Chapitre 2 - PGCD et PPCM

Dans ce chapitre, lorsque nous parlerons de diviseur , cela signifiera diviseur **positif**.

1 Plus grand commun diviseur : PGCD

1.1 Définition du plus grand commun diviseur

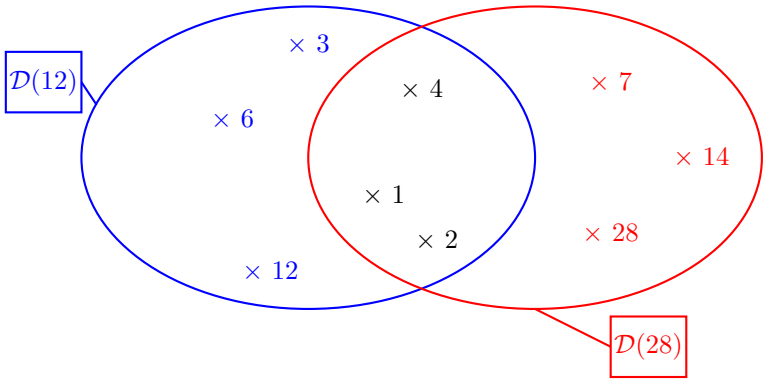
Soit a et b deux entiers naturels.
On note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a et $\mathcal{D}(a,b)$ l'ensemble des diviseurs positifs de a et de b.

Exemple 1

On a $\mathcal{D}(10) = \{1,2,5,10\}$ *et* $\mathcal{D}(11) = \{1,11\}$
$\mathcal{D}(12) = \{1,2,3,4,6,12\}$ *et* $\mathcal{D}(28) = \{1,2,4,7,14,28\}$ *donc on a* $\mathcal{D}(12,28) = \{1,2,4\}$

Remarque 1

- *Lorsque* $a > 1$, $\mathcal{D}(a)$ *contient toujours 1 et* a.
- *Si* $a \neq 0$, $\mathcal{D}(a)$ *ne contient que des entiers naturels inférieurs ou égaux à* a
- $\mathcal{D}(0) = \mathbb{N}$
- $\mathcal{D}(1) = \{1\}$
- $\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b)$
- $\mathcal{D}(0,b) = \mathcal{D}(b)$



$\mathcal{D}(a,b)$ est un ensemble non vide car il contient toujours 1 et tous les éléments de $\mathcal{D}(a,b)$ sont inférieurs à a si $a \neq 0$ et et à b si $b \neq 0$
Donc si a et b sont deux entiers naturels dont l'un d'entre eux est non nul, $\mathcal{D}(a,b)$ est un ensemble non vide et contient un nombre fini d'éléments, il admet donc un plus grand élément.

Définition 1

Soit a *et* b *deux entiers naturels dont l'un est non nul.*
Le plus grand diviseur commun à a *et* b *est le plus grand élément de* $\mathcal{D}(a,b)$.
On le note en abrégé $PGCD(a,b)$

Remarque 2

Pour deux entiers relatifs non tous nuls, il faudrait rajouter les diviseurs négatifs de a *et de* b *en prenant les opposés des éléments de* $\mathcal{D}(a)$ *et de* $\mathcal{D}(b)$. *ainsi , le PGCD de deux entiers relatifs se détermine de la même façon et donc le PGCD de deux entiers relatifs est celui de leur valeur absolue.*

A faire : ex .1 p.31 et ex 1,4,8 p.54

Définition 2

Deux entiers relatifs a et b sont dits premiers entre eux si $PGCD(a,b) = 1$

Propriété 1

Soit a et b deux entiers naturels tels que $a \neq 0$.
Si a divise b alors $PGCD(a,b) = a$

Preuve :
a divise b donc tous les diviseurs de a sont aussi des diviseurs de b.
Donc $\mathcal{D}(a) \subset \mathcal{D}(b)$ et donc $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a)$
Ainsi $\mathcal{D}(a,b) = \mathcal{D}(a)$
donc $PGCD(a,b) = a$

1.2 Recherche du PGCD : algorithme d'Euclide

Propriété 2 *Lemme d'Euclide*

Soient a et b deux entiers non nuls tels que $a \geqslant b$
Effectuons la division euclidienne de a par b : il existe deux entiers q et r tels que $a = bq + r$ où $0 \leqslant r < b$.
Alors $\mathcal{D}(a,b) = \mathcal{D}(b,r)$ et en particulier, $PGCD(a,b) = PGCD(b,r)$.

