Chap 3. PGCD et Théorème de Bézout

Terminale S spécialité

Etienne Bézout (1730 -1783)

Mathématicien français, célèbre pour le théorème de Bachet-Bézout lié aux équations diophantiennes en arithmétique et pour son théorème sur le nombre de points d'intersection de deux courbes algébriques, résultat crucial en géométrie algébrique.

Chap 3. PGCD et Théorème de Bézout
Terminale S spécialité

I. Le PGCD de deux entiers

a et b désignent deux nombres entiers relatifs non nuls.

Notation

On note **$\mathcal{D}(a;b)$ l'ensemble des diviseurs communs à a et b** ainsi $\mathcal{D}(a;b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.

Exemples :

- Déterminer $\mathcal{D}(12;30)$, $\mathcal{D}(a;0)$, $\mathcal{D}(1;a)$ pour tout a.
- Quel élément appartient à $\mathcal{D}(a;b)$ pour tout a et b ?
- Si b divise a, que peut-on en déduire ?

Propriétés :

▶1. Soient a et b deux entiers relatifs

$\mathcal{D}(a;b) = \mathcal{D}(a-b;b)$ et $\forall k \in \mathbb{Z}\ \mathcal{D}(a;b) = \mathcal{D}(a-kb;b)$

▶2. Soient a un entier relatif et b un entier naturel non nul

Si r est le reste de la division euclidienne de a par b alors

$$\mathcal{D}(a;b) = \mathcal{D}(b;r)$$

Démonstration

Propriété et définition :

Soient a et b deux entiers relatifs non nuls, $\mathcal{D}(a;b)$ admet un plus grand élément, on le note $\boldsymbol{PGCD(a;b)}$ (Plus Grand Diviseur Commun).

Propriétés :

Soient a et b deux entiers relatifs non nuls

- $PGCD(a;b) = PGCD(a-b;b)$
- $\forall k \in \mathbb{Z}\ \ PGCD(a;b) = PGCD(a-kb;b)$

Lemme d'Euclide :

Soient a un entier relatif et b un entier naturel non nul

Si $\boldsymbol{r}$ est le reste de la division euclidienne de $\boldsymbol{a}$ par $\boldsymbol{b}$ alors

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

Exemples :

Déterminer le $PGCD$ de 1602 et 2670.

Propriétés :

Soient a et b deux entiers relatifs non nuls

$$\forall k \in \mathbb{Z}^* \quad PGCD(ka; kb) = |k| PGCD(a; b)$$

Définition :

On dit que deux entiers relatifs non nuls, a et b sont **premiers entre eux** lorsque $\boldsymbol{PGCD(a; b) = 1}$.

Propriétés :

Soient a et b deux entiers relatifs non nuls

$PGCD(a; b) = d$ si, et seulement si, il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Propriété :

Soient a et b deux entiers relatifs non nuls
Si $PGCD(a\,;b) = d$ alors il existe deux entiers relatifs u et v tels que $d = au + bv$.

Remarque :

Un tel couple appelé coefficient de Bézout n'est pas unique.

Exemple :

Pour $a = 120$ et $b = 75$, déterminer un couple d'entiers relatifs tels que $au + bv = PGCD(a; b)$.

Théorème de Bézout :

Soient a et b deux entiers relatifs non nuls

$PGCD(a\,;b) = 1$ si, et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Exemple :

Pour tout $n \in \mathbb{N}^*$, $2n + 1$ et $3n + 1$ sont-ils premiers entre eux ?

Exemple :

Pour tout $n \in \mathbb{N}^*$, si n divise 42 alors n divise 6 ou n divise 7.

Vrai ou faux ?

Théorème de Gauss :

Soient a, b et c trois entiers relatifs non nuls

Si a divise bc et a est premier avec b alors a divise c.

Démonstration

Exemple :

Déterminer tous les couples d'entiers relatifs $(x; y)$ solution de l'équation $6x = 5y$.

II. Nombres premiers

Définition :
Un entier naturel p est premier lorsqu'il admet exactement deux diviseurs : 1 et lui-même.
Un nombre ayant au moins trois diviseurs est dit composé.

Exemple :
Parmi les nombres suivants, lesquels sont premiers ?
7 - 6 - 5 - 1 - 154 - 647382915 - 899 – 9059 – 142 661

Propriété :
Tout entier naturel $n \geq 2$ admet au moins un diviseur premier.

Théorème, critère de primalité :
Soit n un entier naturel, $n \geq 2$
Si n n'est pas premier alors il admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$.

Corollaire, test de primalité :
Soit n un entier naturel, $n \geq 2$
Si n n'est divisible par aucun nombre premier inférieur à $\sqrt{n}$ alors il est premier.

Lemme :

Soit p un nombre premier

Si n est un entier naturel alors soit p divise n soit p et n sont premiers entre eux.

démo :

Propriété :

Soit a et b deux entiers relatifs non nuls et p un nombre premier,

Si p divise ab alors p divise a ou p divise b.

démo :

Théorème :
L'ensemble des nombres premiers est infini.
démo :
Théorème de décomposition en nombres premiers :
Tout nombre entier naturel supérieur ou égal à 2 est un produit de nombres premiers. Cette décomposition est unique à l'ordre des facteurs près. C'est-à-dire que, $\forall n \in \mathbb{N}, n \geq 2$

$$\boldsymbol{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}}$$

où $p_1 < p_2 < \cdots < p_k$ sont des nombres premiers et $\alpha_1, \alpha_2, \ldots, \alpha_k$ sont des entiers naturels non nuls.
Exemple : Décomposer 3600 et 420 en facteurs premiers.
Donner le PGCD et le PPCM de 3600 et 420.