Les opérations de base modulo n

1 Les classes résiduelles

Soit n un entier > 1. Si x et y sont deux entiers, nous dirons que :

$$x \equiv y \quad (n),$$

si $y - x$ est divisible par n, c'est-à-dire s'il existe un entier k tel que :

$$y = x + kn.$$

Exemples :

$$17 \equiv 47 \quad (15),$$
$$-3 \equiv 11 \quad (7).$$

Théorème 1.1 *Pour tout entier y, il existe un unique entier x tel que :*

$$\begin{cases} 0 \leq x < n \\ y \equiv x \quad (n) \end{cases}$$

Remarquons que dans le théorème précédent, x n'est rien d'autre que le **reste de la division euclidienne de y par n**.

L'opération qui à y et n fait correspondre x sera notée :

$$x = y \mod n.$$

Exemples :

$$47 \mod 15 = 2,$$
$$-20 \mod 7 = 1.$$

Il ne faudra donc pas confondre les deux notions qu'on a introduites :

- la relation « $\equiv$ » :
$$x \equiv y \quad (n) \iff y = x + kn$$
- l'opération « $\mod$ » :
$$x = y \mod n \iff \begin{cases} x \equiv y \quad (n) \\ 0 \leq x < n \end{cases}$$

2 Quelques manipulations

Théorème 2.1 *L'addition et la multiplication sont compatibles avec la relation « $\equiv$ » :*

$$\begin{cases} x_1 \equiv y_1 \quad (n) \\ \quad \textit{et} \\ x_2 \equiv y_2 \quad (n) \end{cases} \Longrightarrow \begin{cases} x_1 + x_2 \equiv y_1 + y_2 \quad (n) \\ \quad \textit{et} \\ x_1 x_2 \equiv y_1 y_2 \quad (n) \end{cases}$$

En particulier on peut écrire :

$$x \equiv y \quad (n) \Longrightarrow x^k \equiv y^k \quad (n).$$

Remarquons aussi le résultat très simple suivant qui sert parfois : si m est un diviseur de n alors

$$x \equiv y \quad (n) \Longrightarrow x \equiv y \quad (m)$$

(en effet, si $y - x$ est multiple de n il est aussi multiple de m).

3 Un peu de formalisation

Soit n un entier > 1. La relation « $\equiv$ » dans l'ensemble $\mathbb{Z}$ des nombres entiers est une relation d'équivalence. L'ensemble des classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$.

Chaque classe a **un représentant et un seul** dans l'intervalle d'entiers $[0, n[$, et évidemment chaque entier de cet intervalle représente une classe. Autrement dit on peut représenter $\mathbb{Z}/n\mathbb{Z}$ comme l'ensemble $\{0, 1, \cdots, n-1\}$.

Étant donné un entier y on trouve le représentant de sa classe contenu dans cet intervalle en prenant $x = y \mod n$, c'est-à-dire en prenant le reste de la division euclidienne de y par n.

Comme les opération d'addition et de multiplication sur $\mathbb{Z}$ sont compatibles avec la relation d'équivalence « $\equiv$ », on peut les utiliser pour définir une addition et une multiplication dans $\mathbb{Z}/n\mathbb{Z}$: la somme de deux classes représentées respectivement par x et par y est la classe représentée par $x + y$, leur produit est la classe représentée par xy. La compatibilité des opérations avec la relation d'équivalence permet de montrer que les résultats obtenus sont indépendants des représentants choisis et donc de prouver que les définitions données de la somme et du produit dans $\mathbb{Z}/n\mathbb{Z}$ sont cohérentes.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de ces deux opérations est un **anneau commutatif unitaire** (Les opérations dans $\mathbb{Z}/n\mathbb{Z}$ étant définies à partir des opérations de $\mathbb{Z}$, elles retrouvent exactement leurs mêmes propriétés).

Pour l'addition, $\mathbb{Z}/n\mathbb{Z}$ est donc un groupe fini commutatif ayant n élément. Les groupes additifs $\mathbb{Z}/n\mathbb{Z}$ permettent de représenter tous les groupes finis commutatifs grâce au théorème suivant :

Théorème 3.1 *Tout groupe fini commutatif G peut s'écrire sous la forme :*

$$G = \prod_{i=1}^{m} \mathbb{Z}/n_i\mathbb{Z}.$$

De plus les n_i peuvent être pris comme des puissances de nombres premiers.

Il est par ailleurs utile d'étudier les éléments inversibles pour la multiplication. Nous verrons dans d'autres fiches une étude plus complète de cette question (fiches 102, 104, 105 etc.). Résumons brièvement la situation en donnant les résultats suivants ;
– a est inversible modulo n si et seulement si a est premier avec n ;

– $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier ;
– nous noterons $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe multiplicatif formé par les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$; le nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ est $\phi(n)$ où ϕ est la fonction d'Euler.

Remarque : Pour enchaîner des opérations dans $\mathbb{Z}/n\mathbb{Z}$ (additions, multiplications, inverses, puissances) nous venons de voir qu'il suffit de faire toutes les opérations dans $\mathbb{Z}$ et de prendre le modulo à la fin. Cependant, cette façon de faire peut conduire à des débordements (entiers trop grands), si bien qu'il est utile de passer au modulo à des instants bien choisis afin d'éviter l'introduction de résultats intermédiaires ingérables.