Chapitre 4 : PGCD, PPCM, Equation Diophantienne

C. Aupérin D. Zancanaro

2009-2010

« *La physique est trop dure pour les physiciens* »David Hilbert

Dernière modification : 8 mars 2010

Table des matières

Cours : PGCD, PPCM, Equation Diophantienne

La notion de pgcd a déjà été entrevue au collège et dans les chapitres précédents. Elle sera largement approfondie dans ce chapitre avec ses propriétés et son application à la résoltion d'équaitons dites diophantiennes.

1 PGCD et PPCM de deux entiers

Soient a et b deux entiers non tous les deux nuls. On notera $\mathscr{D}(a,b)$ l'ensemble de leurs diviseurs communs.

1.1 Définitions et Premières Propriétés

Définition 1 : *et Propriété*

$\mathscr{D}(a,b)$ est un ensemble non vide fini. Il admet donc un plus grand élément, appelé $PGCD(a,b)$ (Plus Grand Diviseur Commun de a et b). On le note parfois $a \wedge b$.

L'ensemble des multiples communs strictement positifs de a et b est un ensemble dénombrable minoré. Il admet un plus petit élément, appelé $PPCM(a,b)$ (Plus Petit Multiple Commun de a et b).

Exemples :

$PGCD(4,6) = 2$ $PGCD(12,13) = 1$ $PGCD(21,35) = 7$

$PPCM(4,6) = 12$ $PPCM(12,13) = 156$ $PPCM(21,35) = 105$

Définition 2 :

On dit que a et b sont premiers entre eux si et seulement si $PGCD(a,b) = 1$

Exemples :

$PGCD(3,2) = 1$ $PGCD(10,21) = 1$ $PGCD(51,113) = 1$

Propriété 1 : *Immédiates*

1. $0 < PGCD(a,b) = PGCD(b,a) = PGCD(|a|,|b|) < min(|a|,|b|)$
2. $PGCD(a,0) = |a|$
3. $PGCD(a,1) = 1$
4. Si $b|a$ alors $PGCD(a,b) = |b|$

Remarque : Dans tout le chapitre, sauf indication contraire, on considérera désormais les diviseurs positifs communs à deux entiers naturels a et b non tous les deux nuls.

Propriété 2 : *Réduction*

L'ensemble des diviseurs de a et b est égal à l'ensemble des diviseurs de b et $a-b$. En fait :

$$\mathscr{D}(a,b) = \mathscr{D}(a-b,b) = \mathscr{D}(a-kb,b) \quad \text{pour tout } k \in \mathbb{Z}$$

Preuve :

Il s'agit de montrer une double inclusion. Soit $k \in \mathbb{Z}$.

$\mathscr{D}(a,b) \subset \mathscr{D}(a-kb,b)$: Si d divise a et b, il divise aussi $a-kb$.

$\mathscr{D}(a,b) \supset \mathscr{D}(a-kb,b)$: Si d divise b et $a-kb$ alors il divise $(a-kb)+kb = a$.

D'où l'égalité $\mathscr{D}(a,b) = \mathscr{D}(a-kb,b)$. En prenant $k=1$, on obtient la propriété.

Exemple :

p et q étant deux entiers naturels non nuls, on note $a = 9p+4q$ et $b = 2p+q$.

1. Démontrer que $pgcd(a,b) = pgcd(p,q)$
2. Démontrer que $9p+4$ et $2p+1$ sont premiers entre eux.
3. Déterminer $pgcd(9p+4, 2p-1)$ en fonction des valeurs de p. Vérifier pour $p=5$ et $p=9$.

Exercices du livre *: n° 7 - 8 p 80*

Corollaire 1 :

Si $0 < b \leq a$, alors $\mathscr{D}(a,b) = \mathscr{D}(r,b)$ où r est le reste de la division euclidienne de a par b.

Preuve :

Cas particulier de la propriété précédente puisque r est tel que $a = bq + r \Leftrightarrow a - bq = r$ avec $q \in \mathbb{N}$

1.2 Algorithme d'Euclide

On connaît déjà plusieurs méthodes pour trouver le pgcd de deux nombres, tels que :

1. *Lister les diviseurs*
2. *Décomposer les nombres en produits de facteurs premiers*
3. *Faire l'algorithme d'Euclide*

Nous n'utiliserons cette année que l'algorithme d'Euclide, que nous allons démontrer.

On cherche à déteminer $PGCD(a,b)$ où a et b sont deux nombres entiers tels que $0 < b < a$.

On s'appuyera les résultats suivants :

- Si $b|a$ alors $PGCD(a,b) = b$.
- Si b ne divise pas a, alors $\exists\,!\,(q,r) \in \mathbb{N}^2$ tel que $0 < r < b$ et l'on a $\mathscr{D}(a,b) = \mathscr{D}(b,r)$.

