# Chapitre B4
# Arithmétique

## I. Entiers

### A. Ensembles d'entiers

**Définition.** L'ensemble des entiers naturels est :

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

Il vérifie les propriétés :

- $\mathbb{N}$ possède un plus petit élément.
- Tout élément de $\mathbb{N}$ possède un et un seul successeur.

**Propositions.**

*(i) Toute partie non-vide de* $\mathbb{N}$ *possède un plus petit élément.*

*(ii) Toute partie non-vide de* $\mathbb{N}$ *majorée possède un plus grand élément.*

*(iii) Soit* $m$ *et* $n$ *deux entiers naturels. Si* $m > n$ *alors* $m \geqslant n + 1$.

**Définition.** L'ensemble des entiers relatifs ou plus simplement des entiers est :

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

### B. Divisibilité

**Définition.** Soit $a$ et $b$ deux entiers. On dit que $b$ est un diviseur de $a$ ou que $a$ est un multiple de $b$ s'il existe un entier $k$ tel que $a = bk$. On note $b \mid a$.

**Remarques.**

*(i)* La relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre non totale.

*(ii)* Par contre la relation de divisibilité sur $\mathbb{Z}$ n'est pas une relation d'ordre.

*(iii)* Les entiers 1 et $-1$ sont diviseurs de tous les entiers, 0 est multiple de tous les entiers.

*(iv)* On remarque que :

$$b \mid a \iff -b \mid a \iff -b \mid -a \iff b \mid -a$$

On pourra donc souvent se ramener au cas des entiers naturels.

*(v)* L'ensemble des multiples de $b$ est noté $b\mathbb{Z}$ : $b\mathbb{Z} = \{bn \mid n \in \mathbb{Z}\}$.

**Proposition.** *Soit $a$, $b$, $c$ trois entiers. Si $c$ divise $a$ et $b$ alors pour tout couple d'entiers $(u, v)$, $c$ divise $au + bv$.*

Démonstration.

**Notation.** Pour tout entier $n$ on note $\mathcal{D}(n)$ l'ensemble des diviseurs de $n$ dans $\mathbb{Z}$.

**Exemples.**

$\mathcal{D}(7) =$ $\mathcal{D}(6) =$ $\mathcal{D}(0) =$

**Remarques.**

*(i)* L'ensemble $\mathcal{D}(n)$ est non-vide car il contient au moins 1.

*(ii)* Si $n$ est non nul alors il est borné par $-|n|$ et $|n|$.

*(iii)* Par contre $\mathcal{D}(0)$ n'est pas borné.

**Théorème (Division euclidienne).** (Euclide, vers –300 av J. C.) *Soit $a$ un entier* relatif *et $b$ un entier* naturel non-nul*. Alors il existe un unique couple d'entiers $(q, r)$ tel que :*

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

**Exemples.**

*(i)* La division euclidienne de 43 par 5 est : $43 = 8 \times 5 + 3$

Le quotient de la division euclidienne de 43 par 5 est 8 et le reste est 3.

*(ii)* Cette propriété est moins intuitive dans $\mathbb{Z}$, c'est-à-dire si $a$ est négatif. Par exemple la division euclidienne de $-43$ par 5 est : $-43 = (-9) \times 5 + 2$

Le quotient de la division euclidienne de $-43$ par 5 est $-9$ et le reste est 2. Il vérifie bien $0 \leqslant 2 < 5$.

**Remarque.** En Python on obtient le quotient et le reste de la division euclidienne par :

Démonstration de l'unicité.

Démonstration de l'existence si $a \geqslant 0$.

Démonstration de l'existence si $a < 0$ et conclusion.

Soit $a$ un entier strictement négatif, et $b$ un entier strictement positif.

Alors $a + b|a|$ est positif. En effet $b \geqslant 1$ donc $b|a| \geqslant |a| \geqslant -a$.

On applique alors le théorème de la division euclidienne dans $\mathbb{N}$. L'entier $a+b|a|$ est positif, $b$ est strictement positif, donc il existe deux entiers $q_1$ et $r$ tels que $a + b|a| = bq_1 + r$ et $0 \leqslant r < b$.

En posant $q = q_1 - |a|$ on obtient un couple d'entier $(q, r)$ tel que $a = bq + r$ et $0 \leqslant r < b$.

Finalement nous avons démontré que :

- Pour tout couple $(a, b) \in \mathbb{Z}\times\mathbb{N}^*$ il existe un couple d'entiers $(r, q) \in \mathbb{Z}^2$ tel que $a = bq+r$ et $0 \leqslant r < b$.
- Ce couple est unique.

Le théorème est donc démontré. □

▷ **Exercices 1, 2.**

# II. PGCD et PPCM

## A. PGCD

**Définition.** Soit $a$ et $b$ deux entiers naturels non tous les deux nuls.
Le PGCD de $a$ et de $b$ est leur plus grand commun diviseur. Il est noté $a \wedge b$.

**Remarque.** Soit $D$ l'ensemble de tous les diviseurs communs de $a$ et $b$ dans $\mathbb{N}$ :

$$D = \{n \in \mathbb{N} \mid \ n \mid a \quad \text{et} \quad n \mid b\} = \mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathbb{N}$$

Cet ensemble est une partie de $\mathbb{N}$, non-vide car elle contient 1, et majorée par $a$ et $b$ s'ils sont non-nuls.
Il admet donc un maximum que l'on appelle PGCD de $a$ et $b$.
On peut donc définir le PGCD par :

.

**Exemples.**

| | | |
|---|---|---|
| $5 \wedge 7 =$ | $6 \wedge 7 =$ | $6 \wedge 8 =$ |
| $10 \wedge 25 =$ | $28 \wedge 14 =$ | $7 \wedge 100 =$ |
| $10 \wedge 77 =$ | $42 \wedge 150 =$ | $120 \wedge 0 =$ |

**Lemme.** *Soit $a$ et $b$ deux entiers, avec $b$ strictement positif. Alors :*
*(i) Soit $r$ le reste de la division euclidienne de $a$ par $b$. Alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$.*
*(ii) $a \wedge b = b \wedge r$*

Démonstration.

