

## 10.1 Divisibilité

### 10.1.1 Définition et division euclidienne

#### Définition 1: Divisibilité

Soient  $(a, b) \in \mathbb{Z}^2$ .

On dit que  $a$  divise  $b$ , et on note  $a|b$ , s'il existe un entier relatif  $k \in \mathbb{Z}$  tel que  $b = ak$ .

Dans ce cas, on dit que  $a$  est un diviseur de  $b$ , ou que  $b$  est un multiple de (ou est divisible par)  $a$ .

**Remarque 1.** • 1 et  $-1$  divisent tous les entiers relatifs.

- 0 est divisible par tous les entiers relatifs.
- Soit  $a \in \mathbb{Z}$ . Alors  $a$  et  $-a$  divisent  $a$ .

#### Proposition 1: Propriétés de la divisibilité

Soient  $(a, b, c) \in \mathbb{Z}^3$ .

1. Si  $a$  divise  $b$  et  $c$ , alors pour tout couple  $(u, v) \in \mathbb{Z}^2$ ,  $a$  divise  $bu + cv$ .
2. Si  $a$  divise  $b$  et  $b$  divise  $c$ , alors  $a$  divise  $c$ .
3. Si  $a$  divise  $b$ , et  $b \neq 0$ , alors  $|a| \leq |b|$ .
4. Si  $a$  divise  $b$  et  $b$  divise  $a$ , alors  $|a| = |b|$ .

#### Démonstration.

1. Par hypothèse, il existe  $(k, l) \in \mathbb{Z}^2$  tel que  $b = ak$  et  $c = al$ .

Soit  $(u, v) \in \mathbb{Z}^2$ . On a alors

$$bu + cv = aku + alv = a(ku + lv)$$

avec  $ku + lv \in \mathbb{Z}$  donc  $a$  divise  $bu + cv$ .

2. Par hypothèse, il existe  $(k, l) \in \mathbb{Z}^2$ ,  $b = ak$  et  $c = bl$  donc  $c = a(kl)$  avec  $kl \in \mathbb{Z}$ , ce qui prouve que  $a$  divise  $c$ .
3. Par hypothèse, il existe  $k \in \mathbb{Z}$  tel que  $b = ak$  donc  $|b| = |a||k|$ . Puisque  $b \neq 0$ , on a nécessairement  $k \neq 0$  donc  $|k| \geq 1$  et il en découle que

$$|b| = |a||k| \geq |a|.$$

4. • Si  $b = 0$ , puisque  $b$  divise  $a$ , alors  $a = 0$  et on a bien  $|a| = |b|$ .  
 • Si  $b \neq 0$ , d'après le point précédent, puisque  $a$  divise  $b$  alors  $|a| \leq |b|$ .  
 De plus, puisque  $a$  divise  $b$  et que  $b \neq 0$ , on a nécessairement  $a \neq 0$  et d'après le point précédent, puisque  $b$  divise  $a$ , on en déduit que  $|b| \leq |a|$ .  
 Ainsi, on a  $|a| \leq |b|$  et  $|b| \leq |a|$ , d'où  $|a| = |b|$ . ■

**Remarque 2.** En particulier, si  $a$  divise  $b$  et  $c$ , alors  $a$  divise  $b + c$ ,  $a$  divise  $b - c$ ,  $a$  divise tous les multiples de  $b$  et tous les multiples de  $c$  donc  $a$  divise  $bc$ .

En revanche, les réciproques sont fausses : 6 divise  $2 + 4$  mais ne divise ni 2 ni 4, 6 divise  $3 \times 4$  mais ne divise ni 3 ni 4...

### Théorème 1: Théorème de la division euclidienne

Soient  $(a, b) \in \mathbb{Z}^2$  avec  $b \neq 0$ .

Il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que

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

On dit que  $q$  est le quotient de la division euclidienne de  $a$  par  $b$  et que  $r$  en est le reste.

#### Démonstration.

- Montrons l'existence d'un tel couple  $(q, r)$ .

1er cas :  $b > 0$

Soit  $A = \{k \in \mathbb{Z}, bk \leq a\}$ .

Tout d'abord, puisque  $b > 0$ ,  $bk \leq a \Leftrightarrow k \leq \frac{a}{b}$ . Ceci prouve que  $A$  n'est pas vide.

De plus,  $A$  est majorée par  $\frac{a}{b}$ . Ainsi,  $A$  est une partie de  $\mathbb{Z}$  non vide et majorée donc  $A$  admet un plus grand élément (cf. chapitre « Nombres réels »).

Soit  $q = \max(A)$ . Posons  $r = a - bq$ . Puisque  $q \in A$ ,  $bq \leq a$  donc  $r = a - bq \geq 0$ .

De plus,  $q + 1 \notin A$  donc  $b(q + 1) > a$ , ce qui implique que  $r = a - bq < b = |b|$ .

On a donc bien trouvé un couple  $(q, r)$  qui convient.

2ème cas :  $b < 0$

Dans ce cas,  $-b > 0$ . D'après le premier cas, il existe un couple  $(q, r)$  d'entiers relatifs tel que  $a = (-b)q + r$  et  $0 \leq r < -b = |b|$ .

En posant  $q' = -q$ , on a bien  $a = bq' + r$  avec  $(q', r) \in \mathbb{Z}^2$  et  $0 \leq r < |b|$ .

- Montrons l'unicité d'un tel couple  $(q, r)$ .

Supposons qu'il existe deux couples  $(q, r)$  et  $(q', r')$  d'entiers relatifs tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases} \quad \text{et} \quad \begin{cases} a = bq' + r' \\ 0 \leq r' < |b| \end{cases}.$$

On a alors  $bq + r = bq' + r'$  donc  $b(q - q') = r' - r$  ce qui implique que  $|b||q - q'| = |r' - r|$ .

