Chapitre 2 – Théorèmes de Bézout et de Gauss

I – PGCD de deux entiers relatifs

a) Définition et propriétés de réduction

Exemple : *Les diviseurs de 12 sont 1 ; 2 ; 3 ; 4 ; 6 ; 12 et leurs opposés.*
Les diviseurs de – 9 sont 1 ; 3 ; 9 et leurs opposés.
Les diviseurs communs à – 9 et 12 sont donc 1 ; 3 et leurs opposés (– 1 et – 3).

Remarques :

- Pour tout $a\in\mathbb{Z}$, les diviseurs communs à 0 et a sont les diviseurs de a.
- Pour tout $a\in\mathbb{Z}$, les diviseurs communs à 1 et a sont – 1 et 1.

Propriété et définition : Soient a et b deux entiers relatifs non tous les deux nuls.
L'ensemble des diviseurs communs à a et b admet un plus grand élément ; on l'appelle Plus Grand Commun Diviseur de a et b et on le note $PGCD(a;b)$.

Exemples : $PGCD(-9;12)=3$; $PGCD(-1;45)=1$; $PGCD(0;-457)=457$; $PGCD(100;75)=25$.

Preuve : Supposons que $a\neq 0$. L'ensemble des diviseurs communs de a et b est non vide puisqu'il contient 1 et – 1. Cet ensemble est fini car il ne contient que des entiers compris entre $-a$ et a. Donc il admet un plus grand élément qui est le plus grand des diviseurs communs à a et b.

Remarques : Soient a et b deux entiers relatifs non tous les deux nuls.

- $PGCD(a;b)\in\mathbb{N}$.
- $PGCD(a;b)=PGCD(b;a)=PGCD(|a|;|b|)$; on se ramène en général au cas où a et b sont positifs.
- $PGCD(1;b)=1$ et $PGCD(0;b)=|b|$ (avec ici $b\neq 0$).

Définition : a et b sont premiers entre eux si et seulement si $PGCD(a;b)=1$.

Exemple : $PGCD(47;15)=1$ *donc 47 et 15 sont premiers entre eux.*

Propriété : Soit $D(a;b)$ l'ensemble des diviseurs communs à deux entiers relatifs a et b.
Alors $D(a;b)=D(a-k\times b;b)$ pour tout $k\in\mathbb{Z}$.

Preuve :

- Si d divise a et b, alors d divise a et $a-kb$ pour tout $k\in\mathbb{Z}$, donc d divise $a-kb$ et b.
- Si d divise $a-kb$ et b, alors d divise $(a-kb)+kb$ c'est-à-dire a, donc d divise a et b.
  Conclusion : $D(a;b)=D(a-kb;b)$ pour tout $k\in\mathbb{Z}$.

Exemple : $D(63;75)=D(63;75-63)=D(63;12)=D(63-5\times12;12)=D(3;12)=\{-3;-1;1;3\}$

Propriété de réduction du PGCD : Soient a et b deux entiers relatifs non tous les deux nuls.

- **$PGCD(a;b)=PGCD(a-kb;b)$ pour tout $k\in\mathbb{Z}$.**
- **Si $0<b\leqslant a$, $PGCD(a;b)=PGCD(r;b)$ où r est le reste de la division euclidienne de a par b.**
- **Si b est un diviseur positif de a, $PGCD(a;b)=b$.**

Preuve :

- C'est une conséquence immédiate de la propriété précédente.
- Si $0<b\leqslant a$, on applique l'égalité précédente avec $k=q$, quotient de la division euclidienne de a par b.
- Si $b|a$ avec $b>0$, $r=0$ donc $PGCD(a;b)=PGCD(0;b)=b$.

b) L'algorithme d'Euclide

Cet algorithme permet de déterminer le PGCD de deux entiers naturels non tous les deux nuls, en utilisant la relation :
Si $0<b\leqslant a$, $PGCD(a;b)=PGCD(r;b)$ où r est le reste de la division euclidienne de a par b.

Exemple : *Cherchons* $PGCD(240;36)$.

a	=	b	×	q	+	r
240	=	36	×	6	+	24
36	=	24	×	1	+	12
24	=	12	×	2	+	0

On déduit de ces relations que :
$PGCD(240;36)=PGCD(24;36)=PGCD(12;24)=PGCD(12;0)=12$.

Propriété (algorithme d'Euclide) :
Soient a et b deux entiers tels que $0<b\leqslant a$.
L'algorithme suivant permet de calculer en un nombre fini d'étapes $PGCD(a;b)$.

- **Calculer le reste r de la division euclidienne de a par b.**
- **Tant que $r\neq0$, remplacer a par b et b par r.**
- **Calculer le reste r de la division euclidienne de a par b.**
- **Fin Tant que.**
- **Retourner b.**

Preuve : Écrivons les divisions successives : $a=bq_0+r_0$ avec $0\leqslant r_0<b$.

