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 : $23 \equiv 3[5]$ 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 $PGCD(a, b)$.
- **Algorithme d'Euclide Étendu :**
  Donne, en plus du $PGCD(a, b)$, des entiers u et v tels que $PGCD(a, b) = au + bv$, et aussi $au + nv = 1$.
- Cet algorithme est utilisé pour trouver l'inverse d'un entier modulo n (quand $PGCD(a, n) = 1$).
  - $u_i = u_{i-2} - q_i * u_{i-1}$
  - $v_i = v_{i-2} - q_i * v_{i-1}$
  - 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:

$$au + nv = 1$$

$$15u_5 + 26v_5 = 1$$

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

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

Résolution de $ax \equiv b[n]$

- On cherche à résoudre $ax + ny = b$ avec x, y comme inconnues.
- Il faut que $PGCD(a, n) = 1$, sinon il faut diviser a et b par ce leur PGCD.
  - Ex: $9x \equiv 12[33]$, on a $PGCD(9, 33) = 3$ donc on divise tout par 3 et on obtient: $3x \equiv 4[11]$
- On utilise l'algorithme d'Euclide étendu pour obtenir quelque chose de la forme $au \equiv 1[n]$. Les solutions sont ensuites: $S = \{(u \times b) + nk / k \in \mathbf{Z}\}$

Exemple:

On a $2x \equiv 10[21]$, étant donné que $PGCD(2, 21) = 1$, 2 est réversible modulo 21.
On peut effectuer le tableau:

Etape n°k	Dividende	Diviseur	Reste r_k	Quotient q_k	u_k	v_k
1					1	0
2					0	1
3	2	21	2	0	1	0
4	21	2	1	10	-10	1

On obtient donc

$$au + nv$$

$$2 \times -10 + 21 \times 1 = 1$$

On ajoute 21 à -10 pour "le faire passer dans ls positifs".

$$2 \times 11 + 21 \times 1 = 1$$

Et donc, modulo 21, on a $2 \times 11 \equiv 1[21]$

On peut donc déduire les solutions S:

$$S = \{(u \times b) + nk / k \in \mathbf{Z}\}$$

$$S = \{(11 \times 10) + 21k / k \in \mathbf{Z}\}$$

$$S = \{110 + 21k / k \in \mathbf{Z}\}$$