Chapitre 11

ARITHMÉTIQUE

1 Multiples et diviseurs d'un entier

Définition 1 *Soient a et b deux entiers. On dit que b est un* **multiple** *de a, ou que a est un* **diviseur** *de b, ou que b est* **divisible** *par a, ou encore que a* **divise** *b, et on note $a \mid b$, s'il existe un entier k tel que $b = ka$.*

Exemple : 28 est un multiple de 7 (et 7 est un diviseur de 28) car $28 = 4 \times 7$.

Proposition 1 *Soient a, b, c trois entiers.*

(i) Si a divise b et c, alors a divise $b + c$.

(ii) Si a divise b et que b divise c, alors a divise c.

(iii) Si a et b sont de même signe, alors : $(a \mid b$ et $b \mid a) \Leftrightarrow a = b$.

Démonstration : Immédiat. □

2 Division euclidienne dans $\mathbb{N}$

Théorème 2 *Soient a un entier naturel et b un entier naturel non nul. Il existe un unique couple (q, r) d'entiers naturels tels que :*

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}.$$

On dit alors que q est le **quotient** et r le **reste** dans la **division euclidienne de a par b**.

Exemple : Division euclidienne de 27 par 4 : $27 = 4 \times 6 + 3$. Le quotient est 6 et le reste est 3 (on a bien $0 \leqslant 3 < 4$).

Démonstration :

Commençons par établir l'existence de q et r.

Considérons l'ensemble des entiers naturels k tels que $kb \leqslant a$. C'est un sous-ensemble non vide (il contient 0) et majoré (par a par exemple) de $\mathbb{N}$, donc il possède un plus grand élément q. On a donc $qb \leqslant a$ mais $(q+1)b > a$ donc $qb > a - b$.

Posons alors $r = a - qb$. On a ainsi $a = bq + r$ et $0 \leqslant r < b$ puisque $-a \leqslant -qb < b - a$. C'est ce qu'on voulait.

Établissons maintenant l'unicité de q et r.

On suppose donc qu'il existe deux couples d'entiers naturels (q_1, r_1) et (q_2, r_2) tels que $\begin{cases} a = bq_1 + r_1 \\ 0 \leqslant r_1 < b \end{cases}$ et $\begin{cases} a = bq_2 + r_2 \\ 0 \leqslant r_2 < b \end{cases}$.

Alors $bq_1 + r_1 = bq_2 + r_2$, donc $r_2 - r_1 = b(q_1 - q_2)$. On a $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$, donc $-b < r_2 - r_1 < b$. D'autre part, si $q_1 \neq q_2$, alors $b(q_1 - q_2) \geqslant b$ ou $\leqslant -b$: c'est impossible. Par conséquent $q_1 = q_2$ et donc $r_1 = r_2$. □

Remarques :

1) Sans la condition $0 \leqslant r < b$ on perd l'unicité. Par exemple on a aussi $27 = 4 \times 5 + 7$ mais on n'a pas $0 \leqslant 7 < 4$.

2) a est divisible par b si et seulement si le reste dans la division euclidienne de a par b est nul.

3) On peut étendre la division euclidienne au cas où a est un entier relatif. Par exemple la division euclidienne de -27 par 4 est $-27 = 4 \times (-7) + 1$.

3 PGCD, PPCM

• PGCD

Proposition 3 *Soient a et b deux entiers naturels non tous deux nuls. L'ensemble des diviseurs communs à a et b admet un plus grand élément.*

Démonstration : L'ensemble des diviseurs communs à a et b est une partie de $\mathbb{N}$ non vide (1 divise a et b) et majorée (par a ou b). □

Ce plus grand élément est appelé **plus grand diviseur commun** (ou plus grand commun diviseur, en abrégé pgcd) de a et b et est noté $\text{pgcd}(a,b)$ ou $a \wedge b$. On pose $0 \wedge 0 = 0$.

Par exemple, les diviseurs de 18 sont $1, 2, 3, 6, 9$ et 18 et les diviseurs de 24 sont $1, 2, 3, 4, 6, 8, 12$ et 24, donc le pgcd de 18 et 24 est 6.

