Mathématiques

Chapitre B4
Arithmétique

MPSI – Lycée Bellevue – Toulouse

Année 2024-2025

Euclide (Grèce) v. -300

Ératosthène (Grèce) v. -276 – v. -194

Diophante (Grèce) v. 200 – v. 284

Pierre de Fermat (France) v. 1605 – 1665

Étienne Bézout (France) 1730 – 1783

Leonhard Euler (Suisse) 1707 – 1783

Carl Friedrich Gauss
(Allemagne) 1777 – 1855

Chapitre B4. Arithmétique

I. Entiers

Chapitre B4. Arithmétique

Chapitre B4. Arithmétique

Chapitre B4. Arithmétique

Chapitre B4. Arithmétique

Chapitre B4. Arithmétique

Chapitre B4. Arithmétique

Définition

Ensemble des entiers naturels :

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

Définition

Ensemble des entiers naturels :

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

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

David Hilbert (Allemagne) 1862 – 1943

Propositions

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

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.

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 $m \geqslant n + 1$.

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 $m \geqslant n + 1$.

(iv) Si une suite d'entiers naturels est décroissante alors elle est stationnaire.

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 $m \geqslant n + 1$.

(iv) Si une suite d'entiers naturels est décroissante alors elle est stationnaire.

Démonstration. Tout est conséquence de la construction de $\mathbb{N}$. □

Définition

L'ensemble des entiers relatifs est :

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

Chapitre B4. Arithmétique

Définition

a, b entiers naturels.

a est un multiple de b

ou b est un diviseur de a

s'il existe $k \in \mathbb{N}$ tel que : $a = bk$

On note : $b \mid a$

Remarques

(i) Cette relation est une relation d'ordre sur $\mathbb{N}$ car elle est :

- réflexive

$$\forall a \in \mathbb{N} \quad a \mid a$$

- antisymétrique

$$\forall (a,b) \in \mathbb{N}^2 \quad (a \mid b \quad \text{et} \quad b \mid a) \quad \Longrightarrow \quad a = b$$

- transitive

$$\forall (a,b,c) \in \mathbb{N}^3 \quad (a \mid b \quad \text{et} \quad b \mid c) \quad \Longrightarrow \quad a \mid c$$

Elle n'est pas totale.

Remarques

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

Remarques

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

Elle n'est pas antisymétrique.

Remarques

(ii) La relation de divisibilité sur $\mathbb{Z}$ n'est pas une relation d'ordre.
Elle n'est pas antisymétrique.

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

Remarques

(iv) Le signe n'importe pas :

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

On pourra souvent se ramener au cas des entiers naturels.

Remarques

(iv) Le signe n'importe pas :

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

On pourra souvent se ramener au cas des entiers naturels.

(v) L'ensemble des multiples de b est :

$$b\mathbb{Z} = \{bn \mid n \in \mathbb{Z}\}$$

Proposition

$(a, b, c) \in \mathbb{Z}^3 \qquad (u, v) \in \mathbb{Z}^2$

Si c divise a et b alors c divise $au + bv$.

Proposition

$(a, b, c) \in \mathbb{Z}^3 \qquad (u, v) \in \mathbb{Z}^2$

Si c divise a et b alors c divise $au + bv$.

$$(c \mid a) \quad \text{et} \quad (c \mid b) \implies \forall (u, v) \in \mathbb{Z}^2 \quad c \mid au + bv$$

Proposition

$(a, b, c) \in \mathbb{Z}^3 \qquad (u, v) \in \mathbb{Z}^2$

Si c divise a et b alors c divise $au + bv$.

$$(c \mid a) \quad \text{et} \quad (c \mid b) \implies \forall (u, v) \in \mathbb{Z}^2 \quad c \mid au + bv$$

Démonstration.

Proposition

$(a, b, c) \in \mathbb{Z}^3 \qquad (u, v) \in \mathbb{Z}^2$

Si c divise a et b alors c divise $au + bv$.

$$(c \mid a) \quad \text{et} \quad (c \mid b) \implies \forall (u, v) \in \mathbb{Z}^2 \quad c \mid au + bv$$

Démonstration.

□

Notation

$\mathcal{D}(n)$: ensemble des diviseurs de n dans $\mathbb{Z}$

Notation

$\mathcal{D}(n)$: ensemble des diviseurs de n dans $\mathbb{Z}$

Exemples

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

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

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

Notation

$\mathcal{D}(n)$: ensemble des diviseurs de n dans $\mathbb{Z}$

Exemples

$$\mathcal{D}(7) = \{\pm 1, \pm 7\}$$

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

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

Notation

$\mathcal{D}(n)$: ensemble des diviseurs de n dans $\mathbb{Z}$

Exemples

$$\begin{aligned}\mathcal{D}(7) &= \{\pm 1, \pm 7\}\\ \mathcal{D}(6) &= \{\pm 1, \pm 2, \pm 3, \pm 6\}\\ \mathcal{D}(0) &=\end{aligned}$$

Notation

$\mathcal{D}(n)$: ensemble des diviseurs de n dans $\mathbb{Z}$

Exemples

$$\begin{aligned}\mathcal{D}(7) &= \{\pm 1, \pm 7\}\\ \mathcal{D}(6) &= \{\pm 1, \pm 2, \pm 3, \pm 6\}\\ \mathcal{D}(0) &= \mathbb{Z}\end{aligned}$$

Notation

$\mathcal{D}(n)$: ensemble des diviseurs de n dans $\mathbb{Z}$

Exemples

$$\begin{aligned}\mathcal{D}(7) &= \{\pm 1, \pm 7\}\\ \mathcal{D}(6) &= \{\pm 1, \pm 2, \pm 3, \pm 6\}\\ \mathcal{D}(0) &= \mathbb{Z}\end{aligned}$$

Remarques

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

Notation

$\mathcal{D}(n)$: ensemble des diviseurs de n dans $\mathbb{Z}$

Exemples

$$\begin{aligned}\mathcal{D}(7) &= \{\pm 1, \pm 7\}\\ \mathcal{D}(6) &= \{\pm 1, \pm 2, \pm 3, \pm 6\}\\ \mathcal{D}(0) &= \mathbb{Z}\end{aligned}$$

Remarques

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

(ii) Si $n \neq 0$ alors $\mathcal{D}(n)$ est borné par $-|n|$ et $|n|$.

Notation

$\mathcal{D}(n)$: ensemble des diviseurs de n dans $\mathbb{Z}$

Exemples

$$\begin{aligned}\mathcal{D}(7) &= \{\pm 1, \pm 7\}\\ \mathcal{D}(6) &= \{\pm 1, \pm 2, \pm 3, \pm 6\}\\ \mathcal{D}(0) &= \mathbb{Z}\end{aligned}$$

Remarques

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

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

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Définition

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

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Exemples

(i) $43 = \quad ? \times 5 + \quad ?$

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Exemples

(i) $43 = 8 \times 5 + 3$

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Exemples

(i) $43 = 8 \times 5 + 3$

(ii) $-43 = ? \times 5 + ?$

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Exemples

(i) $43 = 8 \times 5 + 3$

(ii) $-43 = -9 \times 5 + 2$

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Remarque

En Python :

$$\texttt{q} = \texttt{a}//\texttt{b} \qquad \texttt{r} = \texttt{a}\%\texttt{b}$$

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Démonstration de l'unicité.

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Démonstration de l'unicité.

□

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

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

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

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

□

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

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

Si $a < 0$ alors $a + b|a| > 0$.

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

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

Si $a < 0$ alors $a + b|a| > 0$.

$$\exists (q_1, r) \in \mathbb{Z}^2 \qquad \begin{cases} a + b|a| = bq_1 + r \\ 0 \leqslant r < b \end{cases}$$

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

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

Si $a < 0$ alors $a + b|a| > 0$.

$$\exists (q_1, r) \in \mathbb{Z}^2 \qquad \begin{cases} a = b(q_1 - |a|) + r \\ 0 \leqslant r < b \end{cases}$$

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

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

Si $a < 0$ alors $a + b|a| > 0$.

$$\exists (q\ , r) \in \mathbb{Z}^2 \qquad \begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

□

Théorème (Division euclidienne)

Soit a et b deux entiers avec $b > 0$.

Alors il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b$$

Démonstration : conclusion.

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

Le théorème est démontré. □

▷ Exercice 1.

Soit a et b deux entiers avec b strictement positif. Démontrer que b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

▷ Exercice 2.

Soit a et b deux entiers avec b non-nul, q le quotient de la division euclidienne de a par b. Démontrer que $q = \left\lfloor \frac{a}{b} \right\rfloor$.

Chapitre B4. Arithmétique

II. PGCD et PPCM

A. PGCD

B. Relation de Bézout

C. PPCM

D. Entiers premiers entre eux

E. Généralisation à plusieurs entiers

Définition

Soit $(a, b) \in \mathbb{N}^2 \setminus \{(0, 0)\}$.

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 $\mathbb{N}$:

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

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 $\mathbb{N}$

Remarque

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

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

Cet ensemble est une partie de $\mathbb{N}$

- non-vide car elle contient 1
- majorée par a et b s'ils sont non-nuls.

Il admet donc un maximum.
Ce maximum est appellé PGCD de a et b.