*(i)* On démontre que pour tout entier $n$ : $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(a - nb)$.
On fixe $n \in \mathbb{Z}$. Soit $c$ un entier.
Si $c$ divise $a$ et $b$ alors $c$ divise $b$ et $a - nb$. Donc $\mathcal{D}(a) \cap \mathcal{D}(b) \subseteq \mathcal{D}(b) \cap \mathcal{D}(a - nb)$.
Si $c$ divise $b$ et $a - nb$ alors $c$ divise $b$ et $(a - nb) + nb = a$.
Donc $\mathcal{D}(b) \cap \mathcal{D}(a - nb) \subseteq \mathcal{D}(a) \cap \mathcal{D}(b)$.
Par double inclusion $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(a - nb)$.
Cette égalité est vraie pour tout $n \in \mathbb{Z}$. Elle est donc vraie pour le quotient de la division euclidienne de $a$ par $b$, que l'on note $q$.
Comme $r = a - bq$ alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$.

*(ii)* Le PGCD de $a$ et $b$ est le maximum de $\mathcal{D}(a) \cap \mathcal{D}(r)$, donc :

$$a \wedge b = \text{Max}\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right) = \text{Max}\left(\mathcal{D}(b) \cap \mathcal{D}(r)\right) = b \wedge r \qquad \square$$

**Méthode (Algorithme d'Euclide).** Calcul du PGCD de deux entiers positifs $a$ et $b$.

On calcule $r$, le reste de la division euclidienne de $a$ par $b$. Puis on calcule le reste de la division euclidienne de $b$ par $r$, et on continue jusqu'à ce que le reste soit nul. Le reste précédent est alors le PGCD de $a$ et $b$.

Plus précisément, on pose $r_0 = a$, $r_1 = b$. Ensuite, par double récurrence, en supposant $r_k$ et $r_{k+1}$ connus, on note $r_{k+2}$ le reste de la division euclidienne de $r_k$ par $r_{k+1}$.

Le PGCD de $a$ et $b$ est alors le dernier $r_k$ non-nul.

**Exemple 1.** PGCD de 150 et 66.

▷ **Exercice 3.**

Démonstration. On construit par double-récurrence une suite $(r_k)_{k\in\mathbb{N}}$ d'entiers naturels de la façon suivante.

Soit $r_0 = a$ et $r_1 = b$. Pour tout $k \in \mathbb{N}^*$ on note $r_{k+1}$ le reste de la division euclidienne de $r_{k-1}$ par $r_k$. On note également $q_k$ le quotient de cette division, si bien que :

$$r_{k-1} = r_k q_k + r_{k+1} \qquad \text{et} \qquad 0 \leqslant r_{k+1} < r_k$$

Cette définition de $r_{k+1}$ est valable si $r_k$ est non-nul. Si $r_k$ est nul alors on arrête la construction de la suite : $r_k = 0$ est son dernier élément.

La dernière inégalité montre que la suite $(r_k)$ est strictement décroissante (au moins à partir du rang 1). Comme c'est une suite d'entiers naturels alors elle aboutit forcément à 0 : Il existe un entier $k_0$ tel que $r_{k_0}$ est nul.

Soit $n = k_0 - 1$. Alors $r_n$ est non-nul et $r_{n+1}$ est nul. L'algorithme renvoie $r_n$, démontrons qu'il s'agit bien du PGCD de $a$ et $b$.

Pour tout $k = 1, \dots, n$, comme $r_{k+1}$ est le reste de la division euclidienne de $r_{k-1}$ par $r_k$ alors d'après le point *(iii)* du lemme ci-dessus :

$$r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$$

La suite $(r_{k-1} \wedge r_k)_{1 \leqslant k \leqslant n+1}$ est constante. En particulier pour $k = 1$ et $k = n + 1$ on obtient :

$$a \wedge b = r_0 \wedge r_1 = r_n \wedge r_{n+1} = r_n \wedge 0 = r_n$$

Ainsi $r_n$ est le PGCD de $a$ et $b$, et l'algorithme renvoie bien le PGCD de $a$ et $b$. □

**Remarque.** On a démontré que l'algorithme est *fini* et *correct*.

**Proposition.** *Soit $a$ et $b$ deux entiers. Alors :*

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$$

Démonstration. On reprend la démonstration précédente. En utilisant le point *(ii)* du lemme on obtient :

$$\begin{aligned}\mathcal{D}(a) \cap \mathcal{D}(b) &= \mathcal{D}(r_0) \cap \mathcal{D}(r_1) = \mathcal{D}(r_1) \cap \mathcal{D}(r_2) = \cdots \\ &= \mathcal{D}(r_n) \cap \mathcal{D}(r_{n+1}) = \mathcal{D}(a \wedge b) \cap \mathcal{D}(0) = \mathcal{D}(a \wedge b)\end{aligned}$$

Ceci car $\mathcal{D}(0) = \mathbb{Z}$. □

**Corollaire.** *Soit $n$ un entier. Si $n$ divise $a$ et $b$ alors $n$ divise leur PGCD.*

**Remarque.** Par définition le PGCD de $a$ et $b$ est le plus grand diviseur commun de $a$ et de $b$ au sens de la relation d'ordre $\leqslant$.

Ce corollaire montre que c'est aussi le plus grand diviseur commun de $a$ et $b$ au sens de la relation d'ordre de divisibilité : Si $n$ divise $a$ et $b$ alors $n$ divise $a \wedge b$.

**Définition.** On pose : $0 \wedge 0 = 0$

**Définition (cas des entiers négatifs).** Soit $a$ et $b$ deux entiers relatifs non tous les deux nuls. Le PGCD de $a$ et $b$ est leur plus grand commun diviseur.

**Remarque.** Soit $a$ un entier relatif. Alors un entier divise $a$ si et seulement si il divise $-a$. Donc $\mathcal{D}(a) = \mathcal{D}(-a)$.

On en déduit que pour tout couple d'entiers relatifs $(a, b)$ : $a \wedge b = |a| \wedge |b|$

En conséquence on peut appliquer l'algorithme d'Euclide au couple $(|a|, |b|)$ pour calculer le PGCD de $a$ et $b$.

On remarque que $a \wedge b$ est toujours positif, même si $a$ ou $b$ est négatif.

## B. Relation de Bézout

**Théorème.** *Soit $a$ et $b$ deux entiers relatifs non tous les deux nuls. Alors il existe un couple $(u, v)$ d'entiers relatifs tels que :*

**Définition.** Les entiers $u$ et $v$ sont appelés coefficients de Bézout du couple $(a, b)$.

**Remarque.** Si $a$ et $b$ sont de même signe, en général $u$ et $v$ sont de signes opposés.

Démonstration. On démontre le théorème en supposant $a$ et $b$ positifs.

Le cas où $a$ ou $b$ est négatif s'en déduit. Par exemple si $a$ est négatif alors on applique le théorème à $-a$ et $b$, puis on remplace $u$ par $-u$ et donc le théorème est valable.

Supposons donc que $a$ et $b$ sont positifs.

