Chapitre 11 - Plus Grand Diviseur Commun

I Définition et premières propriétés

1. Propriété et définition

Soient a et b deux entiers relatifs ~~non nuls~~ tous. Il existe un plus grand diviseur commun à a et b. On appelle ce diviseur PGCD et on note $PGCD(a;b)$.

Exemple : Déterminer $PGCD(-9;12)$

$D(-9) = \{-9, -3, -1, 1, 3, 9\}$ $D^+(12) = \{1, 2, 3, 4, 6, 12\}$

PGCD = 3

Remarque :
Cas où l'un des deux nombres est nul :Si, par exemple, $a=0$ alors $PGCD(0;b)=b$

Propriétés:

- $PGCD(a;b)$ est un entier strictement positif.
- $PGCD(1;b)=1$
- Si a divise b alors $PGCD(a;b)=|a|$
- PGCD(a;b)= $PGCD(|a|;|b|)$. Par conséquent, on se ramène en général à a et b des entiers naturels.

2. Déterminer le PGCD

a) Détermination du PGCD de deux entiers non nuls par décomposition en produit de facteurs premiers

Exemple :
Décomposez 2022 et 3200 en produit de facteurs premiers. Déduisez-en $PGCD(2022;3200)$

$2022 = 2 \times 3 \times 337$ $3200 = 32 \times 100 = 2^7 \times 5^2$

PGCD(2022 ; 3200)

b) Liste de diviseurs

On fait la liste des diviseurs positifs de l'un. Et on teste ces diviseurs pour l'autre entiers

$D^+(48) = \{1; 2, 3, 4, 6, 8, 12, 16, 24, 48\}$

PGCD(327 ; 48) = 3

c) Détermination du PGCD de deux entiers non nuls par l'algorithme d'Euclide *(methode2 p 122)*

Propriété (lemme d'Euclide)

Soient a et b deux entiers non nuls tels que $a=bq+r$, avec r entier.
Alors, l'ensemble des diviseurs communs à a et b est le même que l'ensemble des diviseurs communs à b et r et on a : . $PGCD(a;b)=PGCD(b;r)$

Démonstration :

Soit $D(a)\cap D(b)$ l'ensemble des diviseurs communs à a et b et soit $D(b)\cap D(r)$ l'ensemble des diviseurs communs à b et r Montrons par double inclusion que $D(a)\cap D(b)=D(b)\cap D(r)$

Montrons que $D(a)\cap D(b) = D(b)\cap D(r)$ par double inclusion

→ Soit $n \in D(a)\cap D(b)$, montrons que $n\in D(b)\cap D(r)$

donc que n divise r

$r = a - bq$

$\exists (k,k') \in \mathbb{Z}^2$, $\begin{cases} a = kn \\ b = k'n \end{cases}$ Donc $r = kn - k'nq = n(\underbrace{k-k'q}_{\in \mathbb{Z}})$

Ainsi n/r donc $n\in D(r)$ donc $n\in D(b)\cap D(r)$

Cas particulier

Si $a=bq+r$ est l'écriture de la division euclidienne de a par b ($0\le r<b$), le lemme s'applique et on a $PGCD(a;b)=PGCD(b;r)$.

Algorithme d'Euclide

Exemple

Déterminons le PGCD de 240 et 36 en utilisant plusieurs fois de suite l'égalité $PGCD(a;b)=PGCD(b;r)$ où r est le reste dans la division euclidienne de a par b

Dividende	Diviseur	Quotient	Reste
240	36	6	24
36	24	1	12
24	12	2	0

$PGCD(240,36) = PGCD(36,24) = PGCD(24,12) = PGCD(12,0) = 12$

Cas général

Soient deux entiers a et b tels que $0\le b\le a$. Le but est de déterminer le PGCD de a et b par la méthode d'Euclide.

1er cas : b divise a Alors $PGCD(a;b)=b$

2ème cas : b ne divise pas a

Division euclidienne de a par b : $a=bq_1+r_1$ avec $0\le r_1<b$.

Or b ne divise pas a donc $r_1\neq 0$

$PGCD(a;b)=PGCD(b;r_1)$

1er cas : r_1 divise b Alors $PGCD(b;r_1)=r_1$

2ème cas : r_1 ne divise pas b donc il existe deux entiers $b=r_1q_2+r_2$ et $0\leq r_2<r_1$

On construit une suite strictement décroissante d'entiers naturels positifs

Par conséquent, il existe un entier naturel n tel que $r_n=0$

$PGCD(a;b)=PGCD(b;r_1)=PGCD(r_1;r_2)=....=PGCD(r_{n-1};r_n)=PGCD(r_{n-1};0)=r_{n-1}$

Propriété

Soient deux entiers a et b tels que $0\leq b\leq a$

- Si: b divise a alors $PGCD(a;b)=b$
- S b ne divise pas a alors , le PGCD de a et b est le dernier reste non nul de la suite des divisions de l'algorithme d'Euclide.