Remarque

On peut donc définir le PGCD par :

$$\forall (a,b) \neq (0,0) \qquad a \wedge b = \mathrm{Max}\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right)$$

Exemples

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

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

$10 \wedge 77 =$ $\quad$ $42 \wedge 150 =$ $\quad$ $120 \wedge 0 =$

Exemples

$5 \wedge 7 = 1$ $\quad 6 \wedge 7 =$ $\quad 6 \wedge 8 =$

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

$10 \wedge 77 =$ $\quad 42 \wedge 150 =$ $\quad 120 \wedge 0 =$

Exemples

$5 \wedge 7 = 1$ $\quad$ $6 \wedge 7 = 1$ $\quad$ $6 \wedge 8 =$

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

$10 \wedge 77 =$ $\quad$ $42 \wedge 150 =$ $\quad$ $120 \wedge 0 =$

Exemples

$5 \wedge 7 = 1$ $\quad$ $6 \wedge 7 = 1$ $\quad$ $6 \wedge 8 = 2$

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

$10 \wedge 77 =$ $\quad$ $42 \wedge 150 =$ $\quad$ $120 \wedge 0 =$

Exemples

$5 \wedge 7 = 1$ $\quad$ $6 \wedge 7 = 1$ $\quad$ $6 \wedge 8 = 2$

$10 \wedge 25 = 5$ $\quad$ $28 \wedge 14 =$ $\quad$ $7 \wedge 100 =$

$10 \wedge 77 =$ $\quad$ $42 \wedge 150 =$ $\quad$ $120 \wedge 0 =$

Exemples

$5 \wedge 7 = 1$ $\quad$ $6 \wedge 7 = 1$ $\quad$ $6 \wedge 8 = 2$

$10 \wedge 25 = 5$ $\quad$ $28 \wedge 14 = 14$ $\quad$ $7 \wedge 100 =$

$10 \wedge 77 =$ $\quad$ $42 \wedge 150 =$ $\quad$ $120 \wedge 0 =$

Exemples

$5 \wedge 7 = 1$ $\quad$ $6 \wedge 7 = 1$ $\quad$ $6 \wedge 8 = 2$

$10 \wedge 25 = 5$ $\quad$ $28 \wedge 14 = 14$ $\quad$ $7 \wedge 100 = 1$

$10 \wedge 77 =$ $\quad$ $42 \wedge 150 =$ $\quad$ $120 \wedge 0 =$

Exemples

$5 \wedge 7 = 1$ $\quad$ $6 \wedge 7 = 1$ $\quad$ $6 \wedge 8 = 2$

$10 \wedge 25 = 5$ $\quad$ $28 \wedge 14 = 14$ $\quad$ $7 \wedge 100 = 1$

$10 \wedge 77 = 1$ $\quad$ $42 \wedge 150 =$ $\quad$ $120 \wedge 0 =$

Exemples

$5 \wedge 7 = 1$ $\quad$ $6 \wedge 7 = 1$ $\quad$ $6 \wedge 8 = 2$

$10 \wedge 25 = 5$ $\quad$ $28 \wedge 14 = 14$ $\quad$ $7 \wedge 100 = 1$

$10 \wedge 77 = 1$ $\quad$ $42 \wedge 150 = 6$ $\quad$ $120 \wedge 0 =$

Exemples

$$5 \wedge 7 = 1 \qquad 6 \wedge 7 = 1 \qquad 6 \wedge 8 = 2$$

$$10 \wedge 25 = 5 \qquad 28 \wedge 14 = 14 \qquad 7 \wedge 100 = 1$$

$$10 \wedge 77 = 1 \qquad 42 \wedge 150 = 6 \qquad 120 \wedge 0 = 120$$

Lemme

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

(i) Si $a = bq + r$ avec $0 \leqslant r < b$

Alors : $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$

(ii) $a \wedge b = b \wedge r$

Lemme

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

(i) Si $a = bq + r$ avec $0 \leqslant r < b$

Alors : $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$

(ii) $a \wedge b = b \wedge r$

Démonstration.

(i) $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(a - nb) \quad (n \in \mathbb{Z})$

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 $(a - nb) + nb = a$ et b donc :

$$\mathcal{D}(b) \cap \mathcal{D}(a - nb) \subseteq \mathcal{D}(a) \cap \mathcal{D}(b)$$

Par double inclusion :

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

Démonstration.

(i) $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(a - nb) \quad (n \in \mathbb{Z})$

Si $a = bq + r$ avec $0 \leqslant r < b$ alors

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

Donc

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

Démonstration.

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

(ii) $a \wedge b = b \wedge r$

$$a \wedge b = \mathrm{Max}\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right)$$

Démonstration.

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

(ii) $a \wedge b = b \wedge r$

$$\begin{aligned} a \wedge b &= \operatorname{Max}\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right) \\ &= \operatorname{Max}\left(\mathcal{D}(b) \cap \mathcal{D}(r)\right) \end{aligned}$$

Démonstration.

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

(ii) $a \wedge b = b \wedge r$

$$\begin{aligned} a \wedge b &= \operatorname{Max}\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right) \\ &= \operatorname{Max}\left(\mathcal{D}(b) \cap \mathcal{D}(r)\right) = b \wedge r \end{aligned}$$

□

Méthode (Algorithme d'Euclide)

Détermination du PGCD de deux entiers a et b :

$$r_0 = a \qquad r_1 = b$$

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{n-1} &= r_n q_n \end{aligned}$$

Alors r_n est le PGCD de a et b.

Méthode (Algorithme d'Euclide)

Détermination du PGCD de deux entiers a et b :

$$\begin{aligned} r_0 = a \qquad & r_1 = b \\ r_0 \% r_1 &= r_2 \\ r_1 \% r_2 &= r_3 \\ &\vdots \\ r_{n-1} \% r_n &= 0 \end{aligned}$$

Alors r_n est le PGCD de a et b.

Méthode (Algorithme d'Euclide)

Détermination du PGCD de deux entiers a et b :

$$\begin{aligned} r_0 = a \qquad & r_1 = b \\ r_0 \% r_1 &= r_2 \\ r_1 \% r_2 &= r_3 \\ &\vdots \\ r_{n-1} \% r_n &= 0 \end{aligned}$$

Alors r_n est le PGCD de a et b.

Exemple 1

PGCD de 150 et 66.

Méthode (Algorithme d'Euclide)

Détermination du PGCD de deux entiers a et b :

$$\begin{aligned} r_0 = a \qquad & r_1 = b \\ r_0 \% r_1 &= r_2 \\ r_1 \% r_2 &= r_3 \\ &\vdots \\ r_{n-1} \% r_n &= 0 \end{aligned}$$

Alors r_n est le PGCD de a et b.

▷ Exercice 3.

Programmer en Python cet algorithme.

Démonstration. $r_0 = a$ $r_1 = b$ puis :

$$\forall k = 1 \dots n \qquad \begin{cases} r_{k-1} = r_k q_k + r_{k+1} \\ 0 \leqslant r_{k+1} < r_k \end{cases}$$

Démonstration. $r_0 = a$ $r_1 = b$ puis :

$$\forall k = 1 \dots n \qquad \begin{cases} r_{k-1} = r_k q_k + r_{k+1} \\ 0 \leqslant r_{k+1} < r_k \end{cases}$$

La suite $(r_k)_{k \geqslant 1}$ est une suite d'entiers naturels strictement décroissante, donc à partir d'un certain rang $r_k = 0$.

Démonstration. $r_0 = a$ $r_1 = b$ puis :

$$\forall k = 1 \dots n \qquad \begin{cases} r_{k-1} = r_k q_k + r_{k+1} \\ 0 \leqslant r_{k+1} < r_k \end{cases}$$

La suite $(r_k)_{k \geqslant 1}$ est une suite d'entiers naturels strictement décroissante, donc à partir d'un certain rang $r_k = 0$.

On note k_0 ce rang, et on pose $n = k_0 - 1$.

Démonstration. $r_0 = a$ $r_1 = b$ puis :

$$\forall k = 1 \dots n \qquad \begin{cases} r_{k-1} = r_k q_k + r_{k+1} \\ 0 \leqslant r_{k+1} < r_k \end{cases}$$

La suite $(r_k)_{k \geqslant 1}$ est une suite d'entiers naturels strictement décroissante, donc à partir d'un certain rang $r_k = 0$.

On note k_0 ce rang, et on pose $n = k_0 - 1$.

Donc $r_n > 0$ et $r_{n+1} = 0$.

Démonstration. $r_0 = a$ $r_1 = b$ puis :

$$\forall k = 1 \dots n \qquad \begin{cases} r_{k-1} = r_k q_k + r_{k+1} \\ 0 \leqslant r_{k+1} < r_k \end{cases}$$

La suite $(r_k)_{k \geqslant 1}$ est une suite d'entiers naturels strictement décroissante, donc à partir d'un certain rang $r_k = 0$.

On note k_0 ce rang, et on pose $n = k_0 - 1$.

Donc $r_n > 0$ et $r_{n+1} = 0$.

L'algorithme renvoie r_n.

Démonstration. $r_0 = a$ $r_1 = b$ puis :

$$\forall k = 1 \dots n \qquad \begin{cases} r_{k-1} = r_k q_k + r_{k+1} \\ 0 \leqslant r_{k+1} < r_k \end{cases}$$

Donc $r_n > 0$ et $r_{n+1} = 0$.

L'algorithme renvoie r_n.

Or : $r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_n \wedge r_{n+1} = r_n$

Démonstration. $r_0 = a$ $r_1 = b$ puis :

$$\forall k = 1 \dots n \qquad \begin{cases} r_{k-1} = r_k q_k + r_{k+1} \\ 0 \leqslant r_{k+1} < r_k \end{cases}$$

Donc $r_n > 0$ et $r_{n+1} = 0$.

L'algorithme renvoie r_n.

Or : $r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_n \wedge r_{n+1} = r_n$

Donc $r_n = r_0 \wedge r_1 = a \wedge b$ □

Démonstration. $r_0 = a$ $r_1 = b$ puis :

$$\forall k = 1 \dots n \qquad \begin{cases} r_{k-1} = r_k q_k + r_{k+1} \\ 0 \leqslant r_{k+1} < r_k \end{cases}$$

L'algorithme renvoie r_n.

Or : $r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_n \wedge r_{n+1} = r_n$

Donc $r_n = r_0 \wedge r_1 = a \wedge b$ □

Remarque

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

Proposition

Soit a et b deux entiers. Alors :

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

Proposition

Soit a et b deux entiers. Alors :

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

Démonstration.

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r_0) \cap \mathcal{D}(r_1)$$

Proposition

Soit a et b deux entiers. Alors :

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

Démonstration.

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

Proposition

Soit a et b deux entiers. Alors :

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

Démonstration.

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

Proposition

Soit a et b deux entiers. Alors :

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

Corollaire

Si n divise a et b alors n divise leur PGCD.

$$(n \mid a) \quad \text{et} \quad (n \mid b) \quad \Longrightarrow \quad (n \mid a \wedge b)$$

Proposition

Soit a et b deux entiers. Alors :

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

Corollaire

Si n divise a et b alors n divise leur PGCD.

Remarque

Le PGCD de a et b est le plus grand diviseur commun de a et de b au sens de la relation d'ordre classique et de la relation de divisibilité.

Proposition

Soit a et b deux entiers. Alors :

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

Définition

On pose :

$$0 \wedge 0 = 0$$

Définition (cas des entiers négatifs)

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

Le PGCD de a et b est leur plus grand commun diviseur.

