



Chapitre 6 Récurrence

■ L'ensemble \mathbb{N}

- **Propriété (Axiomes de Peano)** : Il existe un ensemble, noté \mathbb{N} , dont les éléments sont appelés entiers naturels, et une fonction appelée *successeur* définie sur cet ensemble, vérifiant les axiomes suivants :

- (N1) Tout entier naturel n admet un successeur qui est $n+1$.
(N2) 0 est un entier naturel.

(N3) 0 n'est le successeur d'aucun entier naturel.

(N4) Deux entiers naturels ayant le même successeur sont égaux.

(N5) \mathbb{N} n'a pas de plus grand élément.

(N6) Toute partie non vide de \mathbb{N} admet un plus petit élément.

■ Principe de récurrence

- **Axiome du minimum (N6)** : Toute partie B non vide de \mathbb{N} admet un plus petit élément p , ce qui signifie

$$\exists p \in \mathbb{N}, \forall b \in B, (b \geq p) \wedge (p \in B).$$

Théorème (Principe de récurrence) : Si A est une partie de \mathbb{N} satisfaisant aux deux conditions suivantes :

- $0 \in A$,
- $\forall n \in \mathbb{N}, (n \in A \implies n+1 \in A)$,

alors $A = \mathbb{N}$.

■ Raisonnement par récurrence

Théorème (Récurrence à partir du rang 0) : Soit $\mathcal{P}(n)$ une proposition dépendant d'un entier naturel n .

Si

$$\begin{cases} \mathcal{P}(0) \text{ est vraie} \\ \forall n \in \mathbb{N}, \mathcal{P}(n) \implies \mathcal{P}(n+1) \end{cases}$$

alors

$$\forall n \in \mathbb{N}, \mathcal{P}(n) \text{ est vraie.}$$

Corollaire (Récurrence à partir d'un rang n_0) : Soit $\mathcal{P}(n)$ une proposition dépendant d'un entier naturel n et soit $n_0 \in \mathbb{N}$.

Si

$$\begin{cases} \mathcal{P}(n_0) \text{ est vraie} \\ \forall n \geq n_0, \mathcal{P}(n) \implies \mathcal{P}(n+1) \end{cases}$$

alors

$$\forall n \geq n_0, \mathcal{P}(n) \text{ est vraie.}$$

► **Remarques :**

- La première condition est l'*initialisation* de la récurrence.
- La condition $\mathcal{P}(n)$ vraie, pour un entier naturel fixé, est fréquemment appelée *hypothèse de récurrence*, et notée \mathcal{H}_n ; il s'agit donc de prouver

$$\mathcal{H}_n \implies \mathcal{H}_{n+1}.$$

- La seconde condition signifie que la propriété est héréditaire.

► **Exemples :** Démonstration de

- $\forall x \in \mathbb{R}^*, \forall n \in \mathbb{N}, |x^n| = |x|^n$.
- $\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$.

► **Exemple (proposition fausse mais héréditaire) :**

$$\forall n \in \mathbb{N}, 9|(10^n + 1).$$

■ Récurrences fortes

Propriété (Récurrence double) : Soit $\mathcal{P}(n)$ une proposition dépendant d'un entier naturel n .
Si

$$\begin{cases} \mathcal{P}(0) \text{ et } \mathcal{P}(1) \text{ sont vraies} \\ \forall n \geq 1, (\mathcal{P}(n-1) \wedge \mathcal{P}(n)) \implies \mathcal{P}(n+1) \end{cases}$$

alors

$$\forall n \in \mathbb{N}, \mathcal{P}(n) \text{ est vraie.}$$

► Remarques :

1. Dans le cas d'utilisation de cette forme de récurrence, il ne faut surtout pas oublier de procéder à la double initialisation $\mathcal{P}(0)$ et $\mathcal{P}(1)$.
2. On peut, comme pour la récurrence simple, démontrer par récurrence double que $\mathcal{P}(n)$ est vraie pour $n \geq n_0$.

Il faut procéder à la double initialisation aux rangs n_0 et $n_0 + 1$.

- **Exemples :** Recherche du terme général de suites récurrentes linéaires d'ordre 2.

Théorème (Récurrence forte) : Soit $\mathcal{P}(n)$ une proposition dépendant d'un entier naturel n .

