Chapitre 4

PGCD

Table des matières

1 Introduction

1.1 Définitions et propriétés

Définition 1 :

Soient a et b deux entiers relatifs non tous les deux nuls.
L'ensemble des diviseurs communs de a et de b est une partie non vide de $\mathbb{Z}$ (elle contient 1) et majorée par le maximum de $|a|$ et $|b|$.
Cet ensemble admet donc un plus grand élément appelé **Plus Grand Commun Diviseur de a et b** noté $\text{PGCD}(a, b)$.

Exemple 1 :

Pour $a = 105$ et $b = 42$, la liste des diviseurs est respectivement : $\{1, 3, 5, 7, 15, 21, 35, 105\}$ et $\{1, 2, 3, 6, 7, 14, 21, 42\}$.
Les diviseurs commun sont donc : $\{1, 3, 7, 21\}$.
Le plus grand est donc 21. Il s'agit donc du PGCD...

Exercice 1 :

- Donner la liste des diviseurs communs de 12 et de 30, en déduire $\text{PGCD}(12, 30)$.
- Déterminer $\text{PGCD}(24, 18)$.

Propriété 1 :

Soient a et b deux entiers relatifs non tous les deux nuls.
↬ $\text{PGCD}(a, b) = \text{PGCD}(|a|, |b|)$
↬ $\text{PGCD}(a, b) = \text{PGCD}(b, a)$
↬ $\text{PGCD}(a, 0) = a$ car 0 est multiple de tout entier.
↬ Si b divise a, alors $\text{PGCD}(a, b) = |b|$.

Exercice 2 :

- Déterminer $\text{PGCD}(-24, -18)$.
- Déterminer $\text{PGCD}(0, 82)$.
- Déterminer $\text{PGCD}(30, 5)$.

1.2 Algorithme d'Euclide

Dans cette partie, a et b sont deux entiers naturels non nuls tels que b ne divise pas a et $a > b$.

Exercice 3 : Pour a et b deux entiers, et r le reste de la division euclidienne de a par b. Montrer que les diviseurs communs de a et b sont les diviseurs communs de b et r.

Théorème 1 :

Algorithme d'Euclide

↬ On note q et r le quotient et le reste de la division euclidienne de a par b.
On a : PGCD(a, b) =PGCD(b, r).

↬ La suite des divisions euclidiennes du diviseur par le reste de la division précédente finit par s'arrêter.

Division de a par b :	$a = b \times q_0 + r_0$	avec $0 \leq r_0 < b$
Division de b par r_0 :	$b = r_0 \times q_1 + r_1$	avec $0 \leq r_1 < r_0$.
Division de r_0 par r_1 :	$r_0 = r_1 \times q_2 + r_2$	avec $0 \leq r_2 < r_1$.
Division de r_{n-2} par r_{n-1} :	$r_{n-2} = r_{n-1} \times q_n + r_n$	avec $0 \leq r_{n-1} < r_n$.
Division de r_{n-1} par r_n :	$r_{n-1} = r_n \times q_{n+1} + 0$.	

On a alors : PGCD$(a, b) = r_n$

Exercice 4 :

- Déterminer PGCD$(9, 27)$.
- Déterminer PGCD$(27, 59)$.
- Déterminer le PGCD de 450 et de 198.

Propriété 2 :

Pour tous entiers naturels a, b et k, on a : PGCD$(ka, kb) = k$PGCD(a, b).

Exercice 5 :

- Déterminer PGCD$(240, 180)$.
- Déterminer les entiers naturels inférieurs à 450 tels que PGCD$(n, 270) = 45$.

Propriété 3 :

Soient a et b deux entiers relatifs non tous les deux nuls.
d est un diviseur commun de a et b si et seulement si d divise PGCD(a, b).

2 Nombres premiers entre eux

2.1 Définition

Définition 2 :

Soient a et b deux entiers relatifs non nuls.
On dit que a et b sont premiers entre eux si et seulement si PGCD$(a, b) = 1$.

