Arithmétique dans $\mathbb{Z}$

Ensemble des entiers naturels

Définitions

On admet l'existence d'un ensemble ordonné non vide $(\mathbb{N}, \leq)$ vérifiant les trois propriétés suivantes :

Ensemble des entiers naturels

Définitions

On admet l'existence d'un ensemble ordonné non vide $(\mathbb{N}, \leq)$ vérifiant les trois propriétés suivantes :

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

Ensemble des entiers naturels

Définitions

On admet l'existence d'un ensemble ordonné non vide $(\mathbb{N}, \leq)$ vérifiant les trois propriétés suivantes :

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

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

Ensemble des entiers naturels

Définitions

On admet l'existence d'un ensemble ordonné non vide $(\mathbb{N}, \leq)$ vérifiant les trois propriétés suivantes :

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

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

iii) $\mathbb{N}$ n'a pas de plus grand élément.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné,

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré,

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n)

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x, y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x, y) \in \mathbb{N}^2$. On a $\{x, y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x, y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$ et est appelé successeur de n.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$ et est appelé successeur de n.
- Soit $n \in \mathbb{N}^\star$. On considère $A = \{k \in \mathbb{N} / k < n\}$.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$ et est appelé successeur de n.
- Soit $n \in \mathbb{N}^\star$. On considère $A = \{k \in \mathbb{N} / k < n\}$. On a $A \neq \emptyset$ (car $0 \in A$),

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$ et est appelé successeur de n.
- Soit $n \in \mathbb{N}^\star$. On considère $A = \{k \in \mathbb{N} / k < n\}$. On a $A \neq \emptyset$ (car $0 \in A$), $A \subset \mathbb{N}$

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$ et est appelé successeur de n.
- Soit $n \in \mathbb{N}^\star$. On considère $A = \{k \in \mathbb{N} / k < n\}$. On a $A \neq \emptyset$ (car $0 \in A$), $A \subset \mathbb{N}$ et A est majorée (par n)

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$ et est appelé successeur de n.
- Soit $n \in \mathbb{N}^\star$. On considère $A = \{k \in \mathbb{N} / k < n\}$. On a $A \neq \emptyset$ (car $0 \in A$), $A \subset \mathbb{N}$ et A est majorée (par n) d'où A possède un plus grand élément.

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$ et est appelé successeur de n.
- Soit $n \in \mathbb{N}^\star$. On considère $A = \{k \in \mathbb{N} / k < n\}$. On a $A \neq \emptyset$ (car $0 \in A$), $A \subset \mathbb{N}$ et A est majorée (par n) d'où A possède un plus grand élément. Ce plus grand élément de A est noté $n-1$ et

Ensemble des entiers naturels

Définitions

Remarques 1.1

- L'ensemble $\mathbb{N}$ est totalement ordonné, i.e., $\forall (x,y) \in \mathbb{N}^2$, $x \leq y$ ou $y \leq x$. En effet, soit $(x,y) \in \mathbb{N}^2$. On a $\{x,y\}$ est une partie non vide de $\mathbb{N}$ d'où $\{x,y\}$ possède un plus petit élément et ainsi x et y sont comparables.
- L'ensemble $\mathbb{N}$ n'est pas majoré, sinon, $\mathbb{N}$ possède un plus grand élément, ce qui est faux.
- 0 est le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ privé de 0 est noté $\mathbb{N}^\star$.
- Soit $n \in \mathbb{N}$. On considère $A = \{k \in \mathbb{N} / n < k\}$. On a $A \neq \emptyset$ (sinon $\mathbb{N}$ est majorée par n) et $A \subset \mathbb{N}$ d'où A possède un plus petit élément. Ce plus petit élément de A est noté $n+1$ et est appelé successeur de n.
- Soit $n \in \mathbb{N}^\star$. On considère $A = \{k \in \mathbb{N} / k < n\}$. On a $A \neq \emptyset$ (car $0 \in A$), $A \subset \mathbb{N}$ et A est majorée (par n) d'où A possède un plus grand élément. Ce plus grand élément de A est noté $n-1$ et est appelé prédécesseur de n.

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse.

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse. Alors, il existe $c \in \mathbb{N}, d \in \mathbb{N}^\star$ tels que $\forall n \in \mathbb{N} : nd < c$.

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse. Alors, il existe $c \in \mathbb{N}, d \in \mathbb{N}^\star$ tels que $\forall n \in \mathbb{N} : nd < c$. Posons $A = \{c - nd / n \in \mathbb{N}\}$.

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse. Alors, il existe $c \in \mathbb{N}, d \in \mathbb{N}^\star$ tels que $\forall n \in \mathbb{N} : nd < c$. Posons $A = \{c - nd / n \in \mathbb{N}\}$. On a A est une partie non vide de $\mathbb{N}$

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse. Alors, il existe $c \in \mathbb{N}, d \in \mathbb{N}^\star$ tels que $\forall n \in \mathbb{N} : nd < c$. Posons $A = \{c - nd / n \in \mathbb{N}\}$. On a A est une partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément.

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse. Alors, il existe $c \in \mathbb{N}, d \in \mathbb{N}^\star$ tels que $\forall n \in \mathbb{N} : nd < c$. Posons $A = \{c - nd / n \in \mathbb{N}\}$. On a A est une partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément. Soit $c - md$ le plus petit élément de A, avec $m \in \mathbb{N}$.

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse. Alors, il existe $c \in \mathbb{N}, d \in \mathbb{N}^\star$ tels que $\forall n \in \mathbb{N} : nd < c$. Posons $A = \{c - nd / n \in \mathbb{N}\}$. On a A est une partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément. Soit $c - md$ le plus petit élément de A, avec $m \in \mathbb{N}$. On a $c - (m+1)d \in A$;

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse. Alors, il existe $c \in \mathbb{N}, d \in \mathbb{N}^\star$ tels que $\forall n \in \mathbb{N} : nd < c$. Posons $A = \{c - nd / n \in \mathbb{N}\}$. On a A est une partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément. Soit $c - md$ le plus petit élément de A, avec $m \in \mathbb{N}$. On a $c - (m+1)d \in A$; cependant,
$c - (m+1)d = (c - md) - d < c - md$,

Ensemble des entiers naturels

Définitions

Théorème 1.2 (Propriété d'archimède)

$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^\star, \exists n \in \mathbb{N} : nb \geq a.$

Démonstration.

Supposons que la propriété est fausse. Alors, il existe $c \in \mathbb{N}, d \in \mathbb{N}^\star$ tels que $\forall n \in \mathbb{N} : nd < c$. Posons $A = \{c - nd / n \in \mathbb{N}\}$. On a A est une partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément. Soit $c - md$ le plus petit élément de A, avec $m \in \mathbb{N}$. On a $c - (m+1)d \in A$; cependant, $c - (m+1)d = (c - md) - d < c - md$, contradiction car $c - md$ est le plus petit élément de A. □

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{ est fausse}\}$.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{ est fausse}\}$. On a A est une partie de $\mathbb{N}$

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$. Alors, A possède un plus petit élément qu'on note m.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$. Alors, A possède un plus petit élément qu'on note m. Puisque $P(n_0)$ est vraie et $m \in A$, $m > n_0$

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$. Alors, A possède un plus petit élément qu'on note m. Puisque $P(n_0)$ est vraie et $m \in A$, $m > n_0$ d'où $m - 1 \geq n_0$.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$. Alors, A possède un plus petit élément qu'on note m. Puisque $P(n_0)$ est vraie et $m \in A$, $m > n_0$ d'où $m-1 \geq n_0$. Comme $m-1 < m$ et $m-1 \geq n_0$, $m-1 \notin A$ car m est le plus petit élément de A

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{ est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$. Alors, A possède un plus petit élément qu'on note m. Puisque $P(n_0)$ est vraie et $m \in A$, $m > n_0$ d'où $m-1 \geq n_0$. Comme $m-1 < m$ et $m-1 \geq n_0$, $m-1 \notin A$ car m est le plus petit élément de A donc $P(m-1)$ est vraie.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$. Alors, A possède un plus petit élément qu'on note m. Puisque $P(n_0)$ est vraie et $m \in A$, $m > n_0$ d'où $m-1 \geq n_0$. Comme $m-1 < m$ et $m-1 \geq n_0$, $m-1 \notin A$ car m est le plus petit élément de A donc $P(m-1)$ est vraie. Alors, d'après la deuxième propriété, $P(m)$ est vraie,

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{ est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$. Alors, A possède un plus petit élément qu'on note m. Puisque $P(n_0)$ est vraie et $m \in A$, $m > n_0$ d'où $m-1 \geq n_0$. Comme $m-1 < m$ et $m-1 \geq n_0$, $m-1 \notin A$ car m est le plus petit élément de A donc $P(m-1)$ est vraie. Alors, d'après la deuxième propriété, $P(m)$ est vraie, ce qui contredit le fait que $m \in A$.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.3 (Principe de l'induction mathématique)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si $P(n)$ est vraie, alors $P(n+1)$ est vraie,*

alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Supposons qu'il existe $k \in \mathbb{N}$ tel que $k \geq n_0$ et $P(k)$ est fausse. Posons $A = \{n \in \mathbb{N} / n \geq n_0 \text{ et } P(n) \text{ est fausse}\}$. On a A est une partie de $\mathbb{N}$ et A est non vide car $k \in A$. Alors, A possède un plus petit élément qu'on note m. Puisque $P(n_0)$ est vraie et $m \in A$, $m > n_0$ d'où $m-1 \geq n_0$. Comme $m-1 < m$ et $m-1 \geq n_0$, $m-1 \notin A$ car m est le plus petit élément de A donc $P(m-1)$ est vraie. Alors, d'après la deuxième propriété, $P(m)$ est vraie, ce qui contredit le fait que $m \in A$. Alors, Pour tout entier $n \geq n_0$, $P(n)$ est vraie. □

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *:*

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

On a $P(0)$ *est vraie car* $\sum_{k=0}^{0} k = 0$ *et* $\frac{0\times 1}{2} = 0$.

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

On a $P(0)$ *est vraie car* $\sum_{k=0}^{0} k = 0$ *et* $\frac{0\times 1}{2} = 0$. *Supposons que* $P(n)$ *est vraie à un rang* $n \in \mathbb{N}$*, i.e.,* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

On a $P(0)$ *est vraie car* $\sum_{k=0}^{0} k = 0$ *et* $\frac{0\times 1}{2} = 0$. *Supposons que* $P(n)$ *est*

vraie à un rang $n \in \mathbb{N}$*, i.e.,* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. *Alors,*

$\sum_{k=0}^{n+1} k =$

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

On a $P(0)$ *est vraie car* $\sum_{k=0}^{0} k = 0$ *et* $\frac{0\times 1}{2} = 0$. *Supposons que* $P(n)$ *est*

vraie à un rang $n \in \mathbb{N}$*, i.e.,* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. *Alors,*

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) =$$

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

On a $P(0)$ *est vraie car* $\sum_{k=0}^{0} k = 0$ *et* $\frac{0\times 1}{2} = 0$. *Supposons que* $P(n)$ *est vraie à un rang* $n \in \mathbb{N}$*, i.e.,* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. *Alors,*

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

On a $P(0)$ *est vraie car* $\sum_{k=0}^{0} k = 0$ *et* $\frac{0\times 1}{2} = 0$. *Supposons que* $P(n)$ *est vraie à un rang* $n \in \mathbb{N}$*, i.e.,* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. *Alors,*

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1) \quad \text{car d'après } P(n),$$

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2},$$

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

On a $P(0)$ *est vraie car* $\sum_{k=0}^{0} k = 0$ *et* $\frac{0\times 1}{2} = 0$. *Supposons que* $P(n)$ *est vraie à un rang* $n \in \mathbb{N}$*, i.e.,* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. *Alors,*

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1) \quad \text{car d'après } P(n),$$

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}, \quad \text{ainsi} \sum_{k=0}^{n+1} k = \frac{(n+1)(n+2)}{2} \text{ et donc } P(n+1) \text{ est vraie.}$$

Exemple 1.4

Montrons que $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *: Pour* $n \in \mathbb{N}$*, on note*

$P(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

On a $P(0)$ *est vraie car* $\sum_{k=0}^{0} k = 0$ *et* $\frac{0\times 1}{2} = 0$. *Supposons que* $P(n)$ *est*

vraie à un rang $n \in \mathbb{N}$*, i.e.,* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. *Alors,*

$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1)$ *car d'après* $P(n)$,

$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$, *ainsi* $\sum_{k=0}^{n+1} k = \frac{(n+1)(n+2)}{2}$ *et donc* $P(n+1)$ *est vraie.*

Alors, $\forall n \in \mathbb{N}, \sum^{n} k = \frac{n(n+1)}{2}$.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.5 (Récurrence à deux pas)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$.

Théorème 1.5 (Récurrence à deux pas)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ et $P(n_0+1)$ sont vraies,*

Théorème 1.5 (Récurrence à deux pas)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ et $P(n_0+1)$ sont vraies,*
2. *Pour tout entier $n \geq n_0$, $P(n)$ et $P(n+1)$ sont vraies implique $P(n+2)$ est vraie,*

Théorème 1.5 (Récurrence à deux pas)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ et $P(n_0+1)$ sont vraies,*
2. *Pour tout entier $n \geq n_0$, $P(n)$ et $P(n+1)$ sont vraies implique $P(n+2)$ est vraie,*

alors Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Ensemble des entiers naturels

Raisonnement par récurrence

Démonstration.

Posons $Q(n) = P(n) \wedge P(n+1)$.

Démonstration.

Posons $Q(n) = P(n) \wedge P(n+1)$. Puisque $P(n_0)$ et $P(n_0+1)$ sont vraies, $Q(n_0)$ est vraie.

Démonstration.

Posons $Q(n) = P(n) \wedge P(n+1)$. Puisque $P(n_0)$ et $P(n_0+1)$ sont vraies, $Q(n_0)$ est vraie. Soit $n \geq n_0$. Supposons que $Q(n)$ est vraie.

Démonstration.

Posons $Q(n) = P(n) \wedge P(n+1)$. Puisque $P(n_0)$ et $P(n_0+1)$ sont vraies, $Q(n_0)$ est vraie. Soit $n \geq n_0$. Supposons que $Q(n)$ est vraie. Alors, $P(n)$ et $P(n+1)$ sont vraies

Démonstration.

Posons $Q(n) = P(n) \wedge P(n+1)$. Puisque $P(n_0)$ et $P(n_0+1)$ sont vraies, $Q(n_0)$ est vraie. Soit $n \geq n_0$. Supposons que $Q(n)$ est vraie. Alors, $P(n)$ et $P(n+1)$ sont vraies d'où $P(n+2)$ est vraie

Démonstration.

Posons $Q(n) = P(n) \wedge P(n+1)$. Puisque $P(n_0)$ et $P(n_0+1)$ sont vraies, $Q(n_0)$ est vraie. Soit $n \geq n_0$. Supposons que $Q(n)$ est vraie. Alors, $P(n)$ et $P(n+1)$ sont vraies d'où $P(n+2)$ est vraie ainsi $Q(n+1)$ est vraie

Démonstration.

Posons $Q(n) = P(n) \wedge P(n+1)$. Puisque $P(n_0)$ et $P(n_0+1)$ sont vraies, $Q(n_0)$ est vraie. Soit $n \geq n_0$. Supposons que $Q(n)$ est vraie. Alors, $P(n)$ et $P(n+1)$ sont vraies d'où $P(n+2)$ est vraie ainsi $Q(n+1)$ est vraie et donc, d'après le Principe de l'induction mathématique, pour tout entier $n \geq n_0$, $Q(n)$ est vraie,

Démonstration.

Posons $Q(n) = P(n) \wedge P(n+1)$. Puisque $P(n_0)$ et $P(n_0+1)$ sont vraies, $Q(n_0)$ est vraie. Soit $n \geq n_0$. Supposons que $Q(n)$ est vraie. Alors, $P(n)$ et $P(n+1)$ sont vraies d'où $P(n+2)$ est vraie ainsi $Q(n+1)$ est vraie et donc, d'après le Principe de l'induction mathématique, pour tout entier $n \geq n_0$, $Q(n)$ est vraie, alors pour tout entier $n \geq n_0$, $P(n)$ est vraie. □

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$:

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.
On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$.

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$. On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$. Aussi, $P(1)$ est vraie car $u_1 = 5$ et $2^1 + 3^1 = 5$.

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.
On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$. Aussi, $P(1)$ est vraie car $u_1 = 5$ et $2^1 + 3^1 = 5$.
Supposons que $P(n)$ et $P(n+1)$ sont vraies à un rang $n \in \mathbb{N}$.