Si

$$\begin{cases} \mathcal{P}(0) \text{ est vraie} \\ \forall n \in \mathbb{N}, (\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \dots \wedge \mathcal{P}(n)) \implies \mathcal{P}(n+1) \end{cases}$$

alors

$$\forall n \in \mathbb{N}, \mathcal{P}(n) \text{ est vraie.}$$

- **Exemple :** Démonstration par récurrence forte que tout entier supérieur ou égal à 2 s'écrit comme produit d'un ou plusieurs nombres premiers.

Chapitre 21 Congruences dans \mathbb{Z}

■ Définition – Caractérisation

- **Définition :** Soient n un entier naturel non nul, a et b deux entiers relatifs.

On dit que a et b sont *congrus modulo n* si, et seulement si, a et b ont le même reste dans la division euclidienne par n .

Lorsque a et b sont congrus modulo n , nous notons indifféremment

$$a \equiv b \pmod{n} \quad \text{ou} \quad a \equiv b [n].$$

- **Remarque :** L'égalité modulo n est aussi appelée relation de congruence modulo n dans l'ensemble des entiers relatifs.

- **Exemple :** Clé du numéro INSEE.

Propriété (Caractérisation d'une congruence) : Soient n un entier naturel non nul, a et b deux entiers relatifs. Les deux propositions suivantes sont équivalentes

- (i) $a \equiv b [n]$
- (ii) $n \mid a - b$

► Exemples :

- ▷ $-1 \equiv 1 [2]$ car $-1 - 1 = -2$ est divisible par 2.
- ▷ $3 \equiv 0 [3]$ car $3 - 0 = 3$ est divisible par 3.
- ▷ $73 \equiv 52 [7]$ car $73 - 52 = 21$ est divisible par 7.
- ▷ Quel que soit l'entier relatif n , $(2n-1)^2 \equiv 1 [4]$.
- ▷ Quels que soient les entiers relatifs a et b ,

$$(a+b)^3 \equiv a^3 + b^3 [3]$$

Propriété (Lien avec la division euclidienne) : Soient $n \in \mathbb{N}^*$, a un entier relatif et r un entier naturel. Les deux propositions suivantes sont équivalentes.

- (i) $a \equiv r [n]$ et $r \in [0, n-1]$,
- (ii) r est le reste de la division euclidienne de a par n .

- **Exemple :** La division euclidienne de 2022 par 19 restitue un reste égal à 8 car $2022 = 19 \times 106 + 8$, donc

$$2022 \equiv 8 [19].$$

► Remarques :

- Sans la condition $r \in [0, n-1]$, l'implication (i) \Rightarrow (ii) est fausse.

En effet, $52 \equiv 45 [7]$ et 45 n'est pourtant pas le reste de la division euclidienne de 52 par 7.

- La division euclidienne de tout entier relatif a par $n \in \mathbb{N}^*$, induit par disjonction

$$a \equiv 0 [n] \vee a \equiv 1 [n] \vee a \equiv 2 [n] \vee \dots \vee a \equiv n-1 [n],$$

ce qui définit une partition de \mathbb{Z} .

- **Propriété (Lien avec la divisibilité) :** Soient $n \in \mathbb{N}^*$ et a un entier relatif. Nous disposons de l'équivalence

$$n \mid a \iff a \equiv 0 [n].$$

► Remarques (Cas particuliers et extensions) :

- Cas particulier : $n = 0$.
Quels que soient les entiers relatifs a et b , nous avons :

$$a \equiv b [0] \iff a - b = q \times 0 = 0 \iff a = b.$$

Par conséquent, la congruence modulo 0 est l'égalité usuelle dans \mathbb{Z} .

- Cas particulier : $n = 1$.
Quels que soient les entiers relatifs a et b , nous avons

$$a \equiv b [1] \iff a - b = q \times 1 = q, \text{ avec } q \in \mathbb{Z}$$

ce qui signifie

$$a \equiv b [1] \iff a - b \in \mathbb{Z}.$$

- Congruences dans \mathbb{R} .

Un réel ω étant donné, par extension, deux réels x et y sont congrus modulo ω , noté $x \equiv y [\omega]$, si et seulement si

$$\exists k \in \mathbb{Z}, \quad x - y = k\omega.$$

Lorsque $\omega = 2\pi$, on retrouve la congruence modulo 2π de la trigonométrie.