Dans le deuxième cas, comme $b < a$ et $r < b$, on s'est ramené à travailler sur des nombres plus petits.
De plus, comme $r > 0$ (b ne divise pas a), on peut réitérer le processus, autant de fois que nécessaire (c'est-à-dire tant que le reste n'est pas nul).
Il arrivera forcément un moment où le reste de la division sera nul, car la suite des restes est strictement décroissante, minorée par 0.
On aura alors $\mathscr{D}(a,b) = \mathscr{D}(b,r) = \mathscr{D}(r,r_1) = \mathscr{D}(r_1,r_2) = \cdots = \mathscr{D}(r_k,0)$, d'où $pgcd(a,b) = r_k$.

Le principe de l'algorithme d'Euclide est donc d'effectuer des divisions euclidiennes successives et bien choisies. Le *pgcd* des deux nombres sera donc le dernier reste non nul obtenu.

Algorithme d'Euclide

On note $D = pgcd(a,b)$. On cherche D

1. J'effectue la division euclidienne de a par b : $a = bq + r$. On a alors $\mathscr{D}(a,b) = \mathscr{D}(b,r)$
2. Si $r = 0$ alors $\mathscr{D}(a,b) = \mathscr{D}(b,0)$ et $pgcd(a,b) = pgcd(b,0) = b$.
   Sinon :
   - On pose $r_0 := b$, $r_1 := r$, $i :=< 1$
   - Tant que $r_i \neq 0$:
     - J'effectue la division euclidienne de r_{i-1} par r_i : $r_{i-1} = r_i q_{i+1} + r_{i+1}$.
       On a alors $\mathscr{D}(a,b) = \mathscr{D}(r_i, r_{i+1})$
     - i prend la valeur $i + 1$
3. On a alors $\mathscr{D}(a,b) = \mathscr{D}(r_i, r_{i+1}) = \mathscr{D}(r_i, 0)$ et $pgcd(a,b) = pgcd(r_i, 0) = r_i$.

Exemple :

Trouver le pgcd de 246 et 168.

$$\begin{aligned} 264 &= 168 \times 1 + 96 \\ 168 &= 96 \times 1 + 72 \\ 96 &= 72 \times 1 + 24 \\ 72 &= 24 \times 3 + 0 \end{aligned}$$

Le dernier reste non nul est 24 : c'est donc le pgcd de 264 et 168.

Exercices du livre *: n° 13 - 14 - 15 p 80*

1.3 Propriétés

Propriété 3 :
L'ensemble des diviseurs de a et b est aussi l'ensemble des diviseurs de leur pgcd.

$$\mathscr{D}(a,b) = \mathscr{D}(pgcd(a,b))$$

En particulier, tous les diviseurs communs à deux nombres sont aussi des diviseurs de leur pgcd.

Preuve :
Découle du fait que $\mathscr{D}(a,b) = \mathscr{D}(r_k, 0) = \mathscr{D}(r_k)$, avec $r_k = pgcd(a,b)$

Propriété 4 : *Homogénéité*
Pour tout $k \in \mathbb{N}^*$ on a $PGCD(ka, kb) = kPGCD(a,b)$

Preuve :
Si $a = 0$ ou $b = 0$, c'est trivial.
Sinon, on peut faire l'algorithme d'Euclide dans lequel, chaque égalité est multipliée par k, dont celle contenant le dernier reste non nul.

Propriété 5 : *Caractéristique*

Soit $d \in \mathbb{N}$. $\quad d = pgcd(a,b) \iff \begin{cases} a = da' \text{ et } b = db' \\ pgcd(a',b') = 1 \end{cases}$

Preuve :
$\Rightarrow$: Si $d = pgcd(a,b)$ alors $d|a$ et $d|b$ et il existe a', b' tels que $a = da'$ et $b = db'$.
De plus, on a $pgcd(a,b) = pgcd(da', db') = d \times pgcd(a',b')$. Donc nécessairement $pgcd(a',b') = 1$.
$\Leftarrow$: Si $a = da'$ et $b = db'$ avec $pgcd(a',b') = 1$.
Comme a et b ne sont pas tous les deux nuls, on a $d \neq 0$ et donc $pgcd(a,b) = d \times pgcd(a',b') = d$.

Remarque : Toute fraction peut alors s'écrire sous forme irréductible.

