Chapitre 8 - Arithmétique dans $\mathbb{N}$

1 Raisonnement par principe de récurrence

Le principe de récurrence est un outil puissant pour montrer des résultats dépendant d'un entier :

Définition-théorème 1 - Principe de réccurrence.
Considérons une proposition $\mathcal{P}_n$, qui dépend d'une variable entière $\mathbb{N}$. Supposons que $\mathcal{P}_0$ soit vraie (initialisation), et que $\mathcal{P}_n \implies \mathcal{P}_{n+1}$ (hérédite). Alors

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

Remarque 2 - Définition ou théorème ?.
Cet énoncé s'appelle "principe". En fait il est lié à la construction de $\mathbb{N}$ (qui est admise), et est plus proche d'une définition que d'un théorème. Dans tout les cas, il est assez intuitif (pensez à la métaphore de l'échelle), et on ne se gênera pas pour l'appliquer **avec clarté**

✎ **En pratique** ✎ La rédaction d'une preuve par récurrence doit être méticuleuse. On évitera les "c'est évident par récurrence", à moins d'avoir déjà ébahi le correcteur. Voici les différentes étapes :

- On énonce clairement la propriété $\mathcal{P}_n$ que l'on va démontrer par récurrence.
- On effectue l'initialisation.
- On prouve l'hérédité (qui est souvent la partie dure, et peut être faite indépendamment de l'initialisation).
- On conclut par principe de récurrence.

Notez que l'initialisation peut démarrer à $n = 1$ (voire pour d'autres valeurs entières). Pour l'hérédité, on cherchera un mécanisme qui relie $\mathcal{P}_n$ et $\mathcal{P}_{n+1}$ (ou $\mathcal{P}_{n-1}$ et $\mathcal{P}_n$). En cas de blocage, on peut prouver la propriété pour les premières valeurs : la même idée que l'hérédité est souvent cachée derrière.

Voici un exemple facile et très classique du lycée, rédigé avec tous les détails :

Exemple 3 - Une preuve par récurrence. Démontrons par réccurrence : $\forall n \in \mathbb{N},\ n \leqslant 2^n$. Notons donc $\mathcal{P}_n$ la proposition « $n \leqslant 2^n$ ».

- Initialisation : pour $n = 0$, on a $0 \leqslant 1 = 2^0$, donc $\mathcal{P}_0$ est vraie.
- Hérédité : Pour $n \in \mathbb{N}$, supposons que $\mathcal{P}_n$ est vraie, c'est-à-dire que $n \leqslant 2^n$. On a alors $2n \leqslant 2 \times 2^n = 2^{n+1}$. Or, pour tout $n \in \mathbb{N}^*$, on a $n + 1 \leqslant 2n$. On obtient $n + 1 \leqslant 2^{n+1}$. Donc $\mathcal{P}_{n+1}$ est vraie.

On conclut par le principe de récurrence que $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N}$.

✖ **Attention !** ✖ Si un vos de raisonnements avec des entiers comporte des ... ou encore des "et ainsi de suite", c'est sûrement que vous voulez sans le savoir faire une preuve par récurrence !

Exemple 4 - La même en (un peu) plus dur. Montrer que $\forall n \in \mathbb{N}\backslash\{3\}$, on a $n^2 \leqslant 2^n$.

Définition-théorème 5 - Raisonnement par recurrence double ou par récurrence forte.
Considérons une proposition $\mathcal{P}_n$, qui dépend d'une variable entière $\mathbb{N}$.
Supposons que $\mathcal{P}_0$ soit vraie (initialisation). Supposons que l'on a l'un des points suivants :

- (Récurrence double) Pour tout $n \in \mathbb{N}^*$, on a $(\mathcal{P}_{n-1} \text{ et } \mathcal{P}_n) \implies \mathcal{P}_{n+1}$.
- (Récurrence forte). Pour tout $n \in \mathbb{N}^*$, on a $(\forall k \in [\![0, n]\!],\ \mathcal{P}_k) \implies \mathcal{P}_{n+1}$.

Alors

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

La différence réside dans la pratique : lors d'une récurrence forte, pour prouver l'hérédité, on peut supposer non seulement que $\mathcal{P}_n$ est vraie, mais aussi toutes les $\mathcal{P}_k$ avec $k \leqslant n$, afin de prouver que $\mathcal{P}_{n+1}$ est vraie. Nous verrons un exemple dans la section suivante.

2 Divisibilité

Définition 6 - Divisibilité. Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}$. On dit que a divise b, et l'on note a/b, s'il existe $k \in \mathbb{N}$ tel que $b = ka$. On dit alors que b est un multiple de a.