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.
On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$. Aussi, $P(1)$ est vraie car $u_1 = 5$ et $2^1 + 3^1 = 5$.
Supposons que $P(n)$ et $P(n+1)$ sont vraies à un rang $n \in \mathbb{N}$. On a $u_{n+2} = 5u_{n+1} - 6u_n$,

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.
On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$. Aussi, $P(1)$ est vraie car $u_1 = 5$ et $2^1 + 3^1 = 5$.
Supposons que $P(n)$ et $P(n+1)$ sont vraies à un rang $n \in \mathbb{N}$. On a $u_{n+2} = 5u_{n+1} - 6u_n$, alors $u_{n+2} = 5(2^{n+1} + 3^{n+1}) - 6(2^n + 3^n)$ car $u_{n+1} = 2^{n+1} + 3^{n+1}$ et $u_n = 2^n + 3^n$.

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.
On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$. Aussi, $P(1)$ est vraie car $u_1 = 5$ et $2^1 + 3^1 = 5$.
Supposons que $P(n)$ et $P(n+1)$ sont vraies à un rang $n \in \mathbb{N}$. On a $u_{n+2} = 5u_{n+1} - 6u_n$, alors $u_{n+2} = 5(2^{n+1} + 3^{n+1}) - 6(2^n + 3^n)$ car $u_{n+1} = 2^{n+1} + 3^{n+1}$ et $u_n = 2^n + 3^n$. Ainsi,
$u_{n+2} = 5.2^{n+1} + 5.3^{n+1} - 3.2^{n+1} - 2.3^{n+1} =$

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.
On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$. Aussi, $P(1)$ est vraie car $u_1 = 5$ et $2^1 + 3^1 = 5$.
Supposons que $P(n)$ et $P(n+1)$ sont vraies à un rang $n \in \mathbb{N}$. On a $u_{n+2} = 5u_{n+1} - 6u_n$, alors $u_{n+2} = 5(2^{n+1} + 3^{n+1}) - 6(2^n + 3^n)$ car $u_{n+1} = 2^{n+1} + 3^{n+1}$ et $u_n = 2^n + 3^n$. Ainsi,
$u_{n+2} = 5.2^{n+1} + 5.3^{n+1} - 3.2^{n+1} - 2.3^{n+1} = 2^{n+2} + 3^{n+2}$

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.
On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$. Aussi, $P(1)$ est vraie car $u_1 = 5$ et $2^1 + 3^1 = 5$.
Supposons que $P(n)$ et $P(n+1)$ sont vraies à un rang $n \in \mathbb{N}$. On a $u_{n+2} = 5u_{n+1} - 6u_n$, alors $u_{n+2} = 5(2^{n+1} + 3^{n+1}) - 6(2^n + 3^n)$ car $u_{n+1} = 2^{n+1} + 3^{n+1}$ et $u_n = 2^n + 3^n$. Ainsi,
$u_{n+2} = 5.2^{n+1} + 5.3^{n+1} - 3.2^{n+1} - 2.3^{n+1} = 2^{n+2} + 3^{n+2}$ donc $P(n+2)$ est vraie.

Exemple 1.6

Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrons par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$: Pour $n \in \mathbb{N}$, on note $P(n) : u_n = 2^n + 3^n$.
On a $P(0)$ est vraie car $u_0 = 2$ et $2^0 + 3^0 = 2$. Aussi, $P(1)$ est vraie car $u_1 = 5$ et $2^1 + 3^1 = 5$.
Supposons que $P(n)$ et $P(n+1)$ sont vraies à un rang $n \in \mathbb{N}$. On a $u_{n+2} = 5u_{n+1} - 6u_n$, alors $u_{n+2} = 5(2^{n+1} + 3^{n+1}) - 6(2^n + 3^n)$ car $u_{n+1} = 2^{n+1} + 3^{n+1}$ et $u_n = 2^n + 3^n$. Ainsi,
$u_{n+2} = 5.2^{n+1} + 5.3^{n+1} - 3.2^{n+1} - 2.3^{n+1} = 2^{n+2} + 3^{n+2}$ donc $P(n+2)$ est vraie. Alors, $\forall n \in \mathbb{N}$, $u_n = 2^n + 3^n$.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.7 (Récurrence forte)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.7 (Récurrence forte)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*

Théorème 1.7 (Récurrence forte)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si pour tout entier k tel que $n_0 \leq k \leq n$, $P(k)$ est vraie implique $P(n+1)$ est vraie,*

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.7 (Récurrence forte)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si pour tout entier k tel que $n_0 \leq k \leq n$, $P(k)$ est vraie implique $P(n+1)$ est vraie,*

alors Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Ensemble des entiers naturels

Raisonnement par récurrence

Théorème 1.7 (Récurrence forte)

Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si pour tout entier k tel que $n_0 \leq k \leq n$, $P(k)$ est vraie implique $P(n+1)$ est vraie,*

alors Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration.

Comme pour la démonstration du théorème précédent, il suffit de considérer $Q(n) = P(n_0) \wedge \ldots \wedge P(n)$ et appliquer le Principe de l'induction mathématique à $Q(n)$. □

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$:

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k, m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies.

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies.
Montrons que $P(n+1)$ est vraie :

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies.
Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair,

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies.
Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies.
Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair,

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$ et on a $1 \leq q \leq n$

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$ et on a $1 \leq q \leq n$ ainsi $P(q)$ est vraie,

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$ et on a $1 \leq q \leq n$ ainsi $P(q)$ est vraie, i.e., il existe $(k', m) \in \mathbb{N}^2$ tel que $q = 2^{k'}(2m+1)$

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$ et on a $1 \leq q \leq n$ ainsi $P(q)$ est vraie, i.e., il existe $(k', m) \in \mathbb{N}^2$ tel que $q = 2^{k'}(2m+1)$ d'où $n+1 =$

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$ et on a $1 \leq q \leq n$ ainsi $P(q)$ est vraie, i.e., il existe $(k', m) \in \mathbb{N}^2$ tel que $q = 2^{k'}(2m+1)$ d'où $n+1 = 2q =$

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$ et on a $1 \leq q \leq n$ ainsi $P(q)$ est vraie, i.e., il existe $(k', m) \in \mathbb{N}^2$ tel que $q = 2^{k'}(2m+1)$ d'où $n+1 = 2q = 2.2^{k'}(2m+1)$

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$ et on a $1 \leq q \leq n$ ainsi $P(q)$ est vraie, i.e., il existe $(k', m) \in \mathbb{N}^2$ tel que $q = 2^{k'}(2m+1)$ d'où $n+1 = 2q = 2.2^{k'}(2m+1)$ et ainsi il existe $k = k'+1, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.

Exemple 1.8

Soit n un entier naturel non nul. Montrons par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$: pour tout $n \in \mathbb{N}^\star$, on note $P(n)$ la proposition : il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
On a $P(1)$ est vraie car il existe $k = 0, m = 0 \in \mathbb{N}$ tels que $1 = 2^k(2m+1)$.
Soit $n \in \mathbb{N}^\star$ fixé. On suppose que $P(1), P(2), \ldots, P(n)$ sont vraies. Montrons que $P(n+1)$ est vraie :
Si $n+1$ est impair, alors il existe $m \in \mathbb{N}$ tel que $n+1 = 2m+1$ ainsi il existe $k = 0, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$.
Si $n+1$ est pair, alors $q = \frac{n+1}{2} \in \mathbb{N}^\star$ et on a $1 \leq q \leq n$ ainsi $P(q)$ est vraie, i.e., il existe $(k', m) \in \mathbb{N}^2$ tel que $q = 2^{k'}(2m+1)$ d'où $n+1 = 2q = 2.2^{k'}(2m+1)$ et ainsi il existe $k = k'+1, m \in \mathbb{N}$ tels que $n+1 = 2^k(2m+1)$. Alors, $\forall n \in \mathbb{N}^\star$, il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.1 (Théorème de la division euclidienne dans $\mathbb{Z}$)

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.1 (Théorème de la division euclidienne dans $\mathbb{Z}$)

$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$,

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.1 (Théorème de la division euclidienne dans $\mathbb{Z}$)

$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}, \exists ! (q,r) \in \mathbb{Z}^2$ *tel que* $a = bq + r$, *avec* $0 \leq r < |b|$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.1 (Théorème de la division euclidienne dans $\mathbb{Z}$)

$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}, \exists ! (q,r) \in \mathbb{Z}^2$ *tel que* $a = bq + r$, *avec* $0 \leq r < |b|$.
q est appelé ***quotient*** *de la division euclidienne de a par b et r est* ***le reste***.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$.

- Si $b > 0$:

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$,

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb =$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a|$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$,

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors,
  $a - (q+1)b =$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b =$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.
  Cependant, $a - (q+1)b =$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.
  Cependant, $a - (q+1)b = r - b < r$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.
  Cependant, $a - (q+1)b = r - b < r$ ce qui contredit le fait que r est le plus petit élément de A.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \text{ et } a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.
  Cependant, $a - (q+1)b = r - b < r$ ce qui contredit le fait que r est le plus petit élément de A. Ainsi, on a montré qu'il existe $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b = |b|$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \, et \, a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.
  Cependant, $a - (q+1)b = r - b < r$ ce qui contredit le fait que r est le plus petit élément de A. Ainsi, on a montré qu'il existe $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b = |b|$.
- Si $b < 0$:

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \text{ et } a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.
  Cependant, $a - (q+1)b = r - b < r$ ce qui contredit le fait que r est le plus petit élément de A. Ainsi, on a montré qu'il existe $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b = |b|$.
- Si $b < 0$: on a $-b > 0$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \text{ et } a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.
  Cependant, $a - (q+1)b = r - b < r$ ce qui contredit le fait que r est le plus petit élément de A. Ainsi, on a montré qu'il existe $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b = |b|$.
- Si $b < 0$: on a $-b > 0$. Alors, en appliquant le cas précédent, il existe $(q', r') \in \mathbb{Z}^2$ tel que $a = (-b)q' + r'$ avec $0 \leq r' < -b$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

- Si $b > 0$: on considère $A = \{a - xb / x \in \mathbb{Z} \text{ et } a - xb \geq 0\}$. On a $A \neq \emptyset$, en effet, puisque $b \geq 1$, $|a|b \geq |a|$ ainsi, en prenant $x = -|a|$, on a $a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$ d'où $a - xb \in A$. Alors, A est une partie non vide de $\mathbb{N}$ et donc A possède un plus petit élément qu'on note r. Puisque $r \in A$, $r = a - qb$, où $q \in \mathbb{Z}$. Aussi, puisque $r \in A$, $r \geq 0$.
  On a aussi $r < b$, en effet : supposons que $b \leq r$. Alors, $a - (q+1)b = (a - qb) - b = r - b \geq 0$ d'où $a - (q+1)b \in A$.
  Cependant, $a - (q+1)b = r - b < r$ ce qui contredit le fait que r est le plus petit élément de A. Ainsi, on a montré qu'il existe $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b = |b|$.
- Si $b < 0$: on a $-b > 0$. Alors, en appliquant le cas précédent, il existe $(q', r') \in \mathbb{Z}^2$ tel que $a = (-b)q' + r'$ avec $0 \leq r' < -b$ et donc il exsite $q = -q', r = r' \in \mathbb{Z}$ tels que $a = bq + r$ avec $0 < r < -b = |b|$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Unicité :

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Unicité : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Unicité : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q, r), (q', r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$.

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors,
$r - r' = b(q' - q)$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$.

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$,

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$, $-|b| < r - r' < |b|$

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$, $-|b| < r - r' < |b|$ ainsi $|r - r'| < |b|$

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$, $-|b| < r - r' < |b|$ ainsi $|r - r'| < |b|$ d'où $|b||q' - q| < |b|$.

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$, $-|b| < r - r' < |b|$ ainsi $|r - r'| < |b|$ d'où $|b||q' - q| < |b|$. Alors, $|q' - q| = 0$

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$, $-|b| < r - r' < |b|$ ainsi $|r - r'| < |b|$ d'où $|b||q' - q| < |b|$. Alors, $|q' - q| = 0$ ainsi $q - q' = 0$

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$, $-|b| < r - r' < |b|$ ainsi $|r - r'| < |b|$ d'où $|b||q' - q| < |b|$. Alors, $|q' - q| = 0$ ainsi $q - q' = 0$ donc $q' = q$.

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$, $-|b| < r - r' < |b|$ ainsi $|r - r'| < |b|$ d'où $|b||q' - q| < |b|$. Alors, $|q' - q| = 0$ ainsi $q - q' = 0$ donc $q' = q$. Comme $|r - r'| = |b||q' - q|$ et $q = q'$,

Démonstration.

Unicité : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. Supposons qu'il existe $(q,r),(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors, $r - r' = b(q' - q)$ d'où $|r - r'| = |b||q' - q|$. Comme $0 \leq r < |b|$ et $-|b| < -r' \leq 0$, $-|b| < r - r' < |b|$ ainsi $|r - r'| < |b|$ d'où $|b||q' - q| < |b|$. Alors, $|q' - q| = 0$ ainsi $q - q' = 0$ donc $q' = q$. Comme $|r - r'| = |b||q' - q|$ et $q = q'$, $r' = r$. □

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.

Si $a < b$,

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.

Si $a < b$, on a $q = 0$ et $r = a$ car $a = 0 \times b + a$ avec $0 \leq r < b$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.

Si $a < b$, on a $q = 0$ et $r = a$ car $a = 0 \times b + a$ avec $0 \leq r < b$.

Si $a \geq b$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.

Si $a < b$, on a $q = 0$ et $r = a$ car $a = 0 \times b + a$ avec $0 \leq r < b$.

Si $a \geq b$. D'après le thóerème de la division euclidienne dans $\mathbb{Z}$, il existe un, et un seul, $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec avec $0 \leq r < |b| = b$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.

Si $a < b$, on a $q = 0$ et $r = a$ car $a = 0 \times b + a$ avec $0 \leq r < b$.

Si $a \geq b$. D'après le thóerème de la division euclidienne dans $\mathbb{Z}$, il existe un, et un seul, $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec avec $0 \leq r < |b| = b$ ainsi $r \in \mathbb{N}$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.

Si $a < b$, on a $q = 0$ et $r = a$ car $a = 0 \times b + a$ avec $0 \leq r < b$.

Si $a \geq b$. D'après le thóerème de la division euclidienne dans $\mathbb{Z}$, il existe un, et un seul, $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec avec $0 \leq r < |b| = b$ ainsi $r \in \mathbb{N}$. Aussi, on a $a > r$ car $b > r$,

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.

Si $a < b$, on a $q = 0$ et $r = a$ car $a = 0 \times b + a$ avec $0 \leq r < b$.

Si $a \geq b$. D'après le thóerème de la division euclidienne dans $\mathbb{Z}$, il existe un, et un seul, $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec avec $0 \leq r < |b| = b$ ainsi $r \in \mathbb{N}$. Aussi, on a $a > r$ car $b > r$, donc $bq = a - r > 0$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Théorème 2.2 (Théorème de la division euclidienne dans $\mathbb{N}$)

$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists ! (q,r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = bq + r$, *avec* $0 \leq r < b$.

Démonstration.

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$.
Si $a < b$, on a $q = 0$ et $r = a$ car $a = 0 \times b + a$ avec $0 \leq r < b$.
Si $a \geq b$. D'après le thóerème de la division euclidienne dans $\mathbb{Z}$, il existe un, et un seul, $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec avec $0 \leq r < |b| = b$ ainsi $r \in \mathbb{N}$. Aussi, on a $a > r$ car $b > r$, donc $bq = a - r > 0$ et puisque $b \in \mathbb{N}^\star$, on a $q \in \mathbb{N}$. □

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Remarque 2.3

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Remarque 2.3

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$.

Remarque 2.3

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$

Remarque 2.3

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$

Remarque 2.3

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$,

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q + 1$

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$ et $r = a - b.E(\frac{a}{b})$.

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$ et $r = a - b.E(\frac{a}{b})$.
2. Si $b < 0$.

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$ et $r = a - b.E(\frac{a}{b})$.
2. Si $b < 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < -b$

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$ et $r = a - b.E(\frac{a}{b})$.
2. Si $b < 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < -b$ d'où $-\frac{a}{b} = (-q) + (-\frac{r}{b})$ avec $0 \leq -\frac{r}{b} < 1$

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$ et $r = a - b.E(\frac{a}{b})$.
2. Si $b < 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < -b$ d'où $-\frac{a}{b} = (-q) + (-\frac{r}{b})$ avec $0 \leq -\frac{r}{b} < 1$ ainsi $0 \leq -\frac{a}{b} + q < 1$,

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$ et $r = a - b.E(\frac{a}{b})$.
2. Si $b < 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < -b$ d'où $-\frac{a}{b} = (-q) + (-\frac{r}{b})$ avec $0 \leq -\frac{r}{b} < 1$ ainsi $0 \leq -\frac{a}{b} + q < 1$, i.e., $-q \leq -\frac{a}{b} < -q+1$

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$ et $r = a - b.E(\frac{a}{b})$.
2. Si $b < 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < -b$ d'où $-\frac{a}{b} = (-q) + (-\frac{r}{b})$ avec $0 \leq -\frac{r}{b} < 1$ ainsi $0 \leq -\frac{a}{b} + q < 1$, i.e., $-q \leq -\frac{a}{b} < -q+1$ et donc $q = -E(-\frac{a}{b})$

Remarque 2.3

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^{\star}$.

