Répartition des entiers : congruence

<u>Notation</u> : $\mathbb{Z}$ est l'ensemble des entiers relatifs. L'ensemble des multiples de 8 par exemple se note $8\mathbb{Z} = \{8k, k \in \mathbb{Z}\}$.

<u>Propriété de divisibilité</u> : Soit a, b, c dans $\mathbb{Z}$.
Si a divise les deux nombres b et c alors a divise aussi $b + c$, $b - c$ et plus généralement de toute combinaison linéaire $ub + vc$. (ou u et v sont quelconques dans $\mathbb{Z}$)

<u>Propriété</u> : *Répartition des entiers*
On peut se représenter $\mathbb{Z}$ en répartissant les nombres en groupes (qu'on appelle « classes »).
On peut choisir de répartir suivant 2 classes, 3 classes ou n classes :

- 2 classes : les pairs (ils s'écrivent "$2n$" et leur ensemble se note $2\mathbb{Z}$) et les impairs (les "$2n + 1$", $2\mathbb{Z} + 1$)
- 3 classes : ("$3n$", $3\mathbb{Z}$), ("$3n + 1$", $3\mathbb{Z} + 1$), ("$3n + 2$", $3\mathbb{Z} + 2$)
- b classes : $\mathbb{Z} = \{\mathbb{Z},\ b\mathbb{Z} + 1, b\mathbb{Z} + 2, \dots, b\mathbb{Z} + (b - 1)\}$

<u>Notation</u> : On peut utiliser n'importe quel nombre d'une classe pour la désigner.
$\overline{16} = \overline{132} = \overline{0} = 2\mathbb{Z}$ dans le monde $\{2\mathbb{Z}, 2\mathbb{Z} + 1\}$ que l'on note $\mathbb{Z}/2\mathbb{Z}$
$\overline{4} = \overline{223} = \overline{1} = 3\mathbb{Z} + 1$ dans le monde $\{3\mathbb{Z}, 3\mathbb{Z} + 1{,}3\mathbb{Z} + 2\}$ noté $\mathbb{Z}/3\mathbb{Z}$

<u>Définition</u> (*relation de congruence modulo un entier*)
Les entiers relatifs a et a' sont dits congrus modulo b, s'ils sont dans la même classe modulo b. On note $a \equiv a'\ [b]$

<u>Propriété</u> : $a \equiv a'\ [b]$ $\Leftrightarrow$ $a - a'$ est multiple de b
$\Leftrightarrow$ il existe un entier relatif k tel que $a = a' + kb$
$\Leftrightarrow$ a et a' ont même reste dans la division euclidienne par b

<u>Remarque</u> On peut se représenter $b\mathbb{Z}$, $b\mathbb{Z} + 1$, ..., comme des « peignes » identiques qui sont disjoints et qui recouvrent tout $\mathbb{Z}$. On peut aussi les représenter sur un cercle sur lequel serait enroulé la droite des entiers.

Pour ces nouveaux objets mathématiques on définit une addition $\oplus$ et une multiplication $\otimes$.

<u>Exemples</u> : Pour $b = 5$, c'est-à-dire modulo 5, on a les cinq classes : $5\mathbb{Z}$, $5\mathbb{Z} + 1, 5\mathbb{Z} + 2$, $5\mathbb{Z} + 3, 5\mathbb{Z} + 4$.
Le résultat d'une addition ou multiplication est nécessairement l'une de ces 5 classes. Par exemple :

$(5\mathbb{Z} + 2) \oplus (5\mathbb{Z} + 3) = 5\mathbb{Z} + 5 = 5\mathbb{Z}$	$(5\mathbb{Z} + 2) \otimes (5\mathbb{Z} + 3) = 5\mathbb{Z} + 6 = 5\mathbb{Z} + 1$
car $(5k_1 + 2) + (5k_2 + 3) = 5(k_1 + k_2 + 1)$	Car $(5k_1 + 2) \times (5k_2 + 3) = 25k_1k_2 + 15k_1 + 10k_2 + 6$ $= 5(5k_1k_2 + 3k_1 + 2k_2 + 1) + 1$

Pour effectuer ces opérations, il est possible de choisir un représentant de chaque classe (un nombre entier quelconque de cette classe) et d'effectuer les opérations sur ces nombres.
<u>Exemple</u> : modulo 7, cad dans le monde $\mathbb{Z}/7\mathbb{Z}$: $\overline{4} \oplus \overline{6} \equiv \overline{4 + 6} \equiv \overline{10} \equiv \overline{3}\ \ [7]$ et $\overline{4} \otimes \overline{6} \equiv \overline{4 \times 6} \equiv \overline{24} \equiv \overline{3}\ \ [7]$

