PGCD – PPCM – THEOREMES DE BEZOUT ET GAUSS

I) PGCD (*rappels*)

1) Définition

DEFINITION

Soit a et b deux entiers relatifs non nuls.

L'ensemble des diviseurs communs à a et b ***admet un plus grand élément D appelé plus grand commun diviseur.***

On note $D = PGCD\,(a\,;b)$.

• ***L'ensemble D existe-t-il ?***

L'ensemble des diviseurs communs à a et b est un ensemble fini comme intersection de deux ensembles finis. De plus, 1 divise a et b donc l'ensemble des diviseurs communs à a et b est non vide. Or tout ensemble fini non vide admet un plus petit élément donc D existe.

• ***EXEMPLES***

$$PGCD(24\,;18) = 6 \qquad PGCD(60\,;84) = 12 \qquad PGCD(150\,;240) = 30$$

PROPRIETES

- **Si b divise a alors $PGCD(a\,;b) = b$.**
- **Pour tout entier naturel k non nul, on a : $PGCD(k\,a\,;k\,b) = k\,PGCD(a\,;b)$.**

EXEMPLE

Le PGCD de 420 et 540 revient à chercher le PGCD de 21 et 27.

En effet : $420 = \ldots \times \ldots \times \ldots$ et $540 = \cdots \times \ldots \times \ldots$

Or : $PGCD(21\,;27) = 3$ donc $PGCD(420\,;540) = \cdots \times \ldots \times \ldots = 60$

2) Nombres premiers entre eux

DEFINITION

On dit que a et b sont premiers entre eux si et seulement si $PGCD(a\,;b) = 1$.

• Par exemple, 15 et 8 sont premiers entre eux puisque $PGCD(15\,;8) = 1$.

• **ATTENTION** : *il ne faut pas confondre des nombres premiers entre eux et des nombres premiers. 15 et 8 ne sont pas premiers et pourtant ils sont premiers entre eux. Par contre, deux nombres premiers distincts sont nécessairement premiers entre eux.*

3) Algorithme d'Euclide

EXEMPLE (*rappels*)

Calculer le $PGCD(4\,539\,;1\,958)$.

On effectue les divisions euclidiennes suivantes :

$4\,539 = 1\,958 \times \ldots + \ldots$

$1\,958 = 623 \times \ldots + \ldots$

$623 = 89 \times \ldots + \ldots$

Le $PGCD(4\,539\,;1\,958)$ **est le dernier reste non nul soit** $PGCD(4\,539\,;1\,958) = \ldots\ldots$

REMARQUE : LE PETIT NOMBRE D'ETAPES MONTRE LA PERFORMANCE DE CET ALGORITHME.

THEOREME

Soient a et b deux entiers naturels non nuls tels que b ne divise pas a.

La suite des divisions euclidiennes suivantes finit par s'arrêter. Le dernier reste non nul est alors le $PGCD(a\,;b)$.

$$\begin{array}{llll} a \text{ par } b & a = b\,q_0 + r_0 & \text{avec} & b > r_0 \geq 0 \\ b \text{ par } r_0 & b = r_0\,q_1 + r_1 & \text{avec} & r_0 > r_1 \geq 0 \\ r_0 \text{ par } r_1 & r_0 = r_1\,q_2 + r_2 & \text{avec} & r_1 > r_2 \geq 0 \\ \vdots & \vdots & \vdots & \\ r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1}\,q_n + r_n & \text{avec} & r_{n-1} > r_n \geq 0 \\ r_{n-1} \text{ par } r_n & r_{n-1} = r_n\,q_{n-1} + 0 & & \end{array}$$

On a alors $PGCD(a\,;b) = r_n$.

DEMONSTRATION

• *Lorsque vous étiez en 3ème, vous vous êtes bien sûr tous demandés pourquoi cet algorithme fonctionnait à chaque fois… Heureusement, maintenant, nous allons pouvoir le démontrer…*

ALGORITHME

Voici un algorithme qui permet de déterminer le PGCD de deux nombres.

Variables
a, b, d, q, r
Initialisation
Lire a, b
$a \to d$
Si $a < b$
  $b \to a$
  $d \to b$
FinSi
Traitement
$E(a/b) \to q$
$a - bq \to r$
Tantque $r \neq 0$
  $b \to a$
  $r \to b$
  $E(a/b) \to q$
  $a - bq \to r$
FinTantque
Sortie
Afficher b

II) PCM : PLUS PETIT COMMUN MULTIPLE

DEFINITION

Soient a et b deux entiers relatifs non nuls.

L'ensemble des multiples strictement positifs communs à a et b ***admet un plus petit élément M, appelé plus petit commun multiple.***

On le note : $M = PPCM(a\,;b)$.

• L'ensemble des multiples strictement positifs à a et b n'est pas vide : en effet le produit $|a\ b|$ est un multiple positif de a et b. Toute partie non vide de $\mathbb{N}$, admet un plus petit élément, donc M existe.

EXEMPLE

$$PPCM(18\,;12) = 36 \qquad PPCM(24\,;40) = 120$$

• Pour additionner deux fractions, on recherche le dénominateur commun le plus petit, qui n'est autre que le *PPCM*.