On a construit dans la démonstration de l'algorithme d'Euclide une suite d'entiers naturels $(r_0, \dots, r_{n+1})$ telle que $r_0 = a$, $r_1 = b$, $r_n = a \wedge b$, $r_{n+1} = 0$, et pour tout $k = 1, \dots, n$ : $r_{k+1}$ est le reste de la division euclidienne de $r_{k-1}$ par $r_k$, *i.e.,* il existe un entier $q_k$ tel que :

$$r_{k-1} = q_k r_k + r_{k+1} \qquad \text{et} \qquad 0 \leqslant r_{k+1} < r_k$$

On démontre par récurrence double finie que pour tout $k = 0, \dots, n+1$ il existe deux entiers relatifs $u_k$ et $v_k$ tels que :

$$au_k + bv_k = r_k$$

Initialisation. Pour $k = 0$, comme $r_0 = a$ alors il suffit de poser $u_k = 1$ et $v_k = 0$.

Pour $k = 1$, comme $r_1 = b$ alors il suffit de poser $u_k = 0$ et $v_k = 1$.

Hérédité. Supposons que pour un entier $k \in \{1, \dots, n\}$ il existe deux entiers $u_{k-1}$ et $v_{k-1}$ tels que $au_{k-1} + bv_{k-1} = r_{k-1}$ et deux entiers $u_k$ et $v_k$ tels que $au_k + bv_k = r_k$. Alors :

$$\begin{cases} au_{k-1} + bv_{k-1} = r_{k-1} \\ au_k \quad + bv_k \quad = r_k \end{cases} \qquad \text{et} \qquad r_{k-1} - q_k r_k = r_{k+1}$$

L'opération élémentaire $L_1 - q_k L_2$ sur les lignes du système donne :

$$a(u_{k-1} - q_k u_k) + b(v_{k-1} - q_k v_k) = r_{k+1}$$

On pose $u_{k+1} = u_{k-1} - q_k u_k$, $v_{k+1} = v_{k-1} - q_k v_k$. Alors $u_{k+1}$ et $v_{k+1}$ sont des entiers et :

$$au_{k+1} + bv_{k+1} = r_{k+1}$$

Ceci montre que la propriété est vraie au rang $k+1$.

Son hérédité est établie.

Conclusion. Par récurrence double finie, pour tout $k = 0, \dots, n+1$ il existe deux entiers $u_k$ et $v_k$ tels que $au_k + bv_k = r_k$.

Cette propriété est en particulier vraie pour $k = n$, ce qui démontre le théorème. □

**Remarque.** L'algorithme d'Euclide permet d'obtenir des coefficients de Bézout.

**Exemple 1 (suite).** Déterminons des coefficients de Bézout pour $(a, b) = (150, 66)$.

▷ **Exercice 4.**

**Remarque.** La démonstration du théorème de Bézout montre même comment obtenir récursivement les coefficients $u$ et $v$. On calcule :

$$\begin{array}{llll} u_0 = 1 & u_1 = 0 & \text{et} & \forall k = 1, \dots, n \quad u_{k+1} = u_{k-1} - q_k u_k \\ v_0 = 0 & v_1 = 1 & \text{et} & \forall k = 1, \dots, n \quad v_{k+1} = v_{k-1} - q_k v_k \end{array}$$

où les $q_k$ sont les quotients de la division euclidienne de $r_{k-1}$ par $r_k$.

On pose alors $u = u_n$ et $v = v_n$.

## C. PPCM

**Définition.** Soit $a$ et $b$ deux entiers naturels non-nuls.

Le PPCM de $a$ et de $b$ est leur plus petit commun multiple strictement positif.

On note $a \vee b$ cet entier.

Si $a$ ou $b$ est négatif alors on définit : $a \vee b = |a| \vee |b|$. Il s'agit du plus petit commun multiple positif de $a$ et $b$.

**Remarque.** Soit $M$ l'ensemble de tous les multiples communs strictement positifs de $a$ et $b$ :

$$M = \{ n \in \mathbb{N}^* \mid a \mid n \quad \text{et} \quad b \mid n \}$$

Cet ensemble est une partie de $\mathbb{N}$, non-vide car il contient l'entier $ab$. Il admet donc un minimum, que l'on appelle PPCM de $a$ et $b$. Ceci s'écrit :

$$a \vee b = \text{Min}\,(|a|\mathbb{N}^* \cap |b|\mathbb{N}^*)$$

**Exemples.**

$5 \vee 7 =$ $\quad$ $6 \vee 7 =$ $\quad$ $6 \vee 8 =$

$10 \vee 25 =$ $\quad$ $28 \vee 14 =$ $\quad$ $7 \vee 100 =$

$10 \vee 77 =$ $\quad$ $42 \vee 150 =$ $\quad$ $120 \vee 1 =$

**Remarque.** Le PPCM est utilisé pour calculer des fractions :

$$\frac{1}{6} + \frac{7}{8} =$$

**Proposition.** *Soit $n$ un entier. Si $n$ est un multiple de $a$ et de $b$ alors $n$ est un multiple de leur PPCM.*

**Remarque.** Par définition le PPCM de $a$ et $b$ est le plus petit multiple commun de $a$ et de $b$ au sens de la relation d'ordre $\leqslant$.

Cette proposition montre que c'est aussi le plus petit multiple commun de $a$ et $b$ au sens de la relation d'ordre de divisibilité : Si $a$ et $b$ divisent $n$ alors $a \vee b$ divise $n$.

Démonstration.

▷ **Exercice 5.**

### D. Entiers premiers entre eux

**Définition.** Deux entiers $a$ et $b$ sont premiers entre eux si leur PGCD est égal à 1 : $a \wedge b = 1$.

**Théorème de Bézout.** *Deux entiers $a$ et $b$ sont premiers entre eux si et seulement s'il existe deux entiers $u$ et $v$ tels que :*

$$au + bv = 1$$

Démonstration.

**Remarque.** Des entiers $a$ et $b$ sont premiers entre eux si et seulement s'ils n'ont aucun diviseur commun autre que 1 et $-1$.

▷ **Exercice 6.**

**Lemme (réduction des rationnels).** *Soit $a$ et $b$ deux entiers non tous deux nuls. Soit $d$ leur pgcd, soit $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$. Alors $a'$ et $b'$ sont premiers entre eux, et $\frac{a}{b} = \frac{a'}{b'}$.*

Démonstration. Comme $a$ et $b$ ne sont pas tous les deux nuls alors $d$ est non-nul.

Comme $d = a \wedge b$ alors $d$ divise $a$ et $b$ donc $a'$ et $b'$ sont des entiers. De plus $a = a'd$ et $b = b'd$.