- Si $r_0=0$, on s'arrête à cette première étape.
- Si $r_0\neq0$, on remplace a par b et b par r_0 : $b=r_0q_1+r_1$ avec $0\leqslant r_1<r_0$.
- Si $r_1\neq0$, on remplace b par r_0 et r_0 par r_1 : $r_0=r_1q_2+r_2$ avec $0\leqslant r_2<r_1$.
- Si $r_2\neq0$, on remplace r_0 par r_1 et r_1 par r_2 : $r_1=r_2q_3+r_3$ avec $0\leqslant r_3<r_2$.

On construit ainsi une liste strictement décroissante r_0, r_1, r_2, … Or il n'y a qu'un nombre fini d'entiers entre r_0 et 0. Cette liste est donc finie donc il existe $k\in\mathbb{N}$ tel que $r_k\neq0$ et $r_{k+1}=0$.
Comme $r_{k+1}=0$, l'algorithme s'arrête. Il comporte bien un nombre fini d'étapes.
On a donc $PGCD(a;b)=PGCD(r_k;r_{k+1})=PGCD(r_k;0)=r_k$ (dernier reste non nul).

Exercice : Écrire à la calculatrice un programme déterminant le PGCD de deux entiers naturels avec l'algorithme d'Euclide.

Propriété : Soient a et b deux entiers relatifs non tous les deux nuls.
Les diviseurs communs à a et b sont les diviseurs de leur PGCD.

Exemple : Déterminons les diviseurs communs à – 12 458 et 3 272.
Cherchons $PGCD(12458;3272)$:

- $12458=3272\times3+2642$
- $3272=2642\times1+630$
- $2642=630\times4+122$
- $630=122\times5+20$
- $122=20\times6+2$
- $20=2\times10+0$

On a donc $PGCD(-12458;3272)=2$ donc les diviseurs communs à – 12 458 et 3 272 sont : – 2 ; – 1 ; 1 ; 2.

Preuve : Deux nombres entiers opposés ayant les mêmes diviseurs, on peut supposer $0\leqslant b\leqslant a$.

- Si $b=0$, alors $a\neq0$. $D(a,b)=D(a)$ et $PGCD(a;b)=a$ donc la propriété est vraie.
- Si $b\neq0$ et $b|a$, $D(a;b)=D(b)$ avec $b=PGCD(a;b)$ donc la propriété est encore vraie.
- Si $b\neq0$ et $b\nmid a$, avec les notations de la preuve de l'algorithme d'Euclide et la propriété on a : $D(a;b)=D(r_0;b)=D(r_0;r_1)=\ldots=D(r_k;r_{k+1})=D(r_k;0)=D(r_k)$ avec $r_k=PGCD(a;b)$.

c) Autres propriétés du PGCD de deux entiers

Propriété d'homogénéité : Soient a et b deux entiers relatifs non tous les deux nuls.
Pour tout $\lambda\in\mathbb{N}^*$, $PGCD(\lambda a;\lambda b)=\lambda PGCD(a;b)$.

Preuve : Si a ou b est nul, ou si $a|b$, le résultat est trivial.
Sinon, on suppose $0<b<a$. La recherche de $PGCD(\lambda a;\lambda b)$ à l'aide de l'algorithme d'Euclide conduit à écrire des égalités qui sont celles de la recherche de $PGCD(a;b)$ multipliées par λ .
Pour le dernier reste non nul, on aura donc $PGCD(\lambda a;\lambda b)=\lambda PGCD(a;b)$.

Exemple : $PGCD(150;100)=50$ $PGCD(3;2)=50\times1=50$.

Propriété caractéristique : Soient a et b deux entiers relatifs non tous les deux nuls et d un entier naturel. $d=PGCD(a;b)\Leftrightarrow\begin{cases}a=d\,a'\\b=b\,a'\end{cases}$ avec a' et b' premiers entre eux.

Preuve : Si $d=PGCD(a;b)$, il existe a' et b' tels que $a=d\,a'$ et $b=d\,b'$.
Alors, $PGCD(a;b)=PGCD(d\,a';d\,b')=d\,PGCD(a';b')$ par homogénéité, puisque $d\in\mathbb{N}^*$.
Comme $PGCD(a;b)=d$, on en déduit que $PGCD(a';b')=1$ et donc que a' et b' sont premiers entre eux.
Réciproquement, si $a=d\,a'$ et $b=d\,b'$ avec a' et b' premiers entre eux et $d\in\mathbb{N}$, alors $d\neq0$ car a et b sont non tous les deux nuls, donc par homogénéité,
$PGCD(a;b)=d\,PGCD(a';b')=d\times1=d$.