- Classes modulo n .

L'entier naturel r étant le reste de la division de $a \in \mathbb{Z}$ par $n \in \mathbb{N}^*$, on appelle classe de r modulo n , le sous-ensemble de \mathbb{Z} , noté \tilde{r} , défini par

$$\tilde{r} = \{x \in \mathbb{Z} \mid x \equiv r [n]\} = \{x \in \mathbb{Z} \mid x = r + kn, k \in \mathbb{Z}\}.$$

En désignant par \mathbb{Z}_n l'ensemble des classes modulo n , nous obtenons

$$\mathbb{Z}_n = \{\tilde{0}, \tilde{1}, \tilde{2}, \dots, \widetilde{n-1}\}.$$

■ Propriétés algébriques d'une congruence

Propriété : Soient $n \in \mathbb{N}^*$, a , b et c trois entiers relatifs.

La relation congru modulo n est une relation d'équivalence, ce qui signifie

- $a \equiv a [n]$ (réflexivité),
- $a \equiv b [n] \implies b \equiv a [n]$ (symétrie),
- $a \equiv b [n] \wedge b \equiv c [n] \implies a \equiv c [n]$ (transitivité).

- **Propriété (Compatibilité de l'addition avec une congruence) :** Soient $n \in \mathbb{N}^*$, a , b , c et d quatre entiers relatifs.

L'addition dans \mathbb{Z} est compatible avec la congruence modulo n , ce qui signifie

$$a \equiv c [n] \wedge b \equiv d [n] \implies a + b \equiv c + d [n].$$

- **Remarque :** La réciproque de cette proposition est fausse. En effet :

$$23 \equiv 3 [5], \text{ soit } 20 + 3 \equiv 2 + 1 [5],$$

mais ni 20 est congru à 2, ni 3 est congru à 1, modulo 5.

- **Exemples :** Tables d'addition modulo 2 et modulo 3

+	$\tilde{0}$	$\tilde{1}$
$\tilde{0}$	$\tilde{0}$	$\tilde{1}$
$\tilde{1}$	$\tilde{1}$	$\tilde{0}$

+	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$
$\tilde{0}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$
$\tilde{1}$	$\tilde{1}$	$\tilde{2}$	$\tilde{0}$
$\tilde{2}$	$\tilde{2}$	$\tilde{0}$	$\tilde{1}$

- **Propriété (Simplification) :** Soient $n \in \mathbb{N}^*$, a , b et c trois entiers relatifs. Nous disposons de l'équivalence

$$a + c \equiv b + c [n] \iff a \equiv b [n].$$

- **Propriété (Compatibilité avec la soustraction) :** Soient $n \in \mathbb{N}^*$, a , b , c et d quatre entiers relatifs. La soustraction dans \mathbb{Z} est compatible avec la congruence modulo n , ce qui signifie

$$a \equiv c [n] \wedge b \equiv d [n] \implies a - b \equiv c - d [n].$$

- **Propriété (Simplification) :** Soient $n \in \mathbb{N}^*$, a , b et c trois entiers relatifs. Nous disposons de l'équivalence :

$$a - c \equiv b - c [n] \iff a \equiv b [n].$$

- **Exemple (Une équation du 1^{er} degré, modulo 8) :** $x + 5 \equiv 3 [8] \iff x \equiv 6 [8]$

- **Propriété (Compatibilité de la multiplication avec une congruence) :** Soient $n \in \mathbb{N}^*$, a , b , c et d quatre entiers relatifs. La multiplication dans \mathbb{Z} est compatible avec la congruence modulo n , ce qui signifie

$$a \equiv c [n] \wedge b \equiv d [n] \implies a \times b \equiv c \times d [n].$$

- **Remarque :** La réciproque de cette proposition est fausse.

- **Exemple :** $2 \times 4 \equiv 0 [8]$. Dans la multiplication modulo 8, on dit que 2 et 4 sont des diviseurs de 0.

- Pour les parties désignées par un symbole



Propriété : une démonstration est exigible.



- Une colle comporte une question de cours choisie *a priori* parmi celles indiquées dans le programme de la semaine en cours (normalement, ± 15 min).
- Un cours non appris sera sanctionné par une note inférieure à 10 (même si l'exercice est fait correctement!).