Arithmétique dans $\mathbb{N}$

1 Différents modes de raisonnement

1.1 Raisonnement déductif et disjonction des cas :

Principe : Démontrer qu'une implication $P \Longrightarrow Q$ est vraie revient à démontrer que si P est vraie, alors Q est vraie. Dans ce cas, on dit que :

• P est l'hypothèse et Q la conclusion, • Q est une condition nécessaire pour P, • P est une condition suffisante pour Q.

Exemple 1. Soit $n \in \mathbb{Z}\backslash\{-1\}$. Démontrer que $\dfrac{n^2+1}{n+1} \in \mathbb{Z} \Longrightarrow n \in \{-3,-2,0,1\}$.

Remarque : Pour démontrer la véracité d'une implication, on peut raisonner par implications successives. On peut aussi raisonner par disjonction des cas : on "décompose" l'hypothèse en différents cas (recouvrant l'ensemble des possibilités), puis on démontre que la conclusion est vraie dans chacun de ces cas.

1.2 Assertions équivalentes et raisonnement par analyse-synthèse

Principe : Démontrer qu'une équivalence $P \Longleftrightarrow Q$ est vraie revient à démontrer que l'implication $P \Longrightarrow Q$ et sa réciproque $Q \Longrightarrow P$ sont vraies. Dans ce cas, on dit que :

• P est vraie si, et seulement si, Q est vraie, • P est une condition nécessaire et suffisante pour Q.

Exemple 2. Soit $n \in \mathbb{Z}\backslash\{-1\}$. Démontrer que $\dfrac{n^2+1}{n+1} \in \mathbb{Z} \Longleftrightarrow n \in \{-3,-2,0,1\}$.

Remarque : Pour montrer l'équivalence de plusieurs assertions, on peut raisonner par équivalences successives. On peut aussi établir une chaîne circulaire d'implications, par exemple $P \Longrightarrow Q \Longrightarrow R \Longrightarrow P$. Enfin, pour chercher les solutions d'un problème, caractérisé par une hypothèse P, on peut raisonner par **analyse-synthèse** :

• **phase d'analyse** : on cherche une condition nécessaire Q pour l'hypothèse P, • **phase de synthèse** : on teste si Q est aussi une condition suffisante pour P, • **conclusion** : si c'est le cas, on conclut que $P \Longleftrightarrow Q$.

1.3 Raisonnement par l'absurde ou par contraposition

Principe : Démontrer qu'une implication $P \Longrightarrow Q$ est vraie revient à démontrer que sa contraposée Non $Q \Longrightarrow$ Non P est vraie.

Exemple 3. Soit $a \in \mathbb{R}$. Montrer que $\left(\forall n \in \mathbb{N}^*,\ |a| < \dfrac{1}{n}\right) \Longrightarrow a = 0$.

Remarque : Pour démontrer la véracité d'une implication, on peut supposer que l'hypothèse P est vraie et que la conclusion Q est fausse, puis montrer que cela entraine une contradiction. Dans ce cas, l'assertion P et Non Q est fausse et sa négation $P \Longrightarrow Q$ est vraie. Un tel raisonnement est **un raisonnement par l'absurde**.

1.4 Raisonnement par récurrence

Dans ce qui suit, $P(n)$ est une proposition dépendant de $n \in \mathbb{N}$.

Principe de récurrence simple On montre qu'il existe $n_0 \in \mathbb{N}$ tel que :

1. **Initialisation** $P(n_0)$ est vraie.
2. **Hérédité** Pour tout entier $n \geq n_0$, $P(n) \Rightarrow P(n+1)$.

Selon le principe de récurrence (simple), on conclut que $\forall n \geq n_0$, $P(n)$ est vraie.

Principe de récurrence double On montre qu'il existe $n_0 \in \mathbb{N}$ tel que :

1. **Initialisation** $P(n_0)$ et $P(n_0+1)$ sont vraies.
2. **Hérédité** Pour tout entier $n \geq n_0$, $(P(n)$ et $P(n+1)) \Longrightarrow P(n+2)$.

Selon le principe de récurrence (double), on conclut que $\forall n \geq n_0$, $P(n)$ est vraie.

Exemple 4. $u_0 = 2$, $u_1 = 5$ et $\forall\, n \in \mathbb{N}$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrer que $\forall n \in \mathbb{N}$, $u_n = 2^n + 3^n$.

Principe de récurrence forte On montre qu'il existe $n_0 \in \mathbb{N}$ tel que :

1. **Initialisation** $P(n_0)$ est vraie.
2. **Hérédité** Pour tout entier $n \geq n_0$, $\big(\forall k \in [\![n_0, n]\!], P(k)\big) \Rightarrow P(n+1)$.

Selon le principe de récurrence (forte), on conclut que $\forall n \geq n_0$, $P(n)$ est vraie.