D'après la relation de Bézout il existe deux entiers $u$ et $v$ tels que $au + bv = d$. Ceci donne $a'du + b'dv = d$, donc comme $d$ est non-nul : $a'u + b'v = 1$.

D'après le théorème de Bézout $a'$ et $b'$ sont premiers entre eux. □

**Remarque.** Le rationnel $\frac{a}{b}$ est ainsi exprimé sous forme irréductible $\frac{a'}{b'}$.

**Exemple.** Soit $a = 150$ et $b = 42$.

Alors $d =$ $a' =$ $b' =$

**Théorème (Lemme de Gauss).**

*Soit $a$, $b$, $c$ trois entiers. Si $a$ divise le produit $bc$ et $a$ est premier avec $b$ alors $a$ divise $c$.*

Démonstration.

**Proposition.** *Soit $a$ et $b$ deux entiers naturels non-nuls.*

*(i) Si $a$ et $b$ sont premiers entre eux alors leur PPCM est leur produit : $a \vee b = ab$.*

*(ii) Dans tous les cas : $ab = (a \wedge b)(a \vee b)$.*

**Exemple.**

*(i)* Les entiers 5 et 7 sont premiers entre eux, leur PPCM est 35.

*(ii)* Si $a = 6$ et $b = 8$ alors $a \wedge b = 2$ et $a \vee b = 24$, on a bien $6 \times 8 = 2 \times 24$.

**Remarque.** Grâce à la dernière formule on peut calculer le PPCM de deux entiers si on connaît leur PGCD. Celui-ci peut être obtenu grâce à l'algorithme d'Euclide.

Démonstration.

*(i)* Supposons que $a$ et $b$ sont premiers entre eux. Soit $m$ le PPCM de $a$ et $b$.
Comme $m$ est un multiple de $a$ alors il existe un entier $k$ tel que $m = ka$. Comme $b$ divise $m$ alors $b$ divise $ka$. Or $b$ est premier avec $a$, donc d'après le lemme de Gauss $b$ divise $k$. Par produit $ab$ divise $ak = m$.
Ainsi $ab$ divise $a \vee b$, et on sait que $a \vee b$ divise $ab$, donc par antisymétrie $ab = a \vee b$.

*(ii)* Soit $d$ le PGCD de $a$ et $b$.
D'après le lemme de réduction des rationnels il existe deux entiers $a'$ et $b'$ premiers entre eux tels que $a = a'd$ et $b = b'd$.
Le PPCM de $a$ et $b$ est alors : $(a'd) \vee (b'd) = d(a' \vee b')$. En effet :

$$a \vee b = \operatorname{Min}(a\mathbb{N}^* \cap b\mathbb{N}^*) = \operatorname{Min}(d(a'\mathbb{N}^* \cap b'\mathbb{N}^*)) = d \operatorname{Min}(a'\mathbb{N}^* \cap b'\mathbb{N}^*) = d(a' \vee b')$$

Comme $a'$ et $b'$ sont premiers entre eux alors d'après le point *(i)* leur PPCM est $a'b'$, et donc le PPCM de $a$ et $b$ est $a'b'd$.
Finalement $a \wedge b = d$ et $a \vee b = a'b'd$, donc $(a \wedge b)(a \vee b) = a'b'd^2 = (a'd)(b'd) = ab$.
Le résultat est démontré. □

**Exemple 2 (complément sur la relation de Bézout).** *Soit $a$ et $b$ deux entiers non-nuls premiers entre eux. Quels sont les couples $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$ ?*

On détermine deux entiers $u_0$ et $v_0$ tels que $au_0 + bv_0 = 1$.

On démontre par analyse synthèse que les couples $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$ sont les couples $(u_0 + kb, v_0 - ka)$ où $k$ appartient à $\mathbb{Z}$.

▷ **Exercice 7.**

### E. Généralisation à plusieurs entiers

**Lemme.** *Soit $a$, $b$, $c$ trois entiers strictement positifs. Alors :*

$$(a \wedge b) \wedge c = a \wedge (b \wedge c)$$

*Cet entier est noté $a \wedge b \wedge c$, c'est le plus grand commun diviseur de $a$, $b$ et $c$.*

**Remarque.** On dit que la loi $\wedge$ est *associative*.

Démonstration. On sait que pour deux entiers non tous les deux nuls :

$$m \wedge n = \operatorname{Max}(\mathcal{D}(m) \cap \mathcal{D}(n)) \qquad \text{et} \qquad \mathcal{D}(m \wedge n) = \mathcal{D}(m) \cap \mathcal{D}(n)$$

Comme $a$, $b$, $c$ sont non-nuls :

$$\mathcal{D}(a \wedge b) \cap \mathcal{D}(c) = \mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathcal{D}(c) = \mathcal{D}(a) \cap \mathcal{D}(b \wedge c)$$

Les maxima de ces deux ensembles sont donc égaux, ce qui donne :

$$(a \wedge b) \wedge c = a \wedge (b \wedge c)$$ □

**Lemme (suite).** *Soit $a$, $b$, $c$ trois entiers relatifs. Alors $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.*

Démonstration. La formule est valable si un ou plusieurs des entiers est nul. En effet, pour tout entier positif $n$ : $n \wedge 0 = n$.

Elle est valable aussi si un ou plusieurs des entiers est négatif, car pour tous entiers $a$ et $b$ : $a \wedge b = |a| \wedge |b|$. □

**Remarque.** Soit $n$ en entier naturel non-nul et $(a_k)_{1 \leqslant k \leqslant n}$ une famille de $n$ entiers. On définit récursivement :

$$a_1 \wedge \ldots \wedge a_n = (\ldots((a_1 \wedge a_2) \wedge a_3) \ldots \wedge a_n)$$

On démontre par récurrence que :

$$\mathcal{D}(a_1 \wedge \ldots \wedge a_n) = \mathcal{D}(a_1) \cap \ldots \cap \mathcal{D}(a_n)$$

On en déduit que $a_1 \wedge \ldots \wedge a_n$ est le plus grand commun diviseur des entiers $a_1, \ldots, a_n$.

**Définition.** Soit $n$ en entier naturel non-nul et $(a_k)_{1 \leqslant k \leqslant n}$ une famille de $n$ entiers. Le PGCD des entiers $a_1, \ldots, a_n$ est le plus grand commun diviseur de tous les $a_k$.

