Chapitre 5- PGCD-Théorème de Bézout- Théorème de Gauss

Terminale - Maths Expertes

1 PGCD de deux nombres entiers

1.1 Ensemble des diviseurs communs à 2 entiers

Soit a un entier relatif, on note $D(a)$ l'ensemble des entiers relatifs diviseurs de a. Soit b un entier relatif, on note $D(a;b)$ l'ensemble des diviseurs communs à a et à b.

Propriété 1.1.
Soient a et b deux entiers relatifs,

1. Pour tout entier relatif k ; $D(a;b) = D(a-kb, b)$,
2. En particulier $D(a;b) = D(a-b;b)$,
3. Si r est le reste de la division euclidienne de a par b alors $D(a;b) = D(b;r)$.

1.2 Pgcd de deux entiers

Définition 1.1.
Soient 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 diviseur commun**. On note $D = pgcd(a;b)$.

Démonstration. Nous allons démontrer l'existence de ce PGCD. L'ensemble des diviseurs communs à a et b est un ensemble fini car c'est l'intersection de deux ensembles finis. De plus 1 divise a et b donc l'ensemble $D(a;b)$ est non vide, or tout ensemble fini non vide admet un plus grand élément, donc D existe. CQFD

Exemple :

$pgcd(24;18) = 6; pgcd(60;84) = 12$

Propriété 1.2.
Soit a et b deux entiers relatifs non nuls

1. $pgcd(b, 0) = |b|$
2. $pgcd(a; b) = pgcd(|a|; |b|)$
3. $pgcd(a; b) = pgcd(b; a)$
4. $pgcd(a; 1) = 1$
5. Si b divise a alors $pgcd(a; b) = |b|$
6. Pour tout $k \in \mathbb{Z}; pgcd(a; b) = pgcd(a - kb; b)$
7. $pgcd(a; b) = pgcd(a - b; b)$.
8. **Lemme d'Euclide :** Si r est le reste de la division euclidienne de a par b alors $pgcd(a; b) = pgcd(b; r)$.

1.3 Algorithme d'Euclide

Théorème 1.1.
Soit a et b deux entiers non nuls tels que b ne divise pas a. On suppose que $0 < b \leqslant a$ La suite des divisions euclidiennes suivantes est finie et le dernier reste non nul est le $pgcd(a; b)$.

$$\begin{array}{ccc} a \text{ par } b & a = bq_0 + r_0 & b > r_0 \geqslant 0 \\ b \text{ par } r_0 & b = r_0q_1 + r_1 & r_0 > r_1 \geqslant 0 \\ r_0 \text{ par } r_1 & r_0 = r_1q_2 + r_2 & r_1 > r_2 \geqslant 0 \\ \vdots & \vdots & \vdots \\ r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1}q_n + r_n & r_{n-1} > r_n \geqslant 0 \\ r_{n-1} \text{ par } r_n & r_{n-1} = r_nq_n + 0 & \end{array}$$

On a $pgcd(a; b) = r_n$.

Exemple :

Calculer le $pgcd(4539; 1958)$

Propriété 1.3.
Soient a et b deux entiers tels que $b \neq 0$

1. L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de leur pgcd.
2. $pgcd(ka; kb) = |k|pgcd(a; b)$.

2 Nombres premiers entre eux

Définition 2.1.
On dit que deux entiers a et b sont premiers entre eux si et seulement si $pgcd(a; b) = 1$.

Propriété 2.1.
Soient deux entiers relatifs a et b non nuls.
Si $d = pgcd(a; b)$ alors il existe a' et b' deux entiers relatifs premiers entre eux tels que $a = da'$ et $b = db'$.

3 Théorème de Bézout

3.1 Egalité de Bézout

Théorème 3.1.
Soient a et b deux entiers non nuls et $D = pgcd(a;b)$. Il existe un couple (u,v) d'entiers relatifs tel que :

$$au + bv = D$$

.

3.2 Théorème de Bézout

Théorème 3.2.
Soient a et b deux entiers premiers entre eux si et seulement si il existe un couple (u,v) d'entiers relatifs tel que :

$$au + bv = 1$$

.

Exemple :

Montrer que 59 et 27 sont premiers entre eux et déterminer le couple (x ; y) tel que $59x + 27y = 1$.
$59 = 27 \times 2 + 5$ donc $5 = 59 - 2 \times 27$
$27 = 5 \times 5 + 2$ donc $2 = 27 - 5 \times 5$
Donc $2 = 27 - 5 \times (59 - 2 \times 27) = -5 \times 59 + 11 \times 27$
On poursuit : $5 = 2 \times 2 + 1$ donc $1 = 5 - 2 \times 2$
En remplaçant : $1 = 59 - 2 \times 27 - 2 \times (-5 \times 59 + 11 \times 27) = 11 \times 59 - 24 \times 27$

On a trouvé un couple $(x,y) = (11;-24)$ tel que $59x + 27y = 1$ donc, d'après le théorème de Bézout, 59 et 27 sont premiers entre eux.

3.3 Corollaire

Théorème 3.3.
L'équation $ax+by = c$ admet des solutions entières si et seulement si c est un multiple du $PGCD(a,b)$.

4 Théorème de Gauss

4.1 Théorème

Théorème 4.1.
Soit 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.

4.2 Corollaire du théorème

Théorème 4.2.
Soit b et c divise a et si b et c sont premiers entre eux alors le produit bc divise a.