Remarque

- $\mathcal{D}(a) = \mathcal{D}(-a)$
- Donc $a \wedge b = |a| \wedge |b|$
- $a \wedge b \geqslant 0$ même si a ou b est négatif.

II. PGCD et PPCM

Théorème

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.
Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que :

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

Théorème

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.
Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que :

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

Définition

(u, v) : coefficients de Bézout du couple (a, b).

Théorème

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.
Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que :

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

Définition

(u, v) : 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.

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

Quitte à remplacer u par $-u$ ou v par $-v$ on peut supposer que a et b sont positifs tous les deux.

Démonstration. a et b positifs.

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} \qquad \forall k \geqslant 1 \quad r_{k-1} = r_k q_k + r_{k+1}$$

Démonstration. a et b positifs.

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} \qquad \forall k \geqslant 1 \quad r_{k-1} = r_k q_k + r_{k+1}$$

$$\mathcal{P}_k : \quad \exists (u_k, v_k) \in \mathbb{Z}^2 \qquad a u_k + b v_k = r_k$$

Démonstration. a et b positifs.

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} \qquad \forall k \geqslant 1 \quad r_{k-1} = r_k q_k + r_{k+1}$$

$\mathcal{P}_k$: $\quad \exists (u_k, v_k) \in \mathbb{Z}^2 \qquad a u_k + b v_k = r_k$

Initialisation.

$$a \times 1 + b \times 0 = r_0$$
$$a \times 0 + b \times 1 = r_1$$

Démonstration. a et b positifs.

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} \qquad \forall k \geqslant 1 \quad r_{k-1} = r_k q_k + r_{k+1}$$

$\mathcal{P}_k$: $\quad \exists (u_k, v_k) \in \mathbb{Z}^2 \qquad au_k + bv_k = r_k$

Hérédité.

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

Démonstration. a et b positifs.

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} \qquad \forall k \geqslant 1 \quad r_{k-1} = r_k q_k + r_{k+1}$$

$\mathcal{P}_k$: $\quad \exists (u_k, v_k) \in \mathbb{Z}^2 \qquad au_k + bv_k = r_k$

Hérédité.

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

Démonstration. a et b positifs.

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} \qquad \forall k \geqslant 1 \quad r_{k-1} = r_k q_k + r_{k+1}$$

$\mathcal{P}_k$: $\quad \exists (u_k, v_k) \in \mathbb{Z}^2 \qquad au_k + bv_k = r_k$

Hérédité.

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

$L_1 - q_k L_2$:

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

Démonstration. a et b positifs.

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} \qquad \forall k \geqslant 1 \quad r_{k-1} = r_k q_k + r_{k+1}$$

$\mathcal{P}_k$: $\quad \exists (u_k, v_k) \in \mathbb{Z}^2 \qquad au_k + bv_k = r_k$

Hérédité.

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

$L_1 - q_k L_2$:

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

Démonstration. a et b positifs.

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} \qquad \forall k \geqslant 1 \quad r_{k-1} = r_k q_k + r_{k+1}$$

$\mathcal{P}_k$: $\quad \exists (u_k, v_k) \in \mathbb{Z}^2 \qquad a u_k + b v_k = r_k$

Conclusion. $\mathcal{P}_k$ valable pour tout $k = 0, \ldots, n+1$.

En particulier pour $k = n$:

$$a u_n + b v_n = r_n = a \wedge b \qquad \square$$

Théorème

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.
Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que :

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

Remarque

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

Théorème

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.
Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que :

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

Remarque

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

Exemple 1 (suite)

Coefficients de Bézout pour $(a, b) = (150, 66)$.

Théorème

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.
Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que :

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

▷ Exercice 4.

Déterminer des coefficients de Bézout pour (a, b) valant $(6, 7)$, $(6, 8)$, $(7, 100)$ et $(49, 175)$.

Remarque

Pour obtenir récursivement les coefficients u et v :

$$\begin{cases} u_0 = 1 \\ v_0 = 0 \end{cases} \qquad \begin{cases} u_1 = 0 \\ v_1 = 1 \end{cases}$$

$$\text{et} \quad \forall k = 1, \ldots, n \quad \begin{cases} u_{k+1} = u_{k-1} - q_k u_k \\ v_{k+1} = v_{k-1} - q_k v_k \end{cases}$$

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 $v = v_n$.

II. PGCD et PPCM

Définition

Soit $(a, b) \in (\mathbb{N}^*)^2$.
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 on définit : $a \vee b = |a| \vee |b|$
Il s'agit toujours du plus petit commun multiple strictement 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 elle contient l'entier ab.
Il admet donc un minimum.
Ce minimum est appelé PPCM de a et b.
Ceci s'écrit :

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

Exemples

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

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

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

Exemples

$5 \vee 7 = 35$ $\quad 6 \vee 7 = \quad 6 \vee 8 =$

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

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

Exemples

$5 \vee 7 = 35$ $\quad$ $6 \vee 7 = 42$ $\quad$ $6 \vee 8 =$

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

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

Exemples

$5 \vee 7 = 35$ $\quad$ $6 \vee 7 = 42$ $\quad$ $6 \vee 8 = 24$

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

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

Exemples

$5 \vee 7 = 35$ $\quad$ $6 \vee 7 = 42$ $\quad$ $6 \vee 8 = 24$

$10 \vee 25 = 50$ $\quad$ $28 \vee 14 =$ $\quad$ $7 \vee 100 =$

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

Exemples

$5 \vee 7 = 35$ $\quad$ $6 \vee 7 = 42$ $\quad$ $6 \vee 8 = 24$

$10 \vee 25 = 50$ $\quad$ $28 \vee 14 = 28$ $\quad$ $7 \vee 100 =$

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

Exemples

$5 \vee 7 = 35$ $\quad$ $6 \vee 7 = 42$ $\quad$ $6 \vee 8 = 24$

$10 \vee 25 = 50$ $\quad$ $28 \vee 14 = 28$ $\quad$ $7 \vee 100 = 700$

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

Exemples

$5 \vee 7 = 35$ $\quad 6 \vee 7 = 42$ $\quad 6 \vee 8 = 24$

$10 \vee 25 = 50$ $\quad 28 \vee 14 = 28$ $\quad 7 \vee 100 = 700$

$10 \vee 77 = 770$ $\quad 42 \vee 150 =$ $\quad 120 \vee 1 =$

Exemples

$5 \vee 7 = 35$ $\quad 6 \vee 7 = 42$ $\quad 6 \vee 8 = 24$

$10 \vee 25 = 50$ $\quad 28 \vee 14 = 28$ $\quad 7 \vee 100 = 700$

$10 \vee 77 = 770$ $\quad 42 \vee 150 = 1050$ $\quad 120 \vee 1 =$

Exemples

$5 \vee 7 = 35$ $\quad 6 \vee 7 = 42$ $\quad 6 \vee 8 = 24$

$10 \vee 25 = 50$ $\quad 28 \vee 14 = 28$ $\quad 7 \vee 100 = 700$

$10 \vee 77 = 770$ $\quad 42 \vee 150 = 1050$ $\quad 120 \vee 1 = 120$

Remarque

Le PPCM est utilisé pour calculer des fractions :

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

Remarque

Le PPCM est utilisé pour calculer des fractions :

$$\frac{1}{6}+\frac{7}{8}=\frac{4+21}{24}=\frac{25}{24}$$

Proposition

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

Proposition

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

Remarque

Le PPCM de a et b est le plus petit multiple commun de a et de b au sens de la relation d'ordre $\leqslant$, mais aussi pour la relation de divisibilité.
Si a et b divisent n alors $a \vee b$ divise n.

Proposition

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

Démonstration.

Proposition

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

Démonstration.

□

▷ Exercice 5.

Soit a et b deux entiers non-nuls. Déterminer :

$$a\mathbb{Z} \cap b\mathbb{Z}$$

Déterminer aussi l'ensemble de toutes les sommes possibles d'un élément de $a\mathbb{Z}$ et d'un élément de $b\mathbb{Z}$:

$$a\mathbb{Z} + b\mathbb{Z} = \{m + n \mid m \in a\mathbb{Z} \quad \text{et} \quad n \in b\mathbb{Z}\}$$

II. PGCD et PPCM

Définition

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

Définition

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

Exemple

10 et 77 sont 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 :

$$au + bv = 1$$

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 :

$$au + bv = 1$$

Remarque

a et b sont premiers entre eux si et seulement si ils n'ont aucun diviseur commun autre que 1 et -1.

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.

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.

□

▷ Exercice 6.

Soit a, b, n trois entiers. Démontrer que :

a. Si a et b sont premiers entre eux et divisent n, alors ab divise n.

b. Si a et b sont premiers avec n alors ab est premier avec n.

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$ et $\frac{a}{b} = \frac{a'}{b'}$.

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$

Démonstration. $(a, b) \neq (0, 0)$ donc $d \neq 0$.

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$

Démonstration. $(a, b) \neq (0, 0)$ donc $d \neq 0$.

a' et b' sont bien définis et sont entiers.

De plus $a = a'd$ et $b = b'd$.

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$

Démonstration.

Il existe $(u, v) \in \mathbb{Z}^2$ tel que : $au + bv = d$

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$

Démonstration.

Il existe $(u, v) \in \mathbb{Z}^2$ tel que : $au + bv = d$

Donc $a'du + b'dv = d$ puis $a'u + b'v = 1$.

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$

Démonstration.

Il existe $(u, v) \in \mathbb{Z}^2$ tel que : $au + bv = d$

Donc $a'du + b'dv = d$ puis $a'u + b'v = 1$.

Th de Bézout : a' et b' sont premiers entre eux. $\square$

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$ et $\frac{a}{b} = \frac{a'}{b'}$.

Remarque

$$\frac{a}{b} = \frac{a'd}{b'd} = \frac{a'}{b'}$$

Le rationnel $\frac{a}{b}$ est sous forme irréductible.

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$ et $\frac{a}{b} = \frac{a'}{b'}$.

Exemple

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

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$ et $\frac{a}{b} = \frac{a'}{b'}$.

Exemple

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

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

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$ et $\frac{a}{b} = \frac{a'}{b'}$.

Exemple

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

Alors $d = 6$ $a' = 25$ $b' = 7$

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$ et $\frac{a}{b} = \frac{a'}{b'}$.