Exemple : $90=9\times10$ et $40=4\times10$ avec 9 et 4 premiers entre eux donc $PGCD(90;40)=10$.

II – Théorème de Bézout et théorème de Gauss

Propriétés : Soient a et b deux entiers relatifs non tous les deux nuls et $d=PGCD(a;b)$.
1. Il existe u et v entiers relatifs tels que $au+bv=d$: c'est la relation de Bézout.
2. L'ensemble des entiers $au+bv$ (avec $u\in\mathbb{Z}$, $v\in\mathbb{Z}$) est l'ensemble des multiples de d.

Remarque : Il n'y a pas unicité du couple $(u;v)$ tel que $au+bv=d$.

Preuve :
1. On utilise les notations de la démonstration de l'algorithme d'Euclide.
De $a=bq_0+r_0$ on obtient $r_0=a-bq_0=au_0+bv_0$ avec $u_0=1$ et $v_0=-q$ qui sont des entiers.
De $b=r_0q_1+r_1$, on obtient $r_1=b-q_1r_1=b-(au_0+bv_0)q_1=au_1+bv_1$ avec $u_1=-u_0q_1$ et $v_1=1-v_0q_1$ entiers.
Pas-à-pas, on exprime chaque reste comme combinaison linéaire entière de a et b jusqu'à r_k, c'est-à-dire d.
2. Soit $n=au+bv$ avec u et v appartenant à $\mathbb{Z}$. Comme d divise a et b, d divise n. Toute combinaison linéaire de a et b est un multiple de d.
Réciproquement, si n est un multiple de d, il existe $k\in\mathbb{Z}$ tel que $n=kd$. Or, il existe u et v entiers tels que $d=au+bv$ donc $n=(ku)a+(kv)b$. Il existe donc deux entiers u' et v' tels que $n=au'+bv'$. Tout multiple de d est une combinaison linéaire entière de a et b.

Exemple : Pour $a=231$, et $b=165$, on a :
- $231=165+66$
- $165=66\times2+33$
- $66=33\times2+0$

Donc $PGCD(231;165)=33$. En utilisant les relations précédentes, on a :
- $33=165-66\times2$
- $66=231-165$

Donc $\mathbf{33=165-(231-165)\times2=165-2\times231+165\times2=165\times3+231\times(-2)}$.
On remarque que l'on a aussi : $\mathbf{165\times17+231\times(-12)=33}$.

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

Preuve : Si a et b sont premiers entre eux, $d=1$ et d'après la proposition précédente, il existe $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$ tels que $au+bv=1$.
Réciproquement, s'il existe $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$ tels que $au+bv=1$, alors un diviseur commun à a et b divise 1, donc c'est soit 1 soit – 1 donc $PGCD(a;b)=1$.

Exemples :
- *$a=4$ et $b=-9$ sont premiers entre eux car $4\times(-2)+9\times1=1$.*
- *Deux entiers consécutifs sont toujours premiers entre eux, car pour $n\in\mathbb{Z}$, $n\times(-1)+(n+1)\times1=1$.*

<u>Théorème de Gauss :</u> Soient a , b et c trois entiers relatifs non nuls.
Si a divise bc et si a est premier avec b , alors a divise c .

<u>Exemple :</u> 5 divise $75=3\times 25$, 5 et 3 sont premiers entre eux donc 5 divise 25.

<u>Contre-exemple :</u> Pour $a=12$, $b=6$ et $c=10$, a n'est premier ni avec b , ni avec c .
a divise $bc=60$, mais a ne divise ni b ni c .
L'hypothèse a premier avec b est donc capitale.

<u>Preuve :</u> a divise bc donc il existe $k\in\mathbb{Z}$ tel que $bc=ka$. Comme a et b sont premiers entre eux, il existe u et v entiers relatifs tels que $au+bv=1$.
En multipliant par c cette relation, on obtient : $acu+bcv=c$, soit $acu+kav=c$ soit $a(cu+kv)=c$. Comme $cu+kv\in\mathbb{Z}$, a divise c .

<u>Corollaire du théorème de Gauss :</u> Si deux nombres premiers entre eux a et b divisent un entier c , alors ab divise c .

<u>Exemple :</u> 5 divise 100, 4 divise 100. Comme 5 et 4 sont premiers entre eux, $5\times 4=20$ divise 100.

<u>Preuve :</u> $a|c$ donc il existe $k\in\mathbb{Z}$ tel que $c=ka$. Comme b est premier avec a et que $b|ka$, alors d'après le théorème de Gauss il existe $l\in\mathbb{Z}$ tel que $k=lb$. On a donc $c=lba$, donc $ab|c$.