CHAPITRE 6

PGCD ET ÉQUATIONS DIOPHANTIENNES

BÉZOUT (Bezout) Étienne, français, 1730-1783
Son nom est principalement attaché à des travaux sur les équations algébriques et à l'arithmétique.

GAUSS Karl Friedrich, allemand, 1777-1855
Enfant prodige, né à Brunswick dans une famille pauvre. Il étudia à Göttingen de 1795 à 1798 et soutint l'année suivante (1799) à Helmstedt sa thèse portant sur une démonstration rigoureuse du fameux théorème de d'Alembert. Son nom est principalement attaché au théorème de Gauss.

Pierre Simon de Fermat, français, 1601/1608-1665
Reprenant les travaux de Diophante d'Alexandrie, traduits et complétés par Bachet de Méziriac, il redora le blason de l'arithmétique en créant la théorie des nombres.

Le théorème de Fermat (conjecturé par Fermat et démontré par Wiles) nous dit que si $n \in \mathbb{N}$ et $n > 2$ alors il n'existe pas de nombres entiers non nul x, y et z tels que :

$$x^n + y^n = z^n$$

Les contenus du chapitre
- ▷ PGCD de deux entiers. Algorithme d'Euclide.
- ▷ Couples d'entiers premiers entre eux.
- ▷ Théorème de Bézout.
- ▷ Théorème de Gauss.

Les capacités attendues du chapitre
- ▷ Déterminer les PGCD d'un entier.
- ▷ Résoudre des équations diophantiennes simples.

Cours

1. PGCD et PPCM de deux entiers

1.1. Définition

On note $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$.

Définition 1 – PGCD et PPCM

- Le PGCD(a,b) est le plus grand diviseur commun de a et de b.
- Le PPCM(a,b) est le plus petit multiple commun de a et de b.

Exemples :
▷ PGCD$(21;35)$ = ...
▷ PPCM$(21;35)$ = ...

Définition 2 – Nombres premiers entre eux ou étrangers

a et b sont premiers entre eux ou étrangers si et seulement si PGCD$(a;b) = 1$

Le seul diviseur positif commun de a et b est 1.

Exemples :
▷ 2 et 3 sont premiers entre eux.
▷ 22 et 65 sont premiers entre eux.

Propriété 1

On note a, b, u et v quatre nombres entiers relatifs non nuls tels que $au+bv = 1$.
a et b sont premiers entre eux.

Démonstration Condition nécessaire pour être premiers entre eux.

Exemple :
▷ 5 et 3 sont premiers entre eux car $5 \times 2 - 3 \times 3 = 1$.

Propriété 2 – PGCD et division euclidienne

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

où $\text{Mod}(a;b)$ est le reste de la division euclidienne de a par b.

Démonstration

Propriété 3 – PGCD et soustraction

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

Démonstration

1.2. Méthodes de calcul

Méthode 1 – Première méthode de calcul du PGCD

Il suffit de faire la liste des diviseurs de a et de b.
Exemple :
▷ On souhaite trouver PGCD(12;18)
Diviseurs positifs de 12 : 1 ; 2 ; 3 ; 4 ; 6 ; 12
Diviseurs positifs de 18 : 1 ; 2 ; 3 ; 6 ; 9 ; 18
Donc PGCD(12;18) = 6

Méthode 2 – Deuxième méthode de calcul du PGCD

On utilise l'algorithme d'**Euclide**.
On effectue des divisions euclidiennes successives en prenant à chaque fois le diviseur et le reste de la division précédente :

$$\begin{gathered} a = bq_1 + r_1 \text{ avec } 0 \leq r_1 < b \\ b = r_1 q_2 + r_2 \text{ avec } 0 \leq r_2 < r_1 \\ r_1 = r_2 q_3 + r_3 \text{ avec } 0 \leq r_3 < r_2 \\ \vdots \\ \vdots \\ r_{n-2} = r_{n-1} q_n + r_n \text{ avec } 0 \leq r_n < r_{n-1} \end{gathered}$$

Que peut-on dire de la suite des restes (r_n) ? On peut dire que c'est une suite décroissante de nombres entiers naturels, donc elle atteint 0 au bout d'un certain rang.