Or,  $-|b| < r' - r < |b|$  donc  $|r' - r| < |b|$ , ce qui implique que  $|b||q - q'| < |b|$ . Il en découle que  $|q - q'| = 0$  donc  $q = q'$  et par suite,  $r = r'$ , ce qui prouve bien l'unicité d'un tel couple  $(q, r)$ . ■

**Exemple 1.** 1. La division euclidienne de  $-17$  par  $5$  est  $-17 = -4 \times 5 + 3$ . Le quotient de la division euclidienne de  $-17$  par  $5$  est  $-4$  et le reste vaut  $3$ .

2. La division euclidienne de  $29$  par  $-6$  est  $29 = (-6) \times (-4) + 5$ . Le quotient de la division euclidienne de  $29$  par  $-6$  est  $-4$  et le reste vaut  $5$ .

## 10.1.2 PGCD et PPCM

**Définition 2: PGCD de deux entiers relatifs**

Soient  $(a, b) \in \mathbb{Z}^2$  avec  $(a, b) \neq (0, 0)$ .

On appelle PGCD des entiers  $a$  et  $b$ , noté  $\text{PGCD}(a, b)$  ou  $a \wedge b$ , le plus grand diviseur commun à  $a$  et  $b$ .

**Exemple 2.** L'ensemble des diviseurs de 60 est

$$\{-60, -30, -20, -15, -12, -10, -6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$

et l'ensemble des diviseurs de 36 est

$$\{-36, -18, -12, -9, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 9, 12, 18, 36\}.$$

On constate que  $60 \wedge 36 = 12$ .

**Remarque 3.** • Si  $(a, b) = (0, 0)$ ,  $a$  et  $b$  étant divisibles par tous les entiers relatifs, il n'existe pas de plus grand diviseur commun à  $a$  et  $b$ .

• Si  $a \neq 0$ , pour tout  $b \in \mathbb{Z}$ ,  $a \wedge b$  est bien défini car l'ensemble des diviseurs de  $a$  est majoré par  $|a|$ . Ainsi, l'ensemble des diviseurs communs à  $a$  et  $b$  est une partie de  $\mathbb{Z}$  non vide et majorée, donc admet un plus grand élément, ce qui justifie l'existence du PGCD de  $a$  et  $b$ .

• On a toujours  $a \wedge b \geq 1$ . En particulier, c'est un entier naturel non nul.

•  $a$  divise  $b$  si et seulement si  $a \wedge b = |a|$ . En particulier, si  $a \neq 0$ , alors  $a \wedge 0 = a \wedge a = |a|$ .

**Proposition 2: Algorithme d'Euclide**

Soient  $(a, b) \in \mathbb{Z}^2$  avec  $b \neq 0$ ,  $|b| \leq |a|$  et  $b$  ne divise pas  $a$ .

Il existe des suites finies d'entiers  $(a_n)_{n \leq p}$ ,  $(b_n)_{n \leq p}$  et  $(r_n)_{n \leq p}$  où  $p \in \mathbb{N}^*$  telles que :

- $a_0 = a, b_0 = b$  et  $r_0$  est le reste dans la division euclidienne de  $a$  par  $b$ ;
- pour tout  $n \leq p-1$ ,  $a_{n+1} = b_n$  et  $b_{n+1} = r_n$ ;
- pour tout  $n \leq p$ ,  $r_n$  est le reste dans la division euclidienne de  $a_n$  par  $b_n$ ;
- $r_p = 0$ .

Le PGCD de  $a$  et  $b$  est alors le dernier reste non nul apparu dans l'algorithme, i.e.

$$a \wedge b = r_{p-1}.$$

**Remarque 4.** Si  $b$  divise  $a$ , l'algorithme d'Euclide n'est pas nécessaire pour déterminer le PGCD de  $a$  et  $b$ , puisque dans ce cas,  $a \wedge b = |b|$ . Si on n'est pas dans ce cas, il est certain que le premier reste obtenu dans l'algorithme d'Euclide n'est pas nul, ce qui assure que  $p \geq 1$ .

**Démonstration.** • On pose  $a_0 = a$  et  $b_0 = b$ . D'après le théorème de la division euclidienne, il existe  $(q_0, r_0) \in \mathbb{Z}^2$  tels que  $a = bq_0 + r_0$  et  $0 \leq r_0 < |b|$ , i.e.  $a_0 = b_0q_0 + r_0$ .

On pose ensuite  $a_1 = b_0, b_1 = r_0$ . Il existe alors  $(q_1, r_1) \in \mathbb{Z}^2$  tels que  $a_1 = b_1q_1 + r_1$  avec  $0 \leq r_1 < |b_1| = r_0$ .

En répétant ce procédé, on construit une suite strictement décroissante d'entiers naturels  $r_0 > r_1 > \dots$  donc il existe nécessairement un rang  $p \in \mathbb{N}^*$  pour lequel  $r_p = 0$ .

Notons pour tout  $n \leq p$ ,  $a_n = b_nq_n + r_n$  où  $q_n \in \mathbb{Z}$ .

• Montrons que pour tout  $n \leq p$ ,  $a_n \wedge b_n = b_n \wedge r_n$ .

Soit  $n \leq p$ .

Soit  $d \in \mathbb{Z}$ .

Montrons que  $d$  divise  $a_n$  et  $b_n$  si et seulement si  $d$  divise  $b_n$  et  $r_n$ .

Supposons que  $d$  divise  $a_n$  et  $b_n$ . Alors  $d$  divise  $a_n - b_nq_n = r_n$  donc  $d$  divise  $b_n$  et  $r_n$ .

Réciproquement, supposons que  $d$  divise  $b_n$  et  $r_n$ . Alors  $d$  divise  $b_n q_n + r_n = a_n$  donc  $d$  divise  $a_n$  et  $b_n$ .

On a donc montré que pour tout  $n \leq p$ , les diviseurs communs à  $a_n$  et à  $b_n$  sont les diviseurs communs à  $b_n$  et à  $r_n$ .

