P.G.C.D. et P.P.C.M. dans $\mathbb{Z}$

Dans ce chapitre nous présentons les notions, duales l'une de l'autre, de Plus Grand Diviseur Commun et de Plus Petit Multiple Commun. On remarquera que les mots *grand* et *petit* sont opposés tout comme le sont les mots *diviseur* et *multiple*. La notion importante d'entiers *premiers entre eux* apparaîtra comme inévitable et nous rencontrerons alors deux théorèmes fondamentaux : celui de BÉZOUT et celui de GAUSS.


1 P.G.C.D. de deux entiers

Soit $a \in \mathbb{Z}$ un entier relatif. On rappelle que l'on a noté $\mathscr{D}(a)$ l'ensemble des diviseurs de a. Par exemple :

$$\mathscr{D}(6) = \{-6; -3; -2; -1; 1; 2; 3; 6\}$$

On s'aperçoit donc que $\mathscr{D}(a)$ est toujours symétrique par rapport à 0, autrement dit que si $x \in \mathscr{D}(a)$, $-x \in \mathscr{D}(a)$. Afin de simplifier l'étude nous nous intéresserons donc aux diviseurs **positifs** des entiers relatifs. Nous poserons donc :

$$\mathscr{D}_+(a) = \mathscr{D}(a) \cap \mathbb{N} = \{n \in \mathbb{N} \ ; \ n|a\}$$

Par exemple $\mathscr{D}_+(6) = \{1; 2; 3; 6\}$.

1.1 La définition du P.G.C.D.

Soit maintenant deux entiers relatifs a et b. Nous nous intéressons aux *diviseurs communs* (positifs) de a et de b, autrement on cherche les entiers naturels $n \in \mathbb{N}$ tels que $n|a$ et $n|b$. Nous noterons :

$$\mathscr{D}_+(a; b) = \mathscr{D}_+(a) \cap \mathscr{D}_+(b)$$

l'ensemble des diviseurs communs (positifs) de a et de b.

Exemple. $\mathscr{D}_+(12) = \{1;2;3;4;6;12\}$ et $\mathscr{D}_+(8) = \{1;2;4;8\}$ donc les diviseurs communs de 12 et de 8 sont :

$$\mathscr{D}_+(12;8) = \{1;2;4\}$$

Puisque 1 divise tous les nombres, il sera toujours un diviseur commun à deux entiers. Il n'a donc pas d'intérêt de se demander quel est le plus petit diviseur commun : la réponse sera toujours 1. En revanche il est intéressant de se poser la question inverse :

Définition 1.1 *Soit a et b deux entiers relatifs qui ne sont pas simultanément nuls. Alors l'ensemble $\mathscr{D}_+(a;b)$ des diviseurs communs (positifs) de a et de b est une partie finie non vide de $\mathbb{N}$: elle admet donc un plus grand élément appelé* plus grand commun diviseur *de a et b. On le note :*

$$\text{pgcd}(a;b) \quad ou \quad \text{PGCD}(a;b) \quad ou\ parfois \quad a \wedge b$$

Remarque. Pourquoi prendre la précaution $(a;b) \neq (0;0)$ dans la définition précédente ? parce que sinon $\mathscr{D}_+(0;0) = \mathscr{D}_+(0) = \mathbb{N}$ (tous les entiers divisent 0, même 0 lui-même !) et ainsi $\mathscr{D}_+(0,0)$ n'est pas une partie finie et n'admet donc pas de plus grand élément. En revanche on peut très bien avoir l'un des deux entiers a ou b nul. Dans ce cas $\mathscr{D}_+(a;0) = \mathscr{D}_+(a)$ et donc $\text{PGCD}(a;0) = |a|$ (ne pas oublier qu'un PGCD est positif).

Convention. On posera $0 \wedge 0 = 0$.

Exemple. On a vu que $\mathscr{D}_+(12;8) = \{1;2;4\}$ donc $12 \wedge 8 = 4$.

Un cas qui apparaît comme important et tout à fait particulier est celui du cas où le plus grand diviseur commun est... le plus petit possible, à savoir 1 ! Autrement dit, les entiers a et b n'ont «rien en commun» (ou presque) :

Définition 1.2 *Soit a et b deux entiers relatifs. Si $a \wedge b = 1$ on dit que a et b sont* premiers entre eux.

