PGCD, théorèmes de Bézout et de Gauss

Introduction :

Dans ce cours, nous allons d'abord aborder la notion de PGCD de deux nombres entiers, et montrer comment le déterminer à l'aide de l'algorithme d'Euclide. Dans le cas où le PGCD des deux nombres est égal à 1, nous verrons que les deux nombres entiers seront dits « premiers entre eux ».
Ensuite, nous présenterons deux théorèmes importants d'arithmétique, les théorèmes de Bézout et de Gauss, et nous les utiliserons pour résoudre des équations diophantiennes.

1 PGCD et algorithme d'Euclide

a. PGCD

Tout d'abord, il faut noter que par convention dans ce cours, lorsqu'on parlera de diviseurs d'un entier naturel, il s'agira toujours de diviseurs positifs.
Commençons par voir les diviseurs communs à deux nombres. Pour cela, quelques notations sont à connaître.

➜ Pour tout entier naturel a, on note $\mathrm{D}(a)$ l'ensemble des diviseurs de a.

Exemple

- L'ensemble des diviseurs de 0 est l'ensemble des entiers naturels : $\mathrm{D}(0) = \mathbb{N}$.
- L'ensemble des diviseurs de 1 est 1 : $\mathrm{D}(1) = \{1\}$.

Propriété

Comme 1 peut diviser tous les entiers, l'ensemble $\mathrm{D}(a)$ des diviseurs de a contient toujours au moins 1 et a lui-même.
Par ailleurs, le plus grand élément des diviseurs de a est a (quand $a \neq 0$).

➜ Pour tous entiers naturels a et b non nuls, on note $\mathrm{D}(a\ ;\ b)$ l'ensemble des diviseurs communs à a et à b.

À retenir

Quelques remarques s'imposent :

- $\mathrm{D}(a\ ;\ b)$ est non vide puisqu'il contient toujours au moins 1.
- Tous les nombres que contient $\mathrm{D}(a\ ;\ b)$ sont inférieurs ou égaux à a et à b.

Exemple

Intéressons-nous aux diviseurs de 28 et 63 :

$$\mathrm{D}(28) = \{1,\ 2,\ 4,\ 7,\ 14,\ 28\}$$
$$\mathrm{D}(63) = \{1,\ 3,\ 7,\ 9,\ 21,\ 63\}$$

Ainsi, les diviseurs communs à 21 et 63 sont 1 et 7 :

$$\mathrm{D}(28\ ;\ 63) = \{1,\ 7\}$$

Dans l'exemple ci-dessus, nous voyons que 7 est le plus grand diviseur commun à 28 et 63.

➜ Nous allons ainsi définir la notion de **plus grand commun diviseur** (PGCD).

Définition

PGCD :

a et b sont deux entiers naturels non nuls.
En admettant que toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément, le plus grand élément de $\mathrm{D}(a\ ;\ b)$ est appellé plus grand commun diviseur (PGCD) de a et b.

➜ Il est noté : $\mathrm{PGCD}(a\ ;\ b)$.

À retenir

Cette définition peut s'étendre aux entiers relatifs.
Dans le cas d'entiers négatifs, nous nous ramenons à des entiers positifs en prenant leurs valeurs absolues.
Et nous avons, avec a et b des entiers relatifs :

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

Ainsi, si a divise b, alors le PGCD de a et b est égal à la valeur absolue de a :

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

Donnons maintenant quelques propriétés qui vont compléter cette notion de PGCD.

Propriété

a et b sont deux entiers naturels supérieurs ou égaux à 2.

- Si, dans leur décomposition en produit de facteurs premiers, a et b n'ont pas de facteur premier commun, leur PGCD est 1 :

$$\text{PGCD}(a\ ;\ b) = 1$$

- Sinon, le PGCD de a et de b est égal au produit des facteurs premiers communs à a et à b, chacun d'eux étant affecté du plus petit exposant figurant dans la décomposition de a et dans celle de b.