Exemple

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

Alors $d = 6$ $a' = 25$ $b' = 7$

$150 = 25 \times 6$ $42 = 7 \times 6$ $25 \wedge 7 = 1$

Lemme (réduction des rationnels)

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

Soit $d = a \wedge b$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Alors $a' \wedge b' = 1$ et $\frac{a}{b} = \frac{a'}{b'}$.

Exemple

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

Alors $d = 6$ $a' = 25$ $b' = 7$

$$\frac{150}{42} = \frac{25}{7}$$ cette fraction est irréductible.

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.

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Longrightarrow \quad a \mid c$$

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.

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Longrightarrow \quad a \mid c$$

Démonstration.

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.

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Longrightarrow \quad a \mid c$$

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 : $ab = (a \wedge b)(a \vee b)$

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) 5 et 7 sont premiers entre eux, leur PPCM est : $5 \vee 7 = 35$.

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) 5 et 7 sont premiers entre eux, leur PPCM est : $5 \vee 7 = 35$.

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

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 : $ab = (a \wedge b)(a \vee b)$

Remarque

Grâce à cette dernière formule on peut calculer le PPCM si on connaît le PGCD.

On peut obtenir le PGCD grâce à l'algorithme d'Euclide.

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 : $a \vee b = ab$

Démonstration.

(i) Supposons : $a \wedge b = 1$

- Soit $m = a \vee b$. Alors : $\exists k \in \mathbb{N} \quad m = ka$

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 : $a \vee b = ab$

Démonstration.

(i) Supposons : $a \wedge b = 1$

- Soit $m = a \vee b$. Alors : $\exists k \in \mathbb{N} \quad m = ka$
- $b \mid m$ et $a \wedge b = 1 \implies b \mid k$

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 : $a \vee b = ab$

Démonstration.

(i) Supposons : $a \wedge b = 1$

- Soit $m = a \vee b$. Alors : $\exists k \in \mathbb{N} \quad m = ka$
- $b \mid m$ et $a \wedge b = 1 \implies b \mid k$
  $\implies ab \mid ka = m$

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 : $a \vee b = ab$

Démonstration.

(i) Supposons : $a \wedge b = 1$

- Soit $m = a \vee b$. Alors : $\exists k \in \mathbb{N} \quad m = ka$
- $b \mid m$ et $a \wedge b = 1 \implies b \mid k$
  $\implies ab \mid ka = m$
- $ab \mid m$ et $m \mid ab \implies m = ab$

Proposition

Soit a et b deux entiers naturels non-nuls.

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

Démonstration.

(ii) Notons $d = a \wedge b$

Proposition

Soit a et b deux entiers naturels non-nuls.

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

Démonstration.

(ii) Notons $d = a \wedge b$

- $a = a'd \qquad b = b'd \qquad a' \wedge b' = 1$

Proposition

Soit a et b deux entiers naturels non-nuls.

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

Démonstration.

(ii) Notons $d = a \wedge b$

- $a = a'd \qquad b = b'd \qquad a' \wedge b' = 1$
- $a \vee b = (a'd) \vee (b'd) = d(a' \vee b') = da'b'$

Proposition

Soit a et b deux entiers naturels non-nuls.

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

Démonstration.

(ii) Notons $d = a \wedge b$

- $a = a'd \qquad b = b'd \qquad a' \wedge b' = 1$
- $a \vee b = (a'd) \vee (b'd) = d(a' \vee b') = da'b'$
- $(a \wedge b)(a \vee b) = a'b'd^2 = (a'd)(b'd) = ab$ $\square$

Exemple 2 (complément sur la relation de Bézout)

Soit $(a, b) \in \mathbb{Z}^2$ avec $a \wedge b = 1$.

Déterminer tous les couples $(u, v) \in \mathbb{Z}^2$ tels que :

$$au + bv = 1$$

Exemple 2 (complément sur la relation de Bézout)

Soit $(a, b) \in \mathbb{Z}^2$ avec $a \wedge b = 1$.

Déterminer tous les couples $(u, v) \in \mathbb{Z}^2$ tels que :

$$au + bv = 1$$

- Soit u_0 et v_0 tels que : $au_0 + bv_0 = 1$

Exemple 2 (complément sur la relation de Bézout)

Soit $(a, b) \in \mathbb{Z}^2$ avec $a \wedge b = 1$.

Déterminer tous les couples $(u, v) \in \mathbb{Z}^2$ tels que :

$$au + bv = 1$$

- Soit u_0 et v_0 tels que : $au_0 + bv_0 = 1$
- L'ensemble des couples recherchés est :

$$\mathcal{S} = \{(u_0 + kb, v_0 - ka) \mid k \in \mathbb{Z}\}$$

Exemple 2 (suite)

Déterminer tous les couples $(u, v) \in \mathbb{Z}^2$ tels que :

$$11u + 8v = 1$$

Exemple 2 (suite)

Déterminer tous les couples $(u, v) \in \mathbb{Z}^2$ tels que :

$$11u + 8v = 1$$

▷ Exercice 7.

Déterminer tous les couples $(u, v) \in \mathbb{Z}^2$ tels que :

a. $24u + 15v = 20$

b. $24u + 15v = 21$.

II. PGCD et PPCM

Lemme

Soit $(a, b, c) \in (\mathbb{N}^*)^3$. 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.

Lemme

Soit $(a, b, c) \in (\mathbb{N}^*)^3$. 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. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

$(a \wedge b)$ et c ne sont pas tous les deux nuls donc :

$$\begin{aligned}(a \wedge b) \wedge c &= \operatorname{Max}\left(\mathcal{D}(a \wedge b) \cap \mathcal{D}(c)\right) \\ &= \operatorname{Max}\left(\mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathcal{D}(c)\right) \\ &= \operatorname{Max}\left(\mathcal{D}(a) \cap \mathcal{D}(b \wedge c)\right) \\ &= a \wedge (b \wedge c)\end{aligned}$$

□

Lemme

Soit $(a, b, c) \in (\mathbb{N}^*)^3$. 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.

Lemme (suite)

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

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

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

La formule est valable si un ou plusieurs des entiers est nul, car : $\forall n \in \mathbb{Z} \quad n \wedge 0 = n$.

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 - Définition récursive

$(a_k)_{1 \leqslant k \leqslant n}$: famille de n entiers.

$$a_1 \wedge a_2 \qquad = a_1 \wedge a_2$$

Remarque - Définition récursive

$(a_k)_{1 \leqslant k \leqslant n}$: famille de n entiers.

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

Remarque - Définition récursive

$(a_k)_{1 \leqslant k \leqslant n}$: famille de n entiers.

$$
\begin{aligned}
a_1 \wedge a_2 &= a_1 \wedge a_2 \\
a_1 \wedge a_2 \wedge a_3 &= (a_1 \wedge a_2) \wedge a_3 \\
a_1 \wedge a_2 \wedge a_3 \wedge a_4 &= ((a_1 \wedge a_2) \wedge a_3) \wedge a_4
\end{aligned}
$$

Remarque - Définition récursive

$(a_k)_{1 \leqslant k \leqslant n}$: famille de n entiers.

$$\begin{aligned}
a_1 \wedge a_2 &= a_1 \wedge a_2 \\
a_1 \wedge a_2 \wedge a_3 &= (a_1 \wedge a_2) \wedge a_3 \\
a_1 \wedge a_2 \wedge a_3 \wedge a_4 &= ((a_1 \wedge a_2) \wedge a_3) \wedge a_4 \\
&\dots \\
a_1 \wedge \ldots \wedge a_n &= (\ldots((a_1 \wedge a_2) \wedge a_3) \ldots \wedge a_n)
\end{aligned}$$

Par récurrence :

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

Donc $a_1 \wedge \ldots \wedge a_n$ est le PGCD de $a_1, \ldots, a_n$.

Définition

Le PGCD des entiers $a_1, \ldots, a_n$ est le plus grand commun diviseur de tous les a_k.

Il est égal à $a_1 \wedge \ldots \wedge a_n$ et on note également :

$$\bigwedge_{k=1}^{n} a_k = a_1 \wedge \ldots \wedge a_n$$

Définition

Le PGCD des entiers $a_1, \ldots, a_n$ est le plus grand commun diviseur de tous les a_k.

Il est égal à $a_1 \wedge \ldots \wedge a_n$ et on note également :

$$\bigwedge_{k=1}^{n} a_k = a_1 \wedge \ldots \wedge a_n$$

Exemples

$$\bigwedge_{k=1}^{1} a_k = \qquad \bigwedge_{k=1}^{0} a_k =$$

Définition

Le PGCD des entiers $a_1, \ldots, a_n$ est le plus grand commun diviseur de tous les a_k.

Il est égal à $a_1 \wedge \ldots \wedge a_n$ et on note également :

$$\bigwedge_{k=1}^{n} a_k = a_1 \wedge \ldots \wedge a_n$$

Exemples

$$\bigwedge_{k=1}^{1} a_k = a_1 \qquad \bigwedge_{k=1}^{0} a_k = 0$$

Théorème (relation de Bézout)

Soit $(a_k)_{1 \leqslant k \leqslant n}$ 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 :

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

Théorème (relation de Bézout)

Soit $(a_k)_{1\leqslant k\leqslant n}$ 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 :

$$a_1u_1 + \cdots + a_nu_n = d$$

Démonstration.

$\mathcal{P}_n$: $\quad \forall (a_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \setminus \{(0,\ldots,0)\}$

$$\exists (u_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \qquad \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k$$

Théorème (relation de Bézout)

Soit $(a_k)_{1\leqslant k\leqslant n}$ 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 :

$$a_1u_1 + \cdots + a_nu_n = d$$

Démonstration.

$\mathcal{P}_n$: $\quad \forall (a_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \setminus \{(0,\ldots,0)\}$

$$\exists (u_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \qquad \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k$$

Initialisation. $u_1 = 1$

Démonstration.

$$\mathcal{P}_n : \quad \forall (a_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \setminus \{(0,\dots,0)\} \quad \exists (u_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \qquad \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k$$

Hérédité. Supposons $\mathcal{P}_{n-1}$ vraie.

Soit $(a_1,\dots,a_n) \in \mathbb{Z}^n \setminus \{(0,\dots 0)\}$

Démonstration.

$$\mathcal{P}_n : \quad \forall (a_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \setminus \{(0,\dots,0)\} \quad \exists (u_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \qquad \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k$$

Hérédité. Supposons $\mathcal{P}_{n-1}$ vraie.