On dit aussi parfois, qu'ils sont *étrangers*, ou encore *comaximaux* (mais ce dernier terme provient de l'Algèbre de Licence L3).

Exemple. 12 et 8 ne sont pas premiers entre eux car leur PGCD est $12 \wedge 8 = 4$. En revanche 15 et 8 sont premiers entre eux car

$$\mathscr{D}_+(15;8) = \{1;3;5;15\} \cap \{1;2;4;8\} = \{1\}$$

On remarque au passage que a et b sont premiers entre eux si et seulement si $\mathscr{D}_+(a;b)$ est le singleton $\{1\}$.

1.2 Premières propriétés du P.G.C.D.

Tout d'abord il est clair que : $\mathscr{D}_+(a;b) = \mathscr{D}_+(b;a)$ donc :

Propriété 1 (commutativité). Quels que soient les entiers $a, b \in \mathbb{Z}$: $a \wedge b = b \wedge a$.

Ensuite remarquons que $\mathscr{D}_+(a) = \mathscr{D}_+(-a)$ pour tout entier relatif a. Ainsi :

Propriété 2. Quels que soient les entiers $a, b \in \mathbb{Z}$: $(-a)\wedge b = a\wedge(-b) = a\wedge b$.

Le signe d'un entier n'a donc pas d'importance dans un PGCD.

Puisque $\mathscr{D}(0) = \mathbb{Z}$ (tous les entiers divisent 0, même 0), on a $\mathscr{D}_+(a,0) = \mathscr{D}_+(a)$ donc :

Propriété 3. Quel que soit l'entier relatif $a \in \mathbb{Z}$: $a \wedge 0 = |a|$.

N'oublions pas que par convention $0 \wedge 0 = 0$.

Propriété 4. Si $d = a \wedge b$ alors on peut écrire : $a = kd$, $b = k'd$ avec k et k' premiers entre eux.

En effet, d est un diviseur, à la fois de a et de b, donc on peut écrire $a = kd$, $b = k'd$ avec k, k' deux entiers relatifs. Si k et k' n'étaient pas premiers entre eux, leur PGCD serait $\delta > 1$. On aurait donc $k = m\delta$ et $k' = m'\delta$ et donc $a = m\delta d$ et $b = m'\delta d$. L'entier δd serait donc un diviseur commun à a et b et il serait plus grand que d puisque $\delta > 1$: c'est impossible. Donc k et k' sont bien premiers entre eux.

Propriété 5 (différences successives). Soit a et b deux entiers relatifs. Alors $a \wedge b = a \wedge (b - a)$.

En effet, nous allons même montrer que $\mathscr{D}_+(a;b) = \mathscr{D}_+(a;b-a)$ ce qui est encore plus fort. Pour démontrer l'égalité de deux ensembles E et F rappelons qu'il faut montrer que $E \subset F$ et que $F \subset E$.

Supposons donc que $x \in \mathscr{D}_+(a;b)$ et montrons que $x \in \mathscr{D}_+(a;b-a)$:

puisque par hypothèse x divise a et b il divise aussi $b-a$, c'est donc un diviseur commun de a et $b-a$ *i.e.* $x \in \mathscr{D}_+(a; b-a)$.

Réciproquement, supposons que $x \in \mathscr{D}_+(a; b-a)$. x divise a et $b-a$ donc il divise aussi leur somme : $a+(b-a)=b$, ainsi x est un diviseur commun de a et b *i.e.* $x \in \mathscr{D}_+(a; b)$.

En conclusion on a bien $\mathscr{D}_+(a; b) = \mathscr{D}_+(a; b-a)$ donc $a \wedge b = a \wedge (b-a)$.

Application. Cette dernière propriété donne naissance à un algorithme de calcul du PGCD : l'algorithme des *différences successives* : cherchons par exemple le PGCD de 145 et de 258. On a successivement :

$145 \wedge 258 = 145 \wedge (258-145) = 145 \wedge 113$
$113 \wedge 145 = 113 \wedge (145-113) = 113 \wedge 32$
$32 \wedge 113 = 32 \wedge (113-32) = 32 \wedge 81$
$32 \wedge 81 = 32 \wedge (81-32) = 32 \wedge 49$
$32 \wedge 49 = 32 \wedge (49-32) = 32 \wedge 17$
$17 \wedge 32 = 17 \wedge (32-17) = 17 \wedge 15$
$15 \wedge 17 = 15 \wedge (17-15) = 15 \wedge 2 = 1.$

Ainsi le PGCD de 145 et 258 est 1 *i.e.* ils sont premiers entre eux. Le paragraphe suivant donne un autre algorithme célèbre de calcul du PGCD.