1. Si $b > 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < b$ d'où $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < 1$ ainsi $0 \leq \frac{a}{b} - q < 1$, i.e., $q \leq \frac{a}{b} < q+1$ et donc $q = E(\frac{a}{b})$ et $r = a - b.E(\frac{a}{b})$.
2. Si $b < 0$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < -b$ d'où $-\frac{a}{b} = (-q) + (-\frac{r}{b})$ avec $0 \leq -\frac{r}{b} < 1$ ainsi $0 \leq -\frac{a}{b} + q < 1$, i.e., $-q \leq -\frac{a}{b} < -q+1$ et donc $q = -E(-\frac{a}{b})$ et $r = a + b.E(-\frac{a}{b})$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Exemples 2.4

1. *Pour* $a = 2015$ *et* $b = 15$,

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Exemples 2.4

1. *Pour* $a = 2015$ *et* $b = 15$, *on a* $q = E(\frac{a}{b}) = 134$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Exemples 2.4

1. *Pour* $a = 2015$ *et* $b = 15$, *on a* $q = E(\frac{a}{b}) = 134$ *et* $r = a - bq = 5$.

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Exemples 2.4

1. *Pour* $a = 2015$ *et* $b = 15$, *on a* $q = E(\frac{a}{b}) = 134$ *et* $r = a - bq = 5$.
2. *Pour* $a = 2016$ *et* $b = -67$,

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Exemples 2.4

1. *Pour* $a = 2015$ *et* $b = 15$, *on a* $q = E(\frac{a}{b}) = 134$ *et* $r = a - bq = 5$.
2. *Pour* $a = 2016$ *et* $b = -67$, *on a* $q = -[-\frac{a}{b}] = -30$

Divisibilité dans $\mathbb{Z}$

Théorème de la division euclidienne

Exemples 2.4

1. *Pour* $a = 2015$ *et* $b = 15$, *on a* $q = E(\frac{a}{b}) = 134$ *et* $r = a - bq = 5$.
2. *Pour* $a = 2016$ *et* $b = -67$, *on a* $q = -[-\frac{a}{b}] = -30$ *et* $r = a - bq = 16$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Définition 2.5

Soit $a, b \in \mathbb{Z}$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Définition 2.5

Soit $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Définition 2.5

Soit $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $c \in \mathbb{Z}$ tel que $b = ac$. Lorsque a divise b, on écrit $a \mid b$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Définition 2.5

Soit $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $c \in \mathbb{Z}$ tel que $b = ac$. Lorsque a divise b, on écrit $a \mid b$.

Remarque 2.6

Soit $a, b \in \mathbb{Z}$. Si a divise b, on dit que a est un diviseur de b

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Définition 2.5

Soit $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $c \in \mathbb{Z}$ tel que $b = ac$. Lorsque a divise b, on écrit $a \mid b$.

Remarque 2.6

Soit $a, b \in \mathbb{Z}$. Si a divise b, on dit que a est un diviseur de b ou b est un multiple de a

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Définition 2.5

Soit $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $c \in \mathbb{Z}$ tel que $b = ac$. Lorsque a divise b, on écrit $a \mid b$.

Remarque 2.6

Soit $a, b \in \mathbb{Z}$. Si a divise b, on dit que a est un diviseur de b ou b est un multiple de a ou b est divisible par a.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Propriétés 2.7

Soit a, b, c et d des entiers.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Propriétés 2.7

Soit a, b, c et d des entiers.

1) $a \mid 0$ *et si* $0 \mid b$, *alors* $b = 0$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Propriétés 2.7

Soit a, b, c et d des entiers.

1) $a \mid 0$ *et si* $0 \mid b$, *alors* $b = 0$.
2) $a \mid 1$ *si, et seulement si,* $a = \pm 1$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Propriétés 2.7

Soit a, b, c et d des entiers.

1) $a \mid 0$ *et si* $0 \mid b$, *alors* $b = 0$.
2) $a \mid 1$ *si, et seulement si,* $a = \pm 1$.
3) $a \mid b$ *et* $b \mid a$ *si, et seulement si,* $a = \pm b$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Propriétés 2.7

Soit a, b, c et d des entiers.

1) $a \mid 0$ *et si* $0 \mid b$, *alors* $b = 0$.
2) $a \mid 1$ *si, et seulement si,* $a = \pm 1$.
3) $a \mid b$ *et* $b \mid a$ *si, et seulement si,* $a = \pm b$.
4) *Si* $a \mid b$ *et* $c \mid d$, *alors* $ac \mid bd$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Propriétés 2.7

Soit a, b, c et d des entiers.

1) $a \mid 0$ *et si* $0 \mid b$, *alors* $b = 0$.
2) $a \mid 1$ *si, et seulement si,* $a = \pm 1$.
3) $a \mid b$ *et* $b \mid a$ *si, et seulement si,* $a = \pm b$.
4) *Si* $a \mid b$ *et* $c \mid d$, *alors* $ac \mid bd$.
5) *Si* $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Propriétés 2.7

Soit a, b, c et d des entiers.

1) $a \mid 0$ *et si* $0 \mid b$, *alors* $b = 0$.
2) $a \mid 1$ *si, et seulement si,* $a = \pm 1$.
3) $a \mid b$ *et* $b \mid a$ *si, et seulement si,* $a = \pm b$.
4) *Si* $a \mid b$ *et* $c \mid d$, *alors* $ac \mid bd$.
5) *Si* $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$.
6) *Si* $a \mid b$ *et* $b \neq 0$, *alors* $|a| \leq |b|$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Propriétés 2.7

Soit a, b, c et d des entiers.

1) $a \mid 0$ *et si* $0 \mid b$, *alors* $b = 0$.
2) $a \mid 1$ *si, et seulement si,* $a = \pm 1$.
3) $a \mid b$ *et* $b \mid a$ *si, et seulement si,* $a = \pm b$.
4) *Si* $a \mid b$ *et* $c \mid d$, *alors* $ac \mid bd$.
5) *Si* $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$.
6) *Si* $a \mid b$ *et* $b \neq 0$, *alors* $|a| \leq |b|$.
7) *Si* $a \mid b$ *et* $a \mid c$ *; alors pour tout* $(x, y) \in \mathbb{Z}$, $a \mid bx + cy$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$;

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $a = kb$

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $a = kb$ d'où $a = kha$

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $a = kb$ d'où $a = kha$ ainsi $hk = 1$ donc $h = \pm 1$ et par suite $a = \pm b$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $a = kb$ d'où $a = kha$ ainsi $hk = 1$ donc $h = \pm 1$ et par suite $a = \pm b$.
- Montrons 6) : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$ tels que $a \mid b$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $a = kb$ d'où $a = kha$ ainsi $hk = 1$ donc $h = \pm 1$ et par suite $a = \pm b$.
- Montrons 6) : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$ tels que $a \mid b$. Alors, il existe $h \in \mathbb{Z}$ tel que $b = ha$

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $a = kb$ d'où $a = kha$ ainsi $hk = 1$ donc $h = \pm 1$ et par suite $a = \pm b$.
- Montrons 6) : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$ tels que $a \mid b$. Alors, il existe $h \in \mathbb{Z}$ tel que $b = ha$ d'où $h \neq 0$

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $a = kb$ d'où $a = kha$ ainsi $hk = 1$ donc $h = \pm 1$ et par suite $a = \pm b$.
- Montrons 6) : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$ tels que $a \mid b$. Alors, il existe $h \in \mathbb{Z}$ tel que $b = ha$ d'où $h \neq 0$ donc $|b| = |h||a| \geq |a|$ car $|h| \geq 1$.

Démonstration.

Les propriétés 1), 4) et 5) sont évidentes.

- Montrons 2) : Soit $a \in \mathbb{Z}$. Il est évident que si $a = \pm 1$, alors $a \mid 1$. Réciproquement, supposons que $a \mid 1$. Alors, il existe $k \in \mathbb{Z} : 1 = ka$ d'où $1 = |k||a|$ ainsi $|a| \leq 1$; sinon, $|a| > 1$ et par suite $|k||a| > |k| \geq 1$. Alors, $|a| = 1$;
- Montrons 3) : Soit $a, b \in \mathbb{Z}$. Il est évident que si $a = \pm b$, alors $a \mid b$ et $b \mid a$. Réciproquement, supposons que $a \mid b$ et $b \mid a$. Si $a = 0$, alors $b = 0$ car $a \mid b$. Supposons que $a \neq 0$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $a = kb$ d'où $a = kha$ ainsi $hk = 1$ donc $h = \pm 1$ et par suite $a = \pm b$.
- Montrons 6) : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$ tels que $a \mid b$. Alors, il existe $h \in \mathbb{Z}$ tel que $b = ha$ d'où $h \neq 0$ donc $|b| = |h||a| \geq |a|$ car $|h| \geq 1$.

Démonstration.

- Montrons 7) : Soit $(a, b, c) \in \mathbb{Z}^3$ tel que $a \mid b$ et $a \mid c$.

Démonstration.

- Montrons 7) : Soit $(a, b, c) \in \mathbb{Z}^3$ tel que $a \mid b$ et $a \mid c$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $c = ka$

Démonstration.

- Montrons 7) : Soit $(a, b, c) \in \mathbb{Z}^3$ tel que $a \mid b$ et $a \mid c$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $c = ka$ ainsi $\forall x, y \in \mathbb{Z}$,
  $bx + cy =$

Démonstration.

- Montrons 7) : Soit $(a, b, c) \in \mathbb{Z}^3$ tel que $a \mid b$ et $a \mid c$. Alors, il existe $h, k \in \mathbb{Z}$ tels que $b = ha$ et $c = ka$ ainsi $\forall x, y \in \mathbb{Z}$,
  $bx + cy = xha + yka =$

Démonstration.

- Montrons 7) : Soit $(a,b,c) \in \mathbb{Z}^3$ tel que $a \mid b$ et $a \mid c$. Alors, il existe $h,k \in \mathbb{Z}$ tels que $b = ha$ et $c = ka$ ainsi $\forall x,y \in \mathbb{Z}$, $bx + cy = xha + yka = (xh + yk)a$

Démonstration.

- Montrons 7) : Soit $(a,b,c) \in \mathbb{Z}^3$ tel que $a \mid b$ et $a \mid c$. Alors, il existe $h,k \in \mathbb{Z}$ tels que $b = ha$ et $c = ka$ ainsi $\forall x,y \in \mathbb{Z}$, $bx+cy = xha+yka = (xh+yk)a$ et donc $a \mid bx+cy$.

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Remarque 2.8

La relation de divisibilité dans $\mathbb{Z}$ est réflexive

Divisibilité dans $\mathbb{Z}$

Relation de Divisibilité

Remarque 2.8

La relation de divisibilité dans $\mathbb{Z}$ est réflexive et transitive

Remarque 2.8

La relation de divisibilité dans $\mathbb{Z}$ est réflexive et transitive mais n'est pas antisymétrique.

Théorème et définition 2.9

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

Théorème et définition 2.9

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *Il existe un unique entier positif* d *tel que*

Théorème et définition 2.9

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. Il existe un unique entier positif d tel que

1) $d \mid a$ et $d \mid b$,

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème et définition 2.9

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. Il existe un unique entier positif d tel que

1) $d \mid a$ *et* $d \mid b$,
2) *Si c est un entier tel que c divise a et c divise b, alors $c \leq d$.*

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème et définition 2.9

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. Il existe un unique entier positif d tel que

1) *$d \mid a$ et $d \mid b$,*
2) *Si c est un entier tel que c divise a et c divise b, alors $c \leq d$.*

L'entier naturel d est appelé ***le plus grand commun diviseur*** *de a et b.*

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème et définition 2.9

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. Il existe un unique entier positif d tel que

1) *$d \mid a$ et $d \mid b$,*
2) *Si c est un entier tel que c divise a et c divise b, alors $c \leq d$.*

L'entier naturel d est appelé ***le plus grand commun diviseur*** *de a et b. d est noté $a \wedge b$ ou $d = pgcd(a,b)$.*

Démonstration.

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

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax + by / (x,y) \in \mathbb{Z}^2 \text{ et } ax + by > 0\}$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by / (x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$),

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax + b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés :

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$,

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque

$r = a - qd =$

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque

$r = a - qd = a - q(au+bv) =$

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque

$$r = a - qd = a - q(au+bv) = a(1-qu)+b(-qv),$$

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque

$r = a - qd = a - q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$;

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque $r = a - qd = a - q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$; sinon, $r \in A$

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque $r = a-qd = a-q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$; sinon, $r \in A$ et $r < d$ ce qui contredit le fait que d est le plus petit élément de A.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque $r = a-qd = a-q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$; sinon, $r \in A$ et $r < d$ ce qui contredit le fait que d est le plus petit élément de A. Puisque $r = 0$, $a = qd$

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque $r = a-qd = a-q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$; sinon, $r \in A$ et $r < d$ ce qui contredit le fait que d est le plus petit élément de A. Puisque $r = 0$, $a = qd$ et donc $d \mid a$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque $r = a-qd = a-q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$; sinon, $r \in A$ et $r < d$ ce qui contredit le fait que d est le plus petit élément de A. Puisque $r = 0$, $a = qd$ et donc $d \mid a$. De la même façon, on vérifie que $d \mid b$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque $r = a-qd = a-q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$; sinon, $r \in A$ et $r < d$ ce qui contredit le fait que d est le plus petit élément de A. Puisque $r = 0$, $a = qd$ et donc $d \mid a$. De la même façon, on vérifie que $d \mid b$.

Soit c un entier tel que c divise a et c divise b. Montrons que $c \leq d$:

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque $r = a-qd = a-q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$; sinon, $r \in A$ et $r < d$ ce qui contredit le fait que d est le plus petit élément de A. Puisque $r = 0$, $a = qd$ et donc $d \mid a$. De la même façon, on vérifie que $d \mid b$.

Soit c un entier tel que c divise a et c divise b. Montrons que $c \leq d$: Puisque $c \mid a$ et $c \mid b$, $c \mid au+bv = d$

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On considère l'ensemble $A = \{ax+by/(x,y) \in \mathbb{Z}^2 \text{ et } ax+by > 0\}$. Supposons que $a \neq 0$ (de même si $b \neq 0$), alors $|a| = ax+b.0$ avec $x = 1$ si $a > 0$ et $x = -1$ si $a < 0$, et $|a| > 0$ donc $|a| \in A$ et ainsi $A \neq \emptyset$. Comme A est une partie de $\mathbb{N}$ non vide, A possède un plus petit élément qu'on note d. Ainsi, il existe $(u,v) \in \mathbb{Z}^2 : d = au+bv > 0$.

Montrons que d vérifie les deux propriétés : On a $d \mid a$, en effet : d'après le théorème de la division euclidienne, il existe $(q,r) \in \mathbb{Z}^2 : a = qd+r$ avec $0 \leq r < |d| = d$. Puisque $r = a-qd = a-q(au+bv) = a(1-qu)+b(-qv)$, $r = 0$; sinon, $r \in A$ et $r < d$ ce qui contredit le fait que d est le plus petit élément de A. Puisque $r = 0$, $a = qd$ et donc $d \mid a$. De la même façon, on vérifie que $d \mid b$.

Soit c un entier tel que c divise a et c divise b. Montrons que $c \leq d$: Puisque $c \mid a$ et $c \mid b$, $c \mid au+bv = d$ d'où $|c| \leq d$ et par suite $c \leq d$. □

Démonstration.

Unicité : Soit $d, d' \in \mathbb{N}$ tels que d et d' vérifient les deux propriétés :

Démonstration.

Unicité : Soit $d, d' \in \mathbb{N}$ tels que d et d' vérifient les deux propriétés : On a $d' \mid a$ et $d' \mid b$ (car d' vérifie 1))

Démonstration.

Unicité : Soit $d, d' \in \mathbb{N}$ tels que d et d' vérifient les deux propriétés : On a $d' \mid a$ et $d' \mid b$ (car d' vérifie 1)) d'où $d' \leq d$ (car d vérifie 2)).

Démonstration.

Unicité : Soit $d, d' \in \mathbb{N}$ tels que d et d' vérifient les deux propriétés : On a $d' \mid a$ et $d' \mid b$ (car d' vérifie 1)) d'où $d' \leq d$ (car d vérifie 2)). de la même façon, on montre que $d \leq d'$ et ainsi $d' = d$. □

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Remarque 2.10

Remarque 2.10

1. Si $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$, alors il existe $(x,y) \in \mathbb{Z}^2 : a \wedge b = ax + by$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Remarque 2.10

1. Si $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$, alors il existe $(x,y) \in \mathbb{Z}^2 : a \wedge b = ax + by$.
2. Si $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$, alors $a \wedge b = |a| \wedge |b|$.

