Les entiers naturels et notions d'arithmétique

Chapitre 1

Ensemble des entiers naturels

L'ensemble des entiers naturels, noté $\mathbb{N}$, est l'ensemble dont les éléments sont $0, 1, 2, 3, \ldots$. C'est le plus simple des ensembles de nombres : il sert à compter et constitue la base de toute l'arithmétique étudiée dans ce chapitre.

Définition — Ensemble $\mathbb{N}$

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

L'ensemble $\mathbb{N}^*$ désigne l'ensemble des entiers naturels non nuls :

$$\mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{1, 2, 3, \ldots\}.$$

Propriété

Pour tous entiers naturels a et b :

- la somme $a + b$ est un entier naturel ;
- le produit $a \times b$ est un entier naturel ;
- en revanche, la différence $a - b$ n'est pas toujours un entier naturel (par exemple $3 - 5 = -2 \notin \mathbb{N}$).

Ordre dans $\mathbb{N}$

L'ordre usuel sur $\mathbb{N}$ est défini par : $a \leq b$ s'il existe $k \in \mathbb{N}$ tel que $b = a + k$. Cet ordre est **total** (deux entiers sont toujours comparables) et $\mathbb{N}$ admet un plus petit élément, à savoir 0.

Division euclidienne

La division euclidienne est l'outil central de l'arithmétique. Elle exprime qu'on peut toujours « partager équitablement » un entier par un autre, en acceptant un reste plus petit que le diviseur.

Théorème — Division euclidienne dans $\mathbb{N}$

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un **unique** couple (q, r) d'entiers naturels tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

L'entier q est appelé le **quotient** et l'entier r le **reste** de la division euclidienne de a par b.

Démonstration. **Existence.** Considérons l'ensemble $E = \{k \in \mathbb{N} \mid bk \leq a\}$. Il est non vide ($0 \in E$) et majoré par a. Il admet donc un plus grand élément q. On pose $r = a - bq$: par construction $r \geq 0$, et si l'on avait $r \geq b$ alors $b(q+1) = bq + b \leq a$, ce qui contredirait la maximalité de q. Donc $0 \leq r < b$.

Unicité. Supposons que $a = bq + r = bq' + r'$ avec $0 \leq r, r' < b$. Alors $b(q - q') = r' - r$, donc b divise $r' - r$. Comme $|r' - r| < b$, on a nécessairement $r = r'$, puis $q = q'$. ∎

Exemple. Division de 47 par 6 : on cherche le plus grand multiple de 6 inférieur ou égal à 47. Comme $6 \times 7 = 42$ et $6 \times 8 = 48 > 47$, on obtient $q = 7$ et $r = 47 - 42 = 5$. Donc $47 = 6 \times 7 + 5$.

Divisibilité

Définition — Diviseur, multiple
Soient $a, b \in \mathbb{N}$. On dit que b **divise** a, noté $b \mid a$, lorsqu'il existe $k \in \mathbb{N}$ tel que $a = bk$. On dit alors que a est un **multiple** de b.

Exemple. $7 \mid 42$ car $42 = 7 \times 6$. En revanche 5 ne divise pas 23 car la division euclidienne de 23 par 5 donne un reste non nul ($23 = 5 \times 4 + 3$).

Propriétés immédiates

Propriété
Pour tous entiers naturels a, b, c :
1. $1 \mid a$ et $a \mid a$ (réflexivité).
2. Si $a \mid b$ et $b \mid c$, alors $a \mid c$ (transitivité).
3. Si $a \mid b$ et $a \mid c$, alors pour tous $u, v \in \mathbb{N}$, $a \mid (bu + cv)$.
4. Si $a \mid b$ et $b \neq 0$, alors $a \leq b$.

Démonstration. Démontrons (3). Supposons $b = ak$ et $c = al$. Alors $bu + cv = aku + alv = a(ku + lv)$, donc a divise $bu + cv$. ∎

Nombres premiers

Définition — Nombre premier
Un entier $p \in \mathbb{N}$ est dit **premier** lorsque $p \geq 2$ et que ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p lui-même.

Les premiers nombres premiers sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$ Le nombre 1 n'est pas premier (par convention, pour préserver l'unicité de la décomposition en facteurs premiers). L'entier 2 est le seul nombre premier pair.

Théorème — Décomposition en facteurs premiers
Tout entier $n \geq 2$ s'écrit, de manière unique à l'ordre des facteurs près, comme produit de nombres premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k},$$

où les p_i sont des nombres premiers deux à deux distincts et les $\alpha_i \in \mathbb{N}^*$.

Exemple. $360 = 2^3 \times 3^2 \times 5$. En effet $360 = 8 \times 45 = 8 \times 9 \times 5$, et $8 = 2^3$, $9 = 3^2$.

Test de primalité par la racine carrée

Propriété
Si un entier $n \geq 2$ n'a aucun diviseur premier $p \leq \sqrt{n}$, alors n est premier.