1.3 L'algorithme d'Euclide et conséquence

On suppose ici que a et b sont des entiers naturels, ce qui ne nuit pas à la généralité puisque le signe des entiers ne change pas le PGCD. On suppose aussi que $0 < b < a$.

Principe de l'algorithme d'Euclide. Avec les hypothèses ci-dessus, si q et r sont le quotient et le reste de la division euclidienne de a par b (*i.e.* $a = bq + r$ avec $0 \leqslant r < b$) alors :

$$\mathscr{D}_+(a; b) = \mathscr{D}_+(b, r)$$

autrement dit les diviseurs communs de a et b sont exactement les diviseurs communs de b et r. En conséquence :

$$a \wedge b = b \wedge r$$

Preuve. Pour démontrer que $\mathscr{D}_+(a; b) = \mathscr{D}_+(b, r)$ nous allons démontrer

une double inclusion : $\mathscr{D}_+(a;b) \subset \mathscr{D}_+(b,r)$ et $\mathscr{D}_+(a;b) \supset \mathscr{D}_+(b,r)$.

Soit $x \in \mathscr{D}_+(a;b)$. Puisque x divise b, x divise aussi bq. Puisque x divise aussi a il divise donc $a-bq=r$. Ainsi x divise à la fois b et r *i.e.* $x \in \mathscr{D}_+(b;r)$.

Réciproquement, soit $x \in \mathscr{D}_+(b;r)$. Puisque x divise b, x divise aussi bq. Puisque x divise aussi r il divise donc $bq+r=a$. Ainsi x divise à la fois a et b *i.e.* $x \in \mathscr{D}_+(a;b)$. □

Mise en place de l'algorithme d'Euclide. La recherche du PGCD de a et b revient donc à celle du PGCD de b et r ce qui est très intéressant puisque b et r sont des entiers inférieurs à a et b (par hypothèse $b<a$). Deux cas se présentent alors :

- Si $r=0$ c'est que b divise a et donc $a \wedge b = b$.
- Si $r>0$ on peut réitérer le procédé et faire la division euclidienne de b par r :

  $$b = rq_1 + r_1 \qquad \text{avec } 0 \leqslant r_1 < r$$

  et on a donc $a \wedge b = b \wedge r = r \wedge r_1$. On construit de proche en proche une suite strictement décroissante :

  $$r > r_1 > r_2 > \dots$$

  qui se termine nécessairement par 0 puisque tous les r_i sont des entiers naturels. Il existera donc un $r_n \neq 0$ avec $r_{n+1}=0$. On aura, de proche en proche :

  $$a \wedge b = r_i \wedge r_{i+1} = r_n \wedge 0 = r_n$$

  de sorte que le PGCD cherché sera LE DERNIER RESTE NON NUL.

Exemple. Trouver PGCD(145 ; 258). On crée un tabelau comme ci-dessous en grisant la colonne des quotients car les quotients ne participent pas dans le principe d'Euclide :

a	b	q	r	
258	145	1	113	$258 \wedge 145 = 145 \wedge 113$
145	113	1	32	$145 \wedge 113 = 113 \wedge 32$
113	32	3	17	$113 \wedge 32 = 32 \wedge 17$
32	17	1	15	$32 \wedge 17 = 17 \wedge 15$
17	15	1	2	$17 \wedge 15 = 15 \wedge 2$
15	2	7	1	$15 \wedge 2 = 2 \wedge 1$
2	1	2	**0**	

Le dernier reste non nul est 1 donc $258 \wedge 145 = 1$. Cet algorithme a une conséquence immédiate :

Corollaire. Soit a et b des entiers relatifs et d leur PGCD. Alors :

$$\mathscr{D}_+(a;b) = \mathscr{D}_+(d)$$

autrement dit les diviseurs communs de a et b sont tous des diviseurs du PGCD de a et b. Formellement on peut encore écrire :

$$\forall n \in \mathbb{Z} \quad \begin{cases} n|a \\ n|b \end{cases} \Longrightarrow n|d$$

En effet, on vient de montrer que $\mathscr{D}_+(a;b) = \mathscr{D}_+(r_n, 0) = \mathscr{D}_+(r_n)$ où r_n est le dernier reste non nul des divisions euclidiennes successives.