A fortiori,  $a_n \wedge b_n = b_n \wedge r_n$ .

• Ainsi,  $a \wedge b = a_0 \wedge b_0 = b_0 \wedge r_0 = a_1 \wedge b_1 = \dots = a_p \wedge b_p = b_p \wedge r_p = r_{p-1} \wedge 0 = r_{p-1}$ . ■

**Exemple 3.** Déterminons le PGCD de 51 et 42.

Effectuons l'algorithme d'Euclide.

$$\begin{aligned} 51 &= 42 \times 1 + 9 \\ 42 &= 9 \times 4 + 6 \\ 9 &= 6 \times 1 + 3 \\ 6 &= 3 \times 2 + 0 \end{aligned}$$

donc  $51 \wedge 42 = 3$ .

#### Corollaire 1: Identité de Bézout

Soient  $(a, b) \in \mathbb{Z}^2$  avec  $(a, b) \neq (0, 0)$ .

Il existe un couple  $(u, v) \in \mathbb{Z}^2$  tel que

$$au + bv = a \wedge b.$$

**Démonstration.** Reprenons l'algorithme d'Euclide à l'envers, à partir de l'avant-dernière étape. On a

$$\begin{aligned} a \wedge b &= r_{p-1} \\ &= a_{p-1} - b_{p-1}q_{p-1} \\ &= b_{p-2} - r_{p-2}q_{p-1} \\ &= b_{p-2} - (a_{p-2} - b_{p-2}q_{p-2})q_{p-1} \\ &= b_{p-2}(1 + q_{p-2}q_{p-1}) - a_{p-2} \end{aligned}$$

On voit qu'on a d'abord réussi à écrire  $a \wedge b$  comme combinaison linéaire à coefficients entiers de  $a_{p-1}$  et de  $b_{p-1}$ , puis de  $a_{p-2}$  et de  $b_{p-2}$ , etc... En remontant l'algorithme d'Euclide, on arrivera à écrire  $a \wedge b$  comme combinaison linéaire à coefficients entiers de  $a_0 = a$  et de  $b_0 = b$ , c'est à dire qu'on aura trouvé  $(u, v) \in \mathbb{Z}^2$  tel que

$$au + bv = a \wedge b.$$

■

**Exemple 4.** Reprenons l'algorithme d'Euclide de 51 et 42. On a

$$\begin{aligned} 3 &= 9 - 6 \\ &= 9 - (42 - 9 \times 4) \\ &= 9 \times 5 - 42 \\ &= (51 - 42) \times 5 - 42 \\ &= 51 \times 5 - 42 \times 6 \end{aligned}$$

En posant  $u = 5$  et  $v = -6$ , on a donc  $51u + 42v = 3 = 51 \wedge 42$ .

**Remarque 5.** La réciproque est fautive : s'il existe  $d \in \mathbb{N}^*$  et  $(u, v) \in \mathbb{Z}^2$  tels que  $au + bv = d$ , on ne peut pas affirmer que  $a \wedge b = d$  mais simplement que  $a \wedge b$  divise  $d$ .

En effet, si  $au + bv = d$ , puisque  $a \wedge b$  divise  $a$  et  $b$ , alors  $a \wedge b$  divise  $au + bv$  donc  $a \wedge b$  divise  $d$ .

Par exemple,  $6 \times 9 + (-4) \times 12 = 6$  mais  $9 \wedge 12 = 3$ .

### Corollaire 2: Lien entre diviseurs communs et PGCD

Soit  $(a, b) \in \mathbb{Z}^2$  avec  $(a, b) \neq (0, 0)$ .

Soit  $d$  un diviseur commun à  $a$  et à  $b$ .

Alors  $d$  divise  $a \wedge b$ .

**Démonstration.** D'après l'identité de Bézout, il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = a \wedge b$ .

Puisque  $d$  divise  $a$  et  $b$ , alors  $d$  divise  $au + bv = a \wedge b$ . ■

**Remarque 6.** Ceci signifie que  $a \wedge b$  est non seulement le plus grand diviseur commun à  $a$  et à  $b$ , mais également qu'il est divisible par tous les diviseurs communs à  $a$  et à  $b$ .

**Exemple 5.** L'ensemble des diviseurs communs à 60 et 36 est  $\{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$ . On constate que tous les diviseurs communs à 60 et 36 divisent  $12 = 60 \wedge 36$ .

### Définition 3: Entiers premiers entre eux

Soient  $(a, b) \in \mathbb{Z}^2$  avec  $(a, b) \neq (0, 0)$ .

On dit que  $a$  et  $b$  sont premiers entre eux si  $a \wedge b = 1$ .

**Exemple 6.** 91 et 68 sont premiers entre eux. Vérifions-le par l'algorithme d'Euclide.

$$91 = 68 \times 1 + 23$$

$$68 = 23 \times 2 + 22$$

$$23 = 22 \times 1 + 1$$

Le dernier reste non nul de l'algorithme d'Euclide est 1 donc  $91 \wedge 68 = 1$ .

### Théorème 2: Théorème de Bézout

Soient  $(a, b) \in \mathbb{Z}^2$ , avec  $(a, b) \neq (0, 0)$ .

Les entiers  $a$  et  $b$  sont premiers entre eux si et seulement s'il existe un couple  $(u, v) \in \mathbb{Z}^2$  tel que

$$au + bv = 1.$$

**Démonstration.** On a déjà vu qu'il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = a \wedge b$ .

Ainsi, si  $a \wedge b = 1$ , il existe bien  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = 1$ .

Réciproquement, supposons qu'il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = 1$ .

Alors  $a \wedge b$  divise  $au + bv = 1$  donc  $a \wedge b$  divise 1. A fortiori,  $a \wedge b \leq 1$ . Or,  $1 \leq a \wedge b$  donc  $a \wedge b = 1$ . ■

**Exemple 7.** Pour tout  $n \in \mathbb{Z}$ ,  $(n+1) - n = 1$  donc  $n$  et  $n+1$  sont premiers entre eux d'après le théorème de Bézout.