Exemple 5. $u_1 = 3$ et $\forall\, n \in \mathbb{N}^*$, $u_{n+1} = \dfrac{2}{n}(u_1 + \cdots + u_n)$. Exprimer u_n en fonction de $n \in \mathbb{N}^*$.

2 Arithmétique dans $\mathbb{N}$

2.1 Diviseurs et multiples d'un entier naturel

Définition 1. Soient a et b deux entiers naturels.

On dit que b **divise** a s'il existe un entier naturel k tel que $a = kb$.

Dans ce cas, on dit que b est un **diviseur** de a ou que a est un **multiple** de b et on note $b|a$.

Exemple 6. Expliciter l'ensemble des multiples de 5 et l'ensemble des diviseurs de 40 dans $\mathbb{N}$.

Remarque : Tout entier a divise 0. Tout entier a est divisible par 1.

La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$. Pour tout $(a,b,c) \in \mathbb{N}^3$, 1. $a|a$ (réflexivité). 2. $(a|b \text{ et } b|c) \Rightarrow a|c$ (transitivité) 3. $(a|b \text{ et } b|a) \Rightarrow a = b$ (antisymétrie).
De plus, si $a \neq 0$ alors on a : $b|a \Longrightarrow b \leq a$ (réciproque est fausse).

Propriété 1. Soit $(a,b,c) \in \mathbb{N}^3$. Si $c|a$ et $c|b$ alors $\forall (u,v) \in \mathbb{N}^2$, $c|au+bv$.

Théorème 1. et définition Soit $(a,b) \in \mathbb{N}^2$, avec $b \neq 0$.

Il existe un unique couple $(q,r) \in \mathbb{N}^2$ tel que $a = bq + r$ et $0 \leq r < b$.

q et r sont respectivement appelés **quotient et reste de la division euclidienne de a par b.**

Remarque : Le quotient q et le reste r de la division euclidienne de a par b vérifient :

$$q = \left\lfloor \frac{a}{b} \right\rfloor \text{ et } r = a - b \times \left\lfloor \frac{a}{b} \right\rfloor.$$

Exemple 7. Déterminer le quotient et le reste de la division euclidienne de a par b.

a) $a = 221$ et $b = 11$ b) $a = 2n^2 + 1$ et $b = n - 1$, $n \in \mathbb{N}^* \backslash \{1\}$.

Corollaire 1. Soit $(a,b) \in \mathbb{N}^2$, avec $b \neq 0$. b divise a ssi le reste de la division euclidienne de a par b est nul.

Définition 2. Soient a et b deux entiers naturels non nuls.

• On appelle **PGCD** (ou plus grand diviseur commun) de a et b le plus grand entier naturel d qui divise a et b. On le note $a \wedge b$.
• On dit que a et b sont **premiers entre eux** si $a \wedge b = 1$.

• On appelle **PPCM** (ou plus petit multiple commun) de a et b le plus petit entier naturel m non nul divisible par a et b. On le note $a \vee b$.

Exemple 8. Déterminer $12 \wedge 15$ et $12 \vee 15$.

Propriété 2. Soient a et b deux entiers naturels non nuls.

Si r est le reste de la division euclidienne de a par b alors $a \wedge b = b \wedge r$.

Application : Algorithme d'Euclide pour calculer $a \wedge b$:

• On pose $r_0 = a$ et $r_1 = b$.

• Pour tout $n \in \mathbb{N}^*$ tel que $r_n \neq 0$,
r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n.

• Dès que $r_N = 0$, on a $a \wedge b = r_{N-1}$ (dernier reste non nul).

Exemple 9. Déterminer $90 \wedge 40$.

2.2 Nombres premiers et factorisation d'un entier

Définition 3. Un **nombre premier** est un entier $p \geq 2$ dont les seuls diviseurs sont 1 et p.

Exemple 10. Écrire la liste des nombres premiers compris entre 1 et 50.

Théorème 2. Il existe une infinité de nombres premiers.

Crible d'Ératosthène pour déterminer les nombres premiers entre 1 et n :

• On écrit la liste des entiers de 1 à n.

• On raye tous les multiples stricts de 2, puis tous ceux de 3, ..., on s'arrête à $\sqrt{n}$.

Théorème 3. Décomposition d'un entier en produit de facteurs premiers (admis)

Pour tout entier $n \geq 2$ il existe, pour un certain $k \in \mathbb{N}^*$, des nombres premiers $p_1 < p_2 < \ldots < p_k$ et des entiers naturels non nuls $\alpha_1, \alpha_2, \ldots, \alpha_k$ tels que :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

De plus, cette décomposition est unique.

Exemple 11. Décomposer en produit de facteurs premiers les nombres $a = 256$ et $b = 1210$.

En déduire leur PGCD et leur PPCM.