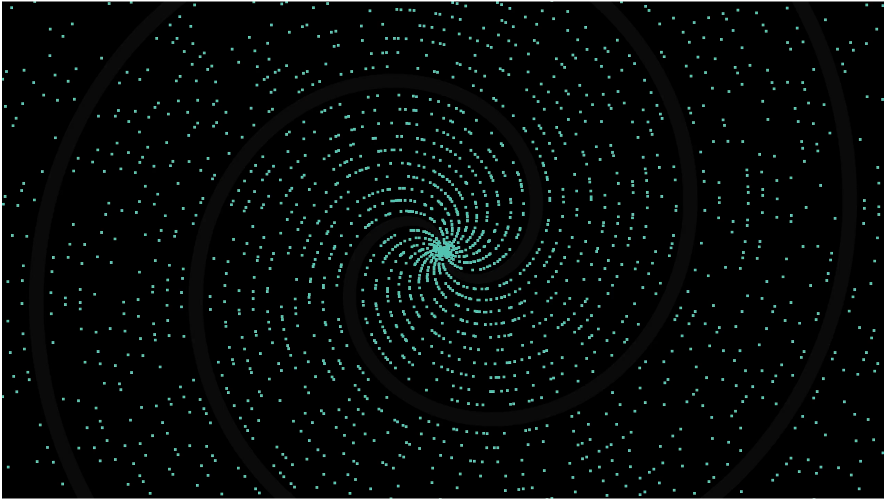
Divisibilité, Division euclidienne et Congruence

MatheX

27 octobre 2024



Divisibilité, Division euclidienne et Congruence

Table des matières :

Divisibilité, Division euclidienne et Congruence

Table des matières :

Divisibilité, Division euclidienne et Congruence

Définition 1 : (définition de la divisibilité)

$$\boxed{b \mid a \iff \text{il existe } k \in \mathbb{Z} \text{ tel que } a = kb}$$

NB

On peut dire de manière équivalente :

- b divise a
- b est un diviseur de a
- a est divisible par b
- a est un multiple de b

Propriété 1 : (propriétés de la divisibilité)

$$b \mid a \text{ et } a \neq 0 \implies |b| \leq |a| \qquad \text{(minoration du diviseur)}$$

$$c \mid b \text{ et } b \mid a \implies c \mid a \qquad \text{(transitivité)}$$

$$b \mid a \text{ et } b \mid c \implies b \mid (ka + k'c) \qquad \text{(combinaison linéaire)}$$

pour tout entier k et k'

$$b \mid a \implies b \mid (ka + k'b) \qquad \text{(combinaison linéaire)}$$

pour tout entier k et k'

Divisibilité, Division euclidienne et Congruence

Démonstration :

Divisibilité, Division euclidienne et Congruence

Table des matières :

Divisibilité, Division euclidienne et Congruence

Théorème 1 : (existence et unicité de la division euclidienne)

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Il existe un unique couple d'entiers $(q\,;\,r)$ tel que :

$$\boxed{a = bq + r \qquad \text{avec } q \in \mathbb{Z} \quad \text{et} \quad 0 \leq r < b}$$

NB

Cette relation est la division euclidienne de a par b avec :

- a le dividende et b le diviseur ;
- q le quotient et r le reste.

Divisibilité, Division euclidienne et Congruence

Démonstration :

Propriété 2 : (formes d'un entier)

Soit b un entier supérieur ou égal à 2.

Tout entier a s'écrit sous une des formes :

$$a = bq + r \qquad \text{avec } r \in \{0\,;\,1\,;\,\cdots\,;\,b-1\} \quad \text{et} \quad q \text{ un entier}$$

Divisibilité, Division euclidienne et Congruence

Table des matières :

Divisibilité, Division euclidienne et Congruence

Définition 2 : (définition de la congruence)

Soit a et $b \in \mathbb{Z}$; et $m \in \mathbb{N}^*$

a et b sont congrus modulo m $\iff$ a et b ont le même reste dans la division euclidienne par m

NB

- On écrit : $a \equiv b\ [m]$ ou $a \equiv b\ mod\ m$ ou $a \equiv b\ (m)$.
- On dit aussi : a est congru à b modulo m.
- $a \equiv b\ [m] \iff$ il existe un entier k tel que $a = b + k \times m$

Divisibilité, Division euclidienne et Congruence

Propriété 3 : (congruence et divisibilité)

$$\boxed{a \equiv b\ [m] \iff m \mid (a-b)}$$

Divisibilité, Division euclidienne et Congruence

Démonstration :

Propriété 4 : (propriétés de la relation de congruence)

$$a \equiv a \ [m] \qquad \text{(réflexivité)}$$

$$a \equiv b \ [m] \ \Rightarrow b \equiv a \ [m] \qquad \text{(symétrie)}$$

$$a \equiv b \ [m] \ \text{ et } \ b \equiv c \ [m] \ \Rightarrow a \equiv c \ [m] \qquad \text{(transitivité)}$$

$$\left.\begin{array}{l} a \equiv b \ [m] \\ c \equiv d \ [m] \end{array}\right\} \Rightarrow a + c \equiv b + d \ [m] \qquad \text{(compatibilité avec la somme)}$$

$$\left.\begin{array}{l} a \equiv b \ [m] \\ c \equiv d \ [m] \end{array}\right\} \Rightarrow a \times c \equiv b \times d \ [m] \qquad \text{(compatibilité avec le produit)}$$

$$a \equiv b \ [m] \ \Rightarrow a^k \equiv b^k \ [m] \qquad \text{(compatibilité avec la puissance)}$$

pour tout entier naturel k non nul

Divisibilité, Division euclidienne et Congruence

Démonstration :

Divisibilité, Division euclidienne et Congruence

Définition 3 : (inverse modulo m)

a est un inverse de b modulo m $\iff$ $\boxed{a \times b = 1\ [m]}$

a est inversible modulo m $\iff$ il existe au moins un inverse de a modulo m