Où trouve t-on le PGCD dans cette suite ? C'est le dernier reste non nul car

$$\text{PGCD}(a;b) = \text{PGCD}(b;r_1) = \text{PGCD}(r_1;r_2) = \ldots = \text{PGCD}(r_k;0) = r_k$$

Exemple :
▷ On souhaite trouver PGCD(1071;1029) :
$1071 = 1029 \times 1 + 42$
$1029 = 42 \times 24 + 21$
$42 = 21 \times 2 + 0$
donc PGCD(1071;1029) = 21

Méthode 3 – Troisième méthode de calcul du PGCD

On utilise l'algorithme des **Soustractions**.
On effectue des divisions euclidiennes successives en prenant à chaque fois le diviseur et le reste de la division précédente :

$$\begin{gathered} a - b = r_1 \\ \text{Si } b < r_1 \text{ , } c \leftarrow b \text{ , } b \leftarrow r_1 \text{ , } r_1 \leftarrow c \text{ et } b - r_1 = r_2 \end{gathered}$$

$$\text{Si } r_1 < r_2 \text{ , } c \leftarrow r_1 \text{ , } r_1 \leftarrow r_2 \text{ , } r_2 \leftarrow c \text{ et } r_1 - r_2 = r_3$$
$$\vdots$$
$$\text{Si } r_{n-2} < r_{n-1} \text{ , } c \leftarrow r_{n-2} \text{ , } r_{n-2} \leftarrow r_{n-1} \text{ , } r_{n-1} \leftarrow c \text{ et } r_{n-2} - r_{n-1} = r_n$$

Que peut-on dire de la suite des restes (r_n) ? On peut dire que c'est une suite décroissante de nombres entiers naturels, donc elle atteint 0 au bout d'un certain rang.

Où trouve t-on le PGCD dans cette suite ? C'est le dernier reste non nul car

$$\text{PGCD}(a;b) = \text{PGCD}(b;r_1) = \text{PGCD}(r_1;r_2) = \ldots = \text{PGCD}(r_k;0) = r_k$$

Exemple :
▷ On souhaite trouver PGCD(12;15) :
$15 - 12 = 3$
$12 - 3 = 9$
$9 - 3 = 6$
$6 - 3 = 3$
$3 - 3 = 0$
donc PGCD(12;15) = 3

Méthode 4 – Quatrième méthode de calcul du PGCD

Dans le chapitre sur les nombres premiers nous allons voir comment exprimer tous les nombres entiers comme produits de nombres premiers.
Supposons que l'on connaisse les décompositions à l'aide des nombres premiers, comment trouver le PGCD des deux nombres ?
Exemple :
$a = 2^3 \times 3^2 \times 5 \times 7^2$ et $b = 2 \times 3^3 \times 5^4 \times 7 \times 11$
Pour trouver le PGCD($a;b$) on prend les facteurs communs avec les exposants les plus petits des deux, donc :

$$\text{PGCD}(a;b) = 2 \times 3^2 \times 5 \times 7 = 630$$

Méthode 5 – Calcul du PPCM

Comment calculer PPCM($a;b$) ?
▷ On fait la liste des multiples de a et des multiples de b puis on cherche le plus petit des nombres communs aux deux listes.

▷ On peut utiliser la formule admise :

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

Exemple :

On sait que PGCD$(12;15) = 3$ donc PPCM$(12;15) = \dfrac{12 \times 15}{3} = 60$

Propriété 4 – Diviseurs du PGCD

Soit a et b deux entiers relatifs non tous deux nuls.
Un entier relatif d est un diviseur commun à a et b si et seulement si d divise le PGCD(a,b).
Autrement dit, l'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de leur PGCD.

Démonstration

Propriété 5

Soit a et b deux entiers non nuls relatifs et $d = \text{PGCD}(a,b)$.