Preuve :

- Soit $m \in \mathcal{D}(a,b)$
  Alors m divise a et b donc m divise toute combinaison linéaire de a et b donc m divise $a - bq$.
  m divise donc r.
  Donc $m \in \mathcal{D}(b,r)$
  On a donc $\mathcal{D}(a,b) \subset \mathcal{D}(b,r)$

- Réciproquement ,soit $p \in \mathcal{D}(b,r)$
  Alors , de la même manière, p divise toute combinaison linéaire de b et r donc m divise $bq + r$.
  m divise donc a.
  Donc $m \in \mathcal{D}(a,b)$
  On a donc $\mathcal{D}(b,r) \subset \mathcal{D}(a,b)$

  En conclusion, on a $\mathcal{D}(a,b) = \mathcal{D}(b,r)$
  Les plus grands éléments sont donc égaux d'où $PGCD(a,b) = PGCD(b,r)$.

Théorème 1 *Théorème de l'algorithme d'Euclide*

Soient a et b deux entiers non nuls tels que $a \geqslant b$
Lorsque b ne divise pas a, on effectue la division euclidienne de a par b puis successivement les divisions du diviseur précédent par le reste précédent, le $PGCD(a,b)$ est alors le dernier reste non nul obtenu.
Lorsque b divise a, on a évidemment $PGCD(a,b) = b$

Preuve :
Effectuons la division euclidienne de a par b :
Il existe q_0 et r_0 tels que $a = bq_0 + r_0$ où $0 < r_0 < b$ et d'après le Lemme d'Euclide, on a donc $\mathcal{D}(a,b) = \mathcal{D}(b,r_0)$ et, en particulier, $PGCD(a,b) = PGCD(b,r_0)$

Continuons :
Il existe q_1 et r_1 tels que $b = r_0q_1 + r_1$ où $0 \leqslant r_1 < r_0$

- Si $r_1 = 0$ alors r_0 divise b donc d'après la propriété 1, $PGCD(b, r_0) = r_0$.
- Si $r_1 \neq 0$, il existe q_1 et r_1 tels que $b = r_0 q_1 + r_1$ où $0 < r_1 < r_0$
  et d'après le Lemme d'Euclide, on a donc $\mathcal{D}(b, r_0) = \mathcal{D}(r_0, r_1)$ c'est-à-dire $\mathcal{D}(a, b) = \mathcal{D}(r_0, r_1)$
  Et aussi, en particulier, $PGCD(a, b) = PGCD(r_0, r_1)$

On effectue ainsi de suite les divisions euclidiennes successives tant qu'on obtient pas de reste nul.

On obtient une suite (r_n) de termes positifs et cette suite est strictement décroissante.
On va donc nécessairement avoir un reste nul que nous noterons r_n.

D'après ce que nous avons vu précédemment, on a $\mathcal{D}(a, b) = \mathcal{D}(r_{n-1}, r_n)$
C'est-à-dire $\mathcal{D}(a, b) = \mathcal{D}(r_{n-1}, 0)$
donc $\mathcal{D}(a, b) = \mathcal{D}(r_{n-1})$ d'après une remarque du 1.1
d'où $PGCD(a, b) = r_{n-1}$ qui est bien le dernier reste non nul .

Exemple 2

Cherchons pgcd(27 ;59), en utilisant l'algorithme d'Euclide :
$59 = 27 \times 2 + 5$
$27 = 5 \times 5 + 2$
$5 = 2 \times 2 + 1$
$2 = 1 \times 2 + 0$
donc PGCD(29 ;57)=1

Théorème 2 *Conséquence importante*

L'ensemble des diviseurs communs à deux entiers positifs a et b est l'ensemble des diviseur de leur PGCD d, autrement dit $\mathcal{D}(a, b) = \mathcal{D}(d)$
En particulier, tout diviseur de a et b est un diviseur de leur PGCD

Preuve : On a vu que $\mathcal{D}(a, b) = \mathcal{D}(r_{n-1})$ et que r_{n-1} est le Pgcd.

