Chapitre 7

PGCD

***

I. Diviseurs communs, PGCD

1. PGCD de deux entiers

Définition.

Soient $a, b \in \mathbb{Z}$ deux entiers, ***non tous les deux nuls***.
Le plus grand entier qui divise à la fois a et b s'appelle le ***plus grand diviseur commun*** de a, b et se note $\text{pgcd}(a, b)$.

Exemples.

- $\text{pgcd}(-21, 14) =$.
- $\text{pgcd}(12, 32) =$.
- $\text{pgcd}(21, 26) =$.

Propriétés.

1. $\text{pgcd}(a\,,\, ka) = a$, pour tout $k \in \mathbb{Z}$ et $a \neq 0$.
2. Cas particuliers : pour tout $a \neq 0$, on a $\text{pgcd}(a, 0) = a$ et $\text{pgcd}(a, 1) = 1$ et enfin pour a et b non nuls tous les deux : $\text{pgcd}(|a|, |b|) = \text{pgcd}(a, b)$

Exercice 1.7.

1. Déterminer tous les diviseurs de 92 et de 64 dans $\mathbb{Z}$.
2. En déduire le PGCD de 92 et 64.

2. Algorithme d'Euclide

Lemme.

Soient $a, b \in \mathbb{N}^*$. Écrivons la division euclidienne $a = bq + r$. Alors :

$$\boxed{\text{pgcd}(a, b) = \text{pgcd}(b, r)}$$

En fait on a même $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$ pour tout $q \in \mathbb{Z}$. Mais pour optimiser l'algorithme d'Euclide on applique le lemme avec q le quotient.

Démonstration. Nous allons montrer que les diviseurs de a et de b sont exactement les mêmes que les diviseurs de b et r. Cela impliquera le résultat car les plus grands diviseurs seront bien sûr les mêmes.

- Soit d un diviseur de a et de b. Alors d divise b donc aussi bq, en plus d divise a donc d divise $a - bq = r$.
- Soit d un diviseur de b et de r. Alors d divise aussi $bq + r = a$.

■

Propriété.

On souhaite calculer le pgcd de $a, b \in \mathbb{N}*$. On peut supposer $a \geqslant b$. On calcule des divisions euclidiennes successives. Le pgcd sera le dernier reste non nul.

- division de a par b, $a = bq_1 + r_1$. Par le lemme précédent $\text{pgcd}(a,b) = \text{pgcd}(b, r_1)$ et si $r_1 = 0$ alors $\text{pgcd}(a,b) = b$ sinon on continue :
- $b = r_1 q_2 + r_2, \quad \text{pgcd}(a,b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$,
- $r_1 = r_2 q_3 + r_3, \quad \text{pgcd}(a,b) = \text{pgcd}(r_2, r_3)$,
- $\dots$
- $r_{k-2} = r_{k-1} q_k + r_k, \quad \text{pgcd}(a,b) = \text{pgcd}(r_{k-1}, r_k)$,
- $r_{k-1} = r_k q_k + 0, \quad \text{pgcd}(a,b) = \text{pgcd}(r_k, 0) = r_k$.

Comme à chaque étape le reste est plus petit que le quotient on sait que $0 \leq r_{i+1} < r_i$. Ainsi l'algorithme se termine car nous sommes sûrs d'obtenir un reste nul, les restes formant une suite décroissante d'entiers positifs ou nuls : $b > r_1 > r_2 > \cdots \geq 0$.

Exemple. Calculons le pgcd de $a = 600$ et $b = 124$.

$$\begin{array}{ccccccc}
600 & = & 124 & \times & 4 & + & 104 \\
124 & = & 104 & \times & 1 & + & 20 \\
104 & = & 20 & \times & 5 & + & \color{red}{4} \\
20 & = & 4 & \times & 5 & + & 0
\end{array}$$

Ainsi $\text{pgcd}(600, 124) = 4$.

Exercice 2.7.

1. À l'aide de l'algorithme d'Euclide, déterminer le pgcd de 1 551 et 132. Vérifier le résultat à l'aide de la calculatrice.
2. En déduire l'ensemble des diviseurs communs de 1 551 et 132.

3. Ensemble des diviseurs communs

Propriété.

Soit a et b deux entiers naturels non nuls et soit d leur pgcd.
L'***ensemble des diviseurs communs*** de a et de b est l'ensemble des ***diviseurs*** de d.

II. Nombres premiers entre eux

1. Couples d'entiers premiers entre eux

Définition.