Remarque 2.10

1. Si $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$, alors il existe $(x,y) \in \mathbb{Z}^2 : a \wedge b = ax + by$.
2. Si $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$, alors $a \wedge b = |a| \wedge |b|$.
3. On vérifie que si a, b et c sont des entiers non nuls, alors $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

Remarque 2.10

1. Si $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$, alors il existe $(x,y) \in \mathbb{Z}^2 : a \wedge b = ax + by$.
2. Si $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$, alors $a \wedge b = |a| \wedge |b|$.
3. On vérifie que si a, b et c sont des entiers non nuls, alors $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ et ainsi on peut généraliser, par récurrence, à un nombre fini quelconque d'entiers non nuls, i.e., $a_1 \wedge \cdots \wedge a_n = (a_1 \wedge \cdots \wedge a_{n-1}) \wedge a_n$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$. Supposons que $d = a \wedge b$. Alors, par définition, $d \mid a$ et $d \mid b$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$. Supposons que $d = a \wedge b$. Alors, par définition, $d \mid a$ et $d \mid b$. Soit c un entier tel que $c \mid a$ et $c \mid b$. Puisque $d = a \wedge b$, il existe $u, v \in \mathbb{Z} : d = au + bv$. Puisque $c \mid a$ et $c \mid b$, $c \mid au + bv = d$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ et $d \in \mathbb{N}$. $d = a \wedge b$ si, et seulement si,

1) $d \mid a$ *et* $d \mid b$,
2) *Si c est un entier tel que $c \mid a$ et $c \mid b$, alors $c \mid d$.*

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$. Supposons que $d = a \wedge b$. Alors, par définition, $d \mid a$ et $d \mid b$. Soit c un entier tel que $c \mid a$ et $c \mid b$. Puisque $d = a \wedge b$, il existe $u, v \in \mathbb{Z} : d = au + bv$. Puisque $c \mid a$ et $c \mid b$, $c \mid au + bv = d$.
Réciproquement, supposons que d vérifie 1) et 2).

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$. Supposons que $d = a \wedge b$. Alors, par définition, $d \mid a$ et $d \mid b$. Soit c un entier tel que $c \mid a$ et $c \mid b$. Puisque $d = a \wedge b$, il existe $u, v \in \mathbb{Z} : d = au + bv$. Puisque $c \mid a$ et $c \mid b$, $c \mid au + bv = d$.
Réciproquement, supposons que d vérifie 1) et 2). On a $d \mid a$ et $d \mid b$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$. Supposons que $d = a \wedge b$. Alors, par définition, $d \mid a$ et $d \mid b$. Soit c un entier tel que $c \mid a$ et $c \mid b$. Puisque $d = a \wedge b$, il existe $u, v \in \mathbb{Z} : d = au + bv$. Puisque $c \mid a$ et $c \mid b$, $c \mid au + bv = d$.

Réciproquement, supposons que d vérifie 1) et 2). On a $d \mid a$ et $d \mid b$. Soit $c \in \mathbb{Z}$ tel que $c \mid a$ et $c \mid b$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$. Supposons que $d = a \wedge b$. Alors, par définition, $d \mid a$ et $d \mid b$. Soit c un entier tel que $c \mid a$ et $c \mid b$. Puisque $d = a \wedge b$, il existe $u, v \in \mathbb{Z} : d = au + bv$. Puisque $c \mid a$ et $c \mid b$, $c \mid au + bv = d$.
Réciproquement, supposons que d vérifie 1) et 2). On a $d \mid a$ et $d \mid b$. Soit $c \in \mathbb{Z}$ tel que $c \mid a$ et $c \mid b$. Alors, $c \mid d$ car d vérifie 2)

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$. Supposons que $d = a \wedge b$. Alors, par définition, $d \mid a$ et $d \mid b$. Soit c un entier tel que $c \mid a$ et $c \mid b$. Puisque $d = a \wedge b$, il existe $u, v \in \mathbb{Z} : d = au + bv$. Puisque $c \mid a$ et $c \mid b$, $c \mid au + bv = d$.

Réciproquement, supposons que d vérifie 1) et 2). On a $d \mid a$ et $d \mid b$. Soit $c \in \mathbb{Z}$ tel que $c \mid a$ et $c \mid b$. Alors, $c \mid d$ car d vérifie 2) et ainsi $|c| \leq |d| = d$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.11

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ *et* $d \in \mathbb{N}$. $d = a \wedge b$ *si, et seulement si,*

1) $d \mid a$ *et* $d \mid b$,
2) *Si* c *est un entier tel que* $c \mid a$ *et* $c \mid b$, *alors* $c \mid d$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$ et $d \in \mathbb{N}$. Supposons que $d = a \wedge b$. Alors, par définition, $d \mid a$ et $d \mid b$. Soit c un entier tel que $c \mid a$ et $c \mid b$. Puisque $d = a \wedge b$, il existe $u, v \in \mathbb{Z} : d = au + bv$. Puisque $c \mid a$ et $c \mid b$, $c \mid au + bv = d$.

Réciproquement, supposons que d vérifie 1) et 2). On a $d \mid a$ et $d \mid b$. Soit $c \in \mathbb{Z}$ tel que $c \mid a$ et $c \mid b$. Alors, $c \mid d$ car d vérifie 2) et ainsi $|c| \leq |d| = d$ d'où $c \leq d$ et donc $d = a \wedge b$. □

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Définition 2.12

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$.

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$.

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. Supposons que a et b sont premiers entre eux, i.e., $a \wedge b = 1$, alors il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. Supposons que a et b sont premiers entre eux, i.e., $a \wedge b = 1$, alors il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Réciproquement, supposons qu'il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. Supposons que a et b sont premiers entre eux, i.e., $a \wedge b = 1$, alors il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Réciproquement, supposons qu'il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Posons $d = a \wedge b$.

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. Supposons que a et b sont premiers entre eux, i.e., $a \wedge b = 1$, alors il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Réciproquement, supposons qu'il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Posons $d = a \wedge b$. Alors, $d \mid a$ et $d \mid b$

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. Supposons que a et b sont premiers entre eux, i.e., $a \wedge b = 1$, alors il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Réciproquement, supposons qu'il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Posons $d = a \wedge b$. Alors, $d \mid a$ et $d \mid b$ ainsi $d \mid ax + by = 1$

Théorème 2.13 (Théorème de Bézout)

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.

Démonstration.

Soit $(a,b) \in \mathbb{Z} - \{(0,0)\}$. Supposons que a et b sont premiers entre eux, i.e., $a \wedge b = 1$, alors il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Réciproquement, supposons qu'il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.
Posons $d = a \wedge b$. Alors, $d \mid a$ et $d \mid b$ ainsi $d \mid ax + by = 1$ et donc $d = 1$ car $d \in \mathbb{N}^\star$. □

Corollaire 2.14

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *Si* $a \wedge b = d$, *alors* $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Corollaire 2.14

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *Si* $a \wedge b = d$, *alors* $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$: $a \wedge b = d$.

Corollaire 2.14

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *Si* $a \wedge b = d$, *alors* $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\} : a \wedge b = d$. Alors, $(\frac{a}{d}, \frac{b}{d}) \in \mathbb{Z}^2 - \{(0,0)\}$.

Corollaire 2.14

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *Si* $a \wedge b = d$, *alors* $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\} : a \wedge b = d$. Alors, $(\frac{a}{d}, \frac{b}{d}) \in \mathbb{Z}^2 - \{(0,0)\}$. Puisque $a \wedge b = d$,

Corollaire 2.14

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *Si* $a \wedge b = d$, *alors* $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$: $a \wedge b = d$. Alors, $(\frac{a}{d}, \frac{b}{d}) \in \mathbb{Z}^2 - \{(0,0)\}$. Puisque $a \wedge b = d$, il existe $(u,v) \in \mathbb{Z}^2$ tel que $d = au + bv$

Corollaire 2.14

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *Si* $a \wedge b = d$, *alors* $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\} : a \wedge b = d$. Alors, $(\frac{a}{d}, \frac{b}{d}) \in \mathbb{Z}^2 - \{(0,0)\}$. Puisque $a \wedge b = d$, il existe $(u,v) \in \mathbb{Z}^2$ tel que $d = au + bv$ ainsi $1 = \frac{a}{d}.u + \frac{b}{d}v$

Corollaire 2.14

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *Si* $a \wedge b = d$, *alors* $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Démonstration.

Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\} : a \wedge b = d$. Alors, $(\frac{a}{d}, \frac{b}{d}) \in \mathbb{Z}^2 - \{(0,0)\}$. Puisque $a \wedge b = d$, il existe $(u,v) \in \mathbb{Z}^2$ tel que $d = au + bv$ ainsi $1 = \frac{a}{d}.u + \frac{b}{d}v$ et donc $\frac{a}{d} \wedge \frac{b}{d} = 1$. □

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$.

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$.

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$,

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = c(au) + c(bv)$.

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = c(au) + c(bv)$. On a aussi $a \mid c$ et $b \mid c$

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = c(au) + c(bv)$. On a aussi $a \mid c$ et $b \mid c$ d'où il existe $h, k \in \mathbb{Z}$ tel que $c = ha$ et $c = kb$

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = c(au) + c(bv)$. On a aussi $a \mid c$ et $b \mid c$ d'où il existe $h, k \in \mathbb{Z}$ tel que $c = ha$ et $c = kb$ ainsi
$c = c(au) + c(bv)$

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = c(au) + c(bv)$. On a aussi $a \mid c$ et $b \mid c$ d'où il existe $h, k \in \mathbb{Z}$ tel que $c = ha$ et $c = kb$ ainsi
$c = c(au) + c(bv) = kb(au) + ha(bv)$

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = c(au) + c(bv)$. On a aussi $a \mid c$ et $b \mid c$ d'où il existe $h, k \in \mathbb{Z}$ tel que $c = ha$ et $c = kb$ ainsi
$c = c(au) + c(bv) = kb(au) + ha(bv) = ab(ku + hv)$

Corollaire 2.15

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Puisque $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = c(au) + c(bv)$. On a aussi $a \mid c$ et $b \mid c$ d'où il existe $h, k \in \mathbb{Z}$ tel que $c = ha$ et $c = kb$ ainsi $c = c(au) + c(bv) = kb(au) + ha(bv) = ab(ku + hv)$ et donc $ab \mid c$. □

Théorème 2.16 (Lemme de Gauss)

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$.

Théorème 2.16 (Lemme de Gauss)

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Si $a \wedge b = 1$, alors $a \mid c$.

Théorème 2.16 (Lemme de Gauss)

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Si $a \wedge b = 1$, alors $a \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$.

Théorème 2.16 (Lemme de Gauss)

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Si $a \wedge b = 1$, alors $a \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Supposons que $a \wedge b = 1$.

Théorème 2.16 (Lemme de Gauss)

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Si $a \wedge b = 1$, alors $a \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Supposons que $a \wedge b = 1$. Alors, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$

Théorème 2.16 (Lemme de Gauss)

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Si $a \wedge b = 1$, alors $a \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Supposons que $a \wedge b = 1$. Alors, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = (ac)u + (bc)v$.

Théorème 2.16 (Lemme de Gauss)

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Si $a \wedge b = 1$, alors $a \mid c$.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Supposons que $a \wedge b = 1$. Alors, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $c = (ac)u + (bc)v$. Comme $a \mid ac$ et $a \mid bc$, $a \mid (ac)u + (bc)v = c$. □

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$,

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$. Posons $d_1 = a \wedge b$ et $d_2 = b \wedge r$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$. Posons $d_1 = a \wedge b$ et $d_2 = b \wedge r$. Puisque $d_1 \mid a$ et $d_1 \mid b$,

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$. Posons $d_1 = a \wedge b$ et $d_2 = b \wedge r$. Puisque $d_1 \mid a$ et $d_1 \mid b$, $d_1 \mid a - qb = r$

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$. Posons $d_1 = a \wedge b$ et $d_2 = b \wedge r$. Puisque $d_1 \mid a$ et $d_1 \mid b$, $d_1 \mid a - qb = r$ d'où $d_1 \mid d_2$ car $d_1 \mid b$ et $d_1 \mid r$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$. Posons $d_1 = a \wedge b$ et $d_2 = b \wedge r$. Puisque $d_1 \mid a$ et $d_1 \mid b$, $d_1 \mid a - qb = r$ d'où $d_1 \mid d_2$ car $d_1 \mid b$ et $d_1 \mid r$. Aussi, Puisque $d_2 \mid b$ et $d_2 \mid r$,

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$. Posons $d_1 = a \wedge b$ et $d_2 = b \wedge r$. Puisque $d_1 \mid a$ et $d_1 \mid b$, $d_1 \mid a - qb = r$ d'où $d_1 \mid d_2$ car $d_1 \mid b$ et $d_1 \mid r$. Aussi, Puisque $d_2 \mid b$ et $d_2 \mid r$, $d_2 \mid qb + r = a$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$. Posons $d_1 = a \wedge b$ et $d_2 = b \wedge r$. Puisque $d_1 \mid a$ et $d_1 \mid b$, $d_1 \mid a - qb = r$ d'où $d_1 \mid d_2$ car $d_1 \mid b$ et $d_1 \mid r$. Aussi, Puisque $d_2 \mid b$ et $d_2 \mid r$, $d_2 \mid qb + r = a$ d'où $d_2 \mid d_1$ car $d_2 \mid a$ et $d_2 \mid b$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Lemme 2.17

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.

Démonstration.

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$ tels que $a = qb + r$, où $q, r \in \mathbb{Z}$. Posons $d_1 = a \wedge b$ et $d_2 = b \wedge r$. Puisque $d_1 \mid a$ et $d_1 \mid b$, $d_1 \mid a - qb = r$ d'où $d_1 \mid d_2$ car $d_1 \mid b$ et $d_1 \mid r$. Aussi, Puisque $d_2 \mid b$ et $d_2 \mid r$, $d_2 \mid qb + r = a$ d'où $d_2 \mid d_1$ car $d_2 \mid a$ et $d_2 \mid b$ et donc $d_1 = d_2$. □

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$.

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$.

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$. *On a* $a = q_1 b + r_1$, *avec* $0 \leq r_1 < b$.

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$. *On a* $a = q_1 b + r_1$, *avec* $0 \leq r_1 < b$. *Si* $r_1 = 0$, *alors* $a \wedge b = b$.

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$. *On a* $a = q_1 b + r_1$, *avec* $0 \leq r_1 < b$. *Si* $r_1 = 0$, *alors* $a \wedge b = b$. *Si* $r_1 \neq 0$, $b = q_2 r_1 + r_2$, *avec* $0 \leq r_2 < r_1$.

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$. *On a* $a = q_1 b + r_1$, *avec* $0 \leq r_1 < b$. *Si* $r_1 = 0$, *alors* $a \wedge b = b$. *Si* $r_1 \neq 0$, $b = q_2 r_1 + r_2$, *avec* $0 \leq r_2 < r_1$. *Si* $r_2 = 0$, *alors* $a \wedge b = b \wedge r_1 = r_1$.

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$. *On a* $a = q_1 b + r_1$, *avec* $0 \leq r_1 < b$. *Si* $r_1 = 0$, *alors* $a \wedge b = b$. *Si* $r_1 \neq 0$, $b = q_2 r_1 + r_2$, *avec* $0 \leq r_2 < r_1$. *Si* $r_2 = 0$, *alors* $a \wedge b = b \wedge r_1 = r_1$. *Si* $r_2 \neq 0$,

$$
\begin{aligned}
a &= bq + r_1, \text{ avec } 0 \leq r_1 < b \\
b &= q_2 r_1 + r_2, \text{ avec } 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \text{ avec } 0 \leq r_3 < r_2 \\
&\vdots
\end{aligned}
$$

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$. *On a* $a = q_1 b + r_1$, *avec* $0 \leq r_1 < b$. *Si* $r_1 = 0$, *alors* $a \wedge b = b$. *Si* $r_1 \neq 0$, $b = q_2 r_1 + r_2$, *avec* $0 \leq r_2 < r_1$. *Si* $r_2 = 0$, *alors* $a \wedge b = b \wedge r_1 = r_1$. *Si* $r_2 \neq 0$,

$$\begin{aligned} a &= bq + r_1, \text{ avec } 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2, \text{ avec } 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, \text{ avec } 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

Puisque $b > r_1 > r_2 > \ldots \geq 0$ *et que* $b, r_1, r_2, \ldots \in \mathbb{N}$,

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$. *On a* $a = q_1 b + r_1$, *avec* $0 \leq r_1 < b$. *Si* $r_1 = 0$, *alors* $a \wedge b = b$. *Si* $r_1 \neq 0$, $b = q_2 r_1 + r_2$, *avec* $0 \leq r_2 < r_1$. *Si* $r_2 = 0$, *alors* $a \wedge b = b \wedge r_1 = r_1$. *Si* $r_2 \neq 0$,

$$\begin{aligned} a &= bq + r_1, \text{ avec } 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2, \text{ avec } 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, \text{ avec } 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

Puisque $b > r_1 > r_2 > \ldots \geq 0$ *et que* $b, r_1, r_2, \ldots \in \mathbb{N}$, *il existe* $n \in \mathbb{N}$ *tel que* $r_{n-2} = q_n r_{n-1} + r_n$, *avec* $0 < r_n < r_{n-1}$ *et* $r_{n-1} = q_{n+1} r_n$.