Exercices du livre *: n° 9 - 10 -11 p 80*

Propriété 6 :
Soient a et b deux entier supérieur ou égaux à 2.
- S'ils n'ont aucun facteur commun, $pgcd(a,b) = 1$
- Sinon, $pgcd(a,b)$ est égal au produit des facteurs premiers communs aux deux nombres, chacun étant affecté du plus petit exposant avec lequel il figure dans leur deux décomposition.

Preuve :
Découle de l'homogénéité.

2 Bezout

Etienne Bezout (1730-1783) fut un génie assez précoce puisqu'à 19 ans, il était déjà adjoint de l'Académie des Sciences. Sa plus grande oeuvre, *Théorie générale des équations algébriques*, un traité clair et détaillé, témoigne de sa pédagogie et de sa volonté de rendre parfaitement accessibles ses découvertes. Bézout fit aussi une brillante carrière dans la marine royale et de chargé de l'enseignement des élèves du corps d'artillerie.

Propriété 7 :
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 $au + bv = d$
2. L'ensemble des entiers $au + bv$ (avec u et v entiers relatifs) est l'ensemble des multiples de d.

Preuve :

1. On utilise l'algorithme d'Euclide. On a :
   $a = bq_0 + r_0 \iff r_0 = a - bq_0 = au_0 + bv_0$ avec $u_0 = 1$ et $v_0 = -q_0$ deux entiers relatifs.
   $b = r_0q_1 + r_1 \iff r_1 = b - r_0q_1 = b - (au_0 + bv_0)q_1 = au_1 + bv_1$ avec $u_1 = -u_0q_1$ et $v_1 = 1 - v_0q_1$ deux entiers.
   Pas à pas, on exprime chaque reste comme combinaison linéaire enitère de a et b jusqu'à r_k, ie le $pgcd(a, b)$.
2. $\subset$: Soit $n = au + bv$ alors comme d divise a et b on a $d|n$, ie n est un multiple de d.
   $\supset$: Soit n un multiple de d. On sait qu'il existe u et v tels que $d = au + bv$. Alors il existe k tel que $n = kd = k(au + bv) = aU + bV$. Donc n est une combinaison linéaire de a et b.

Théorème 1 : *de Bezout*
Deux entiers relatifs a et b sont premiers entre eux si et seulement si il existe des entiers relatifs u et v tels que $au + bv = 1$.

Preuve :
$\Rightarrow$: Si a et b sont premiers entre eux, on applique la propriété pour $d = 1$.
$\Leftarrow$: S'il existe des entiers relatifs u et v tels que $au + bv = 1$ alors d'après la propriété, 1 est un multiple du $pgcd(a, b)$. Par conséquent $d = 1$.

Exemple :
- $a = 4$ et $b = 9$ sont premiers entre eux et $9 \times 1 - 4 \times 2 = 1$. Donc $(u, v) = (-2; 1)$ convient.
- $a = 7$ et $b = 17$
- $a = 71$ et $b = 19$
- Montrer que pour tout $n \in \mathbb{Z}$, n et $n + 1$ sont premiers entre eux
- Même question pour $2n + 1$ et $3n + 1$.

Remarque : Il découle du théorème que l'équation $ax + by = c$, avec $d = pgcd(a, b) \neq 0$ admet des solutions entières si et seulement si $d|c$

Exercices du livre *: n° 25 - 26 - 27 - 32 p 81*

3 Gauss

Carl Friedrich Gauss (1777-1855) fut un mathématicien, astronome et physicien allemand. Il n'existe pas un seul domaine scientifique qu'il n'ait pas abordé, et on lui doit, entre autres, des travaux sur les polygone régulier, sur les nombres complexes, le magnétisme, l'algèbre et bien sûr, l'arithmétique. Il s'impliqua de plus dans les affaires politiques de son temps.

Théorème 2 :
Soient a, b, et c trois entiers relatifs non nuls.
Si $a|bc$ et $pgcd(a,b) = 1$ alors $a|c$.

Preuve :
$a|bc$ donc il existe $k \in \mathbb{Z}$ tel que $bc = ka$.
a et b sont premiers entre eux, donc il existe $(u,v) \in \mathbb{Z}^2$ tels que $au + bn = 1$.
Donc $c = cau + cbv = cau + kav = a(cu + kv)$ avec $cu + kv$ entier. Donc $a|c$.

Corollaire 2 :
Si deux entiers a et b divise un entier c avec $pgcd(a,b) = 1$ alors $ab|c$.

Preuve :
$a|c$ donc il existe un entier k tel que $c = ka$. De même il existe un entier k' tel que $c = bk'$.
Donc $ak = bk'$ et $a|bk'$. Comme a et b sont premiers entre eux on a $a|k'$.
Alors il existe un entier l tel que $k' = al$ et $c = bk' = bal$. Donc $ab|c$.

