

Chapitre 8: Récurrences, éléments d'arithmétique-résumé de cours et TD

1. Le principe de récurrence et ses variantes :

Soit $\mathcal{P}(n)$ une propriété sur \mathbb{N} ou une partie de \mathbb{N} et $n_0 \in \mathbb{N}$.

• Principe de récurrence:

Si $\begin{cases} \mathcal{P}(n_0) \text{ est vraie} \\ \text{Pour tout } n \geq n_0, (\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)) \end{cases}$, alors $\mathcal{P}(n)$ est vraie pour tout $n \geq n_0$.

Vocabulaire:

★ Vérifier $\mathcal{P}(n_0)$ constitue l'**initialisation** du raisonnement par récurrence.

★ Une propriété $\mathcal{P}(n)$ vérifiant $\forall n \geq n_0, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ est dite **héréditaire**.

Attention: Une propriété peut être héréditaire et par ailleurs, fausse! L'étape d'initialisation est donc indispensable pour conclure.

★ Symboliquement, le principe s'écrit:

$$[\mathcal{P}(n_0) \text{ et } (\forall n \in \mathbb{N}, n \geq n_0, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1))] \Rightarrow [\forall n \in \mathbb{N}, n \geq n_0, \mathcal{P}(n)].$$

• Récurrence double:

Si $\begin{cases} \mathcal{P}(n_0) \text{ et } \mathcal{P}(n_0 + 1) \text{ sont vraies} \\ \text{Pour tout } n \geq n_0, (\mathcal{P}(n) \text{ et } \mathcal{P}(n+1) \Rightarrow \mathcal{P}(n+2)) \end{cases}$ alors $\mathcal{P}(n)$ est vraie pour tout $n \geq n_0$.

Remarque: Ce type de récurrence s'utilise lorsque la démonstration de l'hérédité nécessite l'utilisation des deux rangs précédents.

⊗ Preuve : On montre par récurrence simple que la propriété $Q(n) : \mathcal{P}(n) \text{ et } \mathcal{P}(n+1)$ est vraie pour tout $n \geq n_0$.

• Récurrence forte:

Si $\begin{cases} \mathcal{P}(n_0) \text{ est vraie} \\ \text{Pour tout } n \geq n_0, (\mathcal{P}(n_0), \mathcal{P}(n_0 + 1), \dots, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)) \end{cases}$
alors $\mathcal{P}(n)$ est vraie pour tout $n \geq n_0$.

Remarque: Ce type de récurrence s'utilise lorsque la démonstration de l'hérédité nécessite l'utilisation de certains rangs compris entre n_0 et n ou même de tous.

⊗ Preuve : On montre par récurrence simple que la propriété $Q(n) : \forall k \in [1, n], \mathcal{P}(k)$ est vraie pour tout $n \geq n_0$.

• Récurrence finie:

Si $\begin{cases} \mathcal{P}(n_0) \text{ est vraie} \\ \text{Pour tout } n \in [n_0, p-1], \text{ si } \mathcal{P}(n) \text{ est vraie, alors } \mathcal{P}(n+1) \text{ est vraie} \end{cases}$
alors $\mathcal{P}(n)$ est vraie pour tout $n, n_0 \leq n \leq p$

Remarque: ce type de récurrence s'utilise lorsque la propriété à démontrer n'a plus de sens à partir du rang $p + 1$.

Exercices d'application

① Soit u la suite définie par $u_0 = 2$, $u_1 = 3$ et $\forall n \in \mathbb{N}$, $u_{n+2} = 3u_{n+1} - 2u_n$.

Montrer que, $\forall n \in \mathbb{N}$, $u_n = 2^n + 1$.

② Soit $(u_n)_{n \in \mathbb{N}}$ une suite réelle telle que $u_0 = 1$ et $\forall n \in \mathbb{N}$, $u_{n+1} \leq \sum_{k=0}^n u_k$.

Montrer que: $\forall n \in \mathbb{N}$, $u_n \leq 2^n$.

③ On donne les deux propriétés suivantes où $n \in \mathbb{N}^*$:

$$P(n): \sum_{k=0}^n k! = (n+1)! - 1 \text{ et } Q(n): \sum_{k=0}^n k! = (n+1)!$$

a. Montrer que ces deux propriétés sont héréditaires pour tout $n \geq 1$.

b. Laquelle des deux est vraie, pour tout $n \in \mathbb{N}^*$?

④ Montrer que si une trousse contient n stylos alors ils sont tous de la même couleur.



Réponse: Soit $P(n)$: Si une trousse contient n stylos alors ils sont tous de la même couleur.

★ $P(1)$ est trivialement vraie.

★ Soit $n \in \mathbb{N}$, $n \geq 1$, tel que $P(n)$ est vraie. Considérons une trousse contenant $(n+1)$ stylos. On enlève un stylo, la trousse contient alors n stylos tous de la même couleur, par exemple rouge, par hypothèse de récurrence. Remettons le stylo et enlevons un autre. Les n stylos restants sont encore de la même couleur, par exemple encore rouge. Ainsi les $(n+1)$ stylos sont de la même couleur et $P(n+1)$ est vraie.