Démonstration. Si n n'est pas premier, il s'écrit $n = ab$ avec $2 \leq a \leq b$. Alors $a^2 \leq ab = n$, donc $a \leq \sqrt{n}$. Tout diviseur premier de a est donc un diviseur premier de n inférieur ou égal à $\sqrt{n}$.■

Exemple. Pour vérifier que 97 est premier, il suffit de tester les diviseurs premiers $\leq \sqrt{97} \approx 9\{,\}85$, soit $2, 3, 5, 7$. Aucun ne divise 97, donc 97 est premier.

PGCD et PPCM

Définition — PGCD
Soient $a, b \in \mathbb{N}$ non tous deux nuls. Le **plus grand commun diviseur** de a et b, noté $\text{pgcd}(a, b)$ (ou $a \wedge b$), est le plus grand entier naturel qui divise à la fois a et b.

Définition — PPCM
Soient $a, b \in \mathbb{N}^*$. Le **plus petit commun multiple** de a et b, noté $\text{ppcm}(a, b)$ (ou $a \vee b$), est le plus petit entier naturel non nul multiple de a et de b.

Calcul par décomposition en facteurs premiers

Si $a = \prod_i p_i^{\alpha_i}$ et $b = \prod_i p_i^{\beta_i}$ (en complétant par des exposants nuls pour avoir les mêmes premiers), alors

$$\text{pgcd}(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)} \quad \text{et} \quad \text{ppcm}(a, b) = \prod_i p_i^{\max(\alpha_i, \beta_i)}.$$

Exemple. Calculons $\text{pgcd}(360, 84)$ et $\text{ppcm}(360, 84)$.
- $360 = 2^3 \times 3^2 \times 5^1$
- $84 = 2^2 \times 3^1 \times 7^1$

Donc $\text{pgcd}(360, 84) = 2^2 \times 3^1 = 12$ et $\text{ppcm}(360, 84) = 2^3 \times 3^2 \times 5 \times 7 = 2520$.

Algorithme d'Euclide

Théorème — Lemme d'Euclide
Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Si r est le reste de la division euclidienne de a par b, alors

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

Démonstration. Posons $a = bq + r$. Tout diviseur commun de a et b divise $r = a - bq$. Réciproquement, tout diviseur commun de b et r divise $a = bq + r$. Les deux paires (a, b) et (b, r) ont donc les mêmes diviseurs communs, et en particulier le même plus grand. ■

Exemple. Calcul de $\text{pgcd}(252, 105)$ par l'algorithme d'Euclide :
- $252 = 105 \times 2 + 42$
- $105 = 42 \times 2 + 21$
- $42 = 21 \times 2 + 0$

Le dernier reste non nul est 21, donc $\text{pgcd}(252, 105) = 21$.

Lien entre PGCD et PPCM

Théorème
Pour tous entiers $a, b \in \mathbb{N}^*$:

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = a \times b.$$

Démonstration. En décomposant en facteurs premiers, pour chaque premier p apparaissant dans a ou b avec exposants α et β, on a $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$. En multipliant sur tous les premiers, on obtient l'égalité annoncée. ■

Exemple. Avec $a = 360$ et $b = 84$: $12 \times 2520 = 30240 = 360 \times 84$. ✓

Nombres premiers entre eux

Définition — Nombres premiers entre eux
Deux entiers $a, b \in \mathbb{N}^*$ sont dits **premiers entre eux** lorsque $\text{pgcd}(a, b) = 1$.

Exemple. 15 et 28 sont premiers entre eux : $15 = 3 \times 5$, $28 = 2^2 \times 7$, ils n'ont aucun facteur premier en commun.

Propriété
Soit $d = \text{pgcd}(a, b)$. Si l'on pose $a = da'$ et $b = db'$, alors a' et b' sont premiers entre eux.

Démonstration. Si un entier $k > 1$ divisait à la fois a' et b', alors dk diviserait à la fois a et b, contredisant la maximalité de d. ■

Exercices

Exercice 1. Effectuer la division euclidienne de a par b dans les cas suivants : (a) $a = 73$, $b = 8$; (b) $a = 2025$, $b = 47$; (c) $a = 1000$, $b = 17$.

Exercice 2. Lister tous les diviseurs naturels de 60. Combien y en a-t-il ? Retrouver ce nombre à partir de la décomposition $60 = 2^2 \times 3 \times 5$.

Exercice 3. Montrer que la somme de trois entiers naturels consécutifs est divisible par 3.

Exercice 4. Décomposer en facteurs premiers : 504, 1001, 2024. En déduire $\text{pgcd}(504, 2024)$.

Exercice 5. En utilisant l'algorithme d'Euclide, calculer $\text{pgcd}(1071, 462)$, puis $\text{ppcm}(1071, 462)$ via la formule $\text{pgcd} \times \text{ppcm} = ab$.