Propriétés

Soient a et b deux entiers non nuls.

a) L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de leur PGCD.

b) Si k est un entier naturel non nul, $PGCD(ka;kb)=k\,PGCD(a;b)$

II Nombres premiers entre eux

1) Définition

Deux entiers relatifs non nuls a et b sont premiers entre eux si et seulement si $PGCD(a;b)=1$ autrement dit, si et seulement si les seuls diviseurs communs de a et b sont 1 et -1.

Exemple : montrer que 2022 et 55 sont premiers entre eux

55 = 5×11

2) Propriété

Soient a et b deux entiers non nuls.

$d=PGCD(a;b)$ si et seulement si il existe deux entiers a' , b' tels que $a=d\times a'$ et $b=d\times b'$ avec a' et b' premiers entre eux.

Exemple : Déterminer les couples d'entiers naturels (a,b) tel que $\begin{cases} a<b \\ a+b=24 \\ PGCD(a\,,\,b)=4 \end{cases}$

PGCD(a;b) = 4 donc ∃ a' b' ∈ ℕ tel que a = 4a' et b = 4b'

$\begin{cases} a<b \\ 4a'+4b'=24 \\ \exists\, a'b' \in \mathbb{N},\ a=4a' \text{ et } b=4b' \end{cases}$ avec $a' \wedge b' = 1$

$\begin{cases} a<b \\ a'+b'=6 \\ a=4a' \text{ et } b=4b' \text{ avec } a \wedge b \end{cases}$

$\begin{cases} a<b \\ a'=1 \text{ et } b'=5 \\ a=4 \text{ et } b=20 \end{cases}$

III Théorème de Bézout (ou identité de Bézout)

1) Énoncé

Soient a et b deux entiers non nuls.

a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au+bv=1$.

2) Exemples

a) Montrez que 9 et -4 sont premiers entre eux grâce au théorème de Bézout.

$9\times1+2\times(-4)=1$ Donc 9 et -4 sont premiers entre eux

$(-3)\times9+(-4)\times(-7)=1$ Donc 9 et -4 sont premiers entre eux

Remarque : lorsque a et b sont premiers entre eux, il n'y a pas unicité du couple (u,v) tel que $au+bv=1$

b) Montrez que deux entiers consécutifs sont premiers entre eux.

Soit $n\in\mathbb{N}$

$n\times(-1)+(n+1)\times1=1$ donc 2 entiers consécutifs sont premiers entre eux

3) Comment déterminer des entiers u et v ?

1- Montrer qu'il existe deux entiers relatifs u et v tels que $51u + 19v = 1$

PGCD(51,19)=1 car 19 ne divise pas 51 donc u et v existent

2 - Les déterminer

a) avec intuition

b) à la calculatrice

pour nous $51u+19v=1$ *équivaut à* $u=(1-19v)/51$

calculatrice $Y=(1-19X)/51$, *on régle X entier et on fait défier le tableau de valeurs*

c) avec l'algorithme d'Euclide

étape1 : algorithme d'Euclide

étape2 : on exprime les reste à chaque ligne

etape3 : en partant de la dernière ligne, on remplace les restes par l'expression de la ligne précédente

$51 = 19 \times 2 + 13$

$19 = 13 \times 1 + 6$

$13 = 6 \times 2 + \boxed{1}$

$6 = 6 \times 1 + 0$

Donc $1 = 13 - 6 \times 2$

$1 = 13 - (19 - 13 \times 1) \times 2$

$1 = 13 \times 3 - 19 \times 2$

$1 = (51 - 19 \times 2) \times 3 - 19 \times 2$

$1 = 51 \times 3 - 19 \times 8$

On a $1 = 51u + 19v$

avec $u = 3$ et $v = -8$

4) **Identité de Bézout**

Soient a et b deux entiers relatifs non nuls.

Si $d = PGCD(a;b)$ alors il existe deux entiers relatifs u et v tels que $au+bv=d$

Démonstration

On suppose PGCD(a,b)=d

$\exists (a';b') \in \mathbb{N}^2$ tq $a=da'$ et $b=db'$ avec $a' \wedge b'=1$

donc $\exists u$ et $v \in \mathbb{N}^2$ tq $a'u+b'v=1$

$da'u+db'v=d \Leftrightarrow au+bv=d$

Exemple : $PGCD(6;15)=3$ Déterminer un couple d'entiers (u,v) $6u+15v=3$

PGCD(6;15)=3 $\Leftrightarrow$ 3 PGCD(2;5)

On a $2\times-2+5\times1=1$ donc $6\times-2+15=3$

Remarques

- La réciproque de cette propriété est fausse !

  Contre-exemple :

  $2\times1+3\times1=5$ or PGCD(2,3)≠5

- Si $PGCD(a;b)=d$, il n'y a pas unicité du couple (u,v) tel que $au+bv=d$

  Exemple : $PGCD(6;15)=3$

5) Existence d'un inverse modulo *n*

1) Montrer qu'il existence des entiers u et v tels que $4u+9v=1$ puis déterminer un couple $(u\ ;\ v)$ solution de $4u+9v=1$.

2) En déduire une solution de l'équation $4x\equiv1(9)$.

$4u+9v=1$

$4u\equiv1(9)$

$-2 \rightarrow 7$

$9=4\times2+1$

$4=1\times4+0$

$1=9-4\times2$

$1=9+4(-2)$