<u>Propriété</u> (la relation de congruence est « compatible » avec l'addition et la multiplication)
Si $p \equiv p'[b]$ et $q \equiv q'[b]$ alors $p + q \equiv p' + q'[b]$ *(il suffit de sommer des représentants pour sommer des classes)*
Si $p \equiv p'[b]$ et $q \equiv q'[b]$ alors $p \times q \equiv p' \times q'[b]$ *(il suffit de multiplier des représentants)*

<u>Corollaire important pour des calculs efficaces</u> !
Si $a \equiv a'[b]$ alors $a^2 \equiv a'^2\ [b]$, $a^3 \equiv a'^3\ [b]$,..., $a^k \equiv a'^k\ [b]$

<u>Remarque</u> : On dispose aussi de la propriété suivante, pour tout entier non nul k : Si $a \equiv a'[b]$ alors $ka \equiv ka'\ [\boldsymbol{kb}]$

<u>Remarque</u> : La soustraction est compatible aussi car chaque classe possède une classe opposée (soustraire c'est ajouté l'opposé). La division en revanche n'est pas toujours compatible ($20 \equiv 30[10]$ et $5 \equiv 5[10]$ mais 4 n'est pas congru à 6 modulo [10]. Elle l'est lorsque la classe possède un inverse (car diviser, c'est multiplier par l'inverse).

<u>Définition</u> : (inverse d'un entier modulo b)
On dit que l'entier a est inversible modulo b s'il existe un entier a' tel que $a \times a' \equiv 1\ [b]$.

Si a est inversible modulo b, d'inverse a',alors sa classe $\bar{a}$ modulo b l'est et son inverse est la classe de a'.

Table d'addition et multiplication dans $\mathbb{Z}/4\mathbb{Z}$ puis dans $\mathbb{Z}/5\mathbb{Z}$

Table d'additions dans $\mathbb{Z}/4\mathbb{Z}$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$				
$\bar{2}$				
$\bar{3}$				

Table de multiplications dans $\mathbb{Z}/4\mathbb{Z}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$				
$\bar{2}$				
$\bar{3}$				

Table d'additions dans $\mathbb{Z}/5\mathbb{Z}$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

Table de multiplications dans $\mathbb{Z}/5\mathbb{Z}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

Démonstrations de propriétés du cours

Preuve (de la compatibilité de la relation de congruence avec les opérations).

$p + q = (p' + k_1 b) + (q' + k_2 b) = p' + q' + b(k_1 + k_2)$

$pq = (p' + k_1 b) \times (q' + k_2 b) = p'q' + b(q'k_1 + p'k_2 + bk_1k_2)$

Théorème de la division euclidienne.

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ pour lequel $a = qb + r$ avec $0 \leqslant r < b$

●Existence

Cas général $b \leq |a|$; $(q; r) = \left(E\left(\frac{a}{b}\right); a - E\left(\frac{a}{b}\right) \times b\right)$ convient. ($E(.)$ est la partie entière)

En effet la partie entière du nombre $\frac{a}{b}$ est l'entier qui vérifie $E\left(\frac{a}{b}\right) \leq \frac{a}{b} < E\left(\frac{a}{b}\right) + 1$.

On obtient donc bien $bE\left(\frac{a}{b}\right) \leq a < bE\left(\frac{a}{b}\right) + b$ puis $0 \leq a - bE\left(\frac{a}{b}\right) < b$

Cas particuliers $b > |a|$: si $a \geq 0$ $(q; r) = (0; a)$ convient et si $a \leq 0$ $(q; r) = (1; b + a)$ convient

●Unicité :

Supposons qu'il existe deux couples (q, r) et (q', r') vérifiant les conditions : $\begin{cases} a = qb + r \text{ avec } 0 \leqslant r < b \\ a = q'b + r' \text{ avec } 0 \leqslant r' < b \end{cases}$

On a alors $qb + r = q'b + r'$ donc $b(q - q') = r - r'$ donc b divise $r - r'$.

Mais le nombre $r - r'$ est tel que $-b < r - r' < b$

(en effet $0 \leqslant r' < b$ donc $-b < -r' \leqslant 0$ et comme $0 \leqslant r < b$ on obtient en ajoutant les 2 encadrements $-b < r - r' < b$)

Donc seul $r - r' = 0$ est possible, donc $r = r'$ puis on obtient $q - q' = 0$ donc $q = q'$.