Exemple

Pour déterminer le PGCD de $2\,070$ et 368, on décompose ces nombres en produits de facteurs premiers :

$$2\,070 = 2 \times 3^2 \times 5 \times 23$$
$$368 = 2^4 \times 23$$

Donc le PGCD de $2\,070$ et 368 est égal au produit de leurs facteurs premiers commun, 2 et 23, soit 46 :

$$\begin{aligned}\text{PGCD}(2\,070\ ;\ 368) &= 2 \times 23 \\ &= 46\end{aligned}$$

Nous reviendrons plus longuement sur la **décomposition en facteurs premiers** dans le prochain cours.

Propriété

Si le $\text{PGCD}(a\ ;\ b)$ est un entier strictement positif, nous avons :

$$\text{PGCD}(a\ ;\ -a) = |a|$$
$$\text{PGCD}(a\ ;\ 1) = 1$$
$$\text{PGCD}(a\ ;\ 0) = |a|$$

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

Les diviseurs communs à a et b sont les diviseurs de leur PGCD.

Pour tous les entiers relatifs non nuls a et b, et tout c de l'ensemble des entiers naturels strictement positifs $\mathbb{N}^*$:

$$\text{PGCD}(ac\ ;\ bc) = c \times \text{PGCD}(a\ ;\ b)$$

b. Algorithme d'Euclide

Nous allons dans cette partie voir un algorithme qui permet de déterminer le PGCD de deux nombres : l'**algorithme d'Euclide**.
Il s'agit d'effecteur plusieurs divisions euclidiennes consécutives en utilisant, lors d'une dernière étape, une propriété pour obtenir le PGCD.

Théorème

a et b sont deux entiers naturels non nuls tels que la division euclidienne de a par b se traduit par $a = bq + r$, avec $0 \leq r < b$.

Alors l'ensemble des diviseurs communs à a et b est identique à ceux communs à b et r, car $r = a - bq$:

$$\text{D}(a\ ;\ b) = \text{D}(b\ ;\ r)$$
Ce qui amène à : $$\text{PGCD}(a\ ;\ b) = \text{PGCD}(b\ ;\ r)$$

Démonstration

1. Démontrons que, si d divise a et b, alors d divise b et r.

Si d divise a et b, d divise toute combinaison linéaire de a et b, donc en particulier $a - bq$, soit r.

➜ Il en résulte que l'ensemble des diviseurs de a et b sont inclus dans les diviseurs de b et r :

$$\text{D}(a\ ;\ b) \subset \text{D}(b\ ;\ r)$$

(2) Démontrons que, si δ divise b et r, alors δ divise a et b.

Si δ divise b et r, δ divise toute combinaison linéaire de b et r, donc en particulier $bq + r$, soit a.

➜ Il en résulte que l'ensemble des diviseurs de b et r figurent parmi les diviseurs de a et b :

$$\mathrm{D}(b\,;\,r) \subset \mathrm{D}(a\,;\,b)$$

(C) La double inclusion équivaut donc à dire que l'ensemble des diviseurs communs à a et b sont communs à ceux de b et r :

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

➜ Ces deux ensembles étant identiques, ils ont le même plus grand élément, donc :

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

À retenir

Lorsque b ne divise pas a, le PGCD de a et b est le dernier reste non nul dans la succession des divisions de l'algorithme d'Euclide, dont nous allons montrer un exemple ci-dessous.

Exemple

Reprenons le calcul du PGCD de $2\,070$ et 368.
On écrit les divisions euclidiennes successives sous la forme $a = bq + r$, en remplaçant à chaque fois a par le précédent b, et b par le précédent r :

$$\overbrace{2\,070}^{a} = \overbrace{368}^{b} \times \overbrace{5}^{q} + \overbrace{230}^{r}$$
$$\overbrace{368}^{b} = \overbrace{230}^{r} \times 1 + 138$$
$$230 = 138 \times 1 + 92$$
$$138 = 92 \times 1 + 46$$
$$92 = 46 \times 2 + 0$$

➜ $\mathrm{PGCD}(2\,070\,;368) = 46$.