Algorithme 2.18 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. *On peut supposer que* $0 < b \leq a$. *On a* $a = q_1 b + r_1$, *avec* $0 \leq r_1 < b$. *Si* $r_1 = 0$, *alors* $a \wedge b = b$. *Si* $r_1 \neq 0$, $b = q_2 r_1 + r_2$, *avec* $0 \leq r_2 < r_1$. *Si* $r_2 = 0$, *alors* $a \wedge b = b \wedge r_1 = r_1$. *Si* $r_2 \neq 0$,

$$\begin{aligned} a &= bq + r_1, \text{ avec } 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2, \text{ avec } 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, \text{ avec } 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

Puisque $b > r_1 > r_2 > \ldots \geq 0$ *et que* $b, r_1, r_2, \ldots \in \mathbb{N}$, *il existe* $n \in \mathbb{N}$ *tel que* $r_{n-2} = q_n r_{n-1} + r_n$, *avec* $0 < r_n < r_{n-1}$ *et* $r_{n-1} = q_{n+1} r_n$. *Ainsi, on a* $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{n-1} \wedge r_n = r_n$.

Exemple 2.19

En utilisant l'algorithme d'Euclide pour calculer $1008 \wedge 360$*, on obtient :*
$1008 = 2.360 + 288$,

Exemple 2.19

En utilisant l'algorithme d'Euclide pour calculer $1008 \wedge 360$*, on obtient :*
$1008 = 2.360 + 288,\ 360 = 288.1 + 72,\ ,$

Exemple 2.19

En utilisant l'algorithme d'Euclide pour calculer $1008 \wedge 360$*, on obtient :*
$1008 = 2.360 + 288,\ 360 = 288.1 + 72,\ ,\ 288 = 72.4\ ,$

Exemple 2.19

En utilisant l'algorithme d'Euclide pour calculer $1008 \wedge 360$*, on obtient :*
$1008 = 2.360 + 288,\ 360 = 288.1 + 72,\ ,\ 288 = 72.4\ ,$ *ainsi*
$1008 \wedge 360 = 72.$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Algorithme 2.20 (Algorithme d'Euclide étendu)

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. ,

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$:

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$,

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$, puis on exprime d comme combinaison de r_{n-2} et r_{n-3} ,

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$, puis on exprime d comme combinaison de r_{n-2} et r_{n-3} , et en remontant de bas en haut, on écrit d comme combinaison de b et r_1 ,

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$, puis on exprime d comme combinaison de r_{n-2} et r_{n-3} , et en remontant de bas en haut, on écrit d comme combinaison de b et r_1 , et ainsi on obtient d sous la forme $d = au + bv$.

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$, puis on exprime d comme combinaison de r_{n-2} et r_{n-3} , et en remontant de bas en haut, on écrit d comme combinaison de b et r_1 , et ainsi on obtient d sous la forme $d = au + bv$.

Exemple 2.21

On a $1008 \wedge 360 = 72$,

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$, puis on exprime d comme combinaison de r_{n-2} et r_{n-3} , et en remontant de bas en haut, on écrit d comme combinaison de b et r_1 , et ainsi on obtient d sous la forme $d = au + bv$.

Exemple 2.21

On a $1008 \wedge 360 = 72$, *et* $1008 = 2.360 + 288$, $360 = 288.1 + 72$, $288 = 72.4$.

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$, puis on exprime d comme combinaison de r_{n-2} et r_{n-3} , et en remontant de bas en haut, on écrit d comme combinaison de b et r_1 , et ainsi on obtient d sous la forme $d = au + bv$.

Exemple 2.21

On a $1008 \wedge 360 = 72$, *et* $1008 = 2.360 + 288$, $360 = 288.1 + 72$, $288 = 72.4$. *Alors,* $72 = 360 - 288.1 = 360 - (1008 - 2.360)$

Algorithme 2.20 (Algorithme d'Euclide étendu)

Soit a et b deux entiers et $d = a \wedge b$. , L'algorithme suivant permet d'écrire d comme combinaison de a et b, i.e., trouver $u, v \in \mathbb{Z} : d = au + bv$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$, puis on exprime d comme combinaison de r_{n-2} et r_{n-3} , et en remontant de bas en haut, on écrit d comme combinaison de b et r_1 , et ainsi on obtient d sous la forme $d = au + bv$.

Exemple 2.21

On a $1008 \wedge 360 = 72$, *et* $1008 = 2.360 + 288$, $360 = 288.1 + 72$, $288 = 72.4$. *Alors,* $72 = 360 - 288.1 = 360 - (1008 - 2.360)$ *ainsi* $72 = (-1).1008 + 3.360$.

Corollaire 2.22

Si k est un entier non nul, alors $pgcd(ka, kb) = |k|pgcd(a, b)$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Corollaire 2.22

Si k est un entier non nul, alors $pgcd(ka, kb) = |k|pgcd(a, b)$.

Démonstration.

Pusique $pgcd(ka, kb) = pgcd(|ka|, |kb|) = pgcd(|k||a|, |k||b|)$, on peut supposer que $k, a, b \in \mathbb{N}^\star$.

Corollaire 2.22

Si k est un entier non nul, alors $pgcd(ka, kb) = |k|pgcd(a, b)$.

Démonstration.

Pusique $pgcd(ka, kb) = pgcd(|ka|, |kb|) = pgcd(|k||a|, |k||b|)$, on peut supposer que $k, a, b \in \mathbb{N}^\star$. Posons $pgcd(a, b) = r_n$ obtenu à l'aide de l'algorithme d'Euclide :

$$\begin{gathered} a = bq + r_1, \text{ avec } 0 \leq r_1 < b \\ b = q_2 r_1 + r_2, \text{ avec } 0 \leq r_2 < r_1 \\ r_1 = q_3 r_2 + r_3, \text{ avec } 0 \leq r_3 < r_2 \\ \vdots \\ r_{n-2} = q_n r_{n-1} + r_n \text{ avec } 0 \leq r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n \end{gathered}$$

□

Démonstration.

Alors,

$$ka = kbq + kr_1, \text{ avec } 0 \leq kr_1 < kb$$
$$kb = q_2 kr_1 + kr_2, \text{ avec } 0 \leq kr_2 < kr_1$$
$$kr_1 = q_3 kr_2 + kr_3, \text{ avec } 0 \leq kr_3 < kr_2$$
$$\vdots$$
$$kr_{n-2} = q_n kr_{n-1} + kr_n \text{ avec } 0 \leq kr_n < kr_{n-1}$$
$$kr_{n-1} = q_{n+1} kr_n$$

Démonstration.

Alors,

$$\begin{gathered} ka = kbq + kr_1, \text{ avec } 0 \leq kr_1 < kb \\ kb = q_2 kr_1 + kr_2, \text{ avec } 0 \leq kr_2 < kr_1 \\ kr_1 = q_3 kr_2 + kr_3, \text{ avec } 0 \leq kr_3 < kr_2 \\ \vdots \\ kr_{n-2} = q_n kr_{n-1} + kr_n \text{ avec } 0 \leq kr_n < kr_{n-1} \\ kr_{n-1} = q_{n+1} kr_n \end{gathered}$$

et ainsi on obteint l'algorithme d'Euclide appliqué aux entiers ak et bk et $pgcd(ak, bk)$ est le dernier reste non nul, i.e., $kr_n = k.pgcd(a, b)$.

Théorème et définition 2.23

Soit $a, b \in \mathbb{Z}^\star$. Il existe un unique entier positif m tel que

Théorème et définition 2.23

Soit $a, b \in \mathbb{Z}^\star$. Il existe un unique entier positif m tel que

i) $a \mid m$ et $b \mid m$,

Théorème et définition 2.23

Soit $a, b \in \mathbb{Z}^\star$. Il existe un unique entier positif m tel que

i) $a \mid m$ *et* $b \mid m$,

ii) *Si c est un entier tel que a divise c et b divise c, alors m divise c.*

Théorème et définition 2.23

Soit $a, b \in \mathbb{Z}^\star$. Il existe un unique entier positif m tel que

i) $a \mid m$ *et* $b \mid m$,

ii) *Si c est un entier tel que a divise c et b divise c, alors m divise c.*

L'entier naturel m est appelé ***le plus petit commun multiple*** *de a et b.*

Théorème et définition 2.23

Soit $a, b \in \mathbb{Z}^\star$. Il existe un unique entier positif m tel que

i) $a \mid m$ *et* $b \mid m$,

ii) *Si c est un entier tel que a divise c et b divise c, alors m divise c.*

L'entier naturel m est appelé ***le plus petit commun multiple*** *de a et b. m est noté $a \vee b$ ou $m = ppcm(a, b)$.*

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c. En effectuant la division euclidienne de c par m, il existe $(q, r) \in \mathbb{Z}^2 : c = mq + r$, avec $0 \leq r < m$.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c. En effectuant la division euclidienne de c par m, il existe $(q, r) \in \mathbb{Z}^2 : c = mq + r$, avec $0 \leq r < m$.
Puisque $a \mid c$ et $a \mid m$, $a \mid r$.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c. En effectuant la division euclidienne de c par m, il existe $(q, r) \in \mathbb{Z}^2 : c = mq + r$, avec $0 \leq r < m$.
Puisque $a \mid c$ et $a \mid m$, $a \mid r$. Aussi, puisque $b \mid c$ et $b \mid m$, $b \mid r$.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c. En effectuant la division euclidienne de c par m, il existe $(q, r) \in \mathbb{Z}^2 : c = mq + r$, avec $0 \leq r < m$. Puisque $a \mid c$ et $a \mid m$, $a \mid r$. Aussi, puisque $b \mid c$ et $b \mid m$, $b \mid r$. Alors, $r = 0$, sinon, $r \in A$ et $r < m$, contradiction, et donc $m \mid c$.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c. En effectuant la division euclidienne de c par m, il existe $(q, r) \in \mathbb{Z}^2 : c = mq + r$, avec $0 \leq r < m$. Puisque $a \mid c$ et $a \mid m$, $a \mid r$. Aussi, puisque $b \mid c$ et $b \mid m$, $b \mid r$. Alors, $r = 0$, sinon, $r \in A$ et $r < m$, contradiction, et donc $m \mid c$.
Unicité : Supposons que m_1 et m_2 sont des ppcm de a et b.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c. En effectuant la division euclidienne de c par m, il existe $(q, r) \in \mathbb{Z}^2 : c = mq + r$, avec $0 \leq r < m$. Puisque $a \mid c$ et $a \mid m$, $a \mid r$. Aussi, puisque $b \mid c$ et $b \mid m$, $b \mid r$. Alors, $r = 0$, sinon, $r \in A$ et $r < m$, contradiction, et donc $m \mid c$.
Unicité : Supposons que m_1 et m_2 sont des ppcm de a et b. On a $a \mid m_1$ et $b \mid m_1$ d'où $m_2 \mid m_1$ car m_2 est un ppcm de a et b.

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c. En effectuant la division euclidienne de c par m, il existe $(q, r) \in \mathbb{Z}^2 : c = mq + r$, avec $0 \leq r < m$. Puisque $a \mid c$ et $a \mid m$, $a \mid r$. Aussi, puisque $b \mid c$ et $b \mid m$, $b \mid r$. Alors, $r = 0$, sinon, $r \in A$ et $r < m$, contradiction, et donc $m \mid c$.
Unicité : Supposons que m_1 et m_2 sont des ppcm de a et b. On a $a \mid m_1$ et $b \mid m_1$ d'où $m_2 \mid m_1$ car m_2 est un ppcm de a et b. Aussi, on a $a \mid m_2$ et $b \mid m_2$ d'où $m_1 \mid m_2$ car m_1 est un ppcm de de a et b

Démonstration.

Existence : On considère $A = \{x \in \mathbb{N}^\star / a \mid x \text{ et } b \mid x\}$, i.e., l'ensemble des multiples communs positifs de a et b. On a A est une partie de $\mathbb{N}$ et A est non vide car $|ab| \in A$ d'où A possède un plus petit élément qu'on note m. Alors, $m \in \mathbb{N}^\star$, $a \mid m$ et $b \mid m$.
Soit c un entier tel que a divise c et b divise c. En effectuant la division euclidienne de c par m, il existe $(q, r) \in \mathbb{Z}^2 : c = mq + r$, avec $0 \leq r < m$. Puisque $a \mid c$ et $a \mid m$, $a \mid r$. Aussi, puisque $b \mid c$ et $b \mid m$, $b \mid r$. Alors, $r = 0$, sinon, $r \in A$ et $r < m$, contradiction, et donc $m \mid c$.
Unicité : Supposons que m_1 et m_2 sont des ppcm de a et b. On a $a \mid m_1$ et $b \mid m_1$ d'où $m_2 \mid m_1$ car m_2 est un ppcm de a et b. Aussi, on a $a \mid m_2$ et $b \mid m_2$ d'où $m_1 \mid m_2$ car m_1 est un ppcm de de a et b et ainsi puisque $m_2 \mid m_1$, $m_1 \mid m_2$ et $m_1, m_2 \in \mathbb{N}$, $m_1 = m_2$. □

Remarques 2.24

1. On vérifie facilement que $ppcm(a,b) = ppcm(|a|,|b|)$.

Remarques 2.24

1. On vérifie facilement que $ppcm(a,b) = ppcm(|a|,|b|)$.
2. On vérifie que si a, b et c sont des entiers non nuls, alors $(a \vee b) \vee c = a \vee (b \vee c)$

Remarques 2.24

1. On vérifie facilement que $ppcm(a,b) = ppcm(|a|,|b|)$.
2. On vérifie que si a, b et c sont des entiers non nuls, alors $(a \vee b) \vee c = a \vee (b \vee c)$ et ainsi on peut généraliser, par récurrence, à un nombre fini quelconque d'entiers non nuls, i.e., $a_1 \vee \cdots \vee a_n = (a_1 \vee \cdots \vee a_{n-1}) \vee a_n$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$:

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$.

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z}$: $d = au + bv$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z}$: $d = au + bv$ ainsi

$\frac{c}{\frac{ab}{d}} =$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z}$: $d = au + bv$ ainsi
$\frac{c}{\frac{ab}{d}} = \frac{cd}{ab} =$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z}$: $d = au + bv$ ainsi
$\frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} =$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z} : d = au + bv$ ainsi
$\frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} = \frac{cau}{ab} + \frac{cbv}{ab} =$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z} : d = au + bv$ ainsi
$\frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} = \frac{cau}{ab} + \frac{cbv}{ab} = \frac{c}{b}u + \frac{c}{a}v =$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z} : d = au + bv$ ainsi
$\frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} = \frac{cau}{ab} + \frac{cbv}{ab} = \frac{c}{b}u + \frac{c}{a}v = ku + hv \in \mathbb{Z}$ d'où

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z}$: $d = au + bv$ ainsi
$\frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} = \frac{cau}{ab} + \frac{cbv}{ab} = \frac{c}{b}u + \frac{c}{a}v = ku + hv \in \mathbb{Z}$ d'où $\frac{ab}{d} \mid c$

Divisibilité dans $\mathbb{Z}$

Pgcd et Ppcm

Théorème 2.25

Soit $a, b \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a,b)ppcm(a,b) = |ab|$.

Démonstration.

Soit $a, b \in \mathbb{Z} - \{0\}$. Puisque $pgcd(a,b) = pgcd(|a|,|b|)$ et $ppcm(a,b) = ppcm(|a|,|b|)$, on peut supposer que $a, b \in \mathbb{N} - \{0\}$. Posons $d = pgcd(a,b)$ et montrons que $\frac{ab}{d} = ppcm(a,b)$: D'abord, il est évident que puisque $d \mid a$, $\frac{ab}{d}$ est un entier. On a $a = da'$ et $b = db'$ avec $a', b' \in \mathbb{Z}$. Alors, $\frac{ab}{d} = a'b = b'a$ d'où $\frac{ab}{d}$ est un multiple commun positif de a et b.
Soit $c \in \mathbb{Z}$: $a \mid c$ et $b \mid c$. Alors, $c = ah$ et $c = bk$, où $h, k \in \mathbb{Z}$. Puisque $d = pgcd(a,b)$, il existe $u, v \in \mathbb{Z}$: $d = au + bv$ ainsi $\frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} = \frac{cau}{ab} + \frac{cbv}{ab} = \frac{c}{b}u + \frac{c}{a}v = ku + hv \in \mathbb{Z}$ d'où $\frac{ab}{d} \mid c$ et donc $\frac{ab}{d} = ppcm(a,b)$. □

Définition 2.26

Soit $p > 1$ un entier.

Divisibilité dans $\mathbb{Z}$

Nombres premiers

Définition 2.26

Soit $p > 1$ un entier. On dit que p est **premier**

Divisibilité dans $\mathbb{Z}$

Nombres premiers

Définition 2.26

Soit $p > 1$ un entier. On dit que p est **premier** si les seuls diviseurs positifs de p sont 1 et p.

Divisibilité dans $\mathbb{Z}$

Nombres premiers

Définition 2.26

Soit $p > 1$ un entier. On dit que p est **premier** si les seuls diviseurs positifs de p sont 1 et p. Un entier > 1 qui n'est pas premier est dit **composé**.