**Remarque 7.** Une conséquence importante est la suivante : si  $(a, b) \in \mathbb{Z}^2 \neq (0, 0)$ , alors  $\frac{a}{a \wedge b}$  et  $\frac{b}{a \wedge b}$  sont premiers entre eux.

Notons tout d'abord que  $\frac{a}{a \wedge b}$  et  $\frac{b}{a \wedge b}$  sont bien des entiers car  $a \wedge b$  divise  $a$  et  $b$  (et n'est pas nul).

D'après l'identité de Bézout, il existe  $(u, v) \in \mathbb{Z}^2$  tel que

$$au + bv = a \wedge b.$$

En divisant cette identité par  $a \wedge b \neq 0$ , on en déduit que

$$\frac{a}{a \wedge b}u + \frac{b}{a \wedge b}v = 1,$$

ce qui implique d'après le théorème de Bézout que  $\frac{a}{a \wedge b}$  et  $\frac{b}{a \wedge b}$  sont premiers entre eux.

**Exemple 8.** On a vu que  $60 \wedge 36 = 12$ . On a alors  $\frac{60}{12} = 5$ ,  $\frac{36}{12} = 3$  et  $5 \wedge 3 = 1$ .

### Corollaire 3: Lemme de Gauss

Soient  $(a, b, c) \in \mathbb{Z}^3$ .

Si  $a$  divise  $bc$  et  $a$  et  $b$  sont premiers entre eux, alors  $a$  divise  $c$ .

**Démonstration.** Puisque  $a$  et  $b$  sont premiers entre eux, d'après le théorème de Bézout, il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = 1$ . En multipliant cette identité de Bézout par  $c$ , on obtient  $acu + bcv = c$ .

Puisque  $a$  divise  $a$  et  $a$  divise  $bc$  par hypothèse, on en déduit que  $a$  divise  $acu + bcv = c$ , donc  $a$  divise  $c$ . ■

### Corollaire 4: Lemme d'Euclide

Soient  $(a, b, c) \in \mathbb{Z}^3$ .

Supposons que  $a$  et  $b$  divisent  $c$  et que  $a$  et  $b$  sont premiers entre eux.

Alors  $ab$  divise  $c$ .

**Démonstration.** Puisque  $a$  et  $b$  divisent  $c$ , il existe  $(k, l) \in \mathbb{Z}^2$  tels que  $c = ak = bl$ .

Puisque  $ak = bl$ , alors  $a$  divise  $bl$ . Or,  $a$  et  $b$  sont premiers entre eux donc d'après le lemme de Gauss, on en déduit que  $a$  divise  $l$ .

Ainsi, il existe  $u \in \mathbb{Z}$  tel que  $l = au$  d'où  $c = bl = abu$ , ce qui prouve que  $ab$  divise  $c$ . ■

**Exemple 9.** Puisque 3 et 5 divisent 30 et que 3 et 5 sont premiers entre eux, on déduit du lemme d'Euclide que  $3 \times 5 = 15$  divise 30.

En revanche, le résultat n'est plus forcément vrai si  $a$  et  $b$  ne sont pas premiers entre eux.

En effet, 2 divise 12, 4 divise 12 mais  $2 \times 4 = 8$  ne divise pas 12.

### Définition 4: PPCM de deux entiers relatifs

Soient  $(a, b) \in \mathbb{Z}^2$  deux entiers non nuls.

On appelle PPCM de  $a$  et  $b$ , noté  $\text{PPCM}(a, b)$  ou  $a \vee b$ , le plus petit multiple commun strictement positif à  $a$  et à  $b$ .

**Remarque 8.** • Autrement dit,  $a \vee b = \min\{n \in \mathbb{N}^*, a \text{ divise } n \text{ et } b \text{ divise } n\}$ .

L'ensemble  $\{n \in \mathbb{N}^*, a \text{ divise } n \text{ et } b \text{ divise } n\}$  est non vide car il contient  $|ab|$ . Il admet donc un plus petit élément puisque c'est une partie de  $\mathbb{N}$  non vide, ce qui justifie l'existence du PPCM de  $a$  et  $b$ .

• On peut définir pour tout  $a \in \mathbb{Z}$ ,  $\text{PPCM}(a, 0) = 0$ .

**Exemple 10.** • Pour tout  $(a, b) \in \mathbb{Z}^2$ ,  $a$  divise  $b$  si et seulement si  $a \vee b = |b|$ .

En particulier, pour tout  $a \in \mathbb{Z}^*$ ,  $a \vee a = |a|$ .

• Pour tout  $(a, b) \in (\mathbb{Z}^*)^2$ ,  $|ab|$  est un multiple commun strictement positif à  $a$  et à  $b$  donc par définition  $a \vee b \leq |ab|$ , l'inégalité pouvant être stricte.

En effet,  $3 \vee 9 = 9 < 3 \times 9$ .

En fait, on a même pour tout  $(a, b) \in \mathbb{Z}^2$ ,  $a \vee b \leq |ab|$ .

• Si  $(a, b) \in (\mathbb{Z}^*)^2$ , alors  $a \vee b \geq \max(|a|, |b|)$ .

•  $6 \vee 9 = 18$ .

### Proposition 3: Lien entre multiples communs et PPCM

Soient  $(a, b) \in \mathbb{Z}^2$ . Soit  $m$  un multiple commun à  $a$  et à  $b$ .

Alors  $a \vee b$  divise  $m$ .

Autrement dit, le PPCM de  $a$  et  $b$  divise tous les multiples communs à  $a$  et à  $b$ .

**Démonstration.** • Si  $a = 0$  ou  $b = 0$ , alors  $a \vee b = 0$  et tout multiple commun à  $a$  et à  $b$  est nécessairement nul, donc le résultat est vrai.

• Supposons que  $a \neq 0$  et  $b \neq 0$ .

On a nécessairement  $a \vee b > 0$ .