Soit $(a_1,\dots,a_n) \in \mathbb{Z}^n \setminus \{(0,\dots 0)\}$

Si $a_1 = \cdots = a_{n-1} = 0$ alors a_n est non-nul et :

$$a_1 \times 1 + \cdots + a_n \times 1 = a_n = a_1 \wedge \ldots \wedge a_n$$

Démonstration.

$$\mathcal{P}_n : \quad \forall (a_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \setminus \{(0,\dots,0)\} \quad \exists (u_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \qquad \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k$$

Hérédité. Supposons $\mathcal{P}_{n-1}$ vraie.

Soit $(a_1,\dots,a_n) \in \mathbb{Z}^n \setminus \{(0,\dots 0)\}$

Sinon il existe $u_1,\dots,u_{n-1}$ tels que :

$$a_1u_1 + \cdots + a_{n-1}u_{n-1} = a_1 \wedge \dots \wedge a_{n-1}$$

Démonstration.

$$\mathcal{P}_n : \quad \forall (a_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \setminus \{(0,\dots,0)\} \quad \exists (u_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \qquad \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k$$

Hérédité. Supposons $\mathcal{P}_{n-1}$ vraie.

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

Puis il existe u et v tels que :

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

Démonstration.

$$\mathcal{P}_n : \quad \forall (a_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \setminus \{(0,\dots,0)\} \quad \exists (u_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \qquad \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k$$

Hérédité. Supposons $\mathcal{P}_{n-1}$ vraie.

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

Ceci donne :

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

$\mathcal{P}_n$ est vraie.

Théorème (relation de Bézout)

Soit $(a_k)_{1\leqslant k\leqslant n}$ 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 :

$$a_1u_1 + \cdots + a_nu_n = d$$

Démonstration.

$\mathcal{P}_n$: $\quad \forall (a_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \setminus \{(0,\ldots,0)\}$

$$\exists (u_k)_{1\leqslant k\leqslant n} \in \mathbb{Z}^n \qquad \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k$$

Conclusion. $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N}^*$. □

Définitions

Soit $(a_k)_{1 \leqslant k \leqslant n} \in \mathbb{Z}^n$.

(i) $a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble si leur PGCD est égal à 1.

(ii) $a_1, \ldots, a_n$ sont 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 :

$$\begin{aligned} a_1 \wedge \ldots \wedge a_n &= (a_1 \wedge a_2) \wedge \ldots \wedge a_n \\ &= 1 \wedge a_3 \wedge \ldots \wedge a_n = 1 \end{aligned}$$

Remarques

(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 :

$$a = \qquad b = \qquad c =$$

Remarques

(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 :

$$a = 6 \qquad b = 10 \qquad c = 15$$

Remarques

(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 :

$$a = 1 \qquad b = 2 \qquad c = 4$$

Remarques

(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 :

$$a = 858 \qquad b = 910 \qquad c = 1155$$

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 :

$$a_1 u_1 + \cdots + a_n u_n = 1$$

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 :

$$a_1 u_1 + \cdots + a_n u_n = 1$$

Démonstration. Sens direct :
Si $(a_k)_{1 \leqslant k \leqslant n}$ est une famille de n entiers alors il existe des entiers $u_1, \ldots, u_n$ tels que :

$$a_1 u_1 + \cdots + a_n u_n = a_1 \wedge \ldots \wedge a_n$$

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 :

$$a_1 u_1 + \cdots + a_n u_n = 1$$

Démonstration. Sens indirect :
Le PGCD de tous les a_k divise chaque a_k, donc il divise $a_1 u_1 + \cdots + a_n u_n$, donc il est égal à 1. $\square$

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 :

$$a_1 u_1 + \cdots + a_n u_n = 1$$

Exemple 3

Déterminer trois entiers u, v, w tels que :

$$6u + 10v + 15w = 1$$

Remarque

Pour tout $(a, b, c) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$:

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

On définit récursivement $a_1 \vee \ldots \vee a_n$ et on démontre que cet entier est le plus petit commun multiple de $a_1, \ldots, a_n$.
Ceci définit le PPCM de plusieurs entiers. On note :

$$\bigvee_{k=1}^{n} a_k = a_1 \vee \ldots \vee a_n$$

Remarque

Pour tout $(a, b, c) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$:

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

Ceci définit le PPCM de plusieurs entiers. On note :

$$\bigvee_{k=1}^{n} a_k = a_1 \vee \ldots \vee a_n$$

Par exemple :

$$\bigvee_{k=1}^{1} a_k = a_1 \qquad \text{et} \qquad \bigvee_{k=1}^{0} a_k = 1$$

Chapitre B4. Arithmétique

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

III. **Nombres premiers**

A. Généralités

B. Valuations p-adiques

Définition

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

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...

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.

Donner la liste des entiers premiers inférieurs à 100.
(Ils sont au nombre de 25.)

Définition

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

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 $2 \leqslant a \leqslant \sqrt{n}$.

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.

$n = dk$ avec $1 < d < n$ et $1 < k < n$

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.

$n = dk$ avec $1 < d < n$ et $1 < k < n$

Si $d > \sqrt{n}$ et $k > \sqrt{n}$ alors $dk > (\sqrt{n})^2$

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.

$n = dk$ avec $1 < d < n$ et $1 < k < n$

Si $d > \sqrt{n}$ et $k > \sqrt{n}$ alors $dk > (\sqrt{n})^2$

Contradiction. □

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 $\sqrt{n}$.

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.

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 :

$$\pi(n) \sim \frac{n}{\ln n}$$

Proposition

Il existe une infinité de nombres premiers.

Remarques

(iii) Plus grand nombre premier connu à ce jour : (7 décembre 2018)

$$2^{82\,589\,933} - 1 \quad \simeq \quad 1{,}49 \times 10^{24\,862\,047}$$

Remarques

(iv) Conjecture de Goldbach : tout nombre pair supérieur à 3 est somme de deux nombres premiers.

$$
\begin{aligned}
4 &= 2+2 \\
6 &= 3+3 \\
8 &= 3+5 \\
10 &= 3+7 = 5+5 \\
12 &= 5+7 \\
14 &= 3+11 = 7+7 \\
&\vdots \\
22 &= 3+19 = 5+17 = 11+11
\end{aligned}
$$

Propositions

Soit p un nombre premier.

(i) Si a n'est pas multiple de p alors a est premier avec p.

(ii) (Lemme d'Euclide) Soit $(a, b) \in \mathbb{N}^2$.
Si p divise ab alors p divise a ou p divise b.

(iii) Soit $(a_1, \ldots, a_n) \in \mathbb{N}^n$.
Si p divise $a_1 \cdots a_n$ alors p divise l'un des a_k.

Propositions

Soit p un nombre premier.

(i) Si a n'est pas multiple de p alors a est premier avec p.

(ii) (Lemme d'Euclide) Soit $(a, b) \in \mathbb{N}^2$.
Si p divise ab alors p divise a ou p divise b.

(iii) Soit $(a_1, \ldots, a_n) \in \mathbb{N}^n$.
Si p divise $a_1 \cdots a_n$ alors p divise l'un des a_k.

Démonstration.

(i)

Propositions

Soit p un nombre premier.

(i) Si a n'est pas multiple de p alors a est premier avec p.

(ii) (Lemme d'Euclide) Soit $(a, b) \in \mathbb{N}^2$.
Si p divise ab alors p divise a ou p divise b.

(iii) Soit $(a_1, \ldots, a_n) \in \mathbb{N}^n$.
Si p divise $a_1 \cdots a_n$ alors p divise l'un des a_k.

Démonstration.

(ii)

Propositions

Soit p un nombre premier.

(i) Si a n'est pas multiple de p alors a est premier avec p.

(ii) (Lemme d'Euclide) Soit $(a, b) \in \mathbb{N}^2$.
Si p divise ab alors p divise a ou p divise b.

(iii) Soit $(a_1, \ldots, a_n) \in \mathbb{N}^n$.
Si p divise $a_1 \cdots a_n$ alors p divise l'un des a_k.

Démonstration.

(iii) Par récurrence grâce au *(ii)*. □

Théorème

Tout entier naturel non-nul se décompose de façon unique en produit des nombres premiers.

Théorème

Pour tout $n \in \mathbb{N}^*$ il existe une unique suite de nombres premiers $p_1 < p_2 < \cdots < p_r$ et d'entiers strictement positifs $\alpha_1 \dots \alpha_r$ tels que :

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

Théorème

Pour tout $n \in \mathbb{N}^*$ il existe une unique suite de nombres premiers $p_1 < p_2 < \cdots < p_r$ et d'entiers strictement positifs $\alpha_1 \dots \alpha_r$ tels que :

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

Démonstration.

Existence par **récurrence forte**.

Démonstration de l'unicité.

- Chaque nombre premier divise ou ne divise pas n, et seul un nombre fini de nombres premiers est inférieur ou égal à n, donc l'ensemble des nombres premiers $p_1, \ldots, p_r$ qui divisent n est uniquement déterminé.

Démonstration de l'unicité.

- Chaque nombre premier divise ou ne divise pas n, et seul un nombre fini de nombres premiers est inférieur ou égal à n, donc l'ensemble des nombres premiers $p_1, \ldots, p_r$ qui divisent n est uniquement déterminé.
- Ainsi :

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

où les α_k sont dans $\mathbb{N}^*$.

Démonstration de l'unicité.

- Ainsi :

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

où les α_k sont dans $\mathbb{N}^*$.

Démonstration de l'unicité.

- Ainsi :

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

où les α_k sont dans $\mathbb{N}^*$.

- Supposons :

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

Démonstration de l'unicité.

- Supposons :

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

Démonstration de l'unicité.

- Supposons :

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

Si $\alpha_k > \beta_k$:

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

Contradiction : p_k divise le membre de gauche mais pas celui de droite. □

▷ Exercice 9.

Décomposer en produit de facteurs premiers :

60	375	389	899
$1\,001$	$2\,016$	$2\,020$	$777\,000$

Proposition

Il existe une infinité de nombres premiers.

Démonstration.

Proposition

Il existe une infinité de nombres premiers.

Démonstration.

□

Proposition

Il existe une infinité de nombres premiers.

Démonstration.

□

▷ **Exercice 10.**

Démontrer que pour tout $n \in \mathbb{N}$ les facteurs premiers de $n! + 1$ sont strictement supérieurs à n.
En déduire une autre preuve de l'infinité des nombres premiers.