Il existe deux entiers relatifs a' et b' tels que $a = da'$, $b = db'$ et $\text{PGCD}(a',b') = 1$.

Démonstration

2. Théorème de Bézout et théorème de Gauss

Propriété 6 – Théorème de Bézout

Pour tout couple (a, b) d'éléments de $\mathbb{Z}^*$, il existe un couple (u, v) d'éléments de $\mathbb{Z}$ tel que :

$$au + bv = \text{PGCD}(a; b)$$

Démonstration

On note $p = \text{PGCD}(a; b)$
On note $D = \{au + bv \in \mathbb{N} \text{ avec } u \in \mathbb{Z} \text{ et } v \in \mathbb{Z}\}$
► D est une partie non vide de $\mathbb{N}$ car $D \subset \mathbb{N}$ et $|a| \in D$.
Ainsi D admet un plus petit élément que l'on nomme d.

► $p|a$ et $p|b$ donc $p|au + bv$ donc $p|d$ et $p \leq d$

► Montrons par récurrence que $p \in D$:
On sait d'après l'algorithme d'Euclide qu'il existe $k \in \mathbb{N}$ tel que $r_k = p$.
Montrons par récurrence que tous les r_k ($k \in \mathbb{N}$ et $r_k \neq 0$) sont dans D.
On note $\mathbf{P}_n$ la propriété : $r_n \in D$
Initialisation : (Pour $n = 1$)
▷ $r_1 = a - bq_1$ avec $r_1 \geq 0$, donc $r_1 \in \mathbb{N}$ donc $r_1 \in D$
▷ $r_2 = b - r_1 q_2 = b - (a - bq_1) \times q_2 = (1 + q_1 q_2)b - aq_2$ avec $r_2 \geq 0$, donc $r_2 \in \mathbb{N}$ donc $r_2 \in D$

ainsi $\mathbf{P}_1$ et $\mathbf{P}_2$ sont vraies.
Hérédité : on suppose que $\mathbf{P}_{k-2}$ et $\mathbf{P}_{k-1}$ sont vraies, montrons que dans ce cas $\mathbf{P}_k$ l'est aussi.
$\mathbf{P}_{k-2}$ est vraie donc il existe u et v tels que $r_{k-2} = au + bv \geq 0$.
$\mathbf{P}_{k-1}$ est vraie donc il existe u' et v' tels que $r_{k-1} = au' + bv' \geq 0$.

$r_k = r_{k-2} - r_{k-1}q_k = (au + bv) - (au' + bv')q_k = a(u - u'q_k) + b(v - v'q_k)$ et $r_k \geq 0$ donc $\mathbf{P}_k$ est vraie.
Conclusion :
$\left.\begin{array}{l}\mathbf{P}_1 \text{ et } \mathbf{P}_2 \text{ sont vraies} \\ \mathbf{P}_{k-2} \text{ et } \mathbf{P}_{k-1} \text{ impliquent } \mathbf{P}_k\end{array}\right\}$ donc pour tout $n \in \mathbb{N}$, $r_n \in D$.

On peut donc en conclure que $p \in D$ et donc que $p \geq d$.
▷ Comme $p \leq d$ et $p \geq d$ alors $p = d$
Il existe donc un couple (u, v) d'éléments de $\mathbb{Z}$ tel que

$$au + bv = \text{PGCD}(a, b).$$

Exemples :

▷ $\text{PGCD}(3;6) = 3$ et $6 \times 1 + 3 \times (-1) = 3$

▷ $\text{PGCD}(18;30) = 6$ et $30 \times (-1) + 18 \times 2 = 6$

Méthode 6 – Trouver le couple (u, v)

Exemple :
▷ On souhaite trouver u et v tels que $60u + 84v = 12$

On effectue, pour commencer, les divisions euclidiennes de l'algorithme d'euclide jusqu'à obtenir un reste de 12 :
$84 = 60 \times 1 + 24$
$60 = 24 \times 2 + 12$
Ensuite on isole les restes en remontant l'algorithme :
$12 = 60 - 24 \times 2 = 60 - (84 - 60 \times 1) \times 2 = 60 - 84 \times 2 + 60 \times 2 = 60 \times 3 + 84 \times (-2)$
donc $u = 3$ et $v = -2$

Propriété 7 – Propriété de Bézout

a et b sont premiers entre eux

$\Leftrightarrow$

Il existe un couple (u, v) d'éléments de $\mathbb{Z}$ tel que $au + bv = 1$

Démonstration

Exemple :
▷ $143 \times 47 - 210 \times 32 = 1$ donc 143 et 210 sont premiers entre eux.