Notez que 1 divise tous les entiers naturels, et que 0 est multiple de tous les entiers. Notez aussi que si a/b, alors $a \leqslant b$.

Proposition 7 - Ordre et compatibilité. Soient a, b, c et d dans $\mathbb{N}$. Alors on a les propriétés suivantes :

- Relation d'ordre :
  - a/a (réflexivité)
  - (a/b et b/a) $\implies$ $a = b$ (antisymétrie)
  - (a/b et b/c) $\implies$ a/c (antisymétrie)
- Combinaison linéaire : si d/a et d/b, alors
$$\forall (u, v) \in \mathbb{N} \times \mathbb{N}, \quad d/au + bv.$$
- Produit : si a/b et c/d, alors ac/bd.
- Simplification : si $c \neq 0$, alors a/b si et seulement si ac/bc.

Exemple 8 Soient a et b dans $\mathbb{N}$ tels que a/b. Montrer que pour tout $k \in \mathbb{N}$, on a a^k/b^k.

Théorème 9 - Division euclidienne. Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ tel que
$$a = bq + r \quad \text{et } 0 \leqslant r < b.$$
Cette relation s'appelle la division euclidienne de a par b. De plus :

- a est le dividande.
- b est le diviseur.
- q est le quotient.
- r est le reste

Exemple 10 Un jeu de pétanques est composé de 6 boules. Combien de jeux peut-on faire avec 105 boules ?

Proposition 11 - Reste nul. Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. Le reste dans la division euclidienne de a par b est nul si et seulement si b/a.

3 Diviseurs et multiples communs

Définition 12 - Diviseurs et multiples communs. Soient $(a,b) \in \mathbb{N}^2$.

- On appelle diviseur commun de a et b tout entier qui divise à la fois a et b.
- On appelle multiple commun de a et b tout entier qui multiple à la fois de a et de b.

Cette définition inclut le cas où l'un des deux entiers est nul.

Définition 13 - PGCD. Soient $(a,b) \in \mathbb{N}^2$, avec $a \neq 0$ ou $b \neq 0$. On appelle plus grand diviseur commun (PGCD) de a et b, noté $a \wedge b$, le plus grand des diviseurs commun de a et b. Lorsque $a \wedge b = 1$, on dit que a et b sont premiers entre eux.

Notez que l'on a $a \wedge b = b \wedge a$, $a \wedge 1 = 1$ et $a \wedge 0 = a$.

Exemple 14 - PGCD.

- Déterminer $12 \wedge 33$, ainsi que $23 \wedge 2322$.
- Soit n et m deux entiers, déterminer $n \wedge (nm)$.
- Quels sont les couples d'entiers dans $[\![50\,,100]\!]$ dont le PGCD vaut 30 ?
- Déterminer les couples d'entiers dont la somme vaut 1680 et le PGCD 210.
- Existe-il un couple d'entiers dont le PGCD vaut 12 et dont le produit vaut 1443 ?

Proposition 15 - Diviseurs communs et PGCD . Soient $(a,b) \in \mathbb{N} \times \mathbb{N}$. Alors les diviseurs communs à a et à b sont les diviseurs du PGCD de a et b.

Exemple 16 - Diviseurs communs. Donner les diviseurs communs de 105 et 150

Lemme 17 - Division euclidienne et PGCD . Soient $(a,b) \in \mathbb{N} \times \mathbb{N}^*$, et $a = bq + r$ la division euclidienne de a par b. Alors on a $a \wedge b = r \wedge b$.

Théorème 18 - Algorithme d'Euclide. Soient $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$, avec $a \geqslant b$. On considèdre l'algorithme suivant :

1. $r = b$
2. Tant que (while) $r \neq 0$, faire (do) :
   a. Remplacer r par le reste de la division euclidienne de a par b
   b. Remplacer a par b,
   c. Remplacer b par r
   d. Retourner en 1.

Alors lorsque cet algorithme est terminé, la variable a vaut $a \wedge b$.

Exemple 19 - Un calcul de PGCD . Appliquer cet algorithme pour calculer le PGCD de 216 et 512.

Voici quelques propriétés qui permettent d'accéler le calul du PGCD :

Exercice 20 - Simplifier le calcul de PGCD . Soit $(a,b) \in \mathbb{N} \times \mathbb{N}$. Montrer que

1. $\forall k \in \mathbb{N}, (ka) \wedge (kb) = k(a \wedge b)$.
2. Si d est un diviseur commun de a et b, on a $a \wedge b = d(\frac{a}{d} \wedge \frac{b}{d})$.
3. Déterminer le PGCD de 125 et 750 sans appliquer l'algorithme d'Euclide.