III. **Nombres premiers**

Définition

Soit p un nombre premier et $n \in \mathbb{N}^*$.

La valuation p-adique de n est la puissance de p dans la décomposition de n en facteurs premiers.

On la note $v_p(n)$.

Définition

Soit p un nombre premier et $n \in \mathbb{N}^*$.
La valuation p-adique de n est la puissance de p dans la décomposition de n en facteurs premiers.
On la note $v_p(n)$.

Exemples

(i) $56 = 2^3 \times 7$

$v_2(56) =$ $\quad$ $v_3(56) =$ $\quad$ $v_7(56) =$

Définition

Soit p un nombre premier et $n \in \mathbb{N}^*$.
La valuation p-adique de n est la puissance de p dans la décomposition de n en facteurs premiers.
On la note $v_p(n)$.

Exemples

(i) $56 = 2^3 \times 7$

$$v_2(56) = 3 \qquad v_3(56) = 0 \qquad v_7(56) = 1$$

Définition

Soit p un nombre premier et $n \in \mathbb{N}^*$.
La valuation p-adique de n est la puissance de p dans la décomposition de n en facteurs premiers.
On la note $v_p(n)$.

Exemples

(i) $56 = 2^3 \times 7$

$$v_2(56) = 3 \qquad v_3(56) = 0 \qquad v_7(56) = 1$$

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

Définition

Soit p un nombre premier et $n \in \mathbb{N}^*$.
La valuation p-adique de n est la puissance de p dans la décomposition de n en facteurs premiers.
On la note $v_p(n)$.

Exemples

(i) $56 = 2^3 \times 7$

$$v_2(56) = 3 \qquad v_3(56) = 0 \qquad v_7(56) = 1$$

(ii) Pour tout nombre premier p : $v_p(1) = 0$

Définition alternative

Soit p un nombre premier et $n \in \mathbb{N}^*$.

La valuation p-adique de n est :

$$v_p(n) = \text{Max}\left\{k \in \mathbb{N} \mid \ p^k \mid n\right\}$$

Définition alternative

Soit p un nombre premier et $n \in \mathbb{N}^*$.

La valuation p-adique de n est :

$$v_p(n) = \text{Max}\left\{k \in \mathbb{N} \mid \ p^k \mid n\right\}$$

Remarque

$\left\{k \in \mathbb{N} \mid \ p^k \mid n\right\}$ est une partie de $\mathbb{N}$

Définition alternative

Soit p un nombre premier et $n \in \mathbb{N}^*$.

La valuation p-adique de n est :

$$v_p(n) = \mathrm{Max}\left\{k \in \mathbb{N} \mid \ p^k \mid n\right\}$$

Remarque

$\left\{k \in \mathbb{N} \mid \ p^k \mid n\right\}$ est une partie de $\mathbb{N}$

- non-vide,

Définition alternative

Soit p un nombre premier et $n \in \mathbb{N}^*$.

La valuation p-adique de n est :

$$v_p(n) = \mathrm{Max}\left\{k \in \mathbb{N} \mid \ p^k \mid n\right\}$$

Remarque

$\left\{k \in \mathbb{N} \mid \ p^k \mid n\right\}$ est une partie de $\mathbb{N}$

- non-vide,
- majorée.

Définition alternative

Soit p un nombre premier et $n \in \mathbb{N}^*$.

La valuation p-adique de n est :

$$v_p(n) = \mathrm{Max}\left\{k \in \mathbb{N} \mid p^k \mid n\right\}$$

Remarque

$\left\{k \in \mathbb{N} \mid p^k \mid n\right\}$ est une partie de $\mathbb{N}$

- non-vide,
- majorée.

Elle admet donc un maximum : $v_p(n)$ est bien défini.

Remarque

La décomposition de n en facteurs premiers est donc :

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

Remarque

La décomposition de n en facteurs premiers est donc :

$$n = p_1^{v_{p_1}(n)} \times \cdots \times p_r^{v_{pr}(n)} = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Notation

On note $\mathcal{P}$ l'ensemble des nombres premiers.

Remarque

La décomposition de n en facteurs premiers est donc :

$$n = p_1^{v_{p_1}(n)} \times \cdots \times p_r^{v_{pr}(n)} = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Notation

On note $\mathcal{P}$ l'ensemble des nombres premiers.

Exemple

$$56 = 2^3 \times 7^1$$

Remarque

La décomposition de n en facteurs premiers est donc :

$$n = p_1^{v_{p_1}(n)} \times \cdots \times p_r^{v_{pr}(n)} = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Notation

On note $\mathcal{P}$ l'ensemble des nombres premiers.

Exemple

$$56 = 2^3 \times 7^1 = 2^3 \times 3^0 \times 5^0 \times 7^1 \times 11^0 \times \cdots$$

Proposition

Soit p un nombre premier et $(a, b) \in (\mathbb{N}^*)^2$. Alors :

$$v_p(ab) = v_p(a) + v_p(b)$$

Proposition

Soit p un nombre premier et $(a, b) \in (\mathbb{N}^*)^2$. Alors :

$$v_p(ab) = v_p(a) + v_p(b)$$

Démonstration.

$$ab = \left(\prod_{p \in \mathcal{P}} p^{v_p(a)} \right) \left(\prod_{p \in \mathcal{P}} p^{v_p(b)} \right)$$

Proposition

Soit p un nombre premier et $(a, b) \in (\mathbb{N}^*)^2$. Alors :

$$v_p(ab) = v_p(a) + v_p(b)$$

Démonstration.

$$ab = \left(\prod_{p\in\mathcal{P}} p^{v_p(a)}\right)\left(\prod_{p\in\mathcal{P}} p^{v_p(b)}\right) = \prod_{p\in\mathcal{P}} p^{v_p(a)+v_p(b)}$$

Proposition

Soit p un nombre premier et $(a, b) \in (\mathbb{N}^*)^2$. Alors :

$$v_p(ab) = v_p(a) + v_p(b)$$

Démonstration.

$$ab = \left(\prod_{p\in\mathcal{P}} p^{v_p(a)}\right)\left(\prod_{p\in\mathcal{P}} p^{v_p(b)}\right) = \prod_{p\in\mathcal{P}} p^{v_p(a)+v_p(b)}$$

$$\text{Or} \qquad ab = \prod_{p\in\mathcal{P}} p^{v_p(ab)}$$

Proposition

Soit p un nombre premier et $(a, b) \in (\mathbb{N}^*)^2$. Alors :

$$v_p(ab) = v_p(a) + v_p(b)$$

Démonstration.

$$ab = \left(\prod_{p\in\mathcal{P}} p^{v_p(a)}\right)\left(\prod_{p\in\mathcal{P}} p^{v_p(b)}\right) = \prod_{p\in\mathcal{P}} p^{v_p(a)+v_p(b)}$$

$$\text{Or} \qquad ab = \prod_{p\in\mathcal{P}} p^{v_p(ab)}$$

La décomposition en facteurs premiers est unique. □

Proposition

$(a, b) \in (\mathbb{N}^*)^2$

$$b \mid a \iff \forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Proposition

$(a, b) \in (\mathbb{N}^*)^2$

$$b \mid a \iff \forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Démonstration. Supposons que b divise a.

Soit $p \in \mathcal{P}$ et $\beta = v_p(b)$. Alors :

Proposition

$(a, b) \in (\mathbb{N}^*)^2$

$$b \mid a \iff \forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Démonstration. Supposons que b divise a.

Soit $p \in \mathcal{P}$ et $\beta = v_p(b)$. Alors :

$$p^\beta \mid b \quad \text{et} \quad b \mid a \implies p^\beta \mid a$$

Proposition

$(a, b) \in (\mathbb{N}^*)^2$

$$b \mid a \iff \forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Démonstration. Supposons que b divise a.

Soit $p \in \mathcal{P}$ et $\beta = v_p(b)$. Alors :

$$p^\beta \mid b \quad \text{et} \quad b \mid a \quad \Longrightarrow \quad p^\beta \mid a$$

Or $\quad v_p(a) = \operatorname{Max}\left\{k \in \mathbb{N} \mid \ p^k \mid a\right\}$

Donc $\quad \beta \leqslant v_p(a) \quad$ puis $\quad v_p(b) \leqslant v_p(a)$

Proposition

$(a, b) \in (\mathbb{N}^*)^2$

$$b \mid a \quad \Longleftrightarrow \quad \forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Démonstration. Supposons que :

$$\forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Proposition

$(a, b) \in (\mathbb{N}^*)^2$

$$b \mid a \quad \Longleftrightarrow \quad \forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Démonstration. Supposons que :

$$\forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Alors :

$$\frac{a}{b} = \left(\prod_{p \in \mathcal{P}} p^{v_p(a)}\right) / \left(\prod_{p \in \mathcal{P}} p^{v_p(b)}\right) = \prod_{p \in \mathcal{P}} p^{v_p(a) - v_p(b)}$$

Proposition

$(a, b) \in (\mathbb{N}^*)^2$

$$b \mid a \quad \Longleftrightarrow \quad \forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Démonstration. Supposons que :

$$\forall p \in \mathcal{P} \quad v_p(b) \leqslant v_p(a)$$

Alors :

$$\frac{a}{b} = \left(\prod_{p\in\mathcal{P}} p^{v_p(a)}\right) / \left(\prod_{p\in\mathcal{P}} p^{v_p(b)}\right) = \prod_{p\in\mathcal{P}} p^{v_p(a)-v_p(b)}$$

$$\in \mathbb{N}$$

□

▷ Exercice 11.

a. Donner la décomposition en facteurs premiers de $792\,000$.

b. En déduire le nombre de diviseurs positifs de ce nombre.

Exemple 5

PGCD et PPCM de :

$$a = 27\,720 \qquad \text{et} \qquad b = 48\,300$$

Remarque

a, b entiers strictement positifs.

Soit $p_1, p_2, \ldots, p_r$ l'ensemble des nombres premiers qui divisent m **ou** n.

Alors :

$$a = \prod_{i=1}^{r} p_i^{\alpha_i} \qquad \text{et} \qquad b = \prod_{i=1}^{r} p_i^{\beta_i}$$

où les α_i et les β_i sont des entiers naturels **éventuellement nuls.**

Remarque

a, b entiers strictement positifs.

Soit $p_1, p_2, \ldots, p_r$ l'ensemble des nombres premiers qui divisent m **ou** n.