Théorème 2.27

Soit $a, b \in \mathbb{Z}$ et p un nombre premier.

Théorème 2.27

Soit $a, b \in \mathbb{Z}$ et p un nombre premier. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Théorème 2.27

Soit $a, b \in \mathbb{Z}$ et p un nombre premier. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration.

On a $p \wedge a \in \{1, p\}$ car $p \wedge a$ est un diviseur positif de p et p est premier.

Théorème 2.27

Soit $a, b \in \mathbb{Z}$ et p un nombre premier. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration.

On a $p \wedge a \in \{1, p\}$ car $p \wedge a$ est un diviseur positif de p et p est premier.
Si $p \wedge a = p$, alors $p \mid a$.

Théorème 2.27

Soit $a, b \in \mathbb{Z}$ et p un nombre premier. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration.

On a $p \wedge a \in \{1, p\}$ car $p \wedge a$ est un diviseur positif de p et p est premier.
Si $p \wedge a = p$, alors $p \mid a$.
Si $p \wedge a = 1$, alors, d'après le lemme de Gauss, $p \mid b$. □

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) :

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) : Pour un entier $n \geq 2$, on note $P(n)$: Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) : Pour un entier $n \geq 2$, on note $P(n)$: Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.
  D'après le théorème précédent, $P(2)$ est vraie.

Divisibilité dans $\mathbb{Z}$

Nombres premiers

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) : Pour un entier $n \geq 2$, on note $P(n)$: Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.
  D'après le théorème précédent, $P(2)$ est vraie. Supposons que $P(n)$ est vraie à un rang $n \geq 2$.

Divisibilité dans $\mathbb{Z}$

Nombres premiers

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) : Pour un entier $n \geq 2$, on note $P(n)$: Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.
  D'après le théorème précédent, $P(2)$ est vraie. Supposons que $P(n)$ est vraie à un rang $n \geq 2$. Soit p un nombre premier tel que $p \mid a_1 \ldots a_n . a_{n+1}$.

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) : Pour un entier $n \geq 2$, on note $P(n)$: Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.
  D'après le théorème précédent, $P(2)$ est vraie. Supposons que $P(n)$ est vraie à un rang $n \geq 2$. Soit p un nombre premier tel que $p \mid a_1 \ldots a_n.a_{n+1}$. Alors, $p \mid (a_1 \ldots a_n).a_{n+1}$

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) : Pour un entier $n \geq 2$, on note $P(n)$: Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.
  D'après le théorème précédent, $P(2)$ est vraie. Supposons que $P(n)$ est vraie à un rang $n \geq 2$. Soit p un nombre premier tel que $p \mid a_1 \ldots a_n.a_{n+1}$. Alors, $p \mid (a_1 \ldots a_n).a_{n+1}$ d'où $p \mid a_1 \ldots a_n$ ou $p \mid a_{n+1}$

Divisibilité dans $\mathbb{Z}$

Nombres premiers

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) : Pour un entier $n \geq 2$, on note $P(n)$: Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.
  D'après le théorème précédent, $P(2)$ est vraie. Supposons que $P(n)$ est vraie à un rang $n \geq 2$. Soit p un nombre premier tel que $p \mid a_1 \ldots a_n.a_{n+1}$. Alors, $p \mid (a_1 \ldots a_n).a_{n+1}$ d'où $p \mid a_1 \ldots a_n$ ou $p \mid a_{n+1}$ ainsi il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$ ou $p \mid a_{n+1}$ car $P(n)$ est vraie

Corollaire 2.28

Soit p un nombre premier.

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Démonstration.

- Montrons par récurrence 1) : Pour un entier $n \geq 2$, on note $P(n)$: Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.
  D'après le théorème précédent, $P(2)$ est vraie. Supposons que $P(n)$ est vraie à un rang $n \geq 2$. Soit p un nombre premier tel que $p \mid a_1 \ldots a_n.a_{n+1}$. Alors, $p \mid (a_1 \ldots a_n).a_{n+1}$ d'où $p \mid a_1 \ldots a_n$ ou $p \mid a_{n+1}$ ainsi il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$ ou $p \mid a_{n+1}$ car $P(n)$ est vraie et donc il existe $k \in \{1, \ldots, n, n+1\}$ tel que $p \mid a_k$.

Démonstration.

- Soit $p, p_1, \ldots, p_n$ des nombres premiers tels que $p \mid p_1 \ldots p_n$.

Démonstration.

- Soit $p, p_1, \ldots, p_n$ des nombres premiers tels que $p \mid p_1 \ldots p_n$. D'après 1), il existe $k \in \{1, \ldots, n\}$ tel que $p \mid p_k$

Démonstration.

- Soit $p, p_1, \ldots, p_n$ des nombres premiers tels que $p \mid p_1 \ldots p_n$. D'après 1), il existe $k \in \{1, \ldots, n\}$ tel que $p \mid p_k$ d'où $p = p_k$ car p_k est premier et p est un diviseur positif différent de 1 de p_k.

□

Théorème 2.29 (Théorème fondamental d'arithmétique)

Si $n > 1$ est un entier, alors n s'écrit d'une manière unique sous la forme $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier et $p_1 < p_2 < \cdots < p_r$.

Démonstration.

Existence :

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers :

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers.

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers.

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément n.

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément n. On a n est composé, sinon $n = n$ se décompose en produit de nombres premiers et donc $n \notin A$, ce qui est faux.

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément n. On a n est composé, sinon $n = n$ se décompose en produit de nombres premiers et donc $n \notin A$, ce qui est faux. Puisque n est composé, $n = ab$, avec a, b des entiers tels que $1 < a < n$ et $1 < b < n$

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément n. On a n est composé, sinon $n = n$ se décompose en produit de nombres premiers et donc $n \notin A$, ce qui est faux. Puisque n est composé, $n = ab$, avec a, b des entiers tels que $1 < a < n$ et $1 < b < n$ d'où a et b se décomposent en des produit de nombres premiers

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément n. On a n est composé, sinon $n = n$ se décompose en produit de nombres premiers et donc $n \notin A$, ce qui est faux. Puisque n est composé, $n = ab$, avec a, b des entiers tels que $1 < a < n$ et $1 < b < n$ d'où a et b se décomposent en des produit de nombres premiers et par suite n se décompose aussi en un produit de nombres premiers, contradiction.

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément n. On a n est composé, sinon $n = n$ se décompose en produit de nombres premiers et donc $n \notin A$, ce qui est faux. Puisque n est composé, $n = ab$, avec a, b des entiers tels que $1 < a < n$ et $1 < b < n$ d'où a et b se décomposent en des produit de nombres premiers et par suite n se décompose aussi en un produit de nombres premiers, contradiction.
Soit n un entier > 1. Plusieurs des nombres premiers qui apparaissent dans la décomposition de n en produit de nombres premiers peuvent être égaux.

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément n. On a n est composé, sinon $n = n$ se décompose en produit de nombres premiers et donc $n \notin A$, ce qui est faux. Puisque n est composé, $n = ab$, avec a, b des entiers tels que $1 < a < n$ et $1 < b < n$ d'où a et b se décomposent en des produit de nombres premiers et par suite n se décompose aussi en un produit de nombres premiers, contradiction.
Soit n un entier > 1. Plusieurs des nombres premiers qui apparaissent dans la décomposition de n en produit de nombres premiers peuvent être égaux. Dans ce cas, on remplace les produit de ces nombres premiers égaux (à p) par p^{α}

Démonstration.

Existence : Montrons d'abord que tout entier $n > 1$ se décompose en un produit de nombres premiers : Procédons par absurde et supposons qu'il existe un entier > 1 qui n'est pas un produit de nombre premiers. On considère l'ensemble A des entiers > 1 qui ne sont pas des produits de nombres premiers. Alors, A est un partie non vide de $\mathbb{N}$ d'où A possède un plus petit élément n. On a n est composé, sinon $n = n$ se décompose en produit de nombres premiers et donc $n \notin A$, ce qui est faux. Puisque n est composé, $n = ab$, avec a, b des entiers tels que $1 < a < n$ et $1 < b < n$ d'où a et b se décomposent en des produit de nombres premiers et par suite n se décompose aussi en un produit de nombres premiers, contradiction.
Soit n un entier > 1. Plusieurs des nombres premiers qui apparaissent dans la décomposition de n en produit de nombres premiers peuvent être égaux. Dans ce cas, on remplace les produit de ces nombres premiers égaux (à p) par p^{α} et ainsi $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^{\star}$, p_i est premier et $p_1 < p_2 < \cdots < p_r$. □

Démonstration.

Unicité :

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.
On a $p_1 = q_1$:

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.
On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$).

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.
On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.
On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.
On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$ et ainsi $p_1 \nmid q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} = n$, contradiction.

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.

On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$ et ainsi $p_1 \nmid q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} = n$, contradiction.

On a $k_1 = h_1$:

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.

On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$ et ainsi $p_1 \nmid q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} = n$, contradiction.

On a $k_1 = h_1$: en effet, supposons que $k_1 < h_1$ (de même si $h_1 < k_1$).

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.

On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$ et ainsi $p_1 \nmid q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} = n$, contradiction.

On a $k_1 = h_1$: en effet, supposons que $k_1 < h_1$ (de même si $h_1 < k_1$). Alors, $p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1 - k_1} q_2^{h_2} \dots q_s^{h_s}$

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.

On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$ et ainsi $p_1 \nmid q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} = n$, contradiction.

On a $k_1 = h_1$: en effet, supposons que $k_1 < h_1$ (de même si $h_1 < k_1$). Alors, $p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1 - k_1} q_2^{h_2} \dots q_s^{h_s}$ ainsi $q_1 = p_1$ divise $p_2^{k_2} \dots p_r^{k_r}$

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.

On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$ et ainsi $p_1 \nmid q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} = n$, contradiction.

On a $k_1 = h_1$: en effet, supposons que $k_1 < h_1$ (de même si $h_1 < k_1$). Alors, $p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1 - k_1} q_2^{h_2} \dots q_s^{h_s}$ ainsi $q_1 = p_1$ divise $p_2^{k_2} \dots p_r^{k_r}$ d'où il existe $i \in \{2, \dots, r\}$ tel que $p_1 = p_i$, contradiction car $p_1 < p_i, \forall i \in \{2, \dots, r\}$.

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.
On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$ et ainsi $p_1 \nmid q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} = n$, contradiction.
On a $k_1 = h_1$: en effet, supposons que $k_1 < h_1$ (de même si $h_1 < k_1$). Alors, $p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1 - k_1} q_2^{h_2} \dots q_s^{h_s}$ ainsi $q_1 = p_1$ divise $p_2^{k_2} \dots p_r^{k_r}$ d'où il existe $i \in \{2, \dots, r\}$ tel que $p_1 = p_i$, contradiction car $p_1 < p_i, \forall i \in \{2, \dots, r\}$.
Puisque $p_1 = q_1$ et $k_1 = h_1$, $p_2^{k_2} \dots p_r^{k_r} = q_2^{h_2} \dots q_s^{h_s}$.

Démonstration.

Unicité : Soit n un entier > 1 tel que $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$, avec pour tout $i = 1, \dots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier, $p_1 < p_2 < \dots < p_r$ et pour tout $i = 1, \dots, s$, $h_i \in \mathbb{N}^\star$, q_i est premier $q_1 < q_2 < \dots < q_s$.
On a $p_1 = q_1$: en effet, supposons que $p_1 < q_1$ (de même si $q_1 < p_1$). Alors, $\forall i = 1, \dots, s$, $p_1 < q_i$ d'où $\forall i = 1, \dots, s$, $p_1 \nmid q_i$ et ainsi $p_1 \nmid q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} = n$, contradiction.
On a $k_1 = h_1$: en effet, supposons que $k_1 < h_1$ (de même si $h_1 < k_1$). Alors, $p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1 - k_1} q_2^{h_2} \dots q_s^{h_s}$ ainsi $q_1 = p_1$ divise $p_2^{k_2} \dots p_r^{k_r}$ d'où il existe $i \in \{2, \dots, r\}$ tel que $p_1 = p_i$, contradiction car $p_1 < p_i, \forall i \in \{2, \dots, r\}$.
Puisque $p_1 = q_1$ et $k_1 = h_1$, $p_2^{k_2} \dots p_r^{k_r} = q_2^{h_2} \dots q_s^{h_s}$. En procédant de la même façon que précédement, on montre que $p_2 = q_2, h_2 = k_2, \dots, p_r = q_r, h_r = k_r$ et $r = s$. □

Théorème 2.30 (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Démonstration.

Théorème 2.30 (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Démonstration.

Supposons qu'on a un nombre fini de nombres premiers et notons $p_1, \ldots, p_n$ ces nombres permiers.

Théorème 2.30 (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Démonstration.

Supposons qu'on a un nombre fini de nombres premiers et notons $p_1, \ldots, p_n$ ces nombres permiers. On considére l'entier $N = p_1 p_2 \ldots p_n + 1$.

Théorème 2.30 (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Démonstration.

Supposons qu'on a un nombre fini de nombres premiers et notons $p_1, \ldots, p_n$ ces nombres permiers. On considére l'entier $N = p_1 p_2 \ldots p_n + 1$. On a $N > 1$

Théorème 2.30 (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Démonstration.

Supposons qu'on a un nombre fini de nombres premiers et notons $p_1, \ldots, p_n$ ces nombres permiers. On considére l'entier $N = p_1 p_2 \ldots p_n + 1$. On a $N > 1$ d'où, d'après le théorème précédent, il existe $p_i \in \{p_1, \ldots, p_n\} : p_i \mid N$.

Théorème 2.30 (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Démonstration.

Supposons qu'on a un nombre fini de nombres premiers et notons $p_1, \ldots, p_n$ ces nombres permiers. On considére l'entier $N = p_1 p_2 \ldots p_n + 1$. On a $N > 1$ d'où, d'après le théorème précédent, il existe $p_i \in \{p_1, \ldots, p_n\} : p_i \mid N$. Comme $p_i \mid N$ et $p_i \mid p_1 p_2 \ldots p_n$, $p_i \mid 1$, contradiction. □

Divisibilité dans $\mathbb{Z}$

Congruences

Définition 2.31

Soit $n \in \mathbb{N}$. On dit que deux entiers relatifs a et b sont congrus modulo n et on note $a \equiv b \pmod{n}$ si n divise $a - b$.

Divisibilité dans $\mathbb{Z}$

Congruences

Définition 2.31

Soit $n \in \mathbb{N}$. On dit que deux entiers relatifs a et b sont congrus modulo n et on note $a \equiv b \pmod{n}$ si n divise $a - b$. La relation $a \equiv b \pmod{n}$ est appelée **congruence modulo n**.

Remarque 2.32

Si $n = 0$, la relation $a \equiv b \pmod{n}$ n'est autre que $a = b$.

Remarque 2.32

Si $n = 0$, la relation $a \equiv b \pmod{n}$ n'est autre que $a = b$. Si $n = 1$, la relation $a \equiv b \pmod{n}$ est vraie pour tout $(a, b) \in \mathbb{Z}^2$.

Remarque 2.32

Si $n = 0$, la relation $a \equiv b \pmod{n}$ n'est autre que $a = b$. Si $n = 1$, la relation $a \equiv b \pmod{n}$ est vraie pour tout $(a, b) \in \mathbb{Z}^2$.
Dans la suite de cette section, on suppose que $n \geq 2$.

Théorème 2.33

Soit $n \geq 2$ un entier. La relation $a \equiv b \pmod{n}$ définie sur $\mathbb{Z}$ est une relation d'équivalence.

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0, 1 \ldots, n-1\}$,

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0, 1 \ldots, n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0, 1 \ldots, n-1\}$.

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0, 1 \ldots, n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0, 1 \ldots, n-1\}$. En effet, soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$.

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0, 1 \ldots, n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0, 1 \ldots, n-1\}$. En effet, soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $(q, r) \in \mathbb{Z}^2 : x = qn + r$ avec $0 \leq r \leq n-1$

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0,1\ldots,n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0,1\ldots,n-1\}$. En effet, soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $(q,r) \in \mathbb{Z}^2 : x = qn + r$ avec $0 \leq r \leq n-1$ d'où il existe $a = r \in \{0,1\ldots,n-1\} : x \equiv a \pmod{n}$

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0, 1 \ldots, n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0, 1 \ldots, n-1\}$. En effet, soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $(q, r) \in \mathbb{Z}^2 : x = qn + r$ avec $0 \leq r \leq n-1$ d'où il existe $a = r \in \{0, 1 \ldots, n-1\} : x \equiv a \pmod{n}$ ainsi il existe $a = r \in \{0, 1 \ldots, n-1\} : a \in \overline{x}$.

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0,1\ldots,n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0,1\ldots,n-1\}$. En effet, soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $(q,r) \in \mathbb{Z}^2 : x = qn+r$ avec $0 \leq r \leq n-1$ d'où il existe $a = r \in \{0,1\ldots,n-1\} : x \equiv a \pmod{n}$ ainsi il existe $a = r \in \{0,1\ldots,n-1\} : a \in \overline{x}$. Supposons maintenant qu'il existe $a, a' \in \{0,1\ldots,n-1\} : a, a' \in \overline{x}$.