★ D'après le principe de récurrence, $\forall n \geq 1$, si une trousse contient n stylos alors ils sont tous de la même couleur.

Qu'en pensez-vous ?

2. Quelques éléments d'arithmétique :

2.1 Division euclidienne

Théorème et définition: Pour couple (a, b) de $\mathbb{Z} \times \mathbb{N}^*$, il existe un unique couple (q, r) de $\mathbb{Z} \times \mathbb{N}$, vérifiant $a = bq + r$ et $0 \leq r < b$. On dit que q est le quotient et r le reste dans la division euclidienne de a par b .

Attention: La condition $0 \leq r < b$ est indispensable.

Le reste ne peut donc prendre que b valeurs dans $\llbracket 0, b-1 \rrbracket$

- **Exercice 1 :** Ecrire une fonction Python de paramètre (a, b) retournant q et r sans utiliser de division, ni de multiplication.

Proposition 1: Soit $b \in \mathbb{N}^*$, $b \geq 2$, pour tout $r \in \llbracket 0, b-1 \rrbracket$, on pose $A_r = \{bk + r, k \in \mathbb{N}\}$. La famille $(A_r)_{r \in \llbracket 0, b-1 \rrbracket}$ est une partition de \mathbb{N} .

Exemples :

- Pour $b = 2$, les parties $A_0 = \{2k \in \mathbb{N}\}$ et $A_1 = \{2k + 1, k \in \mathbb{N}\}$ forment une partition de \mathbb{N}
- Pour $b = 3$, les parties $A_0 = \{3k \in \mathbb{N}\}$, $A_1 = \{3k + 1, k \in \mathbb{N}\}$ et $A_2 = \{3k + 2, k \in \mathbb{N}\}$ forment une partition de \mathbb{N}

Dans la pratique: On peut faire une disjonction des cas en raisonnant modulo $b \geq 2$.

- **Exercice 2 :** Calculer $S_n = \sum_{k=0}^{3n} \left\lfloor \frac{2k}{3} \right\rfloor$

2.2. Multiples et diviseurs

Déf: Soient a et b deux entiers relatifs.

- On dit que b divise a lorsqu'on peut écrire $a = kb$ avec $k \in \mathbb{Z}$.

Symboliquement $b|a \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $a = kb$

- On dit que a est un multiple de b lorsque b divise a .

Remarque: L'égalité $a = kb$ donne deux diviseurs de a : b et k .

Vocabulaire: Lorsque $b|a$, b est un diviseur de a et a est un multiple de b .

Proposition 2: Propriétés de la relation divise: a, b et c sont des entiers relatifs

- ① $a|a$
- ② si $b|a$ et $a|b$ alors $a = b$ ou $a = -b$
- ③ si $a|b$ et si $b|c$ alors $a|c$
- ④ si $d|a$ et $d|b$ alors $\forall (u, v) \in \mathbb{Z}^2, d|(au + bv)$

Notations

★ On note $a\mathbb{Z}$ l'ensemble des multiples de a . $n \in a\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}, n = ka$

Les entiers naturels pairs sont les multiples de 2 soit $2\mathbb{Z}$.

- On notera $D(a)$ l'ensemble des diviseurs de a . $D(a)$ contient toujours au moins 1 et a . $D(a)$ est une partie finie de \mathbb{Z} car majorée par a et minorée par $-a$

Proposition 3 : Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$, b divise a si et seulement si le reste dans la division de a par b est nul.

- **Exercice 3 :** Montrer que $\forall n \in \mathbb{N}, (n^3 - n)$ est divisible par 3
On proposera au moins deux méthodes différentes.

2.3 PGCD et PPCM

Def : Soit deux entiers naturels a et b non nuls.

- ① L'ensemble des diviseurs positifs commun à a et à b est une partie non vide et majorée de \mathbb{N} qui possède un plus grand élément appelé plus grand commun diviseur de a et b et noté $\text{PGCD}(a,b)$ ou $a \wedge b$.
- ② L'ensemble des multiples strictement positifs commun à a et à b est une partie non vide de \mathbb{N} qui possède un plus petit élément appelé plus petit commun multiple de a et b et noté $\text{PPCM}(a,b)$ ou $a \vee b$.

Remarque : On peut étendre ces notions aux cas suivants :

- $\text{PGCD}(a, 0) = a$ et $\text{PPCM}(a, 0) = 0$
- Si a et b sont dans \mathbb{Z} , $\text{PGCD}(a, b) = \text{PGCD}(|a|, |b|)$ et $\text{PPCM}(a, b) = \text{PPCM}(|a|, |b|)$

Proposition 4 : Soit a et b deux entiers naturels non nuls,
 $\text{PGCD}(a, b) = a \Leftrightarrow a|b$ et $\text{PPCM}(a, b) = a \Leftrightarrow b|a$

- **Exercice 4 :** Soit $n \in \mathbb{N}$,
- Montrer que le PGCD de $2n + 4$ et $3n + 3$ ne peut être que 1, 2, 3 ou 6.
 - Déterminer n tel que $(2n + 4) \wedge (3n + 3) = 3$

Lemme d'Euclide : Soit a et b deux entiers naturels non nuls, et r le reste dans la division euclidienne de a par b . On a $\text{PGCD}(a, b) = \text{PGCD}(b, r)$

Application : algorithme d'Euclide pour l'obtention du PGCD de a et de b

On définit une suite d'entiers naturels (r_n) de la façon suivante.