Exemple 2 :

- $\text{PGCD}(15,8) = 1$ donc 15 et 8 sont premiers entre eux.
- $\forall a \in \mathbb{Z}$, $\text{PGCD}(a,1) = 1$ donc 1 est premier avec tous les entiers.

Remarques :

↬ Il ne faut pas confondre nombres premiers entre eux et nombres premiers.
Les nombres 15 et 8 sont premiers entre eux mais aucun des deux n'est premier. Par contre, deux nombres premiers sont premiers entre eux.

↬ Une fraction irréductible q s'écrit de manière unique sous la forme : $q = \dfrac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ et $\text{PGCD}(a,b) = 1$.

Propriété 4 :

Soient a et b deux entiers relatifs non nuls.
↬ Si $d =$PGCD(a,b) et a' et b' les entiers tels que $a = da'$ et $b = db'$ alors a' et b' sont premiers entre eux.
↬ S'il existe $d \in \mathbb{N}$, et a' et b' des entiers premiers entre eux tels que $a = da'$ et $b = db'$, alors d est le $\text{PGCD}(a,b)$.

Exemple 3 :

$36 = 12 \times 3$ et $60 = 12 \times 5$ et 3 et 5 sont premiers entre eux, donc $\text{PGCD}(36,60) = 12$.

Exercice 6 : Déterminer l'ensemble des couples $(a,b) \in \mathbb{N}^2$ tels que $\left\{\begin{array}{rcl} ab & = & 300 \\ \text{PGCD}(a,b) & = & 5 \end{array}\right.$

2.2 Théorème de Bezout

Propriété 5 :

Tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.

Théorème 2 :

Théorème de Bezout
Soit (a,b) un couple d'entiers relatifs non nuls.
a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que :

$$au + bv = 1$$

Exemple 4 :

Pour $a = 13$ et $b = 16$, on a $5 \times 13 - 4 \times 16 = 1$, donc a et b sont premiers entre eux.

Exercice 7 :

1. Déterminer deux entiers u et v tels que $29u + 12v = 1$.
2. Montrer que pour tout $n \in \mathbb{Z}$, les entiers $(2n + 1)$ et $(3n + 2)$ sont premiers entre eux.

Remarques :
↬ Le théorème de Bezout donne l'existence des entiers u et v mais ne donne par leurs valeurs.
↬ Il n'y a pas unicité des entiers u et v tels que $au + bv = 1$.

Théorème 3 :

Identité de Bezout
Pour tout couple $(a, b) \in (\mathbb{Z}^*)^2$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv =$PGCD(a, b).

Exercice 8 : Une équation diophantienne est une équation à coefficients entiers dont on cherche une solution entière ou rationnelle.
On s'intéresse à l'équation diophantienne $84x + 18y = 6$.
Cette équation admet-elle des solutions ?

Propriété 6 :

Soient a, b et c trois entiers tels que a et b ne sont pas simultanément nuls.
L'équation $ax + by = c$ admet des couples d'entiers $(x; y)$ solutions si et seulement si le nombre c est un multiple de PGCD$(a; b)$.

Exercice 9 :

1. Les équations suivantes ont-elles des solutions entières :
   a. $12x + 4y = 32$ b. $2x + 6y = 3$
2. Après avoir justifié son existence, déterminer un entier a tel que $30a \equiv 1[23]$.

3 Théorème et Gauss et applications

3.1 Théorème de Gauss

Théorème 4 :

Soient a, b et c trois entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Exercice 10 : Déterminer les couples d'entiers relatifs $(x; y)$ tels que $2(x - 1) = 3y$

Exercice 11 :

1. Déterminer le PGCD de 65 et 91.
2. Résoudre dans $\mathbb{Z}^2$, l'équation : $65x = 91y$.

Exercice 12 : Résoudre l'équation (E) : $4x + 3y = 2$