Donnons une rapide explication de ce résultat, en nous servant du théorème que nous avons vu plus haut :

$$\begin{aligned}\text{PGCD}(2\,070\ ;\ 368) &= \text{PGCD}(368\ ;\ 230)\\ &\quad [\text{car PGCD}(a\ ;\ b) = \text{PGCD}(b\ ;\ r)]\\ &= \text{PGCD}(230\ ;\ 138)\\ &= \text{PGCD}(138\ ;\ 92)\\ &= \text{PGCD}(92\ ;\ 46)\\ &= \text{PGCD}(46\ ;\ 0)\\ &= 46\ [\text{car PGCD}(a\ ;\ 0) = |a|]\end{aligned}$$

C. Nombres entiers premiers entre eux

Définition

Nombres entiers premiers entre eux :

Dire que deux entiers naturels non nuls a et b sont premiers entre eux signifie que leur PGCD est égal à 1.

Attention

Ne pas confondre « nombres premiers entre eux » et « nombres premiers ».

➜ Le prochain cours sera consacré à ces derniers.

Définition

Caractérisation du PGCD :

a et b sont deux entiers naturels non nuls.
Dire que d est le PGCD de a et b équivaut à dire qu'il existe deux entiers naturels a' et b' tels que :

$$\begin{aligned}a &= da'\\ b &= db'\\ \text{PGCD}(a'\ ;\ b') &= 1\end{aligned}$$

$\text{PGCD}(a'\ ;\ b') = 1$ signifie que a' et b' sont premiers entre eux, c'est-à-dire qu'ils n'ont aucun diviseur en commun autre que 1.

Démonstration

Raisonnons par l'absurde et supposons que $\text{PGCD}(a' ; b') = d' \neq 1$, alors $a' = d'a''$ et $b' = d'b''$, où a'' et b'' sont des entiers naturels.

Par conséquent, $a = dd'a''$ et $b = dd'b''$.
Ainsi, dd' (qui est strictement supérieur à d) est un diviseur de a et de b, ce qui contredit $\text{PGCD}(a ; b) = d$.

➜ Donc $\text{PGCD}(a' ; b') = 1$.

Nous allons maintenant appliquer cette notion aux congruences, que nous avons découvertes dans le cours précédent.

À retenir

Pour deux entiers naturels non nuls a et n, si a et n sont premiers entre eux, alors a admet un **inverse** modulo n, c'est-à-dire qu'il existe un entier relatif x tel que :

$$ax \equiv 1\,[n]$$

Prenons un exemple, pour montrer comment déterminer l'inverse d'un nombre modulo n.

Exemple

Nous cherchons donc à déterminer un inverse de 3 modulo 13.

3 et 13 sont bien premiers entre eux, donc 3 admet bien un inverse modulo 13.

➜ Nous allons donc rechercher un entier relatif x tel que $3x \equiv 1\,[13]$.

$$3 \times 1 = 3 \equiv 3\,[13]$$
$$3 \times 2 = 6 \equiv 6\,[13]$$
$$3 \times 3 = 9 \equiv 9\,[13]$$
$$3 \times 4 = 12 \equiv 12\,[13] \equiv -1\,[13]$$

En multipliant par -1 la dernière relation, nous obtenons donc :

$$3 \times (-4) \equiv 1\,[13]$$

➜ -4 est donc un inverse entier relatif de 3 modulo 13.

Pour trouver une solution positive, nous pouvons passer la relation au carré :

$$(3 \times 4)^2 \equiv (-1)^2\ [13]$$
$$\equiv 1\ [13]$$
C'est-à-dire : $3 \times 4 \times 3 \times 4 \equiv 1\ [13]$
Puis : $3 \times 48 \equiv 1\ [13]$

➜ 48 est donc un inverse entier naturel de 3 modulo 13.