Propriété 8 – Théorème de Gauss

a, b et c sont des entiers relatifs non nuls.

Si $a|bc$ et PGCD$(a;b) = 1$ alors $a|c$

Démonstration

Exemples :
▷ 7 divise $42 = 3 \times 14$ or PGCD$(7;3) = 1$ donc $7|14$

▷ Si $au = bv$ avec PGCD$(a;b) = 1$ alors $a|v$ et $b|u$.

⚠ Si $5|15k$ alors on ne peut pas affirmer que $5|k$ car 5 et 15 ne sont pas premiers entre eux.

Propriété 9 – Corollaire du théorème de Gauss

a, b, c sont trois entiers relatifs non nuls.
Si b et c sont premiers entre eux et divisent tous les deux a alors bc divise a.

Démonstration

3. Les équations diophantiennes

Définition 3 – Equation diophantienne

Une équation diophantienne est une équation à coefficients entiers et dont les inconnues sont des entiers. En classe de terminale, nous ne résolvons que les équations de la forme :

$$ax + by = k \times \text{PGCD}(a; b)$$

Exemples :
▷ $3x + 5y = 1$
▷ $15x + 21y = 3$
▷ Un peu d'histoire : Le théorème de Fermat (conjecturé par Fermat et démontré par Wiles) nous dit que si $n \in \mathbb{N}$ et $n > 2$ alors il n'existe pas de nombres entiers non nuls x, y et z tels que

$$x^n + y^n = z^n.$$

Propriété 10 – Solutions

Les solutions de $ax + by = k \times \text{PGCD}(a; b)$ sont :

$$S = \{(kx_1 + \delta b'; ky_1 - a'\delta), \delta \in \mathbb{Z}\}$$

où
x_1, y_1 sont des solutions de $ax+by=\text{PGCD}(a;b)$
$a'=\dfrac{a}{\text{PGCD}(a;b)}$ et $b'=\dfrac{b}{\text{PGCD}(a;b)}$.

Démonstration

Cette démonstration n'est pas à connaître par cœur mais à comprendre car elle donne la démarche pour résoudre les équations diophantiennes de l'année de terminale.

On souhaite résoudre l'équation diophantienne

$$(E)\ :\ ax+by=k\times\text{PGCD}(a;b)$$

Première étape : recherche d'une solution particulière de (E)
On calcule $\text{PGCD}(a,b)$ par l'algorithme d'Euclide.
On cherche une solution particulière $(x_1;y_1)$ telle que $ax_1+by_1=\text{PGCD}(a;b)$.
On a donc $a(kx_1)+b(ky_1)=k\times\text{PGCD}(a;b)$ et le couple $(kx_1;ky_1)$ est une solution particulière de (E).
On nomme ce couple $(x_0;y_0)$.

Deuxième étape : recherche de toutes les solutions de (E)
On note $(x;y)$ un couple solution de (E) donc :

.....

$(x_0;y_0)$ est aussi une solution de (E) donc :

.....

Par soustraction des deux équations précédentes on obtient :

.....

On a donc $a(x-x_0)=b(\ldots\ldots)$ et en divisant par $\text{PGCD}(a;b)$ on obtient

$$\ldots\ldots(x-x_0)=\ldots\ldots(y_0-y)$$

avec $\text{PGCD}(a';b')=1$ puisque $a'=\dfrac{a}{\text{PGCD}(a;b)}$ et $b'=\dfrac{b}{\text{PGCD}(a;b)}$.