Cet entier est $a_1 \wedge \ldots \wedge a_n$ et on note également :

**Exemples.** Si $n = 1$ alors $\bigwedge_{k=1}^{1} a_k = a_1$ et si $n = 0$ alors $\bigwedge_{k=1}^{0} a_k = 0$.

**Théorème (relation de Bézout).** *Soit $n$ en entier naturel non-nul, $(a_k)_{1 \leqslant k \leqslant n}$ une famille de $n$ entiers non tous nuls, et $d$ le PGCD de cette famille. Alors il existe des entiers $u_1, \ldots, u_n$ tels que*

$$a_1 u_1 + \cdots + a_n u_n = d$$

Démonstration. On démontre cette propriété par récurrence.

Initialisation. Si $n = 1$ le résultat est évident, $d = a_1$ donc on peut poser $u_1 = 1$.

Hérédité. Si $a_1, \ldots, a_n$ est une famille de $n$ entiers non tous nuls, alors la propriété pour $n - 1$ entiers montre qu'il existe des entiers $u_1, \ldots, u_{n-1}$ tels que :

$$a_1 u_1 + \cdots + a_{n-1} u_{n-1} = a_1 \wedge \ldots \wedge a_{n-1}$$

La relation de Bézout appliquée à $a_1 \wedge \ldots \wedge a_{n-1}$ et $a_n$ montre qu'il existe deux entiers $u$ et $v$ tels que :

$$(a_1 \wedge \ldots \wedge a_{n-1})u + a_n v = (a_1 \wedge \ldots \wedge a_{n-1}) \wedge a_n$$

Ceci donne :

$$a_1 u_1 u + \cdots + a_{n-1} u_{n-1} u + a_n v = a_1 \wedge \ldots \wedge a_n$$

Les $u_k u$ et $v$ sont entiers, donc la proposition est vraie pour $n$ entiers.

Conclusion. Le théorème est démontré par récurrence. □

**Définitions.** Soit $n$ en entier naturel non-nul, $(a_k)_{1\leqslant k\leqslant n}$ une famille de $n$ entiers.

*(i)* Les entiers $a_1, \ldots, a_n$ sont dits premiers entre eux dans leur ensemble si leur PGCD est égal à 1, ce qui signifie qu'il n'existe aucun autre entier que 1 et $-1$ qui les divise tous.

*(ii)* Les entiers $a_1, \ldots, a_n$ sont dits premiers entre eux deux à deux si pour tout couple $(i, j) \in \{1, \ldots, n\}^2$ avec $i \neq j$ les entiers $a_i$ et $a_j$ sont premiers entre eux.

**Remarques.**

*(i)* Si les entiers $a_1, \ldots, a_n$ sont premiers entre eux deux-à-deux alors ils sont premiers entre eux dans leur ensemble. En effet, s'ils sont premiers entre eux deux à deux alors en particulier $a_1 \wedge a_2 = 1$, puis :

$$a_1 \wedge \ldots \wedge a_n = (a_1 \wedge a_2) \wedge \ldots \wedge a_n = 1 \wedge a_3 \wedge \ldots \wedge a_n = 1$$

Donc les entiers $a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble.

*(ii)* La réciproque est fausse. Des entiers peuvent être premiers entre eux dans leur ensemble dans être premiers entre eux deux à deux.

Un exemple avec trois entiers $a$, $b$, $c$ :

**Théorème de Bézout.** *Avec les notations précédentes, les entiers $a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble si et seulement s'il existe des entiers $u_1, \ldots, u_n$ tels que :*

$$a_1u_1 + \cdots + a_nu_n = 1$$

Démonstration. Le sens direct est conséquence de la relation de Bézout ci-dessus.

Le sens indirect se démontre de la même façon que pour le cas de deux entiers : le PGCD de tous les $a_k$ divise chaque $a_k$, donc il divise $a_1u_1 + \cdots + a_nu_n$, donc il est égal à 1. □

**Exemple 3.** Déterminer trois entiers $u$, $v$, $w$ tels que $6u + 10v + 15w = 1$.

**Remarque.** On démontre également que si $a$, $b$, $c$ sont trois entiers non-nuls tous les trois alors :

$$(a \vee b) \vee c = a \vee (b \vee c)$$

Ceci est conséquence de la formule : $a\mathbb{N}^* \cap b\mathbb{N}^* = (a \vee b)\mathbb{N}^*$.

On définit récursivement $a_1 \vee \ldots \vee a_n$, et on démontre que cet entier est le plus petit commun multiple strictement positif de $a_1, \ldots, a_n$.

Ceci définit le PPCM de plusieurs entiers. On note :

Par exemple : $\bigvee_{k=1}^{1} a_k = a_1$ et $\bigvee_{k=1}^{0} a_k = 1$

# III. Nombres premiers

Dans toute cette partie on ne considère que des entiers naturels.

## A. Généralités

**Définition.** Un entier naturel $p$ est dit premier s'il admet exactement deux diviseurs. Ces deux diviseurs sont alors 1 et lui-même.

**Exemple 4.** Les premiers nombres premiers sont 2, 3, 5, 7, 11...

▷ **Exercice 8.**

**Définition.** Un entier naturel strictement supérieur à 1 non premier est dit composé.

**Proposition.** *Soit $n$ un entier composé. Alors $n$ admet un diviseur $a$ tel que $2 \leqslant a \leqslant \sqrt{n}$.*

Démonstration. Comme $n$ n'est pas premier et différent de 1 alors il admet au moins trois diviseurs : 1, $n$, et un autre que l'on note $d$. Celui-ci est alors strictement compris entre 1 et $n$ : $1 < d < n$.

Soit $k = \frac{n}{d}$. Alors $k$ est entier et $n = dk$, donc $k$ est un autre diviseur de $n$. Comme $d < n$ alors $1 < k$.

Si $d > \sqrt{n}$ et $k > \sqrt{n}$ alors par produit $dk > n$ ce qui est faux car $dk = n$.

Donc $d \leqslant \sqrt{n}$ ou $k \leqslant \sqrt{n}$. L'un des deux diviseurs $d$ et $k$ est inférieur à $\sqrt{n}$. De plus les deux sont strictement supérieurs à 1, donc supérieurs ou égaux à 2.

Ainsi $n$ admet un diviseur $a$ tel que $2 \leqslant a \leqslant \sqrt{n}$. □

**Méthode.**

*(i)* Pour vérifier qu'un entier $n$ est premier on peut chercher s'il est divisible par tous les entiers compris entre 2 et $\sqrt{n}$.

*(ii)* L'algorithme du crible d'Ératosthène permet, pour un entier $N$ donné, de déterminer tous les nombres premiers inférieurs ou égaux à $N$.