A faire : ex 1 à 8 p.54

2 Théorème de Bezout

Théorème 3
Soient a et b deux entiers naturels non nuls.
a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que $au + bv = 1$

Preuve :

($\Leftarrow$)
Supposons qu'il existe deux entiers relatifs u et v tels que $au + bv = 1$
Soit g=PGCD(a ;b)
g divise a et b donc g divise $au + bv$
Donc g divise 1. D'où $g = 1$ et a et b sont premiers entre eux

($\Rightarrow$)
Soit $\mathcal{F}$ l'ensemble des nombres $au + bv$ où u et v sont dans $\mathbb{Z}$
$\mathcal{F}$ est non vide et contient des nombres strictement positifs (en prenant u et v dans $\mathbb{N}$)
Notons alors $\mathcal{F}^+$ les éléments strictement positifs de $\mathcal{F}$

Cet ensemble $\mathcal{F}^+$ est un sous ensemble de $\mathbb{N}$ et non vide donc il admet un plus petit élément m . Notons $m = au_1 + bv_1$

Démontrons que m divise a et b (donc $m \in \mathcal{D}(a; b)$)
Effectuons la division euclidienne de a par m :
Il existe deux entiers q et r tels que $a = mq + r$ et avec $0 \leqslant r < m$

Donc $r = a - mq$ c'est-à-dire $r = a - (au_1 + bv_1)q$
puis $r = a - aqu_1 + bqv_1$ et donc $r = a(1 - qu_1) + bqv_1$
Donc ,si $r \neq 0$, $r \in \mathcal{F}^+$ mais $r < m$ ce qui est impossible puisque m est le plus petit élément de $\mathcal{F}^+$.
Donc $r = 0$, c'est-à-dire que m divise a.

De même, on pourrait montrer que m divise b.

Donc $m \in \mathcal{D}(a;b)$ mais a et b sont premiers entre eux donc $m = 1$
D'où il existe deux entiers u_1 et v_1 tels que $au_1 + bv_1 = 1$

Méthode :
Pour trouver les deux entiers u et v du théorème, on remonte l'algorithme d'Euclide.
Cela revient à résoudre une équation dite "diophantienne" que nous verrons au V)

Exemple 3

Nous avons vu que pgcd(27;59)=1 en utilisant l'algorithme d'Euclide. Cherchons u et v pour que $27u + 59v = 1$ *à l'aide ces opérations, en isolant à chaque fois le reste, en partant de la fin et en remontant afin d'obtenir le dernier reste non nul en fonction de 27 et 59 :*
$5 - 2 \times 2 = 1$
$27 - 5 \times 5 = 2$ *donc* $5 - (27 - 5 \times 5) \times 2 = 1$
Ce qui donne donc $5 - 27 \times 2 + 10 \times 5 = 1$
Puis on a $11 \times 5 - 27 \times 2 = 1$
$59 - 27 \times 2 = 5$ *donc* $11 \times (59 - 27 \times 2) - 27 \times 2 = 1$
Ce qui donne $59 \times 11 - 27 \times 22 - 27 \times 2 = 1$
Et donc $59 \times 11 - 27 \times 24 = 1$

3 Caractérisation et propriété du PGCD

3.1 Caractérisation du PGCD

Théorème 4
Soient a, b, d trois entiers strictement positifs. Les trois propositions suivantes sont équivalentes :

1. $PGCD(a;b) = d$
2. *soit* a' *et* b' *tels que* $a = da'$ *et* $b = db'$ *alors* $PGCD(a';b') = 1$
3. *d est un diviseur de a et b et il existe deux entiers u et v tels que* $au + bv = d$

Preuve :
(1) $\Rightarrow$ (2)

Soit $PGCD(a;b) = d$ alors d divise a et b et il existe a' et b' tels que $a = da'$ et $b = db'$.
Soit δ un diviseur commun de a' et b'.
Il existe donc a'' et b'' tels que $a' = \delta a''$ et $b' = \delta b''$
Alors on peut écrire $a = d\delta a''$ et $b = d\delta b''$ donc $d\delta$ est un diviseur commun de a et b.
Si $\delta > 1$, on a un diviseur commun à a et b qui est plus grand que le $pgcd(a;b)$ ce qui est impossible.
Donc le seul diviseur commun possible pour a' et b' est 1
D'où $pgcd(a';b') = 1$

(2) $\Rightarrow$ (3)

soit a' et b' tels que $a = da'$ et $b = db'$ alors $PGCD(a';b') = 1$
Donc, d'après le théorème de Bezout, il existe deux entiers u et v tels que $a'u + b'v = 1$
Multiplions par d : $da'u + db'v = d$ puis, $au + bv = d$
Donc il existe deux entiers u et v tels que $au + bv = d$

(3) $\Rightarrow$ (1)

Soit d un diviseur de a et b et supposons qu'il existe deux entiers u et v tels que $au + bv = d$

