11 | 4 | 3 | 2 | -5 | 3 |
| 7 | 4 | 3 | 1 | 1 | 7 | -4 |

On s'arrête à l'étape juste avant que le reste soit nul.

On a donc:

$$15u_5 + 26v_5 = 1$$

$$15 \times 7 + 26 \times (-4) = 1$$

Ainsi, $[26]$ on obtient $15 \times 7 \equiv 1[26]$. L'inverse modulaire de 15 modulo 26 est 7.