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

Exemple. Pour tout $a \in \mathbb{Z}$, a et $a+1$ sont premiers entre eux. En effet soit d un diviseur commun à a et à $a+1$. Alors d divise aussi $a + 1 - a$. Donc d divise 1 ce qui induit que $d = -1$ ou $d = +1$. Le plus grand diviseur de a et $a+1$ est donc 1. Et donc $\text{pgcd}(a, a+1) = 1$ et par suite a et $a+1$ sont premiers entre eux.

Définition.

Soit a un entier relatif et b un entier naturel non nul.
La fraction $\frac{a}{b}$ est ***irréductible*** si les entiers a et b sont ***premiers entre eux***.

Propriété.

Soit a et b deux entiers relatifs non nuls.
Si $d = \text{pgcd}(a, b)$ alors il existe deux entiers a' et b' ***premiers entre eux*** tels que :

$$\boxed{a = da' \quad \text{et} \quad b = db'}.$$

Exercice 3.7. Déterminer tous les couples d'entiers naturels $(x\,;\,y)$ tels que :

$$\begin{cases} x & < & y \\ x+y & = & 600 \\ \text{pgcd}(x\,;\,y) & = & 50 \end{cases}$$

2. Théorème de Bachet-Bézout

Théorème.

Soit a et b deux entiers relatifs non nuls.
a et b sont ***premiers entre eux*** si et seulement il existe ***deux entiers relatifs*** u et v tels :

$$\boxed{au + bv = 1}$$

Exercice 4.7.

1. Démontrer qu'il existe deux entiers relatifs u et v tels que $38u + 15v = 1$.
2. À l'aide de l'algorithme d'Euclide, déterminer un tel couple $(u\,;\,v)$.

3. Caractérisation du pgcd

Théorème.

Soit a et b deux entiers relatifs non nuls.
$\text{pgcd}(a, b) = d$ si et seulement si d ***divise*** a et b et s'il ***existe*** deux entiers relatifs u et v tels que :

$$\boxed{au + bv = d}$$

III. Conséquences du théorème de Bézout

1. Lemme de Gauss

Lemme.

Soit a, b et c des entiers non nuls.
Si a divise bc et a est ***premier*** avec b alors a divise c.

Démonstration. a divise bc donc il existe un entier k tel que $bc = ka$. Or a et b étant premiers entre eux, il existe u et v entiers tels que $au + bv = 1$. Alors, en multipliant par c cette égalité, on obtient $auc + bvc = c$ soit $acu + vka = c$ donc $a(cu + vk) = c$ avec $cu + vk$ entier. Donc c est multiple de a ou a divise c ■

Corollaire.

Soit a, b et c trois entiers non nuls.
Si a divise c et b divise c avec a et b ***premiers entre eux*** alors ab divise c.

2. Équations de Diophante

Proposition.

Soit a et b deux entiers non nuls et c un entier quelconque. Une ***équation diophantienne*** est une équation de la forme $ax + by = c$, d'inconnues entières x et y.
Cette équation admet des solutions si et seulement si c est ***un multiple*** du pgcd de a et b.
Si $c = \text{pgcd}(a, b)$, le théorème de Bézout généralisé donne l'existence d'un couple d'entiers $(x\,;\,y)$ solution de l'équation $ax + by = c$.

Exercice 5.7. Parmi les équations suivantes où les inconnues x et y sont des entiers relatifs, quelles sont celles qui admettent au moins une solution ? Justifier ?

1. $(E_1)\ :\ 13x + 14y = 3$.
2. $(E_2)\ :\ 39x - 42y = 2$.
3. $(E_3)\ :\ 5x - 9y = 1$.

Exercice 6.7. On considère l'équation $(E)\ :\ 2x + 5y = 4$ où $(x\,;\,y) \in \mathbb{Z}^2$.

1. Trouver deux entiers relatifs u et v tels que $2u + 5v = 1$.
2. En déduire une solution particulière $(x_0\,;\,y_0)$ de (E).
3. Justifier que $(E) \iff 2(x - x_0) = 5(y_0 - y)$.
   En déduire toutes les solutions de (E).

3. Homogénéité du pgcd

Propriété.

Soit a et b deux entiers relatifs non nuls.
Pour tout entier naturel k non nul, $\text{pgcd}(ka\,;\,kb) = k\text{pgcd}(a, b)$.

Exercice 7.7. En utilisant l'homogénéité du pgcd, déterminer :

1. $\text{pgcd}(1\,200\,;\,350)$.
2. $\text{pgcd}(2^3 \times 5^2 \times 13^5\,;\,2^2 \times 5^2 \times 13^4 \times 17)$