P.G.C.D. DE DEUX ENTIERS

1 Diviseurs communs

Définition 1

- Pour un entier n, on note $\mathrm{D}(n)$ l'ensemble des diviseurs positifs de n.
- Pour deux entiers a et b tous les deux non nuls, on note $\mathrm{D}(a\,;b)$ l'ensemble des diviseurs positifs communs à a et à b.

Exemple 1

- $\mathrm{D}(0) = \mathbb{N}^{\times}$, $\mathrm{D}(1) = \{1\}$.
- $\mathrm{D}(729) = \{1\,;3\,;9\,;27\,;81\,;243\,;729\}$.
- $\mathrm{D}(12) = \{1\,;2\,;3\,;4\,;6\,;12\}$.
- $\mathrm{D}(12\,;729) = \{1\,;3\}$.
- $\mathrm{D}(512\,;729) = \{1\}$.

Propriété 1

Pour deux entiers a et b tous les deux non nuls, $\mathrm{D}(a\,;b) = \mathrm{D}(a) \cap \mathrm{D}(b)$.

Définition 2

Pour deux entiers a et b tels que $ab \neq 0$, le **plus grand commun diviseur (p.g.c.d)** de a et de b est le plus grand élément de l'ensemble $\mathrm{D}(a\,;b)$.

Exemple 2

- Le p.g.c.d. de 12 et 729 est 3.
- Le p.g.c.d. de 512 et 729 est 1.

Propriété 2

Pour deux entiers a et b non nuls, on note $\mathrm{M}(a)$ et $\mathrm{M}(b)$ l'ensemble de leurs multiples. Le plus petit entier de $\mathrm{M}(a) \cap \mathrm{M}(b)$ est le **plus petit commun multiple** (p.p.c.m.) de a et b. En outre, $\mathrm{pgcd}(a\,;b) \times \mathrm{ppcm}(a\,;b) = a \times b$.

2 Algorithme d'Euclide

Propriété 3

Pour deux entiers $a \geqslant b$, et r le reste de la division euclidienne de a par b, on a $\mathrm{D}(a\,;b) = \mathrm{D}(b\,;r)$.
Le dernier reste non nul est le p.g.c.d. de a et de b.

Les entrées sont deux entiers a et b avec $a \geqslant b$.
La sortie est a (dernier reste non nul).

Tant que $b \neq 0$
  $a \leftarrow b$
  $b \leftarrow \mathrm{mod}(a\,;b)$
Fin Tant que

Exemple 3

$\mathrm{D}(1\ 824\,;656) = \mathrm{D}(656\,;512) = \mathrm{D}(512\,;144) = \mathrm{D}(144\,;80) = \mathrm{D}(80\,;64) = \mathrm{D}(64\,;16) = \mathrm{D}(16,0)$.
Ainsi, $\mathrm{pgcd}(1\ 824\,;656) = 16$.

Propriété 4

a et b sont deux entiers non nuls.

- $\mathrm{D}(a\,;b) = \mathrm{D}\left(\mathrm{pgcd}(a\,;b)\right)$.
- Si d divise a et d divise b, alors d divise $\mathrm{pgcd}(a\,;b)$.
- Si $d = \mathrm{pgcd}(a\,;b)$, alors il existe deux entiers a' et b' tels que $a = da'$ et $b = db'$ avec $\mathrm{pgcd}(a'\,;b') = 1$.

3 Nombres premiers entre eux

♯ Propriété 5

Deux entiers naturels a et b non nuls sont **premiers entre eux** si $\text{pgcd}(a\,;b)=1$.

↪ Exemple 4

- 12 et 729 ne sont pas premiers entre eux.
- 512 et 729 sont premiers entre eux.

⊛ Théorème 1 : Théorème de Bézout

a et b sont deux entiers naturels non nuls.

- a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au+bv=1$.
- $\text{pgcd}(a\,;b)=d$ si et seulement si il existe deux entiers relatifs u et v tels que $au+bv=d$.

↪ Exemple 5

1. Déterminer le p.g.c.d. de 921 et 737.
   En déduire une relation de la forme $921u+737v=d$.
   $921=737\times1+184$ et $737=184\times4+1$.
   Ainsi, $\text{pgcd}(921\,;737)=1$ et
   $737=184\times4+1$, donc $737=(921-737)\times4+1 \Leftrightarrow -4\times921+5\times737=1$.
2. Démontrer que, pour tout entier naturel n, $2n+1$ et $3n+2$ sont premiers entre eux.
   $2\times(3n+2)-3\times(2n+1)=6n+4-6n-3=1$
   donc $2n+1$ et $3n+2$ sont premiers entre eux et ce, pour tout n.

4 Propriétés supplémentaires de la relation de divisibilité

♯ Propriété 6

Pour a ; b et c trois entiers non nuls et $d=\text{pgcd}(a\,;b)$,

- $c\,\text{pgcd}(a\,;b)=\text{pgcd}(ac\,;bc)$;
- si c divise a et b, on note $a=ca'$, $b=cb'$ et $d=cd'$, alors $d'=\text{pgcd}(a'\,;b')$.

↪ Exemple 6

On a vu que $\text{pgcd}(12;729)=3$. Ainsi,

- $\text{pgcd}(120;7\ 290)=30$;
- $\text{pgcd}\left(\dfrac{12}{3};\dfrac{729}{3}\right)=\dfrac{3}{3}$, donc $\text{pgcd}(4;243)=1$.

⊛ Théorème 2 : Lemme de Gauß

Pour a ; b et c trois entiers non nuls,

- si a divise bc et $\text{pgcd}(a\,;b)=1$, alors a divise c.
- si a divise c et b divise c et $\text{pgcd}(a\,;b)=1$), alors ab divise c.

↪ Exemple 7

Déterminer tous les couples d'entiers $(x\,;y)$ tels que $11(x-3)=7(y+2)$.