Effectuons la division euclidienne de  $m$  par  $a \vee b$ .

Il existe  $(q, r) \in \mathbb{Z}^2$  avec  $0 \leq r < a \vee b$  tel que  $m = (a \vee b)q + r$ , d'où  $r = m - (a \vee b)q$ .

Puisque  $a$  divise  $m$  et  $a$  divise  $a \vee b$ , alors  $a$  divise  $m - (a \vee b)q = r$ .

Par le même raisonnement, on montre que  $b$  divise  $r$ .

Ainsi,  $r$  est un multiple commun positif à  $a$  et à  $b$ .

Si on avait  $r > 0$ , ceci contredirait la minimalité de  $a \vee b$  parmi les multiples communs strictement positifs à  $a$  et à  $b$  donc  $r = 0$ .

Il en découle que  $m = (a \vee b)q$  donc  $a \vee b$  divise  $m$ . ■

**Remarque 9.** Ceci signifie que, si  $a$  et  $b$  sont non nuls,  $a \vee b$  est non seulement le plus petit multiple commun strictement positif à  $a$  et à  $b$ , mais également qu'il divise tous les multiples communs à  $a$  et à  $b$ .

**Exemple 11.** Tous les multiples communs à 6 et à 9 sont divisibles par  $6 \vee 9 = 18$ .

### Lemme 1

Soit  $(a, b) \in \mathbb{Z}^2$ . Soit  $k \in \mathbb{Z}$ .

On a

$$(ka) \vee (kb) = |k|(a \vee b).$$

Autrement dit,  $\text{PPCM}(ka, kb) = |k|\text{PPCM}(a, b)$ .

**Démonstration.** • Si  $k = 0$ , le résultat est évident.

• Supposons que  $k \neq 0$ .

On sait que  $a \vee b$  est un multiple commun à  $a$  et à  $b$  donc  $k(a \vee b)$  est un multiple commun à  $ka$  et à  $kb$ . D'après la proposition précédente, on en déduit que  $(ka) \vee (kb)$  divise  $k(a \vee b)$ .

Réciproquement, soit  $m = (ka) \vee (kb)$ . Alors  $m$  est un multiple commun à  $ka$  et à  $kb$  donc  $\frac{m}{k}$  est un multiple commun à  $a$  et à  $b$ . D'après la proposition précédente, on en déduit que  $(a \vee b)$  divise  $\frac{m}{k}$  donc  $k(a \vee b)$  divise  $m$ , i.e.  $k(a \vee b)$  divise  $(ka) \vee (kb)$ .

On a donc montré que  $k(a \vee b)$  divise  $(ka) \vee (kb)$  et que  $(ka) \vee (kb)$  divise  $k(a \vee b)$ .

On en conclut que  $|k(a \vee b)| = |(ka) \vee (kb)|$  d'où  $(ka) \vee (kb) = |k|(a \vee b)$ . ■

**Proposition 4: Lien entre PGCD et PPCM**

Soient  $(a, b) \in \mathbb{Z}^2 \neq (0, 0)$ .

Alors

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

Autrement dit,  $\text{PGCD}(a, b) \times \text{PPCM}(a, b) = |ab|$ .

**Démonstration.****•1er cas :  $a \wedge b = 1$** 

Montrons dans ce cas que  $a \vee b = |ab|$ .

Puisque  $ab$  est un multiple commun à  $a$  et à  $b$ , d'après la proposition précédente, on sait que  $a \vee b$  divise  $ab$ .

Réciproquement, puisque  $a$  et  $b$  divisent  $a \vee b$  et que  $a$  et  $b$  sont premiers entre eux, on déduit du lemme d'Euclide que  $ab$  divise  $a \vee b$ .

On a donc montré que  $a \vee b$  divise  $ab$  et que  $ab$  divise  $a \vee b$ , ce qui implique que

$$|ab| = |a \vee b| = a \vee b.$$

**•2ème cas : cas général**

On sait que  $\frac{a}{a \wedge b}$  et  $\frac{b}{a \wedge b}$  sont premiers entre eux.

D'après le lemme précédent et le premier cas, on en déduit que

$$a \vee b = \left( (a \wedge b) \times \frac{a}{a \wedge b} \right) \vee \left( (a \wedge b) \times \frac{b}{a \wedge b} \right) = (a \wedge b) \times \left( \frac{a}{a \wedge b} \vee \frac{b}{a \wedge b} \right) = (a \wedge b) \times \frac{|a|}{a \wedge b} \times \frac{|b|}{a \wedge b}$$

$$\text{d'où } |ab| = (a \wedge b) \times (a \vee b).$$

■

**Exemple 12.** On a bien  $(6 \wedge 9) \times (6 \vee 9) = 3 \times 18 = 54 = 9 \times 6$ .

**Corollaire 5**

Soient  $(a, b) \in \mathbb{Z}^2$  avec  $a \neq 0$  et  $b \neq 0$ .

Alors  $a \vee b = |ab|$  si et seulement si  $a \wedge b = 1$ .

Autrement dit,  $\text{PPCM}(a, b) = |ab|$  si et seulement si  $\text{PGCD}(a, b) = 1$ .

**Démonstration.** Si  $a$  et  $b$  sont premiers entre eux, on a montré dans la proposition précédente que  $|ab| = a \vee b$ .

Réciproquement, supposons que  $a \vee b = |ab|$ . D'après la proposition précédente, on sait que  $(a \wedge b) \times (a \vee b) = |ab|$  d'où  $(a \wedge b) \times |ab| = |ab|$ .

Puisque  $a \neq 0$  et  $b \neq 0$ , alors  $|ab| \neq 0$  donc on peut simplifier par  $|ab|$  et on obtient  $a \wedge b = 1$ . ■

## 10.2 Nombres premiers

### 10.2.1 Définition et premières propriétés

**Définition 5: Nombre premier**

Soit  $p$  un entier supérieur ou égal à 2.