Remarque : Par conséquent :

- Si un nombre premier p divise un produit ab, alors $p|a$ ou $p|b$
- Si un entier a est premier avec des entiers b_1, b_2, $\ldots$, b_n, alors a est premier avec $b_1 \times b_2 \times \cdots \times b_n$.
- L'unicité de la décomposition en nombre premier vu au chapitre 2 en découle.

Exercices du livre *: n° 19 - 20 - 21 - 22 p 80*

4 Application

4.1 Equation Diophantienne

Définition 3 :
Une équation diophantienne est une équation à coefficients entiers et dont les inconnues sont entières.
Cette année, nous ne résolvons que les équations de la forme $ax + by = k \times PGCD(a, b)$.

Exemples :
- $5x + 7y = 1$
- $6x + 15y = 3$
- $5x - 8y = 2$
- $6x + 14y = 100$

Méthode de Résolution
1. Simplification de l'équation.
   - On calcule $d = pgcd(a, b)$
   - On divise l'équation par d : on obtient $a'x + b'y = d'$ avec $pgcd(a', b') = 1$
2. Recherche d'une solution particulière :
   - On cherche $(x_0, y_0) \in \mathbb{Z}^2$ tels que $a'x_0 + b'y_0 = d'$ à l'aide des divisions euclidiennes
3. Recherche de toutes les solutions :
   - On désigne par x et y d'autres solutions. On a alors $a'(x-x_0)+b'(y-y_0) = 0 \Leftrightarrow a'(x-x_0) = -b'(y-y_0)$
   - D'après le théorème de Gauss, on a alors que $a'|(y-y_0)$ ie qu'il existe $k \in \mathbb{Z}$ tel que $ka' = y - y_0 \Leftrightarrow y = ka' + y_0$.
   - Alors $a'(x-x_0) = -b' \times ka' \Leftrightarrow x = -b'k + x_0$
4. Conclusion : Les solutions sont les couples de la forme $(-b'k + x_0; a'k + y_0)$, avec $k \in \mathbb{Z}$

Exercices du livre *: n° 30 - 31 - 34 p 81*

4.2 Fermat

Théorème 3 : *Petit Théorème de Fermat*
Si p est un entier premier et a un entier naturel non divisble par p, alors a^{p-1} est divisble par p (ou encore $a^{p-1} \equiv 1\,[p]$)

Exemple :
$2^{2002} - 1$ est divisible par 2003 (qui est premier).

Corollaire 3 :
Si p est un entier premier et a un entier naturel, alors $a^p - a$ est divisible par p (ou encore $a^p \equiv a\,[p]$)

Exemple :

Déterminer tous les entiers p premiers tels que $p|(2^p+1)$.

Exercices du livre *: n° 37 - 38 - 39 p 81*

4.3 PPCM

Propriété 8 : *Relation PGCD-PPCM*

Si $d = pgcd(a,b)$ et $m = ppcm(a,b)$ alors $md = ab$.

Preuve :

$d = pgcd(a,b)$ donc il existe a' et b' deux entiers tels que $a = da'$ et $b = db'$ avec $pgcd(a',b') = 1$.
Considérons l'ensemble des multiples communs à a et b. Soi tM l'un quelconque d'entre eux. Alors il existe deux entiers p et q tels que :

$$M = ap = bq \Rightarrow a'dp = b'dq \Leftrightarrow a'p = b'q$$

D'après le théorème de Gauss, on a alors que $a'|q$ d'où il existe un entier k tel que $ka' = q$. Donc $M = ap = bq = ba'k = db'a'k$.
Ainsi tout multiple commun à a et b peut s'écrire sous la forme $M = da'b'k$.
De plus, tout nombre de la forme $da'b'k$ est un multiple de a et b car $da'b'k = ab'k = a'bk$.
Le multiples communs à a et b sont donc les multiples de $da'b'$. Le plus petit étant $m = da'b' = \dfrac{ab}{d}$.

Propriété 9 : *Homogénéité*

Pour tout $k \in \mathbb{N}^*$ on a $PPCM(ka,kb) = kPPCM(a,b)$

Preuve :

Découle directement de la propriété ci-dessus et de l'homogénéité du pgcd.

Propriété 10 :

Soient a et b deux entier supérieur ou égaux à 2. Leur PPCM est le produit des facteurs premiers figurant dans l'une ou l'autre de leurs décompositions, chacun étant affecté de son plus grand exposant.

Preuve :

Découle du lien PGCD-PPCM et de la manière de trouve le PGCD de deux nombres à partir de leurs décompositions.

Exercices du livre *: n° 45-46 p 82 + TYPE BAC : n° 93 - 94 - 103 - 104 - ... p 87 - 90*