$r_0 = a$ et $r_1 = b$.

Pour tout $k \geq 1$, si $r_k > 0$ alors r_{k+1} est le reste dans la division de r_{k-1} par r_k .
 si $r_k = 0$ on s'arrête.

Le dernier reste non nul est alors le PGCD de a et de b

- **Exercice 5 :** Compléter cette fonction Python mettant en œuvre cet algorithme.

```
def euclide(a,b):
    r = .....
    while r > 0 :
        r =
        a = .....
        b = .....
    return .....
```

Vocabulaire :

- On dit que a et b sont premiers entre eux lorsque $\text{PGCD}(a, b) = a \wedge b = 1$.
- Une fraction est dite irréductible lorsque son numérateur et son dénominateur sont premiers entre eux.

2.4 Nombres premiers

Déf: Un entier naturel p est premier s'il admet exactement deux diviseurs positifs. En notant \mathbb{P} l'ensemble des nombres premiers, on a : $p \in \mathbb{P} \Leftrightarrow D(p) = \{1, p\}$

Conséquence : 1 n'est pas premier et 2 est le seul premier pair.

Propriété 6 : Tout entier $n \geq 2$ admet au moins un diviseur premier p avec $p \leq \sqrt{n}$ si n n'est pas premier.

- **Exercice 6 :**
- Démontrer par récurrence forte que tout entier $n \geq 2$ admet au moins un diviseur

premier p .

Dans l'hérédité, on pourra distinguer deux cas suivant que $n + 1$ est ou non premier.

- b. Soit n un entier non premier, en écrivant $n = a \cdot b$ avec $a \geq 2$ et $b \geq 2$, montrer que n admet un diviseur premier p vérifiant $p \leq \sqrt{n}$
- c. Ecrire une fonction Python qui renvoie True si n est premier et False sinon.

Proposition 7 : L'ensemble des nombres premiers \mathbb{P} est infini

➤ **Exercice 7**

Démontrer par l'absurde la proposition 7

➤ **Exercice 8**

1. Soit a et b deux entiers naturels. Montrer que si a et b ont pour reste 1 dans la division par 4, alors il en est de même pour ab .
2. Soit p un nombre premier. Quelle peut être son reste dans la division par 4 ?
3. Montrer par l'absurde qu'il existe une infinité de nombres premiers dont le reste dans la division par 4 est 3. On pourra s'inspirer fortement de la démonstration précédente.

Théorème fondamental de l'arithmétique : Tout entier $n \geq 2$ s'écrit de manière unique à l'ordre des facteurs près comme produits de nombres premiers

Exemple : $60 = 2 \times 30 = 2 \times 2 \times 15 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3 \times 5$

➤ **Exercice 9 Le petit théorème de Fermat** : Soit p un nombre premier.

a. Prouver que $\forall k \in \llbracket 1, p-1 \rrbracket$, $\binom{p}{k}$ est divisible par p .

b. Montrer par récurrence sur n que $\forall n \in \mathbb{N}^*$, $n^p - n$ est divisible par p .

c. Déterminer tous les entiers $p \in \mathbb{P}$ tels que p divise $2^p + 1$.

➤ **Exercice 10** : Déterminer par combien de zéros se termine l'entier $N = 2024$!

Application au calcul du PGCD et du PPCM

• En notant $\alpha_p(n)$ l'exposant du nombre premier p dans la décomposition primaire de n avec $\alpha_p(n) > 0$ si p figure dans la décomposition et $\alpha_p(n) = 0$ sinon, on peut écrire $n = \prod_{p \in \mathbb{P}} p^{\alpha_p(n)}$.

• Le PGCD de a et de b est le produit des facteurs premiers communs aux deux décompositions, affectés du plus petit exposant rencontré.

Ou encore si $a = \prod_{p \in \mathbb{P}} p^{\alpha_p(a)}$ et $b = \prod_{p \in \mathbb{P}} p^{\alpha_p(b)}$ alors $a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(\alpha_p(a), \alpha_p(b))}$

Deux nombres entiers sont premiers entre eux si et seulement si ils n'ont aucun facteur premier en commun dans leur décomposition.

• Le PPCM de a et de b est le produit des facteurs premiers présents dans chacune des deux décompositions, affectés du plus grand exposant rencontré.

Ou encore si $a = \prod_{p \in \mathbb{P}} p^{\alpha_p(a)}$ et $b = \prod_{p \in \mathbb{P}} p^{\alpha_p(b)}$ alors $a \vee b = \prod_{p \in \mathbb{P}} p^{\max(\alpha_p(a), \alpha_p(b))}$

Proposition 8 : $\text{PPCM}(a, b) \times \text{PGCD}(a, b) = a \cdot b$