On dit que  $p$  est un nombre premier s'il possède exactement deux diviseurs positifs : 1 et lui-même.

**Remarque 10.** • Il est important de noter qu'au vu de la définition, 1 **N'EST PAS** un nombre premier.

- Si un nombre  $n \geq 2$  n'est pas premier, alors il admet un diviseur strict  $d$  tel que  $1 < d < n$ .
- Soit  $p$  un nombre premier, soit  $n$  un entier relatif. Si  $p$  ne divise pas  $n$ , alors  $p$  et  $n$  sont premiers entre eux.

**Exemple 13.** • 2, 3, 5, 7, 11, 13, 17, 19... sont des nombres premiers.

- 1, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20... ne sont pas des nombres premiers.

#### Proposition 5

Soit  $n$  un entier naturel supérieur ou égal à 2.  
Alors  $n$  admet au moins un diviseur premier.

**Démonstration.** Soit  $d = \min\{k \geq 2, k \text{ divise } n\}$ . L'entier  $d$  existe bien car l'ensemble  $\{k \geq 2, k \text{ divise } n\}$  est une partie de  $\mathbb{N}$  non vide (puisqu'il contient  $n$ ).

Montrons que  $d$  est premier.

Supposons par l'absurde que  $d$  n'est pas premier. Alors il existe un entier  $d'$  tel que  $d'$  divise  $d$  et  $1 < d' < d$ .

Or, puisque  $d$  divise  $n$ , si  $d'$  divise  $d$ , alors  $d'$  divise  $n$ .

Ainsi,  $d'$  est un entier supérieur ou égal à 2 qui divise et qui vérifie  $d' < d$ , ce qui contredit la minimalité de  $d$  dans l'ensemble  $\{k \geq 2, k \text{ divise } n\}$ .

Il est donc nécessaire que  $d$  soit premier, ce qui prouve que  $d$  est un diviseur premier de  $n$ . ■

**Remarque 11.** Dans la preuve précédente, si  $n$  est premier, alors  $d = n$ .

**Exemple 14.** Les diviseurs supérieurs ou égaux à 2 de 63 sont  $\{3, 7, 9, 21, 63\}$ . On constate que le minimum de cet ensemble, qui est 3, est bien un nombre premier.

#### Proposition 6: Corollaire du lemme de Gauss

Soit  $p$  un nombre premier. Soient  $(a, b) \in \mathbb{Z}^2$  tels que  $p$  divise  $ab$ .  
Alors  $p$  divise  $a$  ou  $p$  divise  $b$ .

**Démonstration.** • Si  $p$  divise  $a$ , c'est terminé.

- Si  $p$  ne divise pas  $a$ , alors  $p$  est premier avec  $a$ . Puisque  $p$  divise  $ab$ , le lemme de Gauss implique alors que  $p$  divise  $b$ .

On en conclut donc que  $p$  divise  $a$  ou  $p$  divise  $b$ . ■

**Remarque 12.** • Ceci signifie que si un nombre premier divise un produit d'entiers, il divise nécessairement un des termes du produit.

- On a déjà vu que cette propriété n'est plus forcément vraie si  $p$  n'est pas premier : en effet, 6 divise  $3 \times 4$  mais ne divise ni 3 ni 4.

#### Proposition 7: Infinité de l'ensemble des nombres premiers

L'ensemble des nombres premiers est infini.

**Démonstration.** Soit  $\mathcal{P}$  l'ensemble des nombres premiers.

Supposons par l'absurde que  $\mathcal{P}$  est fini.

$$\text{Soit } N = \left( \prod_{p \in \mathcal{P}} p \right) + 1.$$

Puisque  $N \geq 2$ ,  $N$  admet un diviseur premier  $p_0 \in \mathcal{P}$ .

De plus, puisque  $p_0 \in \mathcal{P}$ ,  $p_0$  divise  $\prod_{p \in \mathcal{P}} p$ .

Ainsi,  $p_0$  divise  $N$  et  $\prod_{p \in \mathcal{P}} p$  donc  $p_0$  divise  $N - \prod_{p \in \mathcal{P}} p = 1$ , ce qui est absurde pour un nombre premier !

On en conclut que  $\mathcal{P}$  est infini. ■

## 10.2.2 Décomposition en produit de nombres premiers

### Théorème 3: Existence et unicité de la décomposition en produit de nombres premiers

Soit  $n$  un entier naturel supérieur ou égal à 2.

Il existe un entier  $r \in \mathbb{N}^*$ , des nombres premiers  $p_1, \dots, p_r$  distincts deux à deux et des entiers naturels non nuls  $\alpha_1, \dots, \alpha_r$  tels que

$$n = \prod_{k=1}^r p_k^{\alpha_k}.$$

De plus, cette décomposition est unique à l'ordre près des facteurs.

#### Démonstration.

##### ▷ Existence

Montrons l'existence de cette décomposition par récurrence forte sur  $n \geq 2$ .

• **Initialisation** : Soit  $n = 2$ . En prenant  $p_1 = 2$  et  $\alpha_1 = 1$ , on a bien  $n = 2 = p_1^{\alpha_1}$ .

• **Hérédité** : Soit  $n \geq 2$  fixé. On suppose prouvée l'existence d'une telle décomposition pour tous les entiers  $k \in [2, n]$ . Montrons que  $n + 1$  admet également une telle décomposition.

Si  $n + 1$  est premier, en prenant  $p_1 = n + 1$  et  $\alpha_1 = 1$ , on a bien  $n + 1 = p_1^{\alpha_1}$ .

Supposons dorénavant que  $n + 1$  n'est pas premier. Alors  $n + 1$  admet un diviseur premier  $p \in [2, n]$ . Ainsi  $\frac{n+1}{p} \in [2, n]$ .