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0,1\ldots,n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0,1\ldots,n-1\}$. En effet, soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $(q,r) \in \mathbb{Z}^2 : x = qn+r$ avec $0 \leq r \leq n-1$ d'où il existe $a = r \in \{0,1\ldots,n-1\} : x \equiv a \pmod{n}$ ainsi il existe $a = r \in \{0,1\ldots,n-1\} : a \in \overline{x}$. Supposons maintenant qu'il existe $a, a' \in \{0,1\ldots,n-1\} : a, a' \in \overline{x}$. Alors, $x \equiv a \pmod{n}$ et $x \equiv a' \pmod{n}$

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0, 1 \ldots, n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0, 1 \ldots, n-1\}$. En effet, soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $(q, r) \in \mathbb{Z}^2 : x = qn + r$ avec $0 \leq r \leq n-1$ d'où il existe $a = r \in \{0, 1 \ldots, n-1\} : x \equiv a \pmod{n}$ ainsi il existe $a = r \in \{0, 1 \ldots, n-1\} : a \in \overline{x}$. Supposons maintenant qu'il existe $a, a' \in \{0, 1 \ldots, n-1\} : a, a' \in \overline{x}$. Alors, $x \equiv a \pmod{n}$ et $x \equiv a' \pmod{n}$ d'où $x = qn + a$ et $x = q'n + a'$, avec $q, q' \in \mathbb{Z}$

Remarques 2.34

1. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.
2. Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0,1\ldots,n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0,1\ldots,n-1\}$. En effet, soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $(q,r) \in \mathbb{Z}^2 : x = qn+r$ avec $0 \leq r \leq n-1$ d'où il existe $a = r \in \{0,1\ldots,n-1\} : x \equiv a \pmod{n}$ ainsi il existe $a = r \in \{0,1\ldots,n-1\} : a \in \overline{x}$. Supposons maintenant qu'il existe $a, a' \in \{0,1\ldots,n-1\} : a, a' \in \overline{x}$. Alors, $x \equiv a \pmod{n}$ et $x \equiv a' \pmod{n}$ d'où $x = qn+a$ et $x = q'n+a'$, avec $q, q' \in \mathbb{Z}$ et donc, par unicité du reste dans la division euclidienne, $a = a'$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$*

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec l'addition dans** $\mathbb{Z}$).*

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec l'addition dans** $\mathbb{Z}$).*

2) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 a_2 \equiv b_1 b_2 \pmod{n}$*

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec l'addition dans** $\mathbb{Z}$).*

2) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec la multiplication dans** $\mathbb{Z}$)*

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec l'addition dans** $\mathbb{Z}$).*
2) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec la multiplication dans** $\mathbb{Z}$)*

Démonstration.

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec l'addition dans** $\mathbb{Z}$).*
2) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec la multiplication dans** $\mathbb{Z}$)*

Démonstration.

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec l'addition dans** $\mathbb{Z}$).*
2) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec la multiplication dans** $\mathbb{Z}$)*

Démonstration.

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$. Alors, $n \mid a_1 - b_1$ et $n \mid a_2 - b_2$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec l'addition dans** $\mathbb{Z}$).*
2) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec la multiplication dans** $\mathbb{Z}$)*

Démonstration.

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$. Alors, $n \mid a_1 - b_1$ et $n \mid a_2 - b_2$ d'où $n \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.35

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

1) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec l'addition dans** $\mathbb{Z}$).*
2) *Si $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$, alors $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ (**Compatibilité de la congruence** $\bmod n$ **avec la multiplication dans** $\mathbb{Z}$)*

Démonstration.

Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$. Alors, $n \mid a_1 - b_1$ et $n \mid a_2 - b_2$ d'où $n \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$ et donc $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$.

□

Démonstration.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Démonstration.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$. On a $a_1 a_2 - b_1 b_2 =$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Démonstration.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$. On a $a_1 a_2 - b_1 b_2 = a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2 =$

Démonstration.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$. On a $a_1 a_2 - b_1 b_2 = a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2 = (a_1 - b_1)a_2 + (a_2 - b_2)b_1$

Démonstration.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$. On a $a_1 a_2 - b_1 b_2 = a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2 = (a_1 - b_1)a_2 + (a_2 - b_2)b_1$ d'où $n \mid a_1 a_2 - b_1 b_2$ car $n \mid a_1 - b_1$ et $n \mid a_2 - b_2$.

Démonstration.

- Supposons que $a_1 \equiv b_1 \pmod{n}$ et $a_2 \equiv b_2 \pmod{n}$. On a $a_1 a_2 - b_1 b_2 = a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2 = (a_1 - b_1)a_2 + (a_2 - b_2)b_1$ d'où $n \mid a_1 a_2 - b_1 b_2$ car $n \mid a_1 - b_1$ et $n \mid a_2 - b_2$. Donc $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Proposition 2.36

Les correspondances suivantes $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $(\overline{x}, \overline{y}) \mapsto \overline{x+y}$ *et* $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $(\overline{x}, \overline{y}) \mapsto \overline{x \cdot y}$ *sont des applications et ainsi* $+$ *et* $\cdot$ *sont des lois de composition internes définies dans* $\mathbb{Z}/n\mathbb{Z}$.

Démonstration.

- Soit $(\overline{x_1}, \overline{y_1}), (\overline{x_2}, \overline{y_2}) \in (\mathbb{Z}/n\mathbb{Z})^2$ tels que $(\overline{x_1}, \overline{y_1}) = (\overline{x_2}, \overline{y_2})$. Alors,
$\begin{cases} \overline{x_1} = \overline{x_2} \\ \overline{y_1} = \overline{y_2} \end{cases}$ d'où $\begin{cases} x_1 \equiv x_2 \pmod{n} \\ y_1 \equiv y_2 \pmod{n} \end{cases}$ ainsi $x_1 + y_1 \equiv x_2 + y_2 \pmod{n}$ et donc $\overline{x_1 + y_1} = \overline{x_2 + y_2}$.
- Soit $(\overline{x_1}, \overline{y_1}), (\overline{x_2}, \overline{y_2}) \in (\mathbb{Z}/n\mathbb{Z})^2$ tels que $(\overline{x_1}, \overline{y_1}) = (\overline{x_2}, \overline{y_2})$. Alors,
$\begin{cases} \overline{x_1} = \overline{x_2} \\ \overline{y_1} = \overline{y_2} \end{cases}$ d'où $\begin{cases} x_1 \equiv x_2 \pmod{n} \\ y_1 \equiv y_2 \pmod{n} \end{cases}$ ainsi $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{n}$ et donc $\overline{x_1 \cdot y_1} = \overline{x_2 \cdot y_2}$.

□

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.37

L'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ munissent cet ensemble d'une structure d'anneau commutatif non trivial. Cet anneau admet $\overline{0}$ pour élément nul et $\overline{1}$ pour unité.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts*

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective :

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$.

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in \{0, 1, \ldots, n-1\}$ tel que $a \in \overline{x}$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in \{0, 1, \ldots, n-1\}$ tel que $a \in \overline{x}$ d'où il existe $a \in \{0, 1, \ldots, n-1\} : \overline{a} = \overline{x}$,

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in \{0, 1, \ldots, n-1\}$ tel que $a \in \overline{x}$ d'où il existe $a \in \{0, 1, \ldots, n-1\} : \overline{a} = \overline{x}$, i.e., il existe $a \in \{0, 1, \ldots, n-1\} : f(a) = \overline{x}$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in \{0, 1, \ldots, n-1\}$ tel que $a \in \overline{x}$ d'où il existe $a \in \{0, 1, \ldots, n-1\} : \overline{a} = \overline{x}$, i.e., il existe $a \in \{0, 1, \ldots, n-1\} : f(a) = \overline{x}$. On a aussi f est injective :

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in \{0, 1, \ldots, n-1\}$ tel que $a \in \overline{x}$ d'où il existe $a \in \{0, 1, \ldots, n-1\} : \overline{a} = \overline{x}$, i.e., il existe $a \in \{0, 1, \ldots, n-1\} : f(a) = \overline{x}$. On a aussi f est injective : en effet, Soit $a, a' \in \{0, 1, \ldots, n-1\}$ tels que $f(a) = f(a')$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in \{0, 1, \ldots, n-1\}$ tel que $a \in \overline{x}$ d'où il existe $a \in \{0, 1, \ldots, n-1\} : \overline{a} = \overline{x}$, i.e., il existe $a \in \{0, 1, \ldots, n-1\} : f(a) = \overline{x}$. On a aussi f est injective : en effet, Soit $a, a' \in \{0, 1, \ldots, n-1\}$ tels que $f(a) = f(a')$. Alors, $\overline{a} = \overline{a'}$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in \{0, 1, \ldots, n-1\}$ tel que $a \in \overline{x}$ d'où il existe $a \in \{0, 1, \ldots, n-1\} : \overline{a} = \overline{x}$, i.e., il existe $a \in \{0, 1, \ldots, n-1\} : f(a) = \overline{x}$. On a aussi f est injective : en effet, Soit $a, a' \in \{0, 1, \ldots, n-1\}$ tels que $f(a) = f(a')$. Alors, $\overline{a} = \overline{a'}$ d'où $a' \in \overline{a}$ et ainsi il existe $a, a' \in \{0, 1, \ldots, n-1\} : a, a' \in \overline{a}$

Théorème 2.38

La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ *et une bijection et ainsi* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ *sont deux à deux distincts et* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration.

Il est évident que f est une application bien définie. Montrons que f est surjective : Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in \{0, 1, \ldots, n-1\}$ tel que $a \in \overline{x}$ d'où il existe $a \in \{0, 1, \ldots, n-1\} : \overline{a} = \overline{x}$, i.e., il existe $a \in \{0, 1, \ldots, n-1\} : f(a) = \overline{x}$. On a aussi f est injective : en effet, Soit $a, a' \in \{0, 1, \ldots, n-1\}$ tels que $f(a) = f(a')$. Alors, $\overline{a} = \overline{a'}$ d'où $a' \in \overline{a}$ et ainsi il existe $a, a' \in \{0, 1, \ldots, n-1\} : a, a' \in \overline{a}$ donc $a = a'$. □

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$,

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$. Comme $d \mid d$ et $d \mid n$, $d \mid 1$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$. Comme $d \mid d$ et $d \mid n$, $d \mid 1$ et donc $d = 1$.
Réciproquement, supposons que n est premier.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$. Comme $d \mid d$ et $d \mid n$, $d \mid 1$ et donc $d = 1$.
Réciproquement, supposons que n est premier. Soit $\overline{d} \in (\mathbb{Z}/n\mathbb{Z})^{\star}$.

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$. Comme $d \mid d$ et $d \mid n$, $d \mid 1$ et donc $d = 1$.
Réciproquement, supposons que n est premier. Soit $\overline{d} \in (\mathbb{Z}/n\mathbb{Z})^{\star}$. Puisque $n \nmid d$ et n est premier, $n \wedge d = 1$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$. Comme $d \mid d$ et $d \mid n$, $d \mid 1$ et donc $d = 1$.
Réciproquement, supposons que n est premier. Soit $\overline{d} \in (\mathbb{Z}/n\mathbb{Z})^{\star}$. Puisque $n \nmid d$ et n est premier, $n \wedge d = 1$ d'où il existe $(u, v) \in \mathbb{Z}^2 : un + vd = 1$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$. Comme $d \mid d$ et $d \mid n$, $d \mid 1$ et donc $d = 1$.
Réciproquement, supposons que n est premier. Soit $\overline{d} \in (\mathbb{Z}/n\mathbb{Z})^{\star}$. Puisque $n \nmid d$ et n est premier, $n \wedge d = 1$ d'où il existe $(u, v) \in \mathbb{Z}^2 : un + vd = 1$ ainsi $\overline{v}\,\overline{d} = \overline{1}$

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$. Comme $d \mid d$ et $d \mid n$, $d \mid 1$ et donc $d = 1$.
Réciproquement, supposons que n est premier. Soit $\overline{d} \in (\mathbb{Z}/n\mathbb{Z})^{\star}$. Puisque $n \nmid d$ et n est premier, $n \wedge d = 1$ d'où il existe $(u, v) \in \mathbb{Z}^2 : un + vd = 1$ ainsi $\overline{v}\,\overline{d} = \overline{1}$ et par suite $\overline{d}$ est inversible

Divisibilité dans $\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

Théorème 2.39

$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soit d un diviseur positif de n différent de n. Alors, $\overline{d}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z}$ est un corps et $\overline{d} \neq \overline{0}$ d'où il existe $\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \overline{1}$ ainsi $1 - dk = hn$, avec $h \in \mathbb{Z}$, et par suite $1 = hn + dk$. Comme $d \mid d$ et $d \mid n$, $d \mid 1$ et donc $d = 1$.
Réciproquement, supposons que n est premier. Soit $\overline{d} \in (\mathbb{Z}/n\mathbb{Z})^{\star}$. Puisque $n \nmid d$ et n est premier, $n \wedge d = 1$ d'où il existe $(u, v) \in \mathbb{Z}^2 : un + vd = 1$ ainsi $\overline{v}\,\overline{d} = \overline{1}$ et par suite $\overline{d}$ est inversible donc $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

Théorème 2.40 (Petit théorème de Fermat)

Soit $a \in \mathbb{Z}$ et p un nombre premier.

Théorème 2.40 (Petit théorème de Fermat)

Soit $a \in \mathbb{Z}$ et p un nombre premier. Si p ne divise pas a, alors $a^{p-1} \equiv 1 \pmod{p}$.

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a.

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$.

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$,

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$.

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^{\star}$.

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts :

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\}$: $\overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$.

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\}$: $\overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h - k$

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\}$: $\overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$.

Divisibilité dans $\mathbb{Z}$

Petit théorème de Fermat

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\}$: $\overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\}$: $\overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$.

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\}$: $\overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$. Puisque $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} \subset (\mathbb{Z}/p\mathbb{Z})^\star$ et $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts,

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$. Puisque $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} \subset (\mathbb{Z}/p\mathbb{Z})^\star$ et $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts, $X = (\mathbb{Z}/p\mathbb{Z})^\star$.

Divisibilité dans $\mathbb{Z}$

Petit théorème de Fermat

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$. Puisque $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} \subset (\mathbb{Z}/p\mathbb{Z})^\star$ et $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts, $X = (\mathbb{Z}/p\mathbb{Z})^\star$. Donc $\overline{a}.\overline{2a} \ldots \overline{(p-1)a} = \overline{1}.\overline{2} \ldots \overline{(p-1)}$

Divisibilité dans $\mathbb{Z}$

Petit théorème de Fermat

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$. Puisque $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} \subset (\mathbb{Z}/p\mathbb{Z})^\star$ et $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts, $X = (\mathbb{Z}/p\mathbb{Z})^\star$. Donc $\overline{a}.\overline{2a} \ldots \overline{(p-1)a} = \overline{1}.\overline{2} \ldots \overline{(p-1)}$ ainsi $\overline{(p-1)!}\overline{a^{p-1}} = \overline{(p-1)!}$,

Divisibilité dans $\mathbb{Z}$

Petit théorème de Fermat

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$. Puisque $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} \subset (\mathbb{Z}/p\mathbb{Z})^\star$ et $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts, $X = (\mathbb{Z}/p\mathbb{Z})^\star$. Donc $\overline{a}.\overline{2a} \ldots \overline{(p-1)a} = \overline{1}.\overline{2} \ldots \overline{(p-1)}$ ainsi $\overline{(p-1)!}\overline{a^{p-1}} = \overline{(p-1)!}$, i.e., $((p-1)!)a^{p-1} \equiv ((p-1)!) \pmod{p}$

Divisibilité dans $\mathbb{Z}$

Petit théorème de Fermat

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$. Puisque $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} \subset (\mathbb{Z}/p\mathbb{Z})^\star$ et $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts, $X = (\mathbb{Z}/p\mathbb{Z})^\star$. Donc $\overline{a}.\overline{2a} \ldots \overline{(p-1)a} = \overline{1}.\overline{2} \ldots \overline{(p-1)}$ ainsi $\overline{(p-1)!}\overline{a^{p-1}} = \overline{(p-1)!}$, i.e., $((p-1)!)a^{p-1} \equiv ((p-1)!) \pmod{p}$ d'où $p \mid (p-1)!(a^{p-1}-1)$.

Divisibilité dans $\mathbb{Z}$

Petit théorème de Fermat

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$. Puisque $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} \subset (\mathbb{Z}/p\mathbb{Z})^\star$ et $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts, $X = (\mathbb{Z}/p\mathbb{Z})^\star$. Donc $\overline{a}.\overline{2a} \ldots \overline{(p-1)a} = \overline{1}.\overline{2} \ldots \overline{(p-1)}$ ainsi $\overline{(p-1)!}\overline{a^{p-1}} = \overline{(p-1)!}$, i.e., $((p-1)!)a^{p-1} \equiv ((p-1)!) \pmod{p}$ d'où $p \mid (p-1)!(a^{p-1}-1)$. Comme p ne divise pas $(p-1)!$, $p \mid (a^{p-1}-1)$,

Divisibilité dans $\mathbb{Z}$

Petit théorème de Fermat

Démonstration.

Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. On considère l'ensemble $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. On a $\forall \overline{x} \in X, \overline{x} \neq \overline{0}$, sinon il existe $k \in \{1, \ldots, (p-1)\} : \overline{ka} = \overline{0}$ d'où $p \mid ka$ donc $p \mid k$ ce qui est faux car $1 \leq k < p$. Alors, $X \subset (\mathbb{Z}/p\mathbb{Z})^\star$. Aussi, les éléments $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts : en effet, supposons que $\overline{ha} = \overline{ka}$, où $h, k \in \{1, \ldots, (p-1)\}$. Alors, $p \mid ha - ka = (h-k)a$ d'où $p \mid h-k$ ainsi $p \mid |h-k|$. Puisque $1 \leq h, k < p$, $|h-k| < p$. Comme $p \mid |h-k|$ et $|h-k| < p$, $|h-k| = 0$ donc $h = k$. Puisque $X = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} \subset (\mathbb{Z}/p\mathbb{Z})^\star$ et $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sont deux à deux distincts, $X = (\mathbb{Z}/p\mathbb{Z})^\star$. Donc $\overline{a}.\overline{2a} \ldots \overline{(p-1)a} = \overline{1}.\overline{2} \ldots \overline{(p-1)}$ ainsi $\overline{(p-1)!}\overline{a^{p-1}} = \overline{(p-1)!}$, i.e., $((p-1)!)a^{p-1} \equiv ((p-1)!) \pmod{p}$ d'où $p \mid (p-1)!(a^{p-1}-1)$. Comme p ne divise pas $(p-1)!$, $p \mid (a^{p-1}-1)$, i.e., $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire 2.41

Si p est un nombre premier, alors pour tout $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

Démonstration.

Soit $a \in \mathbb{Z}$.
Si $p \mid a$, alors $a \equiv 0 \pmod{p}$ et ainsi $a^p \equiv a \pmod{p}$.
Si $p \nmid a$, alors, d'après le théorème précédent, $a^{p-1} \equiv 1 \pmod{p}$ d'où $a^p \equiv a \pmod{p}$. □

Définition 2.42

Pour tout entier $n \geq 1$, on note $\varphi(n)$ le nombre des entiers $k \in \{0, 1, \ldots, n-1\}$ tels que $k \wedge n = 1$, i.e., $\varphi(n) = card\{k \in \{0, 1, \ldots, n-1\} / k \wedge n = 1\}$.
L'application φ est appelée la **fonction indicatrice d'Euler** ou **l'indicateur d'Euler** et $\varphi(n)$ est dit indicateur d'Euler de n.

Remarque 2.43

Soit $n \in \mathbb{N}^{\star}$. On a $\varphi(n) = card\{k \in \{1, \ldots, n\} / k \wedge n = 1\}$.

Exemple 2.44

On a $\varphi(1) = 1, \varphi(2) = 1, \varphi(10) = 4$.

Théorème 2.45

Si p est un nombre premier et $k > 0$ est un entier, alors $\varphi(p^k) = p^k - p^{k-1}$.

Démonstration.

On a $\varphi(p^k) = card\{m \in \{1,2,\ldots,p^k\}/m \wedge p^k = 1\}$. Au lieu de compter les entiers $m \in \{1,2,\ldots,p^k\}$ tels que $m \wedge p^k = 1$, nous allons compter les entiers $m \in \{1,2,\ldots,p^k\}$ tels que $m \wedge p^k \neq 1$. Soit $m \in \{1,2,\ldots,p^k\}$. On a $m \wedge p^k \neq 1$ si, et seulement si, $p \mid m$, i.e., si, et seulement si, m est un multiple de p. Ainsi, $m \wedge p^k \neq 1$ si, et seulement si, $m \in \{1.p, 2.p, \ldots, p^{k-1}p\}$ d'où le nombre des entiers $m \in \{1,2,\ldots,p^k\}$ tels que $m \wedge p^k \neq 1$ est p^{k-1} et donc $\varphi(p^k) = p^k - p^{k-1}$. □

Lemme 2.46

Soit $a, b, c \in \mathbb{N}$. $a \wedge bc = 1$ si, et seulement si, $a \wedge b = 1$ et $a \wedge c = 1$.

Démonstration.

Supposons que $a \wedge bc = 1$. Posons $d = a \wedge b$. Alors, $d \mid b$ d'où $d \mid bc$. Puisque $d \mid a$ et $d \mid bc$, $d \mid (a \wedge bc)$ ainsi $d \mid 1$ donc $d = 1$. De la même façon, on montre que $a \wedge c = 1$.

Réciproquement, supposons que $a \wedge b = 1$ et $a \wedge c = 1$. Alors, il existe $u, v \in \mathbb{Z} : ua + vb = 1$ et il existe $s, t \in \mathbb{Z} : sa + tc = 1$ d'où $usa^2 + utac + vsab + vtbc = 1$,i.e., $(usa + utc + vsb)a + (vt)bc = 1$ et donc, d'après le lemme de Bézout, $a \wedge bc = 1$. □

Théorème 2.47

Soit $m, n \in \mathbb{N} - \{0, 1\}$. Si m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.

Divisibilité dans $\mathbb{Z}$

Fonction indicatrice d'Euler

Démonstration.

On écrit les entiers de 1 à mn sous la forme du tableau suivant avec n lignes et m colonnes :

$$\begin{array}{cccccc} 1 & 2 & \dots & r & \dots & m \\ m+1 & m+2 & & m+r & & 2m \\ 2m+1 & 2m+2 & & 2m+r & & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & & (n-1)m+r & & nm \end{array}$$

Démonstration.

On écrit les entiers de 1 à mn sous la forme du tableau suivant avec n lignes et m colonnes :

$$\begin{array}{ccccccc} 1 & & 2 & \dots & r & \dots & m \\ m+1 & & m+2 & & m+r & & 2m \\ 2m+1 & & 2m+2 & & 2m+r & & 3m \\ \vdots & & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & & (n-1)m+2 & & (n-1)m+r & & nm \end{array}$$

On sait que $\varphi(mn)$ est le nombre des entiers $k \in \{1, \dots, mn\}$ tels que $k \wedge mn = 1$, i.e., $\varphi(mn)$ est le nombre des éléments de ce tableau qui sont premiers avec mn

Démonstration.

On écrit les entiers de 1 à mn sous la forme du tableau suivant avec n lignes et m colonnes :

$$\begin{array}{ccccccc} 1 & & 2 & \dots & r & \dots & m \\ m+1 & & m+2 & & m+r & & 2m \\ 2m+1 & & 2m+2 & & 2m+r & & 3m \\ \vdots & & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & & (n-1)m+2 & & (n-1)m+r & & nm \end{array}$$

On sait que $\varphi(mn)$ est le nombre des entiers $k \in \{1, \dots, mn\}$ tels que $k \wedge mn = 1$, i.e., $\varphi(mn)$ est le nombre des éléments de ce tableau qui sont premiers avec mn et donc, d'après le lemme précédent, $\varphi(mn)$ est le nombre des éléments de ce tableau qui sont premiers à la fois avec m et avec n.

□

Démonstration.

On considère un élément de la r ième colonne.

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm + r$

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux.

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.
Montrons que dans chaque colonne de ces $\varphi(m)$ colonnes, il y a exactement $\varphi(n)$ éléments qui sont premiers avec n :

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.
Montrons que dans chaque colonne de ces $\varphi(m)$ colonnes, il y a exactement $\varphi(n)$ éléments qui sont premiers avec n : Supposons que $r\wedge m = 1$. dans la r ième colonne, on a exactement n entiers qui sont
$r, m+r, 2m+r \ldots, (n-1)m+r$.

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.
Montrons que dans chaque colonne de ces $\varphi(m)$ colonnes, il y a exactement $\varphi(n)$ éléments qui sont premiers avec n : Supposons que $r\wedge m = 1$. dans la r ième colonne, on a exactement n entiers qui sont
$r, m+r, 2m+r \ldots, (n-1)m+r$.
Aussi, ces entiers sont deux à deux non congrus modulo n, en effet :

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.
Montrons que dans chaque colonne de ces $\varphi(m)$ colonnes, il y a exactement $\varphi(n)$ éléments qui sont premiers avec n : Supposons que $r\wedge m = 1$. dans la r ième colonne, on a exactement n entiers qui sont
$r, m+r, 2m+r \ldots, (n-1)m+r$.
Aussi, ces entiers sont deux à deux non congrus modulo n, en effet : si $hm+r \equiv km+r \pmod{n}$, avec $0 \leq h,k \leq n-1$,

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.

Montrons que dans chaque colonne de ces $\varphi(m)$ colonnes, il y a exactement $\varphi(n)$ éléments qui sont premiers avec n : Supposons que $r\wedge m = 1$. dans la r ième colonne, on a exactement n entiers qui sont

$r, m+r, 2m+r \ldots, (n-1)m+r$.

Aussi, ces entiers sont deux à deux non congrus modulo n, en effet : si $hm+r \equiv km+r \pmod{n}$, avec $0 \leq h,k \leq n-1$, alors $hm \equiv km \pmod{n}$

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.

Montrons que dans chaque colonne de ces $\varphi(m)$ colonnes, il y a exactement $\varphi(n)$ éléments qui sont premiers avec n : Supposons que $r\wedge m = 1$. dans la r ième colonne, on a exactement n entiers qui sont

$r, m+r, 2m+r \ldots, (n-1)m+r$.

Aussi, ces entiers sont deux à deux non congrus modulo n, en effet : si $hm+r \equiv km+r \pmod{n}$, avec $0 \leq h,k \leq n-1$, alors $hm \equiv km \pmod{n}$ d'o'u $n \mid (h-k)m$

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.

Montrons que dans chaque colonne de ces $\varphi(m)$ colonnes, il y a exactement $\varphi(n)$ éléments qui sont premiers avec n : Supposons que $r\wedge m = 1$. dans la r ième colonne, on a exactement n entiers qui sont

$r, m+r, 2m+r \ldots, (n-1)m+r$.

Aussi, ces entiers sont deux à deux non congrus modulo n, en effet : si $hm+r \equiv km+r \pmod{n}$, avec $0 \leq h,k \leq n-1$, alors $hm \equiv km \pmod{n}$ d'o'u $n \mid (h-k)m$ ainsi $n \mid h-k$ car $n\wedge m = 1$ et par suite $n \mid |h-k| < n$

Démonstration.

On considère un élément de la r ième colonne. Cet élément est de la forme $qm+r$ et puisque $(qm+r)\wedge m = r\wedge m$, on a $qm+r$ et m sont premiers entre eux si, et seulement si, r et m sont premiers entre eux. Alors, on a exactement $\varphi(m)$ colonnes contenant des entiers premiers avec m et dans une telle colonne, chaque élément est premiers avec m.
Montrons que dans chaque colonne de ces $\varphi(m)$ colonnes, il y a exactement $\varphi(n)$ éléments qui sont premiers avec n : Supposons que $r\wedge m = 1$. dans la r ième colonne, on a exactement n entiers qui sont
$r, m+r, 2m+r \ldots, (n-1)m+r$.
Aussi, ces entiers sont deux à deux non congrus modulo n, en effet : si $hm+r \equiv km+r \pmod{n}$, avec $0 \leq h,k \leq n-1$, alors $hm \equiv km \pmod{n}$ d'o'u $n \mid (h-k)m$ ainsi $n \mid h-k$ car $n\wedge m = 1$ et par suite $n \mid |h-k| < n$ et donc $|h-k| = 0$, i.e., $h = k$.

Démonstration.

Puisque les n entiers $r, m+r, 2m+r \ldots, (n-1)m+r$ sont deux à deux non congrus modulo n, ces n entiers de la r ième colonne sont, dans un certain ordre, congrus modulo n à $0, 1, 2, \ldots, n-1$

Démonstration.

Puisque les n entiers $r, m+r, 2m+r \ldots, (n-1)m+r$ sont deux à deux non congrus modulo n, ces n entiers de la r ième colonne sont, dans un certain ordre, congrus modulo n à $0, 1, 2, \ldots, n-1$ et donc la r ième colonne et $\{0, 1, \ldots, n-1\}$ contient le même nombre d'entiers qui sont premiers avec n (car si $s \equiv t \pmod{n}$, alors $s \wedge n = 1$ si, et seulement si, $t \wedge n = 1$)

Démonstration.

Puisque les n entiers $r, m+r, 2m+r \ldots, (n-1)m+r$ sont deux à deux non congrus modulo n, ces n entiers de la r ième colonne sont, dans un certain ordre, congrus modulo n à $0, 1, 2, \ldots, n-1$ et donc la r ième colonne et $\{0, 1, \ldots, n-1\}$ contient le même nombre d'entiers qui sont premiers avec n (car si $s \equiv t \pmod{n}$, alors $s \wedge n = 1$ si, et seulement si, $t \wedge n = 1$) et donc on a $\varphi(n)$ éléments qui sont premiers avec n dans la r ième colonne.

Démonstration.

Puisque les n entiers $r, m+r, 2m+r \ldots, (n-1)m+r$ sont deux à deux non congrus modulo n, ces n entiers de la r ième colonne sont, dans un certain ordre, congrus modulo n à $0, 1, 2, \ldots, n-1$ et donc la r ième colonne et $\{0, 1, \ldots, n-1\}$ contient le même nombre d'entiers qui sont premiers avec n (car si $s \equiv t \pmod{n}$, alors $s \wedge n = 1$ si, et seulement si, $t \wedge n = 1$) et donc on a $\varphi(n)$ éléments qui sont premiers avec n dans la r ième colonne.
Alors, le nombre total des éléments de ce tableau qui sont premiers avec mn est $\varphi(m)\varphi(n)$

Démonstration.

Puisque les n entiers $r, m+r, 2m+r \ldots, (n-1)m+r$ sont deux à deux non congrus modulo n, ces n entiers de la r ième colonne sont, dans un certain ordre, congrus modulo n à $0, 1, 2, \ldots, n-1$ et donc la r ième colonne et $\{0, 1, \ldots, n-1\}$ contient le même nombre d'entiers qui sont premiers avec n (car si $s \equiv t \pmod{n}$, alors $s \wedge n = 1$ si, et seulement si, $t \wedge n = 1$) et donc on a $\varphi(n)$ éléments qui sont premiers avec n dans la r ième colonne.
Alors, le nombre total des éléments de ce tableau qui sont premiers avec mn est $\varphi(m)\varphi(n)$ et donc $\varphi(mn) = \varphi(m)\varphi(n)$. □

Divisibilité dans $\mathbb{Z}$

Fonction indicatrice d'Euler

Théorème 2.48

Soit $n > 1$ un entier et $n = p_1^{k_1} \dots p_r^{k_r}$, avec $p_1, \dots, p_r$ des nombres premiers deux à deux distincts et $k_1, \dots, k_r$ des entiers > 0, alors
$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \dots (p_r^{k_r} - p_r^{k_r-1}) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r})$.

Démonstration.

Utilisons une récurrence sur r :
On a déjà vu que si $r = 1$, le résultat est vrai.
Supposons que le résultat est vrai à un rang $r \geq 1$.
Soit $p_1^{k_1} \dots p_r^{k_r} p_{r+1}^{k_{r+1}}$, avec $p_1, \dots, p_{r+1}$ des nombres premiers deux à deux distincts et $k_1, \dots, k_{r+1}$ des entiers > 0. Puisque $(p_1^{k_1} \dots p_r^{k_r}) \wedge p_{r+1}^{k_{r+1}} = 1$,
$\varphi(p_1^{k_1} \dots p_r^{k_r} p_{r+1}^{k_{r+1}}) = \varphi((p_1^{k_1} \dots p_r^{k_r}).p_{r+1}^{k_{r+1}}) = \varphi(p_1^{k_1} \dots p_r^{k_r})\varphi(p_{r+1}^{k_{r+1}})$ ainsi
$\varphi(p_1^{k_1} \dots p_r^{k_r} p_{r+1}^{k_{r+1}}) = \varphi(p_1^{k_1} \dots p_r^{k_r}).(p_{r+1}^{k_{r+1}} - p_{r+1}^{k_{r+1}-1}$ et donc, d'après l'hypothèse de récurrence,
$\varphi(p_1^{k_1} \dots p_r^{k_r} p_{r+1}^{k_{r+1}}) = (p_1^{k_1} - p_1^{k_1-1}) \dots (p_r^{k_r} - p_r^{k_r-1})(p_{r+1}^{k_{r+1}} - p_{r+1}^{k_{r+1}-1}$. Alors, le résultat est vrai pour tout entier $r \geq 1$.

Exemple 2.49

On a $1800 = 2^3 3^2 5^2$. *Alors,*
$\varphi(1800) = 2^2(2-1).3(3-1).5(5-1) = 480.$