2 Théorème de Bézout

Nous allons maintenant découvrir deux théorèmes importants d'arithmétique, en commençant par le **théorème de Bézout**, qui découle de **l'égalité de Bézout** (aussi appelée **identité de Bézout**).

Théorème

Égalité de Bézout :

Soit a et b sont deux entiers relatifs non nuls, et d leur PGCD.
Il existe deux entiers relatifs u et v tels que $au + bv = d$.

Démonstration

Soit a et b sont deux entiers relatifs non nuls, et d leur PGCD.

➜ Démontrons que d s'écrit sous la forme $au + bv$.

1 Soit ε l'ensemble des nombres de la forme $au + bv$, avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.

- L'ensemble ε n'est pas vide, car, par exemple pour $u = 1$ et $v = 0$, $a \in \varepsilon$. Il en est de même pour b, en prenant $u = 0$ et $v = 1$.
- ε contient des entiers strictement positifs (par exemple a ou $-a$) et, parmi eux, un plus petit que tous les autres.

Notons $m = au_1 + bv_1$ ce plus petit élément, avec u_1 et v_1 deux entiers relatifs.

D'une part, d'après cette égalité, tout diviseur commun à a et b divise m, donc leur PGCD d divise m.

➜ On a donc $d \leq m$.

2 D'autre part, montrons que m divise a et b.

La division euclidienne de a par m s'écrit $a = mq + r$, avec $0 \leq r < m$. Soit :

$$\begin{aligned} r &= a - mq \\ &= a - (au_1 + bv_1)q \\ &= a(1 - u_1q) + b(-v_1q) \\ &= aU + bV \text{ [avec } U = 1 - u_1q \text{ et } V = -v_1q\text{]} \end{aligned}$$

U et V, comme produit et somme d'entiers relatifs, sont aussi des entiers relatifs. Ainsi, $r \in \varepsilon$.

Or, m est le plus petit entier strictement positif de ε, donc, comme $0 \leq r < m$, nécessairement $r = 0$.

➜ Ainsi, m divise a. On montre de même que m divise b.

(C) m est un diviseur commun à a et b vérifiant $d \leq m$.

Or, d est le plus grand nombre vérifiant cette propriété, donc $d = m$.

➜ On a donc $d = au_1 + bv_1$, avec u_1 et v_1 deux entiers relatifs.

Voyons maintenant le théorème de Bézout, cas particuliers lorsque les nombres a et b sont premiers entre eux.

Théorème

Théorème de Bézout :

Soit a et b deux entiers relatifs non nuls.
Dire que a et b sont premiers entre eux équivaut à dire qu'il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Démonstration

Soit a et b sont deux entiers relatifs non nuls.

(1) Si a et b sont premiers entre eux, alors leur PGCD est 1.

➜ D'après l'égalité de Bézout, il existe deux entiers relatifs u et v tels que $au + bv = 1$, car $d = 1$.

(2) Réciproquement, s'il existe deux entiers relatifs u et v tels que $au + bv = 1$, le PGCD de a et de b divise au ,\,et bv, et donc aussi leur somme $au + bv = 1$.

➜ Le PGCD de a et de b est donc 1, c'est-à-dire que les nombres a et b sont premiers entre eux.

À retenir

En pratique, pour trouver u et v, on utilise d'abord l'algorithme d'Euclide pour démontrer que les deux nombres sont premiers entre eux.
Puis, on reprend chaque division euclidienne pour exprimer chaque reste au fur et à mesure.

➜ On trouve ainsi le couple solution.

Nous allons prendre un exemple pour illustrer cette méthodologie.

Exemple

Soit $a = 392$ et $b = 33$.

➜ Nous cherchons u et v, entiers relatifs, tels que : $au + bv = 1$.