Si a et b sont des entiers relatifs, on pose $a \wedge b = |a| \wedge |b|$.

Proposition 4 *Soient a et b deux entiers naturels. Alors :*

(i) $a \wedge b = b \wedge a$.

(ii) $a \wedge 0 = 0 \wedge a = a$.

(iii) Si a divise b, alors $a \wedge b = a$.

(iv) Si $a = bq + r$ avec $q, r \in \mathbb{N}$, alors $a \wedge b = b \wedge r$.

Démonstration :

Si $a = 0$, c'est immédiat. On suppose $a \neq 0$.

(i) : Immédiat.

(ii) : Tout entier naturel est un diviseur de 0, donc le plus grand diviseur commun à a et 0 est le plus grand diviseur de a, c'est-à-dire a.

(iii) : Si a divise b, alors les diviseurs de a sont aussi des diviseurs de b. L'ensemble des diviseurs communs à a et b est donc l'ensemble des diviseurs de a, dont le plus grand élément est a.

(iv) : L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs communs à b et r. En effet, si d divise a et b, alors il divise bq et donc aussi $r = a - bq$, et réciproquement si d divise b et r, il divise bq et donc aussi $a = bq + r$. □

La propriété (iv) permet de calculer le pgcd de a et b en procédant par divisions euclidiennes successives : on appelle cette méthode **l'algorithme d'Euclide**. Soient $r_0 = a$, $r_1 = b$ et, tant que $r_{n+1} \neq 0$, soit r_{n+2} le reste de la division euclidienne de r_n par r_{n+1}. Alors, par récurrence immédiate, on a $a \wedge b = r_n \wedge r_{n+1}$ pour tout n. Or (r_n) est une suite strictement décroissante d'entiers naturels, donc il existe un p tel que $r_p = 0$. On a alors $a \wedge b = r_{p-1} \wedge 0 = r_{p-1}$. Le pgcd de a et b est donc le dernier reste non nul.

Exemple : Calculons le pgcd de 336 et de 276. On a $336 = 1 \times 276 + 60$, $276 = 4 \times 60 + 36$, $60 = 1 \times 36 + 24$, $36 = 1 \times 24 + 12$, $24 = 2 \times 12 + 0$. Le pgcd de 336 et de 276 est donc 12.

Proposition 5 *Les diviseurs communs à deux entiers naturels a et b sont exactement les diviseurs de $a \wedge b$.*

Démonstration :

Si d divise $a \wedge b$, alors d divise a et b. Pour la réciproque, on utilise l'algorithme d'Euclide : soient $(r_n)_{1 \leqslant n \leqslant p-1}$ la suite des restes obtenus dans les divisions successives comme ci-dessus, avec $r_{p-1} = a \wedge b$. Si d divise $a = r_0$ et $b = r_1$, alors il divise r_2. Puisqu'il divise r_1 et r_2, alors il divise r_3, etc. Il divise donc $r_{p-1} = a \wedge b$. □

• PPCM

Proposition 6 *Soient a et b deux entiers naturels non nuls. L'ensemble des multiples non nuls communs à a et b admet un plus petit élément.*

Ce plus petit élément est appelé **plus petit multiple commun** (ou plus petit commun multiple, en abrégé ppcm) de a et b et est noté $\text{ppcm}(a,b)$ ou $a \vee b$. Si $a = 0$ ou $b = 0$, on pose $a \vee b = 0$.

Démonstration : L'ensemble des multiples non nuls communs à a et à b est une partie de $\mathbb{N}^*$ non vide (il contient ab). □

Par exemple, les multiples non nuls de 18 sont $18, 36, 54, 72, \ldots$ et les multiples non nuls de 24 sont $24, 48, 72, \ldots$, donc le ppcm de 18 et 24 est 72.

Le lien entre pgcd et ppcm est donné par la proposition suivante, que l'on admettra :

Proposition 7 *Soient a et b deux entiers naturels. Alors* $(a \wedge b) \times (a \vee b) = ab$.

On a vu, par exemple, que le pgcd de 336 et de 276 est 12. Leur ppcm est donc $\dfrac{336 \times 276}{12} = 7728$.