Par hypothèse de récurrence forte, on sait qu'il existe un entier  $r \in \mathbb{N}^*$ , des nombres premiers  $p_1, \dots, p_r$  distincts deux à deux et des entiers naturels non nuls  $\alpha_1, \dots, \alpha_r$  tels que

$$\frac{n+1}{p} = \prod_{k=1}^r p_k^{\alpha_k},$$

d'où  $n + 1 = p \prod_{k=1}^r p_k^{\alpha_k}$ .

Si  $p \notin \{p_1, \dots, p_r\}$ , on pose  $p_{r+1} = p$ ,  $\alpha_{r+1} = 1$  et on a  $n + 1 = \prod_{k=1}^{r+1} p_k^{\alpha_k}$ .

S'il existe  $i \in [1, r]$  tel que  $p = p_i$ , on pose  $\alpha'_i = \alpha_i + 1$ , pour tout  $k \in [1, r] \setminus \{i\}$ ,  $\alpha'_k = \alpha_k$  et on obtient  $n + 1 = \prod_{k=1}^r p_k^{\alpha'_k}$ .

Dans tous les cas, on a prouvé la propriété au rang  $n + 1$ , ce qui achève la récurrence et prouve l'existence d'une telle décomposition pour tous les entiers supérieurs ou égaux à 2.

##### ▷ Unicité

Soit  $n \geq 2$ . Supposons que  $n$  admette deux décompositions

$$n = \prod_{k=1}^r p_k^{\alpha_k} = \prod_{i=1}^{r'} p_i^{\alpha'_i}$$

où  $(r, r') \in (\mathbb{N}^*)^2$ ,  $p_1, \dots, p_r$  sont des nombres premiers deux à deux distincts, idem pour  $p'_1, \dots, p'_{r'}$ , et où  $\alpha_1, \dots, \alpha_r, \alpha'_1, \dots, \alpha'_{r'}$  sont des entiers naturels non nuls.

Soit  $k \in \llbracket 1, r \rrbracket$ .

Alors  $p_k$  divise  $\prod_{i=1}^{r'} p_i^{\alpha'_i}$ . D'après le corollaire du lemme de Gauss, il existe nécessairement un indice  $i \in \llbracket 1, r' \rrbracket$  tel que  $p_k$  divise  $p_i^{\alpha'_i}$ , ce qui implique que  $p_k = p'_i$ . Ainsi, tous les nombres premiers  $p_1, \dots, p_r$  apparaissent dans la décomposition  $\prod_{i=1}^{r'} p_i^{\alpha'_i}$ .

Réciproquement, le même raisonnement montre que tous les nombres premiers  $p'_1, \dots, p'_{r'}$  apparaissent dans la décomposition  $\prod_{k=1}^r p_k^{\alpha_k}$ .

On en déduit que  $r = r'$  et quitte à renuméroter les  $p_k$  et les  $p'_i$ , on peut supposer que pour tout  $k \in \llbracket 1, r \rrbracket$ ,  $p_k = p'_k$ .

A ce stade, on a donc les deux décompositions suivantes :

$$n = \prod_{k=1}^r p_k^{\alpha_k} = \prod_{k=1}^r p_k^{\alpha'_k}.$$

Il reste à montrer que pour tout  $k \in \llbracket 1, r \rrbracket$ ,  $\alpha_k = \alpha'_k$ .

Soit  $k \in \llbracket 1, r \rrbracket$ . On sait que  $p_k^{\alpha_k}$  divise  $\prod_{i=1}^r p_i^{\alpha'_i}$ . En appliquant de nouveau le lemme de Gauss, puisque  $p_k^{\alpha_k}$  est premier avec  $\prod_{\substack{i=1 \\ i \neq k}}^r p_i^{\alpha'_i}$ , on en déduit que  $p_k^{\alpha_k}$  divise  $p_k^{\alpha'_k}$ , ce qui implique que  $\alpha_k \leq \alpha'_k$ .

En faisant le même raisonnement à partir de  $p_k^{\alpha'_k}$ , on en déduit que  $\alpha'_k \leq \alpha_k$  et donc finalement que  $\alpha_k = \alpha'_k$ .

On a donc bien montré que la décomposition est unique, à l'ordre près des facteurs. ■

**Exemple 15.** La décomposition en facteurs premiers de 756 est  $756 = 2^2 \times 3^3 \times 7$ .

### Définition 6: Valuation $p$ -adique

Soit  $n$  un entier supérieur ou égal à 2. Soit  $p$  un nombre premier. On appelle valuation  $p$ -adique de  $n$ , notée  $v_p(n)$ , l'entier naturel

$$v_p(n) = \max\{k \in \mathbb{N}, p^k \text{ divise } n\}.$$

Autrement dit,  $v_p(n)$  est la puissance de  $p$  qui apparaît dans la décomposition en facteurs premiers de  $n$ .

**Remarque 13.** • Si  $p$  ne divise pas  $n$ , alors  $v_p(n) = 0$ .

• Soient  $p_1, \dots, p_r$  les nombres premiers deux à deux distincts qui divisent  $n$ .

$$\text{Alors } n = \prod_{i=1}^r p_i^{v_{p_i}(n)}.$$

**Exemple 16.**  $v_2(756) = 2$ ,  $v_3(756) = 3$ ,  $v_5(756) = 0$ ,  $v_7(756) = 1$ .

**Proposition 8: Nombre de diviseurs positifs**

Soit  $n$  un entier supérieur ou égal à 2. Soit  $r \in \mathbb{N}^*$ , et  $p_1, \dots, p_r$  des nombres premiers deux à deux distincts tels que

$$n = \prod_{i=1}^r p_i^{v_{p_i}(n)}.$$

L'ensemble des diviseurs de  $n$  est alors

$$\left\{ \prod_{i=1}^r p_i^{\alpha_i}, \forall 1 \leq i \leq r, \alpha_i \in \llbracket 0, v_{p_i}(n) \rrbracket \right\}.$$

En particulier,  $n$  admet  $\prod_{i=1}^r (v_{p_i}(n) + 1)$  diviseurs positifs.