On a donc $b'|a'(x-x_0)$ avec $\text{PGCD}(a';b')=1$, et d'après le théorème de Gauss $b'|(x-x_0)$ ainsi il existe $\delta\in\mathbb{Z}$ tel que $x-x_0=\ldots\ldots\ldots\ldots\Leftrightarrow x=\ldots\ldots\ldots\ldots$

De plus $a'(x-x_0)=b'(y_0-y)\Leftrightarrow\ldots\ldots\ldots\ldots\Leftrightarrow y=\ldots\ldots\ldots\ldots$..

On obtient donc : $S=\left\{(x_0+\delta b';y_0-a'\delta),\delta\in\mathbb{Z}\right\}$.

Troisième étape : vérification.
$ax+by = a(x_0+\delta b') + b(y_0 - a'\delta) = ax_0 + by_0 + \delta ab' - \delta ba'$
or $a = a' \times \text{PGCD}(a;b)$ et $b = b' \times \text{PGCD}(a;b)$ donc :

$$ab' = a'b \text{ et } \delta ab' - \delta ba' = 0$$

de plus $ax_0 + by_0 = \text{PGCD}(a;b)$, donc :

$$ax + by = k \times \text{PGCD}(a;b).$$

Méthode 7 – Résolution d'équations diophantiennes

Exemple :

▷ On veut résoudre $5x+7y = 1$ (E)
Première étape : solution particulière de (E).
$7 = 5 \times 1 + 2$
$5 = 2 \times 2 + 1$
donc $1 = 5 - 2 \times 2 = 5 - 2(7-5) = 3 \times 5 - 2 \times 7$
donc $(3;-2)$ est une solution particulière de (E).

Deuxième étape : solution de (E).
Si $(x;y)$ est une solution de (E) :

$$5x+7y = 1$$

$(3;-2)$ est une solution de (E) :

$$5 \times 3 + 7 \times (-2) = 1$$

Par soustraction des deux équations, on obtient :

$$5(x-3) + 7(y+2) = 0 \Leftrightarrow 5(x-3) = 7(-y-2) \ (1)$$

donc $5|7(-x-2)$ et $\text{PGCD}(5;7) = 1$, d'après le théorème de Gauss $5|-y-2$
Il existe donc $k \in \mathbb{Z}$ tel que $5k = -y-2 \Leftrightarrow y = -2-5k$
En injectant dans (1), on obtient : $5(x-3) = 7(5k) \Leftrightarrow x-3 = 7k \Leftrightarrow x = 7k+3$

Troisième étape : vérification.
$5(7k+3) + 7(-2-5k) = 35k + 15 - 14 - 35k = 1$

Conclusion : $S = \{(7k+3; -5k-2),\ k \in \mathbb{Z}\}$

▷ On veut résoudre $6x+15y = 3$ (E)
Première étape : solution particulière de (E).
$15 = 6 \times 2 + 3$
donc $3 = 15 \times 1 + 6 \times (-2)$

donc $(-2;1)$ est une solution particulière de (E).

Deuxième étape : solution de (E).
Si $(x;y)$ est une solution de (E) :

$$6x+15y=3$$

$(-2;1)$ est une solution de (E) :

$$6(-2)+15\times 1=3$$

Par soustraction des deux équations on obtient :

$$6(x+2)+15(y-1)=0 \Leftrightarrow 6(x+2)=15(1-y) \Leftrightarrow 2(x+2)=5(1-y)\ (1)$$

donc $2|5(1-y)$ et PGCD$(2;5)=1$, d'après le théorème de Gauss $2|1-y$
Il existe donc $k\in\mathbb{Z}$ tel que $1-y=2k \Leftrightarrow y=1-2k$
En injectant dans (1), on obtient : $2(x+2)=5\times 2k \Leftrightarrow x+2=5k \Leftrightarrow x=5k-2$

Troisième étape : vérification.
$6(5k-2)+15(1-2k)=30k-12+15-30k=3$

Conclusion : $S=\{(5k-2;1-2k),\ k\in\mathbb{Z}\}$