Soit g le pgcd de a et b.
g divise a et b donc g divise $au + bv$ c'est-à-dire g divise d.
Mais d divise a et b donc d divise g d'après le théorème 2.
Donc $d = g$ c'est-à-dire $d = pgcd(a; b)$

3.2 propriété du PGCD

Propriété 3

Soit a, b et k trois entiers naturels non nuls.
Alors $PGCD(ka, kb) = k \times PGCD(a, b)$

Preuve :

Soit $d = PGCD(a, b)$
Nous voulons utiliser le th 4 :
d divise a et b donc kd divise ka et kb

Montrons maintenant qu'il existe deux entiers u et v tels que $kau + kbv = kd$
D'après le th 4, comme $d = PGCD(a, b)$, il existe deux entiers u et v tels que $au + bv = d$.
En effectuant le produit par k, on a donc $kau + kbv = kd$

Donc kd est un diviseur de ka et kb et il existe deux entiers u et v tels que $kau + kbv = kd$
donc $pgcd(ka; kb) = kd$ c'est-à-dire $pgcd(ka; kb) = k \times pgcd(a, b)$

Exemple 4

$PGCD(45; 120) = 15 \times PGCD(3; 8)$ *donc* $PGCD(45; 120) = 15$

4 Applications

4.1 Théorème de Gauss

Théorème 5 *de Gauss*
Soient a,b et c trois entiers strictement positifs.
Si a divise bc et si a est premier avec b alors a divise c

Preuve :
a est premier avec b donc, d'après le théorème de Bezout, il existe deux entiers u et v tels que $au + bv = 1$
En effectuant le produit par c, on a $acu + bcv = c$
Or a divise acu et a divise bc par hypothèse, donc a divise c.

Propriété 4 *corollaire du th. de Gauss*
Si un entier n est divisible par deux entiers naturels a et b ***premiers entre eux****, alors il est divisible par $a \times b$*

Exemple 5

Trouvons les couples d'entiers $(x; y)$ tels que $11x = 6y$ et $0 \leqslant x < 25$

6 divise $11x$ et 6 et 11 sont premiers entre eux donc, d'après le théorème de Gauss, 6 divise x
donc x peut prendre les valeurs 0, 6, 12 ,18 ou 24
Les couples possibles sont donc (0,0) ; (6,11) ; (12,22) ; (18,33) et (24,44)

4.2 Fractions irréductibles

Définition 3
Une fraction $\frac{a}{b}$ *est dite irréductible si* a *et* b *sont premiers entre eux.*

Théorème 6
On peut toujours rendre une fraction irréductible

Preuve :
Si elle n'est pas irréductible, il suffit de la simplifier par le pgcd du numérateur et du dénominateur pour obtenir une fraction irréductible.

5 Equations diophantiennes

Diophante d'Alexandrie, parfois appelé le « père de l'algèbre », est connu par son ouvrage les Arithmétiques, qui traite des solutions des équations algébriques.
On ne sait pratiquement rien de sa vie et ses dates de naissance et de mort sont très controversées.
Les Arithmétiques sont une collection de solutions numériques de 130 équations.
La méthode de résolution des équations indéterminées constitue ce qu'on a appelé l'analyse diophantienne.
Diophante considère des équations linéaires et du second degré, mais ne retient que les solutions rationnelles positives.

Nous allons donc chercher à résoudre des équations du type $ax + by = c$ où a, b, c sont dans $\mathbb{Z}$ et où les solutions sont dans $\mathbb{Z}$.
Ce sont des équations diophantiennes.

Théorème 7
L'équation $ax + by = c$ *admet des solutions si et seulement si le* $PGCD(a; b)$ *divise* c

Preuve :
($\Rightarrow$)
Supposons que $ax + by = c$ admet une solution.
Notons cette solution $(x_o; y_o)$, on a donc $ax_o + by_o = c$.
$pgcd(a; b)$ divise a et b donc $pgcd(a; b)$ divise $ax_o + by_o$
Donc $pgcd(a; b)$ divise c.

($\Leftarrow$)
Supposons que $PGCD(a; b)$ divise c.
Cela signifie que , si on note $d = PGCD(a; b)$, on a d divise c.
Donc d divise, a, b et c.
On a alors l'existence de 3 entiers a',b' et c' tels que $a = da'$, $b = db'$ et $c = dc'$
Et, de plus, d'après le théorème 4, $PGCD(a'; b') = 1$
D'après le théorème de Bezout, il existe deux entiers u et v tels que $a'u + b'v = 1$
Effectuons le produit par c' :
$a'uc' + b'vc' = c'$
puis le produit par d :
$auc' + bvc' = c$
Donc il existe une solution $(uc'; vc')$ à l'équation $ax + by = c$.

