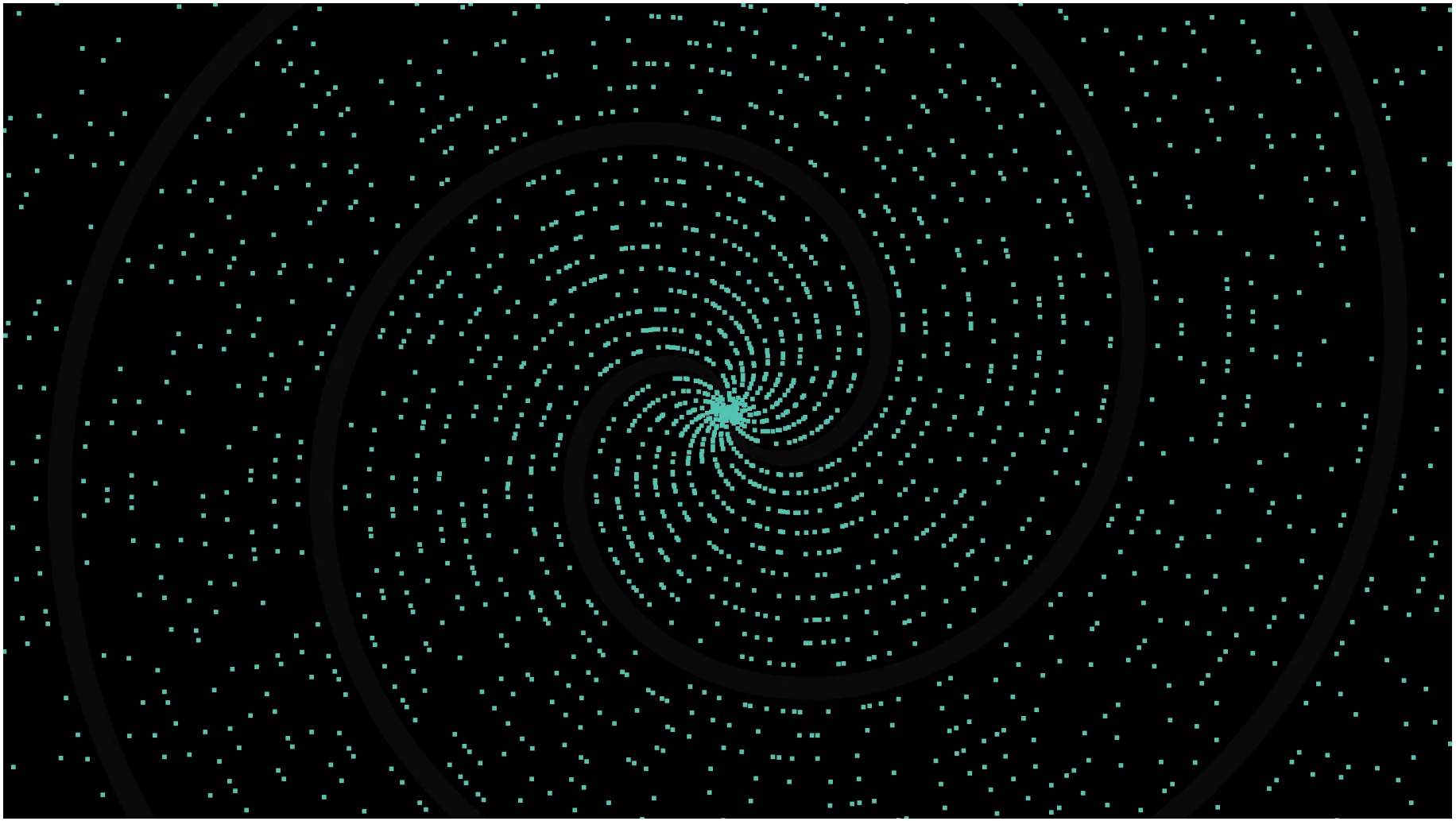
PGCD

MatheX

7 mars 2025



PGCD

Table des matières :

PGCD

Table des matières :

PGCD

Définition 1 : (définition du PGCD)

Soit a et b deux entiers relatifs non simultanément nuls.