Alors :

$$a = \prod_{i=1}^{r} p_i^{\alpha_i} \qquad \text{et} \qquad b = \prod_{i=1}^{r} p_i^{\beta_i}$$

où les α_i et les β_i sont des entiers naturels **éventuellement nuls.**

De plus :

$$b \mid a \iff \forall i = 1 \ldots r \quad \beta_i \leqslant \alpha_i$$

Théorème

On considère les décompositions de a et b suivantes :

$$a = \prod_{i=1}^{r} p_i^{\alpha_i} \qquad \text{et} \qquad b = \prod_{i=1}^{r} p_i^{\beta_i}$$

Alors leurs PGCD et PPCM sont :

$$a \wedge b = \prod_{i=1}^{r} p_i^{\gamma_i} \qquad \text{et} \qquad a \vee b = \prod_{i=1}^{r} p_i^{\delta_i}$$

avec pour tout i :

$$\gamma_i = \mathrm{Min}\left\{\alpha_i, \beta_i\right\} \quad \text{et} \quad \delta_i = \mathrm{Max}\left\{\alpha_i, \beta_i\right\}$$

Remarque

En corollaire :

$$(a \wedge b)(a \vee b) = ab$$

Remarque

En corollaire :

$$(a \wedge b)(a \vee b) = ab$$

Démonstration. En effet :

$$ab = \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i} \qquad (a \wedge b)(a \vee b) = \prod_{i=1}^{r} p_i^{\gamma_i+\delta_i}$$

et pour tout $i = 1 \cdots r$:

$$\gamma_i + \delta_i = \mathrm{Min}\{\alpha_i, \beta_i\} + \mathrm{Max}\{\alpha_i, \beta_i\} = \alpha_i + \beta_i \quad \square$$

Démonstration. Pour le PGCD :

$$(d \mid a \quad \text{et} \quad d \mid b)$$

$$\iff \forall p \in \mathcal{P} \quad v_p(d) \leqslant v_p(a) \quad \text{et} \quad v_p(d) \leqslant v_p(b)$$

Démonstration. Pour le PGCD :

$$(d \mid a \quad \text{et} \quad d \mid b)$$

$$\iff \forall p \in \mathcal{P} \quad v_p(d) \leqslant v_p(a) \quad \text{et} \quad v_p(d) \leqslant v_p(b)$$

$$\iff \forall p \in \mathcal{P} \quad v_p(d) \leqslant \operatorname{Min}\{v_p(a), v_p(b)\}$$

Démonstration. Pour le PGCD :

$$(d \mid a \quad \text{et} \quad d \mid b)$$

$$\iff \forall p \in \mathcal{P} \quad v_p(d) \leqslant v_p(a) \quad \text{et} \quad v_p(d) \leqslant v_p(b)$$

$$\iff \forall p \in \mathcal{P} \quad v_p(d) \leqslant \operatorname{Min}\{v_p(a), v_p(b)\}$$

Donc :

$$d = a \wedge b$$

$$\iff \forall p \in \mathcal{P} \quad v_p(d) = \operatorname{Min}\{v_p(a), v_p(b)\}$$

Démonstration. Pour le PPCM :

$$(a \mid m \quad \text{et} \quad b \mid m)$$

$$\iff \forall p \in \mathcal{P} \quad v_p(a) \leqslant v_p(m) \quad \text{et} \quad v_p(b) \leqslant v_p(m)$$

$$\iff \forall p \in \mathcal{P} \quad \operatorname{Max}\{v_p(a), v_p(b)\} \leqslant v_p(m)$$

Donc :

$$m = a \vee b$$

$$\iff \forall p \in \mathcal{P} \quad v_p(m) = \operatorname{Max}\{v_p(a), v_p(b)\}$$

Démonstration. Pour le PPCM :

$$(a \mid m \quad \text{et} \quad b \mid m)$$

$$\iff \forall p \in \mathcal{P} \quad v_p(a) \leqslant v_p(m) \quad \text{et} \quad v_p(b) \leqslant v_p(m)$$

$$\iff \forall p \in \mathcal{P} \quad \operatorname{Max}\{v_p(a), v_p(b)\} \leqslant v_p(m)$$

Donc :

$$m = a \vee b$$

$$\iff \forall p \in \mathcal{P} \quad v_p(m) = \operatorname{Max}\{v_p(a), v_p(b)\} \qquad \square$$

▷ Exercice 12.

Calculer la valeur exacte du PGCD de

$$15 \times 39^2 \times 77^3 \times 101 \times 10^4$$

et

$$22^2 \times 26^3 \times 91^3 \times 102 \times 10^3$$

Chapitre B4. Arithmétique

Définition

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

$$a \equiv b \ [n] \qquad \Longleftrightarrow \qquad n \mid a - b$$

On dit que a et b sont congrus modulo n,
ou a est congru à b modulo n.

Remarque

Division euclidienne de a par n :

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

Alors : $a \equiv r \ [n]$

Remarque

Division euclidienne de a par n :

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

Alors : $a \equiv r \ [n]$

Ainsi :

$$\forall a \in \mathbb{N} \qquad \exists! r \in \{0, \ldots, n-1\} \quad a \equiv r \ [n]$$

Remarque

Division euclidienne de a par n :

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

Alors : $a \equiv r \ [n]$

Ainsi :

$$\forall a \in \mathbb{N} \qquad \exists! r \in \{0, \ldots, n-1\} \quad a \equiv r \ [n]$$

Chaque classe d'équivalence de la relation de congruence modulo n est représentée par un élément de $\{0, \ldots, n-1\}$.

Proposition

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

Proposition

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

$$\forall (a, b, a', b') \in \mathbb{Z}^4$$

$$\begin{cases} a \equiv a' & [n] \\ b \equiv b' & [n] \end{cases} \Longrightarrow \begin{cases} a + b \equiv a' + b' & [n] \\ a \times b \equiv a' \times b' & [n] \end{cases}$$

Proposition

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

Démonstration. $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$

$\Longrightarrow \ \exists (k, \ell) \in \mathbb{Z}^2 \ \ a = a' + kn$ et $b = b' + \ell n$

Proposition

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

Démonstration. $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$

$\Longrightarrow \ \exists (k, \ell) \in \mathbb{Z}^2 \ \ a = a' + kn$ et $b = b' + \ell n$

$\Longrightarrow \ a + b = a' + b' + (k + \ell)n$

Proposition

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

Démonstration. $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$

$$\implies \exists (k, \ell) \in \mathbb{Z}^2 \quad a = a' + kn \quad \text{et} \quad b = b' + \ell n$$

$$\implies a + b = a' + b' + (\underbrace{k + \ell}_{\in \mathbb{Z}})n$$

$$\implies a + a' \equiv b + b' \ [n]$$

Proposition

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

Démonstration. $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$

$$\implies \exists (k, \ell) \in \mathbb{Z}^2 \quad a = a' + kn \quad \text{et} \quad b = b' + \ell n$$

$$\implies ab = a'b' + (kb' + \ell a' + k\ell n)n$$

Proposition

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

Démonstration. $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$

$$\implies \exists (k, \ell) \in \mathbb{Z}^2 \quad a = a' + kn \quad \text{et} \quad b = b' + \ell n$$

$$\implies ab = a'b' + (\underbrace{kb' + \ell a' + k\ell n}_{\in \mathbb{Z}})n$$

$$\implies ab \equiv a'b' \ [n]$$

Proposition

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

Démonstration. $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$

$$\implies \exists (k, \ell) \in \mathbb{Z}^2 \quad a = a' + kn \quad \text{et} \quad b = b' + \ell n$$

$$\implies ab = a'b' + (\underbrace{kb' + \ell a' + k\ell n}_{\in \mathbb{Z}})n$$

$$\implies ab \equiv a'b' \ [n]$$

□

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.

Le but de cet exercice est de démontrer qu'un entier naturel est différence de deux carrés si et seulement si il n'est pas congru à 2 modulo 4.

a. Quels sont les carrés modulo 4 ? En déduire le sens direct.

b. Calculer $(n+1)^2 - n^2$ et $(n+1)^2 - (n-1)^2$ et en déduire le sens indirect.

c. Écrire 27, 28 et 29 comme différence de deux carrés.

Définition

$(a, b, n) \in \mathbb{Z}^2 \times \mathbb{N}^*$. Si

$$ba \equiv 1 \ [n]$$

alors on dit que b est un inverse de a modulo n.

Définition

$(a, b, n) \in \mathbb{Z}^2 \times \mathbb{N}^*$. Si

$$ba \equiv 1 \ [n]$$

alors on dit que b est un inverse de a modulo n.

Remarque

Dans ce cas : $ax \equiv c \ [n] \iff x \equiv bc \ [n]$

Définition

$(a, b, n) \in \mathbb{Z}^2 \times \mathbb{N}^*$. Si

$$ba \equiv 1 \ [n]$$

alors on dit que b est un inverse de a modulo n.

Remarque

Dans ce cas : $ax \equiv c \ [n] \iff x \equiv bc \ [n]$

Exemple 7

Donner un inverse de 7 modulo 10 puis résoudre :

$$7x \equiv 6 \ [10]$$

Définition

$(a, b, n) \in \mathbb{Z}^2 \times \mathbb{N}^*$. Si

$$ba \equiv 1 \ [n]$$

alors on dit que b est un inverse de a modulo n.

▷ Exercice 14.

Résoudre dans $\mathbb{Z}$ les équations :

(a) $9x \equiv 7 \ [20]$

(b) $4x \equiv 5 \ [13]$

(c) $6x \equiv 5 \ [14]$

(d) $x^2 + 5x \equiv 3 \ [11]$

Théorème (petit théorème de Fermat)

Soit p un nombre premier. Alors :

$$\forall n \in \mathbb{N} \qquad n^p \equiv n \ [p]$$

Lemme

Soit p un premier. Alors :

$$\forall k = 1, \ldots, p-1 \qquad p \mid \binom{p}{k}$$

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

p											
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1
11	1	11	55	165	330	462	462	330	165	55	11	1

Lemme

Soit p un premier. Alors :

$$\forall k = 1, \ldots, p-1 \qquad p \mid \binom{p}{k}$$

Lemme

Soit p un premier. Alors :

$$\forall k = 1, \ldots, p-1 \qquad p \mid \binom{p}{k}$$

Démonstration. Soit $k \in \{1, \ldots, p-1\}$.

$$p! = \binom{p}{k} k!(p-k)!$$

Lemme

Soit p un premier. Alors :

$$\forall k = 1, \ldots, p-1 \qquad p \mid \binom{p}{k}$$

Démonstration. Soit $k \in \{1, \ldots, p-1\}$.

$$p! = \binom{p}{k} k!(p-k)!$$

Comme $1 \leqslant k \leqslant p-1$ alors $1 \leqslant p-k \leqslant p-1$.