**Proposition.** *Il existe une infinité de nombres premiers.*

**Remarques.**

*(i)* Soit $p_n$ le $n$-ème nombre premier. Alors $p_n \simeq n \ln n$.

*(ii)* Soit $\pi(n)$ le nombre de nombres premiers inférieurs à $n$. Alors : $\pi(n) \sim \frac{n}{\ln n}$

*(iii)* Le plus grand nombre premier connu à ce jour est $2^{82\,589\,933} - 1$ (7 décembre 2018), il contient 24 862 048 chiffres.

**Propositions.** *Soit $p$ un nombre premier.*

*(i) Tout entier naturel $a$ non multiple de $p$ est premier avec $p$.*

*(ii) (Lemme d'Euclide) Soit $a$ et $b$ deux entiers naturels. Si $p$ divise le produit $ab$ alors $p$ divise $a$ ou $p$ divise $b$.*

*(iii) Soit $a_1, \ldots, a_n$ des entiers naturels. Si $p$ divise $a_1 \cdots a_n$ alors $p$ divise l'un des $a_k$.*

Démonstration.

*(iii)* Ce point se démontre par récurrence sur $n \in \mathbb{N}^*$, en appliquant le point *(ii)*. □

**Théorème.** *Tout entier naturel non-nul se décompose de façon unique en produit des nombres premiers : pour tout $n \in \mathbb{N}^*$, il existe une unique suite de nombres premiers $p_1 < p_2 < \cdots < p_r$ et d'entiers $\alpha_1, \ldots, \alpha_r$ strictement positifs tels que :*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$$

Démonstration. On démontre l'existence par récurrence forte, *cf* chapitre B3 (Logique).

Démontrons l'unicité. Soit $n$ un entier naturel. Soit $p_1, \ldots, p_s$ l'ensemble des nombres premiers inférieurs à $n$. Chacun d'entre eux divise ou ne divise pas $n$. Quitte à les réordonner on note $p_1, \ldots, p_r$ ceux qui divisent $n$.

Ainsi la décomposition de $n$ est de la forme $n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$ où les $\alpha_k$ sont des entiers strictement positifs.

Supposons qu'il existe deux telles décompositions distinctes :

$$n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r} = p_1^{\beta_1} \times \cdots \times p_r^{\beta_r}$$

où les $\alpha_k$ et les $\beta_k$ sont des entiers strictement positifs.

Ces deux décompositions sont distinctes si et seulement si il existe $k \in \{1, \ldots, n\}$ tel que $\alpha_k \neq \beta_k$. Quitte à intervertir les deux décompositions, on suppose que $\alpha_k > \beta_k$. En divisant par $p_k^{\beta_k}$ on obtient :

$$p_1^{\alpha_1} \times \cdots \times p_{k-1}^{\alpha_{k-1}} \times p_k^{\alpha_k - \beta_k} \times p_{k+1}^{\alpha_{k+1}} \times \cdots \times p_r^{\alpha_r} = p_1^{\beta_1} \times \cdots \times p_{k-1}^{\beta_{k-1}} \times p_{k+1}^{\beta_{k+1}} \times \cdots \times p_r^{\beta_r}$$

Comme $\alpha_k > \beta_k$ alors $\alpha_k - \beta_k \geqslant 1$, donc $p_k$ divise le membre de gauche.

D'après le point *(iii)* de la propriété ci-dessus, si $p_k$ divise le membre de droite alors il divise l'un des facteurs, donc l'un des $p_i$ pour $i$ différent de $k$. Ceci est une contradiction car les $p_i$ sont tous distincts.

Les deux décompositions ne peuvent donc être différentes. L'unicité est démontrée. □

▷ **Exercice 9.**

Démonstration de l'existence d'une infinité de nombres premiers.

▷ **Exercice 10.**

## B. Valuations $p$-adiques

**Définition.** Soit $p$ un nombre premier. Pour tout entier naturel $n$ non-nul on appelle valuation $p$-adique de $n$ et on note $v_p(n)$ la puissance de $p$ dans la décomposition de $n$ en facteurs premiers.

**Exemples.**

*(i)* Pour $n = 56$ : $v_2(56) =$ $v_3(56) =$ $v_7(56) =$

*(ii)* Pour tout nombre premier $p$ : $v_p(1) =$

**Définition alternative.**

Avec les mêmes notations, $v_p(n)$ est le plus grand entier $k$ tel que $p^k$ divise $n$.

**Remarque.** L'ensemble $\left\{ k \in \mathbb{N} \mid p^k \mid n \right\}$ est une partie de $\mathbb{N}$, non-vide car il contient 0. Comme $p$ est strictement supérieur à 1 alors l'inégalité $p^k \leqslant n$ équivaut à $k \leqslant \frac{\ln n}{\ln p}$, donc l'ensemble $\left\{ k \in \mathbb{N} \mid p^k \mid n \right\}$ est majoré.
Il admet donc un plus grand élément, ce qui justifie la définition alternative.

**Remarques.**

*(i)* La décomposition de $n$ en facteurs premiers est :

$$n = p_1^{v_{p_1}(n)} \times \cdots \times p_r^{v_{p_r}(n)}$$

où les $p_k$ sont les nombres premiers divisant $n$.

*(ii)* On note $\mathcal{P}$ l'ensemble des nombres premiers.

Si un nombre premier $p$ ne divise pas $n$ alors $v_p(n) = 0$, donc $p^{v_p(n)} = 1$. On note :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Par exemple :

$56 =$

**Proposition.** *Soit $p$ un nombre premier.*
*Alors pour tous entiers naturels non-nuls $a$ et $b$ :* $v_p(ab) = v_p(a) + v_p(b)$

Démonstration. La multiplication des produits donne :

$$a = \prod_{p \in \mathcal{P}} p^{v_p(a)} \qquad b = \prod_{p \in \mathcal{P}} p^{v_p(b)} \qquad \text{donc} \qquad ab = \prod_{p \in \mathcal{P}} p^{v_p(a)+v_p(b)}$$

Or par définition de la valuation $p$-adique : $ab = \prod_{p \in \mathcal{P}} p^{v_p(ab)}$

Par unicité de la décomposition en facteurs premiers on a bien $v_p(ab) = v_p(a) + v_p(b)$ pour tout $p$ premier. □

**Proposition.** *Soit $a$ et $b$ deux entiers naturels non-nuls. Alors $b$ divise $a$ si et seulement si pour tout nombre premier $p$ :* $v_p(b) \leqslant v_p(a)$

Démonstration. Supposons que $b$ divise $a$.