L'ensemble des diviseurs communs à a et b admet un plus grand élément d appelé Plus Grand Diviseur Commun de a et b :

$$d = \text{PGCD}(a\,;b)$$

NB On note aussi (dans le supérieur) : $d = a \wedge b$

PGCD

Propriété 1 : (propriétés du PGCD)

Soit a et b deux entiers relatifs non simultanément nuls et k un entier relatif.

$$PGCD(a\,;\,b) = PGCD(b\,;\,a) \qquad \text{(commutatitivité)}$$
$$PGCD(a\,;\,b) = PGCD(|a|\,;\,|b|) \qquad (a \text{ et } -a \text{ ont les mêmes diviseurs})$$
$$1 \leq PGCD(a\,;\,b) \leq min(|a|, |b|) \qquad \text{(1 est toujours diviseur commun)}$$
$$\text{(les diviseurs de } a \text{ sont} \leq |a|)$$
$$PGCD(a\,;\,0) = |a| \qquad \text{(tous les entiers non nuls divisent 0)}$$
$$PGCD(a\,;\,1) = 1 \qquad (1|a \text{ et les diviseurs de 1 sont} \leq 1)$$

$$PGCD(a\,;\,b) = PGCD(a-b\,;\,a) \qquad \text{(méthode de la soustraction)}$$
$$PGCD(ka\,;\,kb) = |k| \times PGCD(a\,;\,b) \qquad \text{(multiplication par un scalaire)}$$

PGCD

Démonstration :

PGCD

Définition 2 : (nombres premiers entre eux)

Soit a et b deux entiers relatifs non nuls.

a et b pemier entre eux $\iff$ PGCD(a ; b) = 1

NB les diviseurs communs de a et b sont 1 et -1

PGCD

Propriété 2 : (PGCD et nombres premiers entre eux)

a, b, a' et b' sont des entiers relatifs non nuls.
d est un entier naturel non nul.

$$d = PGCD(a\,;\,b) \iff \begin{cases} a = da' \\ b = db' \end{cases} \text{ avec } PGCD(a'\,;\,b') = 1$$

PGCD

Démonstration :

PGCD

Propriété 3 : (PGCD et division euclidienne)

Soit a et b deux entiers naturels non nuls.

Soit r le reste de la division euclidienne de a par b :

$$a = bq + r$$

On a alors :

$$\text{PGCD}(a\ ;\ b) = \text{PGCD}(b\ ;\ r)$$

PGCD

Démonstration :

PGCD

Théorème 1 : (algorithme d'Euclide)

Soit a et b deux entiers naturels non nuls.

Soit la suite (r_n) des restes définit récursivement par :

- $r_0 = b$ et r_1 est le reste de la division euclidienne de a par b ;
- pour tout $i \geq 2$:
  - si $r_{i-1} = 0$ alors $r_i = 0$;
  - sinon r_i est le reste de la division euclidienne de r_{i-2} par r_{i-1}.

La suite (r_n) est nulle à partir d'un certain rang et le dernier terme non nul est le PGCD de a et b .

$$
\begin{aligned}
a &= b\,q_1 + r_1 \\
b &= r_1\,q_2 + r_2 \\
r_1 &= r_2\,q_3 + r_3 \\
&\vdots \quad\quad \vdots \quad\quad \vdots \\
r_{k-2} &= r_{k-1}\,q_k + r_k \\
r_{k-1} &= r_k\,q_{k+1} + 0
\end{aligned}
$$

$$PGCD(a;b) = r_k$$

PGCD

Démonstration :

PGCD

Table des matières :

PGCD

Théorème 2 : (identité de Bézout)

Soit a et b deux entiers relatifs non simultanément nuls.

Il existe un couple $(u; v)$ d'entiers relatifs tel que :

$$a\,u + b\,v = PGCD(a\,;b)$$

NB Ce couple n'est pas unique

PGCD

Démonstration :

PGCD

Théorème 3 : (corrolaire de Bézout)

Soit a et b deux entiers relatifs non simultanément nuls et c un entier relatif

L'équation $\boxed{ax + by = c}$ admet des solutions entières $\iff$ c est un multiple de $PGCD(a; b)$

NB Une équation diophantienne est une équation polynomiale à coefficients entiers dont on cherche des solutions entières (ou rationnelles)

PGCD

Démonstration :

PGCD

Théorème 4 : (théorème de Bézout)

Soit a et b deux entiers relatifs non nuls.

a et b premier entre eux $\iff$ il existe deux entiers relatifs u et v tel que $\boxed{au + bv = 1}$

NB Ce couple n'est pas unique

PGCD

Démonstration :

Table des matières :

PGCD

Théorème 5 : (théorème de Gauss)

Soit a, b et c trois entiers relatifs non nuls.

$$\left.\begin{array}{r} a \text{ et } b \text{ premier entre eux} \\ a \text{ divise le produit } bc \end{array}\right\} \Longrightarrow \quad a \text{ divise } c$$

PGCD

Démonstration :

PGCD

Théorème 6 : (corrolaire du théorème de Gauss)

Soit a, b et c trois entiers relatifs non nuls.

$$\left.\begin{array}{r} b \text{ et } c \text{ premier entre eux} \\ b \text{ divise } a \\ c \text{ divise } a \end{array}\right\} \Longrightarrow \quad \text{le produit } bc \text{ divise } a$$

PGCD

Démonstration :