Définition 21 - PPCM. Soient $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$. On appelle plus petit commun multiple (PPCM) de a et b, noté $a \vee b$, le plus petit des multiples communs de a et b.

La plupart des propriétés du PGCD ont un analogue pour le PPCM :

Proposition 22 - PPCM. Soient $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$. Les multiples communs de a et b sont des multiples de $a \vee b$.

Exercice 23 - Simplifier le calcul de PPCM. Donner des propriétés pour le PPCM analogues à celles de l'exercice 20

Il y a un multiple commun évident à a et b, il s'agit du produit ab. Ainsi, on sait qu'on a toujours $a \vee b \leqslant ab$. La proposition suivante précise ce lien :

Théorème 24 - produit, PGDC et PPCM. Soient $(a, b) \in \mathbb{N}^2$. On a

$$ab = (a \wedge b) \times (a \vee b).$$

4 Nombres premiers

Définition 25 - Nombres premiers. On appelle nombre premier tout entier naturel admettant exactement deux diviseurs, à savoir 1 et lui-même. On note $\mathcal{P}$ l'ensemble des nombres premiers

Notez qu'avec cette définition, le nombre 1 n'est pas premier ! Tout nombre premier est impair, sauf 2, qui est le plus petit des nombres premiers.

Voici l'occasion d'appliquer une récurrence forte :

Exemple 26 - Tout nombre a un diviseur premier. Montrer que tout nombre entier $n \geqslant 2$ possède au moins un diviseur premier. On pourra appliquer une récurrence forte.

Exemple 27 - Liste des nombres premiers. Vérifiez que vous connaissez les nombres premiers entre 1 et 50

En pratique, on cherche souvent à savoir quels sont les diviseurs d'un nombre, et comme on va le voir il suffit de se concentrer sur les diviseurs premiers. Les deux critères suivants donnent un critère précis pour chercher des diviseurs premiers :

Proposition 28 - Diviseurs premier. Soit $n \in \mathbb{N}$, alors n est premier si et seulement si il n'est divisible par aucun des nombres premiers qui lui sont inférieurs

Proposition 29 - Crible d'Eratosthène. Soit $n \in \mathbb{N}$ non premier, et soit $p \in \mathcal{P}$ un diviseur de n. Alors $p \leqslant \sqrt{n}$.

Exemple 30 - Critères de divisibilité. Voici quelques critères bien connus de divisibilité :

- Un nombre est divisble par 2 si et seulement si son dernier chiffre est pair.
- Un nombre est divisible par 3 si et seulement si la somme de ses chiffres l'est.
- Un nombre est divisible par 4 si et seulement si le nombre formé par ses deux derniers chiffres l'est.
- Un nombre est divisible par 5 si et seulement si son dernier chiffre est 0 ou 5.

Démontrer ces critères.

Exercice 31 - Critères de divisibilité par 7. Voici un critère un peu moins connu :

1. Soit n un entier, que l'on écrit sous la forme
$$n = 10d + r, \quad d \in \mathbb{Z},\ r \in [\![0\,,9]\!]\,.$$
Montrer que $7/n$ si et seulement si $7/50d + 5r$.
2. En déduire que $7/n$ si et seulement si $7/d + 5r$.
3. Enoncer le critère démontré. Le vérifier avec le nombre 105.

Proposition 32 - Infinité des nombres premiers. L'ensemble des nombres premiers est infini.

Théorème 33 - Décomposition en facteurs premiers. Soit n un entier avec $n \geqslant 2$, alors n admet une décomposition en facteurs premiers, qui est unique à l'ordre des facteurs près. On peut écrire : il existe des nombres premiers $p_1, \dots p_N$ et des entiers $m_1, \dots, m_N$, appelés multiplicités des facteurs, tels que
$$n = p_1^{m_1} \dots p_N^{m_N} = \prod_{k=1}^{N} p_i^{m_i}.$$

Exemple 34 - Quelques décompositions en facteurs premiers.

- Décomposer en facteurs premiers les nombres 24, 31, 36, 105, 512, 6 !=720.
En déduire les nombres $105 \wedge 720$ et $512 \wedge 720$.
- Calculer le PGCD de $a = 2^3 \times 3^2 \times 5 \times 11 \times 23^2$ et $b = 2 \times 3^4 \times 5^2 \times 23$.