Méthode pour résoudre une équation diophantienne $ax + by = c$:

1. Vérifier si elle a des solutions à l'aide du théorème précédent
2. Résoudre l'équation $ax + by = pgcd(a; b)$ avec la méthode vue au II)
3. Trouver une solution particulière à $ax + by = c$ en mutipliant par c' où c' est tel que $c = c' \times pgcd(a; b)$
4. Trouver toutes les solutions à $ax + by = c$ à l'aide du théorème de Gauss comme dans l'exemple 5

Exemple 6

Résoudre $175x + 129y = 4$

1. *Vérifions s'il y a des solutions :*

   Calculons le PGCD(175 ;129) à l'aide de l'algorithme d'Euclide :
   $175 = 129 \times 1 + 46$
   $129 = 46 \times 2 + 37$
   $46 = 37 \times 1 + 9$
   $37 = 9 \times 4 + 1$
   $9 = 1 \times 9 + 0$
   donc PGCD(175 ;129)=1 et donc PGCD(175 ;129) divise 4 donc il existe des solutions

2. *Utilisons le théorème de Bezout pour trouver une solution particulière à l'équation* $175x + 129y = 1$ *:*

   $37 - 9 \times 4 = 1$
   puis $46 - 37 \times 1 = 9$ *donc* $37 - (46 - 37 \times 1) \times 4 = 1$
   Ce qui donne $37 \times 5 - 46 \times 4 = 1$
   Puis $129 - 46 \times 2 = 37$ *donc* $(129 - 46 \times 2) \times 5 - 46 \times 4 = 1$
   Ce qui donne $129 \times 5 - 46 \times 14 = 1$
   Puis $175 - 129 \times 1 = 46$ *donc* $129 \times 5 - (175 - 129 \times 1) \times 14 = 1$
   Ce qui donne $129 \times 19 - 175 \times 14 = 1$

   Donc , en posant $x_o = -14$ *et* $y_o = 19$ *, on a* $175x_o + 129y_o = 1$

3. *Trouvons une solution particulière de* $175x + 129y = 4$ *en multipliant par 4 :*

   Comme $175x_o + 129y_o = 1$*, on a* $175 \times 4x_o + 129 \times 4y_o = 4$.
   Donc (-56,76) est solution particulière de l'équation $175x + 129y = 4$.

4. *Déduisons en toutes les solutions de* $175x + 129y = 4$ *à l'aide du théorème de Gauss :*

   Nous cherchons les couples (x, y) *tels que* $175x + 129y = 4$
   Nous avons $175 \times -56 + 129 \times 76 = 4$
   En soustrayant ces deux équations, nous avons donc $175(x + 56) + 129(y - 76) = 0$
   D'où $175(x + 56) = -129(y - 76)$

   $$\left.\begin{array}{r} 129 \text{ divise } 175(x+56) \\ \\ 129 \text{ et } 175 \text{ sont premiers entre eux} \end{array}\right\} \text{129 divise } x+56 \text{ d'après le théorème de Gauss}$$

   Donc $x + 56 = 129k$ *avec* $k \in \mathbb{Z}$
   D'où $x = -56 + 129k$
   En remplaçant , on obtient $y = 76 + 175k$

En conclusion, les solutions de cette équation sont les couples $(-56 + 129k; 76 + 175k)$ *avec* $k \in \mathbb{Z}$

Exemple 7

Résoudre $4x + 8y = 10$

1. *pgcd(4 ;8)=4.*
   Or 4 ne divise pas 10 donc il n'y a pas de solution.

6 Plus Petit Commun Multiple

Deux entiers positifs ont des multiples communs (par exemple le produit de ces deux entiers) .
L'ensemble des multiples communs est un sous ensemble non vide de $\mathbb{N}$ donc il admet un plus petit élément.

Définition 4
On appelle PPCM de a et b et on note $PPCM(a;b)$ le plus petit multiple commun à a et b

Propriété 5
Soient a et b deux entiers naturels non nuls.
Soit $m = PPCM(a;b)$
Si c est un multiple commun de a et b alors m divise c.

Propriété 6
Soient a , b et k trois entiers naturels non nuls.
Alors $PPCM(ka;kb) = k \times PPCM(a;b)$

Théorème 8
Soient a et b des entiers strictement positifs.
$PGCD(a;b) \times PPCM(a;b) = a \times b$