Soit $p$ un nombre premier, et soit $\beta = v_p(b)$. Alors $p^\beta$ divise $b$, donc $p^\beta$ divise $a$ par transitivité, et ainsi $\beta \leqslant v_p(a)$ car $v_p(a)$ est le plus grand entier $k$ tel que $p^k$ divise $a$.

Donc $v_p(b) \leqslant v_p(a)$.

Réciproquement, supposons que pour tout nombre premier $p$ : $v_p(b) \leqslant v_p(a)$.

On écrit alors le quotient des décompositions en facteurs premiers de $a$ et $b$ :

$$a = \prod_{p \in \mathcal{P}} p^{v_p(a)} \qquad b = \prod_{p \in \mathcal{P}} p^{v_p(b)} \qquad \text{donc} \qquad \frac{a}{b} = \prod_{p \in \mathcal{P}} p^{v_p(a)-v_p(b)}$$

Par hypothèse pour tout $p$ premier on a $v_p(a) - v_p(b) \geqslant 0$, donc $\frac{a}{b}$ est un entier, ce qui montre que $b$ divise $a$. □

▷ **Exercice 11.**

**Exemple 5.** Calcul du PGCD et du PPCM de $a = 27\,720$ et $b = 48\,300$.

**Théorème.** *On considère les décompositions de $a$ et $b$ suivantes :*

$$a = \prod_{k=1}^{r} p_k^{\alpha_k} \qquad et \qquad b = \prod_{k=1}^{r} p_k^{\beta_k}$$

*où les $p_k$ sont premiers distincts, et les $\alpha_k$, $\beta_k$ éventuellement nuls.*
*Alors le PGCD et le PPCM de $a$ et $b$ sont :*

$$a \wedge b = \prod_{k=1}^{r} p_k^{\gamma_k} \qquad et \qquad a \vee b = \prod_{k=1}^{r} p_k^{\delta_k}$$

*avec pour tout $k$ :* $\gamma_k = \mathrm{Min}\,\{\alpha_k, \beta_k\}$ *et* $\delta_k = \mathrm{Max}\,\{\alpha_k, \beta_k\}$

**Remarque.** On retrouve la propriété : $(a \wedge b)(a \vee b) = ab$
En effet, pour tout couple d'entiers $(\alpha, \beta)$ :

$$\mathrm{Min}\,\{\alpha, \beta\} + \mathrm{Max}\,\{\alpha, \beta\} = \alpha + \beta$$

Démonstration. Pour tout entier $d$ :

$$\begin{array}{rcl} (d \mid a \quad \text{et} \quad d \mid b) & \iff & \forall p \in \mathcal{P} \quad v_p(d) \leqslant v_p(a) \quad \text{et} \quad v_p(d) \leqslant v_p(b) \\ & \iff & \forall p \in \mathcal{P} \quad v_p(d) \leqslant \mathrm{Min}\,\{v_p(a), v_p(b)\} \end{array}$$

Le plus grand entier divisant $a$ et $b$ est donc celui pour lequel :

$$\forall p \in \mathcal{P} \qquad v_p(d) = \mathrm{Min}\,\{v_p(a), v_p(b)\}$$

Il s'agit du PGCD de $a$ et $b$.

Pour le PPCM on écrit pour tout entier $m$ :

$$\begin{array}{rcl} (a \mid m \quad \text{et} \quad b \mid m) & \iff & \forall p \in \mathcal{P} \quad v_p(a) \leqslant v_p(m) \quad \text{et} \quad v_p(b) \leqslant v_p(m) \\ & \iff & \forall p \in \mathcal{P} \quad \mathrm{Max}\,\{v_p(a), v_p(b)\} \leqslant v_p(m) \end{array}$$

Le plus petit multiple de $a$ et de $b$ est donc celui pour lequel :

$$\forall p \in \mathcal{P} \qquad v_p(m) = \mathrm{Max}\,\{v_p(a), v_p(b)\}$$

Il s'agit du PPCM de $a$ et $b$. □

▷ **Exercice 12.**

## IV. Congruence

**Définition.** Soit $n$ un entier strictement positif. On dit que deux entiers $a$ et $b$ sont congrus modulo $n$, ou que $a$ est congru à $b$ modulo $n$ si $a - b$ est un multiple de $n$. On note alors $a \equiv b \ [n]$.

**Remarque.** Soit $a$ et $n$ deux entiers, avec $n > 0$. Soit $q$ et $r$ le quotient et le reste de la division euclidienne de $a$ par $n$ :

$$a = qn + r \qquad \text{et} \qquad 0 \leqslant r < n$$

Alors $a$ est congru à $r$ modulo $n$ .

Ainsi tout entier $a$ est congru à un et un seul élément de $\{0, \dots, n-1\}$ modulo $n$.

Ceci montre que chaque classe d'équivalence de la relation de congruence modulo $n$ admet un représentant dans l'ensemble $\{0, \dots, n-1\}$.

**Proposition.** *La relation de congruence est compatible avec l'addition et la multiplication :*

Démonstration. On suppose que $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$. Ainsi il existe deux entiers $k$ et $\ell$ tels que $a = a' + kn$ et $b = b' + \ell n$.

Alors $a + b = a' + b' + (k + \ell)n$ et $ab = a'b' + (kb' + \ell a' + k\ell n)n$.

Ainsi $k + \ell$ et $kb' + \ell a' + k\ell n$ sont des entiers, donc $a + b \equiv a' + b' \ [n]$ et $ab \equiv a'b' \ [n]$.□

**Exemple 6.** Le dernier chiffre d'un entier naturel est le reste de sa division euclidienne par 10. En déduire que le carré d'un entier ne peut pas se terminer par 7.

▷ **Exercice 13.**

**Définition.** Soit $a$, $b$, $n$ trois entiers, avec $n > 0$. Si $\quad ba \equiv 1 \ [n] \quad$ alors on dit que $b$ est un inverse de $a$ modulo $n$.

**Remarque.** On a alors l'équivalence :

$$\forall (x, c) \in \mathbb{Z}^2 \qquad ax \equiv c \ [n] \quad \Longleftrightarrow \quad x \equiv bc \ [n]$$

**Exemple 7.** Déterminer un inverse de 7 modulo 10 puis résoudre l'équation $7x \equiv 6 \ [10]$.

▷ **Exercice 14.**

**Théorème (petit théorème de Fermat).**

*Soit $p$ un nombre premier. Alors :*

**Lemme.** *Soit $p$ un nombre premier. Alors pour tout $k = 1, \dots, p-1$, $p$ divise $\binom{p}{k}$.*

Démonstration. On sait que $\binom{p}{k}$ est un entier, et que $\binom{p}{k} = \frac{p!}{k!(p-k)!}$.