Lemme

Soit p un premier. Alors :

$$\forall k = 1, \ldots, p-1 \qquad p \mid \binom{p}{k}$$

Démonstration. Soit $k \in \{1, \ldots, p-1\}$.

$$p! = \binom{p}{k} k!(p-k)!$$

Comme $1 \leqslant k \leqslant p-1$ alors $1 \leqslant p-k \leqslant p-1$.

Donc p ne peut diviser ni $k!$ ni $(p-k)!$.

Lemme

Soit p un premier. Alors :

$$\forall k = 1, \ldots, p-1 \qquad p \mid \binom{p}{k}$$

Démonstration. Soit $k \in \{1, \ldots, p-1\}$.

$$p \mid p! = \binom{p}{k} k!(p-k)!$$

Comme $1 \leqslant k \leqslant p-1$ alors $1 \leqslant p-k \leqslant p-1$.

Donc p ne peut diviser ni $k!$ ni $(p-k)!$.

Or p divise $p!$ donc p divise $\binom{p}{k}$. □

Théorème (petit théorème de Fermat)

Soit p un nombre premier. Alors :

$$\forall n \in \mathbb{N} \qquad n^p \equiv n \ [p]$$

Démonstration.

Théorème (petit théorème de Fermat)

Soit p un nombre premier. Alors :

$$\forall n \in \mathbb{N} \qquad n^p \equiv n \ [p]$$

Démonstration.

□

Exemple 8

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

Pour quels n a-t-on $n \mid S_n$?

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

Chapitre B4. Arithmétique

V. **Rationnels**

A. Généralités

B. Densité

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 $r \in \mathbb{Q}$ un rationnel. Alors :

$$\exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad r = \frac{p}{q} \quad \text{et} \quad p \wedge q = 1$$

Cette écriture est la forme irréductible de r.

Proposition

Soit $r \in \mathbb{Q}$ un rationnel. Alors :

$$\exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad r = \frac{p}{q} \quad \text{et} \quad p \wedge q = 1$$

Cette écriture est la forme irréductible de r.

Démonstration. Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{a}{b}$.

Proposition

Soit $r \in \mathbb{Q}$ un rationnel. Alors :

$$\exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad r = \frac{p}{q} \quad \text{et} \quad p \wedge q = 1$$

Cette écriture est la forme irréductible de r.

Démonstration. Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{a}{b}$.

Soit $\quad d = a \wedge b \qquad a' = \frac{a}{d} \qquad b' = \frac{b}{d}$

Alors : $\quad a' \wedge b' = 1 \quad$ et $\quad r = \frac{a'}{b'}$

Proposition

Soit $r \in \mathbb{Q}$ un rationnel. Alors :

$$\exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad r = \frac{p}{q} \quad \text{et} \quad p \wedge q = 1$$

Cette écriture est la forme irréductible de r.

Démonstration. Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{a}{b}$.

Soit $\quad d = a \wedge b \qquad a' = \frac{a}{d} \qquad b' = \frac{b}{d}$

Alors : $\quad a' \wedge b' = 1 \quad$ et $\quad r = \frac{a'}{b'}$

L'existence est démontrée.

Proposition

Soit $r \in \mathbb{Q}$ un rationnel. Alors :

$$\exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad r = \frac{p}{q} \quad \text{et} \quad p \wedge q = 1$$

Démonstration.

Soit $(m,n) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{m}{n}$ et $m \wedge n = 1$.

Proposition

Soit $r \in \mathbb{Q}$ un rationnel. Alors :

$$\exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad r = \frac{p}{q} \quad \text{et} \quad p \wedge q = 1$$

Démonstration.

Soit $(m,n) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{m}{n}$ et $m \wedge n = 1$.

Alors $\frac{p}{q} = \frac{m}{n}$ donc $pn = qm$.

Proposition

Soit $r \in \mathbb{Q}$ un rationnel. Alors :

$$\exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad r = \frac{p}{q} \quad \text{et} \quad p \wedge q = 1$$

Démonstration.

Soit $(m,n) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{m}{n}$ et $m \wedge n = 1$.

Alors $\frac{p}{q} = \frac{m}{n}$ donc $pn = qm$.

- $n \mid qm \quad \text{et} \quad m \wedge n = 1 \quad \Longrightarrow \quad n \mid q$
- $q \mid pn \quad \text{et} \quad p \wedge q = 1 \quad \Longrightarrow \quad q \mid n$

Proposition

Soit $r \in \mathbb{Q}$ un rationnel. Alors :

$$\exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad r = \frac{p}{q} \quad \text{et} \quad p \wedge q = 1$$

Démonstration.

Soit $(m,n) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{m}{n}$ et $m \wedge n = 1$.

Alors $\frac{p}{q} = \frac{m}{n}$ donc $pn = qm$.

- $n \mid qm \quad \text{et} \quad m \wedge n = 1 \quad \Longrightarrow \quad n \mid q$
- $q \mid pn \quad \text{et} \quad p \wedge q = 1 \quad \Longrightarrow \quad q \mid n$

Par antisymétrie $q = n$, puis $p = m$. □

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

L'ensemble des nombres décimaux est :

$$\mathbb{D} = \left\{ \frac{p}{10^n} \;\middle|\; p \in \mathbb{Z},\, n \in \mathbb{N} \right\}$$

Définition

L'ensemble des nombres décimaux est :

$$\mathbb{D} = \left\{ \frac{p}{10^n} \;\middle|\; p \in \mathbb{Z},\, n \in \mathbb{N} \right\}$$

Ce sont les nombres dont le développement décimal est fini.

Définition

L'ensemble des nombres décimaux est :

$$\mathbb{D} = \left\{ \frac{p}{10^n} \;\middle|\; p \in \mathbb{Z},\, n \in \mathbb{N} \right\}$$

Ce sont les nombres dont le développement décimal est fini.

Remarques

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

Définition

L'ensemble des nombres décimaux est :

$$\mathbb{D} = \left\{ \frac{p}{10^n} \;\middle|\; p \in \mathbb{Z},\, n \in \mathbb{N} \right\}$$

Ce sont les nombres dont le développement décimal est fini.

Remarques

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

(ii) Il est entre $\mathbb{Z}$ et $\mathbb{Q}$: $\mathbb{Z} \subsetneq \mathbb{D} \subsetneq \mathbb{Q}$

Définition

Un réel non rationnel est dit irrationnel.

Définition

Un réel non rationnel est dit irrationnel.

Exemple

Les réels e, π sont irrationnels.

Définition

Un réel non rationnel est dit irrationnel.

Exemple

Les réels e, π sont irrationnels.

Remarque

L'ensemble des irrationnels est $\mathbb{R} \setminus \mathbb{Q}$.

Proposition

$\sqrt{2}$ est irrationnel.

Proposition

$\sqrt{2}$ est irrationnel.

Démonstration.

Proposition

$\sqrt{2}$ est irrationnel.

Démonstration.

Autre démonstration : $2 = \frac{p^2}{q^2}$

$v_2(2q^2) = v_2(2) + 2v_2(q)$ est impair

$v_2(p^2) = 2v_2(p)$ est pair : contradiction. □

▷ Exercice 15.

Démontrer que $\log 3$ et $\frac{\ln 8}{\ln 7}$ sont irrationnels.

V. Rationnels

A. Généralités

B. Densité

Théorème

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

Théorème

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

Remarque

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

Théorème

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

Remarque

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

Démonstration.

Théorème

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

Remarque

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

Démonstration.

□

Théorème

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

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 $|x - r| \leqslant \varepsilon$.

Théorème

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

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.

Proposition (Autres formulations de la densité)

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

Démonstration. Soit x un réel et $\varepsilon > 0$.

Proposition (Autres formulations de la densité)

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

Démonstration. Soit x un réel et $\varepsilon > 0$.

Alors $[x - \varepsilon, x + \varepsilon]$ est un intervalle non réduit à un point.

Proposition (Autres formulations de la densité)

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

Démonstration. 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.

Proposition (Autres formulations de la densité)

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

Démonstration. 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 $|x - r| \leqslant \varepsilon$ $\square$

Proposition (Autres formulations de la densité)

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

Démonstration. Soit x un réel.

Proposition (Autres formulations de la densité)

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

Démonstration. Soit x un réel.

$\forall n \in \mathbb{N}^* : \quad \frac{1}{n} > 0 \quad$ donc $\quad \exists r_n \in \mathbb{Q} \quad |x - r_n| \leqslant \frac{1}{n}$

Proposition (Autres formulations de la densité)

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

Démonstration. Soit x un réel.

$$\forall n \in \mathbb{N}^* : \quad \frac{1}{n} > 0 \quad \text{donc} \quad \exists r_n \in \mathbb{Q} \quad |x - r_n| \leqslant \frac{1}{n}$$

La suite $(r_n)_{n\in\mathbb{N}^*}$ est une suite de rationnels, elle converge vers x.

Proposition (Autres formulations de la densité)

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

Démonstration. Soit x un réel.

$\forall n \in \mathbb{N}^* : \quad \frac{1}{n} > 0 \quad$ donc $\quad \exists r_n \in \mathbb{Q} \quad |x - r_n| \leqslant \frac{1}{n}$

La suite $(r_n)_{n\in\mathbb{N}^*}$ est une suite de rationnels, elle converge vers x.

Ceci d'après le théorème d'encadement. □

Remarque

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

Remarque

Tout intervalle non réduit à un point contient également un irrationnel.
$\mathbb{R} \setminus \mathbb{Q}$ est également dense dans $\mathbb{R}$.

Remarque

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

Démonstration.
L'intervalle $\left[\frac{a}{\sqrt{2}}, \frac{b}{\sqrt{2}}\right]$ contient un rationnel r :

$$\frac{a}{\sqrt{2}} \leqslant r \leqslant \frac{b}{\sqrt{2}}$$

Donc

$$a \leqslant r\sqrt{2} \leqslant b$$

Or $r\sqrt{2}$ n'est pas rationnel. □

Prochain chapitre

Chapitre A5
Primitives