**Démonstration.** Soit  $d$  un diviseur de  $n$  supérieur ou égal à 2. Soit  $p$  un diviseur premier de  $d$ . Alors  $p$  est un diviseur premier de  $n$  donc  $p$  appartient à l'ensemble  $\{p_1, \dots, p_r\}$ .

Ainsi, l'ensemble des facteurs premiers de  $d$  est inclus dans  $\{p_1, \dots, p_r\}$  donc  $d = \prod_{i=1}^r p_i^{v_{p_i}(d)}$ , avec éventuellement  $v_{p_i}(d) = 0$  si  $p_i$  ne divise pas  $d$ .

Par ailleurs, puisque  $d$  divise  $n$ , on a forcément pour tout  $i \in \llbracket 1, r \rrbracket$ ,  $v_{p_i}(d) \leq v_{p_i}(n)$ .

Réciproquement, tout nombre de la forme indiquée est bien un diviseur de  $n$ . ■

**Remarque 14.** Si pour tout  $i \in \llbracket 1, r \rrbracket$ ,  $\alpha_i = 0$ , on retrouve 1 comme diviseur positif de  $n$ .

**Exemple 17.**  $60 = 2^2 \times 3 \times 5$ . 60 admet donc  $(2+1) \times (1+1) \times (1+1) = 12$  diviseurs positifs que sont  $\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$

**Proposition 9: Décomposition en facteurs premiers du PGCD et du PPCM de deux entiers naturels**

Soient  $a$  et  $b$  deux entiers naturels supérieurs ou égaux à deux.

Soit  $\{p_1, \dots, p_r\}$ , avec  $r \in \mathbb{N}^*$ , l'ensemble des nombres premiers qui divisent  $a$  ou  $b$  (mais pas nécessairement les deux).

Notons  $a = \prod_{i=1}^r p_i^{v_{p_i}(a)}$  et  $b = \prod_{i=1}^r p_i^{v_{p_i}(b)}$ , avec ici éventuellement  $v_{p_i}(a) = 0$  ou  $v_{p_i}(b) = 0$ .

Alors

$$\text{PGCD}(a, b) = \prod_{i=1}^r p_i^{\min(v_{p_i}(a), v_{p_i}(b))} \quad \text{et} \quad \text{PPCM}(a, b) = \prod_{i=1}^r p_i^{\max(v_{p_i}(a), v_{p_i}(b))}.$$

**Démonstration.** • Puisque pour tout  $i \in \llbracket 1, r \rrbracket$ ,  $\min(v_{p_i}(a), v_{p_i}(b)) \leq v_{p_i}(a)$  et  $\min(v_{p_i}(a), v_{p_i}(b)) \leq v_{p_i}(b)$ , il est clair que  $\prod_{i=1}^r p_i^{\min(v_{p_i}(a), v_{p_i}(b))}$  divise  $a$  et  $b$ , donc divise  $\text{PGCD}(a, b)$ .

Réciproquement, soit  $d$  un diviseur positif commun à  $a$  et à  $b$ . D'après la proposition précédente, on a nécessairement  $d = \prod_{i=1}^r p_i^{v_{p_i}(d)}$ , où pour tout  $i \in \llbracket 1, r \rrbracket$ ,  $v_{p_i}(d) \leq v_{p_i}(a)$  et

$v_{p_i}(d) \leq v_{p_i}(b)$  donc  $v_{p_i}(d) \leq \min(v_{p_i}(a), v_{p_i}(b))$ . Il en découle que  $d$  divise  $\prod_{i=1}^r p_i^{\min(v_{p_i}(a), v_{p_i}(b))}$ .

Ainsi,  $\prod_{i=1}^r p_i^{\min(v_{p_i}(a), v_{p_i}(b))}$  est un diviseur commun à  $a$  et à  $b$  et est divisible par tous les

diviseurs communs à  $a$  et à  $b$  : c'est donc le PGCD de  $a$  et  $b$ .

• Puisque pour tout  $i \in \llbracket 1, r \rrbracket$ ,  $\max(v_{p_i}(a), v_{p_i}(b)) \geq v_{p_i}(a)$  et  $\max(v_{p_i}(a), v_{p_i}(b)) \geq v_{p_i}(b)$ , il est clair que  $\prod_{i=1}^r p_i^{\max(v_{p_i}(a), v_{p_i}(b))}$  est un multiple commun à  $a$  et  $b$ , donc est un multiple de  $\text{PPCM}(a, b)$ .

Réciproquement, soit  $m$  un multiple positif commun à  $a$  et à  $b$ . D'après la proposition précédente, on a nécessairement  $m = \prod_{i=1}^r p_i^{v_{p_i}(d)}$ , où pour tout  $i \in \llbracket 1, n \rrbracket$ ,  $v_{p_i}(d) \geq v_{p_i}(a)$  et  $v_{p_i}(d) \geq v_{p_i}(b)$  donc  $v_{p_i}(d) \geq \max(v_{p_i}(a), v_{p_i}(b))$ . Il en découle que  $m$  est un multiple de  $\prod_{i=1}^r p_i^{\max(v_{p_i}(a), v_{p_i}(b))}$ .

Ainsi,  $\prod_{i=1}^r p_i^{\max(v_{p_i}(a), v_{p_i}(b))}$  est un multiple commun à  $a$  et à  $b$  et divise tous les diviseurs communs à  $a$  et à  $b$  : c'est donc le PPCM de  $a$  et  $b$ . ■

**Remarque 15.** On retrouve bien  $\text{PGCD}(a, b) \times \text{PPCM}(a, b) = ab$ .

**Exemple 18.** On a  $60 = 2^2 \times 3 \times 5$  et  $126 = 2 \times 3^2 \times 7$ .

Ainsi,  $\text{PGCD}(60, 126) = 2 \times 3 = 6$  et  $\text{PPCM}(60, 126) = 2^2 \times 3^2 \times 5 \times 7 = 1260$ .