Nous commençons par utiliser l'algorithme d'Euclide pour prouver que a et b sont premiers entre eux.
On écrit les divisions euclidiennes successives :

1. $392 = 33 \times 11 + 29$
2. $33 = 29 \times 1 + 4$
3. $29 = 4 \times 7 + 1$
4. $4 = 1 \times 4 + 0$

Donc $\text{PGCD}(392\ ;33) = 1$.

➜ Ainsi, $a = 392$ et $b = 33$ sont premiers entre eux.

Ceci fait, et afin de trouver u et v, nous réécrivons les divisions euclidiennes en exprimant les restes.

1. $392 = 33 \times 11 + 29$, donc :

$$\begin{aligned} 29 &= 392 - 33 \times 11 \\ &= a - 11b \end{aligned}$$

2. $33 = 29 \times 1 + 4$, donc :

$$\begin{aligned} 4 &= 33 - 29 \times 1 \\ &= b - (a - 11b) \times 1 \\ &= 12b - a \end{aligned}$$

3. $29 = 4 \times 7 + 1$, donc :

$$\begin{aligned} 1 &= 29 - 4 \times 7 \\ &= (a - 11b) - (12b - a) \times 7 \\ &= 8a - 95b \end{aligned}$$

C Ainsi, $a \times 8 + b \times (-95) = 1$.

➜ $u = 8$ et $v = -95$ sont les valeurs qui conviennent.

3 Théorèmes de Gauss et équation diophantienne

Voyons le deuxième théorème que nous évoquions, le **théorème de Gauss**.

a. Théorème de Gauss

Théorème

Théorème de Gauss :

Soit a, b et c des entiers naturels non nuls.
Si a divise le produit bc tout en étant premier avec b, alors a divise c.

À retenir

Autrement dit, si un entier naturel divise un produit de deux facteurs et s'il est premier avec l'un d'eux, il divise l'autre.

Nous allons en donner la démonstration, rapide, et qui repose sur le théorème de Bézout.

Démonstration

Puisque a et b sont premiers entre eux, d'après le théorème de Bézout, il existe des entiers relatifs u et v tels que $au + bv = 1$.
Donc $(ac)u + (bc)v = c$.

Or, a divise ac et bc, donc a divise $acu + bcv$.

➜ Il en résulte que a divise c.

Théorème

Corollaires du théorème de Gauss :

- Si un entier relatif n est divisible par deux entiers relatifs a et b premiers entre eux, il est divisible par leur produit.
- Si un nombre premier p divise un produit ab, alors p divise a ou p divise b.

Entre autres, on se sert de ces notions dans la résolution d'**équations diophantiennes**, que nous allons découvrir dans le chapitre suivant.

b. Équation diophantienne

Définition

Équation diophantienne :

Une équation diophantienne est une équation de la forme $ax + by = c$ où les coefficients a, b et c sont des nombres entiers relatifs et dont les solutions recherchées x et y sont également des entiers relatifs.

À retenir

Pour que l'équation diophantienne $ax + by = c$ admette des solutions, il faut que c soit un multiple de $d = \text{PGCD}(a\ ;\ b)$.

Nous allons, à travers deux exemples, apprendre à résoudre des équations diophantiennes.

Exemple

Commençons par déterminer les entiers x et y tels que $2x + 3y = 1$.

1. On remarque que $2 \times (-1) + 3 \times 1 = 1$, donc le couple $(-1\ ;\ 1)$ est solution particulière de cette équation.

Astuce

Une façon de trouver une solution particulière d'une équation diophantienne de la forme $ax + by = c$ (avec $b \neq 0$) est de l'écrire sous la forme $y = \frac{c-ax}{b}$, puis de chercher un x tel que $c - ax$ soit un multiple de b.

(2) Supposons que $(x\ ;\ y)$ soit solution de $2x + 3y = 1$.