PROPRIETES

- **Si a divise b alors $PPCM(a\,;b) = b$.**
- **Si a et b sont premiers entre eux alors $PPCM(a\,;b) = |a\ b|$.**
- **On a $a\ b = PPCM(a\,;b) \times PGCD(a\,;\ b)$.**

III) THEOREME DE BÉZOUT

1) Egalité de BÉZOUT

THEOREME

Soient a et b deux entiers non nuls, et $D = PGCD(a\,;b)$.

Il existe alors un couple $(u\,;v)$ d'entiers relatifs tels que : $\boldsymbol{a\,u + b\,v = D}$

DEMONSTRATION

- **CONSEQUENCE** : ***Tout diviseur commun à a et b divise leur PGCD.***

2) Théorème de BÉZOUT

THEOREME

Deux entiers relatifs a et b sont premiers entre eux, si et seulement si, il existe deux entiers relatifs u et v tels que :

$$\boldsymbol{a\,u + b\,v = 1}$$

DEMONSTRATION **- ROC -**

→ Dans le sens « ⇒ » : Immédiat grâce à l'égalité de Bézout.

→ Dans le sens « ⇐ » : réciproquement.

On suppose qu'il existe deux entiers u et v tels que $a\,u + b\,v = 1$.

……

……

EXEMPLES

a) Montrer que $2\,n + 1$ et $3\,n + 2$ sont premiers entre eux pour tout $n \in \mathbb{N}$.

b) Montrer que 59 et 27 sont premiers entre eux puis déterminer un couple $(x\,;y)$ tel que $59\,x + 27\,y = 1$.

AUTRE EXEMPLE

Montrer que 71 et 19 sont premiers entre eux puis déterminer un couple $(x\,;y)$ tel que $71\,x + 19\,y = 1$.

3) Corollaire de BÉZOUT

THEOREME

> ***L'équation $a\,x + b\,y = c$ admet des solutions entières si et seulement si c est un multiple du $PGCD(a\,;b)$.***

DEMONSTRATION

- Dans le sens « ⇒ » :

  $a\,x + b\,y = c$ admet une solution $(x_0\,;\,y_0)$.

……

……

- Dans le sens « ⇐ » : réciproquement

  c est un multiple de $D = PGCD(a\,;b)$.

……

……

……

……

EXEMPLES

- L'équation $4\,x + 9\,y = 2$ admet des solutions car $PGCD(4\,;9) = 1$ et 2 est un multiple de 1.
- L'équation $9\,x - 15\,y = 2$ n'admet pas de solution car $PGCD(9\,;15) = 3$ et 2 non multiple de 3.

IV) THEOREME DE GAUSS

1) Théorème

THEOREME

> ***Soient a, b et c trois entiers relatifs non nuls.***
>
> ***Si a divise le produit bc et si a et b sont premiers entre eux alors a divise c.***

DEMONSTRATION **ROC**

- Si a divise le produit bc, alors il existe un entier k tel que $b\,c = k\,a$.
- Si a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que :

$$a\,u + b\,v = 1.$$

En multipliant par c, on a : $a\,c\,u + b\,c\,v = c$ or $b\,c = k\,a$, donc :

$$a\,c + k\,a\,v = c \quad \rightarrow \quad a(c + k\,v) = c$$

Donc a *divise* c.

EXEMPLE

Trouver les solutions dans $\mathbb{Z}^2$ de l'équation $5(x-1) = 7\,y$.

2) Corollaire du théorème de GAUSS

THEOREME

Si b et c divise a et si b et c sont premiers entre eux alors bc divise a.

DEMONSTRATION **ROC**

Si b et c divise a alors il existe k et k' entiers relatifs tels que :

$$a = k\,b \quad \text{et} \quad a = k'c \quad \text{donc} \quad k\,b = k'c$$

b divise $k'c$ or $PGCD(b\,;c) = 1$ donc d'après le théorème de GAUSS b divise k' donc $k' = k''b$

D'où $a = k'c = k''b\,c$

Donc bc divise a.

EXEMPLE : Si 5 et 12 divise a, comme 5 et 12 sont premiers entre eux, $5 \times 12 = 60$ divise a.

3) Propriétés

Ces propriétés découlent du théorème de Bézout et de Gauss.

PROPRIETES

Soient a et b deux entiers non nuls, D leur $PGCD$ et M leur $PPCM$.

- ***Il existe deux entiers a' et b' premiers entre eux tels que :*** $a = D\,a'$ ***et*** $b = D\,b'$.
- ***On a les relations suivantes :*** $M = D\,a'b'$ ***et*** $a\,b = M\,D$.

EXERCICES DIVERS

1) Méthode : Déterminer le reste d'une division euclidienne à l'aide de congruences

Déterminer le reste de la division de 2^{456} par 5 et de 2^{437} par 7.

2) Méthode : Résoudre une équation avec des congruences

Déterminer les entiers x tels que $6 + x \equiv 5[3]$ puis les entiers x tels que $3x \equiv 5[4]$

3) Méthode : Démontrer que deux entiers sont premiers entre eux

Démontrer que pour tout entier naturel n, $2n + 3$ et $5n + 7$ sont premiers entre eux.

4) Méthode : Résoudre une équation du type $ax + by = c$

Déterminer les entiers x et y tels que $5x + 7y = 1$ puis les entiers x et y tels que $5x + 7y = 12$.