Proposition 8 *Soient a et b deux entiers naturels. Alors :*

(i) $a \vee b = b \vee a$.

(ii) Si a divise b, alors $a \vee b = b$.

(iii) Les multiples communs à a et b sont exactement les multiples de $a \vee b$.

Démonstration : Immédiat avec la proposition précédente et les propriétés du pgcd. □

4 Nombres premiers

Définition 2 *Un entier naturel p est* **premier** *s'il possède exactement 2 diviseurs dans $\mathbb{N}$: 1 et lui-même.*

Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ... Noter que 1 n'est pas premier : il n'a qu'un seul diviseur (lui-même).

Exercice 1 Les entiers 127, 323, 353, 413, 12345678987654321, 1000000000000000000001 sont-ils premiers ?

Le **crible d'Ératosthène** est une méthode efficace permettant de trouver l'ensemble des nombres premiers inférieurs ou égaux à un entier naturel n donné. Le principe est le suivant : on écrit tous les entiers compris entre 2 et n. Ensuite, à chaque étape, on garde le premier entier non barré, et on barre tous ses multiples stricts. On s'arrête quand le premier nombre non barré est strictement supérieur à $\sqrt{n}$.

Exercice 2 Appliquer la méthode pour $n = 100$.

Le résultat suivant (que l'on admettra) est appelé **théorème fondamental de l'arithmétique** :

Théorème 9 *Tout entier naturel non nul n s'écrit de manière unique (à l'ordre des facteurs près) sous la forme :*

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

où $p_1, p_2, \dots, p_r$ sont des nombres premiers deux à deux distincts et $k_1, k_2, \dots, k_r$ sont des entiers naturels non nuls.

Cette écriture est appelée **décomposition de n en produit de facteurs premiers**. Par exemple, on a $12 = 2^2 \times 3$ et $270 = 2 \times 3^3 \times 5$.

Le résultat suivant, que l'on admettra également, permet de calculer le pgcd et le ppcm de deux entiers naturels à partir de leurs décompositions en produits de facteurs premiers.

Proposition 10 *Soient $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ où $p_1, p_2, \dots, p_r$ sont des nombres premiers deux à deux distincts et $\alpha_1, \beta_1, \dots, \alpha_r, \beta_r$ sont des entiers naturels. Alors $a \wedge b = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}$ et $a \vee b = p_1^{\delta_1} p_2^{\delta_2} \dots p_r^{\delta_r}$ où $\gamma_i = \min(\alpha_i, \beta_i)$ et $\delta_i = \max(\alpha_i, \beta_i)$ pour tout i.*

Attention, ici les α_i et les β_i peuvent être nuls. Par exemple, on a $12 = 2^2 \times 3^1 \times 5^0$ et $270 = 2^1 \times 3^3 \times 5^1$ donc $12 \wedge 270 = 2^1 \times 3^1 \times 5^0 = 6$ et $12 \vee 270 = 2^2 \times 3^3 \times 5^1 = 540$.

Exercice 3

1) Décomposer en produits de facteurs premiers 660, 1125, 660×1125.

2) Calculer le pgcd et le ppcm de 660 et 1125.

3) Simplifier $\dfrac{660}{1125}$, $\dfrac{12^{111} \times 15^{333}}{6^{222} \times 1125^{111}}$, $\sqrt{1125}$.

Théorème 11 *(Théorème d'Euclide) L'ensemble des nombres premiers est infini.*

Démonstration :

Notons $\mathcal{P}$ cet ensemble. On raisonne par l'absurde : supposons que $\mathcal{P}$ est fini. Notons $p_1, p_2, \dots, p_n$ ses éléments.

Considérons alors $m = p_1 \times p_2 \times \dots \times p_n + 1$. Ce n'est pas un nombre premier, puisqu'il est strictement supérieur à tous les éléments de $\mathcal{P}$. D'après le théorème fondamental de l'arithmétique, il admet donc un diviseur premier p_k. Mais alors, puisque p_k divise $p_1 \times p_2 \times \dots \times p_n$ et m, il divise 1 : contradiction. □