$2x + 3y = 1$ implique :

$$2x + 3y = 2 \times (-1) + 3 \times 1 \Leftrightarrow 2(x + 1) = 3(-y + 1)$$

➜ Donc 3 divise $2(x + 1)$.

(3) Comme 3 est premier avec 2, d'après le théorème de Gauss, 3 divise $(x + 1)$.

➜ Il existe donc un entier relatif k tel que $x + 1 = 3k$, soit $x = -1 + 3k$.

(4) En reportant la valeur de x dans l'égalité $2(x + 1) = 3(-y + 1)$, on obtient :

$$\begin{aligned} 2 \times 3k = 3(-y + 1) &\Leftrightarrow -y + 1 = 2k \\ &\Leftrightarrow y = 1 - 2k \end{aligned}$$

(5) Réciproquement, si $x = -1 + 3k$ et $y = 1 - 2k$, pour k un entier relatif :

$$\begin{aligned} 2x + 3y &= 2(-1 + 3k) + 3(1 - 2k) \\ &= -2 + 6k + 3 - 6k \\ &= 1 \end{aligned}$$

➜ Nous retrouvons bien : $2x + 3y = 1$.

(C) Les solutions de cette équation sont les couples $(-1 + 3k\ ;\ 1 - 2k)$ avec $k \in \mathbb{Z}$.

Exemple

Déterminons maintenant les entiers x et y tels que $16x - 3y = 4$.

(1) Donnons une façon d'identifier une solution particulière à cette équation :

$$\begin{aligned} 16x - 3y = 4 &\Leftrightarrow y = \frac{16x - 4}{3} \\ &\Leftrightarrow y = \frac{4(4x - 1)}{3} \end{aligned}$$

Nous cherchons donc, pour le numérateur, un multiple de 4 et de 3.

Nous remarquons facilement que, avec $x = 1$, nous obtenons $4(4x - 1) = 12$.

➜ Le couple $(1\ ;\ 4)$ est une solution particulière de l'équation.

Nous allons appliquer la même méthodologie que dans le premier exemple.

(2) Supposons que $(x\ ;\ y)$ soit solution de $16x - 3y = 4$.

$16x - 3y = 4$ implique :

$$16x - 3y = 16 \times 1 - 3 \times 4 \Leftrightarrow 16(x-1) = 3(y-4)$$

➜ Donc 3 divise $16(x-1)$.

(3) Comme 3 est premier avec 16, d'après le théorème de Gauss, 3 divise $(x-1)$.

➜ Il existe donc un entier relatif k tel que $x - 1 = 3k$, soit $x = 1 + 3k$.

(4) En reportant la valeur de x dans l'égalité $16(x-1) = 3(y-4)$, on obtient :

$$\begin{aligned} 16 \times 3k = 3(y-4) &\Leftrightarrow y - 4 = 16k \\ &\Leftrightarrow y = 4 + 16k \end{aligned}$$

(5) Réciproquement, si $x = 1 + 3k$ et $y = 4 + 16k$, pour k un entier relatif :

$$\begin{aligned} 16x - 3y &= 16(1 + 3k) - 3(4 + 16k) \\ &= 16 + 48k - 12 - 48k \\ &= 4 \end{aligned}$$

➜ Nous retrouvons bien : $16x - 3y = 4$.

(C) Les solutions de cette équation sont les couples $(1 + 3k \ ; \ 4 + 16k)$, avec $k \in \mathbb{Z}$.

Conclusion :

Dans ce cours, nous avons vu la définition du PGCD de deux nombres entiers relatifs, qui est le plus grand diviseur commun de ces deux nombres, et du cas particulier des nombres premiers entre eux lorsque le PGCD est égal à 1.

Nous avons aussi vu l'égalité puis le théorème de Bézout, ainsi que le théorème de Gauss et son corollaire. Et enfin, nous avons introduit les équations diophantiennes et leur résolution.