Ceci donne $p! = \binom{p}{k} k!(p-k)!$. Or $p$ divise $p!$, donc il divise le produit de trois entiers $\binom{p}{k} k!(p-k)!$.

Si $k \in \{1, \dots, p-1\}$ alors $p - k \in \{1, \dots, p-1\}$. Tous les entiers entre 1 et $k$ et entre 1 et $p-k$ sont strictement inférieurs à $p$ donc il ne sont pas multiples de $p$, et donc $k!$ et $(p-k)!$ sont premiers avec $p$.

Ainsi $p$ divise $\binom{p}{k} k!(p-k)!$ mais il ne divise ni $k!$ ni $(p-k)!$.

Donc $p$ divise $\binom{p}{k}$ d'après le lemme d'Euclide. □

Démonstration du petit théorème de Fermat.

**Exemple 8.**

a. Calculer, pour $n$ allant de 2 à 13 : $S_n = \sum_{k=0}^{n-2} 2^k$.

Pour quelles valeurs de $n$ la somme $S_n$ est-elle multiple de $n$ ?

b. Démontrer que si $p$ est premier impair alors $p$ divise $S_p$.

# V. Rationnels

## A. Généralités

**Définition.** L'ensemble des nombres rationnels est :

$$\mathbb{Q} = \left\{ \frac{p}{q} \;\middle|\; p \in \mathbb{Z},\, q \in \mathbb{N}^* \right\}$$

**Proposition.** *Soit $r$ un rationnel. Alors il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{p}{q}$ et $p$, $q$ sont premiers entre eux.*
*Cette écriture est appelée forme irréductible de $r$.*

Démonstration. Comme $r$ appartient à $\mathbb{Q}$ alors il existe $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ tels que $r = \frac{a}{b}$.

Soit $d = a \wedge b$, $a' = \frac{a}{d}$, $b' = \frac{b}{d}$. D'après le lemme de réduction des rationnels, $a'$ et $b'$ sont des entiers premiers entre eux. On note $p = a'$ et $q = b'$, alors $\frac{p}{q} = \frac{b}{a} = r$ avec $p$, $q$ premiers entre eux.

Le rationnel $r$ admet donc une forme irréductible. Démontrons qu'elle est unique.

Soit $(m, n)$ un autre couple de $\mathbb{Z} \times \mathbb{N}^*$ d'entiers premiers entre eux tels que $r = \frac{m}{n}$. Alors $\frac{p}{q} = \frac{m}{n}$ donc $pn = qm$.

Ainsi $n$ divise $qm$. Comme $m$ et $n$ sont premiers entre eux alors $n$ divise $q$ d'après le lemme de Gauss.

Mais $q$ divise $pn$. Comme $p$ et $q$ sont premiers entre eux alors $q$ divise $n$. Par antisymétrie de la divisibilité $q = n$. Comme $\frac{p}{q} = \frac{m}{n}$ alors $p = m$, ce qui démontre l'unicité. □

**Proposition.**

*(i) L'ensemble $\mathbb{Q}$ est stable par addition, soustraction et multiplication.*

*(ii) Tout élément non-nul de $\mathbb{Q}$ possède un inverse dans $\mathbb{Q}$.*

**Remarque.** Le développement d'un nombre rationnel non décimal en base quelconque présente une ration.

**Exemple 9.** Développement décimal de : $\frac{2}{3}$ $\frac{25}{9}$ $\frac{4}{11}$ $\frac{2}{7}$

**Définition.** Les nombres décimaux sont les nombres de la forme $\frac{p}{10^n}$, avec $p \in \mathbb{Z}$ et $n \in \mathbb{N}$.
De façon équivalente, il s'agit des nombres dont le développement décimal est fini.

L'ensemble des nombres décimaux est noté $\mathbb{D}$.

**Remarques.**

*(i)* L'ensemble $\mathbb{D}$ est stable par addition, soustraction et multiplication, mais pas par quotient.

*(ii)* Il est strictement compris entre $\mathbb{Z}$ et $\mathbb{Q}$ : $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{D} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$

**Définition.** Un réel non rationnel (*i.e.,* un élément de $\mathbb{R} \setminus \mathbb{Q}$) est dit irrationnel.

**Exemple.** Les réels $e$, $\pi$ sont irrationnels.

**Proposition.** $\sqrt{2}$ *est irrationnel.*

Démonstration.

▷ **Exercice 15.**

### B. Densité

**Théorème.** *Tout intervalle de* $\mathbb{R}$ *non réduit à un point contient un rationnel.*

**Définition.** On dit que $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Démonstration. À part.

**Proposition (Autres formulations de la densité).** *De façon équivalente :*

*(i) Pour tout réel* $x$ *et tout* $\varepsilon > 0$*, il existe un rationnel* $r$ *tel que* $|x - r| \leqslant \varepsilon$.

*(ii) Pour tout réel* $x$*, il existe une suite* $(r_n)$ *de rationnels convergeant vers* $x$.

Démonstration. On suppose que tout intervalle de $\mathbb{R}$ non réduit à un point contient un rationnel.

*(i)* Soit $x$ un réel et $\varepsilon > 0$. Alors $[x - \varepsilon, x + \varepsilon]$ est un intervalle non réduit à un point. Il contient donc un rationnel $r$. Ainsi $x - \varepsilon \leqslant r \leqslant x + \varepsilon$, donc $|x - r| \leqslant \varepsilon$.

*(ii)* Soit $x$ un réel. Pour tout entier naturel $n$ non-nul, comme $\frac{1}{n} > 0$ alors d'après le point précédent il existe un rationnel $r_n$ tel que $|x - r_n| \leqslant \frac{1}{n}$.
On a ainsi construit une suite de rationnels $(r_n)_{n\in\mathbb{N}^*}$. D'après le théorème d'encadrement, comme $\frac{1}{n}$ converge vers 0 alors la suite $(r_n)$ converge vers $x$. □

**Remarque.** Tout intervalle non réduit à un point contient également un irrationnel.

En d'autre termes $\mathbb{R} \setminus \mathbb{Q}$ est également dense dans $\mathbb{R}$.

En effet, l'intervalle $\left[\frac{a}{\sqrt{2}}, \frac{b}{\sqrt{2}}\right]$ contient un rationnel $r$ d'après ce qui précède. On peut le supposer non-nul. Ainsi $r\sqrt{2}$ appartient à l'intervalle $[a, b]$. Or $r\sqrt{2}$ est irrationnel, sinon par produit $\frac{1}{r} \times r\sqrt{2}$ serait rationnel, ce qui est faux.