2 Le théorème de Bézout et conséquences

Le théorème de Bézout est l'un des plus important résultat de ce chapitre. Il permettra de résoudre un type d'équations diophantiennes très classiques.

2.1 L'énoncé et la preuve du théorème

On rappelle que deux entiers relatifs sont dits premiers entre eux lorsque leur PGCD est le plus petit possible : 1. Ils n'ont ainsi (presque) aucun diviseur en commun. Le théorème de Bézout donne une caractérisation (*i.e.* avec un «si et seulement si») des entiers premiers entre eux.

Théorème (de Bézout). Soit a et b des entiers relatifs. Alors a et b sont premiers entre eux si et seulement s'il existe un couple $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.

Attention, ce couple (u, v) n'est pas unique ! on expliquera comment en trouver un grâce à un algorithme.

Preuve. Il s'agit de démontrer un «si et seulement si», on le fera donc en deux étapes : une partie «nécessaire» et une partie «suffisante».

Supposons qu'il existe des entiers relatifs u et v tels que $au+bv = 1$ et montrons alors que a et b sont premiers entre eux. Le PGCD d de a et b étant un diviseur commun de a et b, il divise aussi $au+bv = 1$ donc $d = 1$ (car d est positif). Ainsi a et b sont premiers entre eux.

Réciproquement, supposons que a et b soient premiers entre eux. Considérons alors l'ensemble de toutes les combinaisons linéaires entières de a et de b *i.e.* l'ensemble de tous les entiers de la forme $au + bv$ où u et v parcourent $\mathbb{Z}$. Cet ensemble se note :

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv \ ; \ u, v \in \mathbb{Z}\}$$

Il est évident que a et b sont dans cet ensemble (car $a = a \times 1 + b \times 0$ et $b = a \times 0 + b \times 1$). De plus $-a$ et $-b$ sont aussi dans cet ensemble (car $-a = a \times (-1) + b \times 0$, etc.) Ainsi $a\mathbb{Z} + b\mathbb{Z}$ est un ensemble qui contient au moins un entier strictement positif : en effet a et b ne sont pas simultanément nuls sinon ils ne pourraient pas être premiers entre eux. Dans ce cas notons d le plus petit entier strictement positif appartenant à $a\mathbb{Z} + b\mathbb{Z}$: il s'écrit donc $d = au + bv$ avec u et v dans $\mathbb{Z}$. Nous allons prouver maintenant que $d = 1$. En effet, la division de a par d puis celle de b par d donnent :

$$a = dq + r \qquad b = dq' + r'$$

avec $0 \leqslant r < d$ et $0 \leqslant r' < d$. On a donc, en se rappelant que $d = au + bv$:

$$r = a - dq = a - (au + bv)q = a(1 - uq) + b \times (-vq) = aU + bV$$

donc $r \in a\mathbb{Z} + b\mathbb{Z}$. Oui mais r est aussi positif et strictement inférieur à d : comme d est le plus petit élément strictement positif de $a\mathbb{Z}+b\mathbb{Z}$ on a nécessairement $r = 0$. On montrerait de la même manière que $r' = 0$. Ainsi $a = dq$ et $b = dq'$ donc d est un diviseur commun de a et b. Par hypothèse ils sont premiers entre eux donc $d = 1$. Finalement on a trouvé des entiers relatifs u et v tels que $au + bv = d = 1$. □

Exemple. 8 et 11 sont premiers entre eux car $4 \times 8 = 32$ et $3 \times 11 = 33$ donc $8u + 11v = 1$ si on prend $u = -4$ et $v = 3$. Mais on peut aussi remarquer que $7 \times 8 = 56$ et $5 \times 11 = 55$ donc $8u + 11v = 1$ avec $u = 7$ et $v = -5$. On voit bien que le couple (u, v) n'est pas unique.

Le théorème de Bézout (enfin une partie) s'utilise aussi tout à fait pour les entiers qui ne sont pas premiers entre eux : c'est un corollaire immédiat

de ce qui précède.

Corollaire 1. Soit a et b des entiers relatifs et d leur PGCD. Alors il existe des entiers relatifs u et v tels que $au + bv = d$.

PIEGE ! On remarquera qu'il n'y a pas de «si et seulement si». En effet, $3 \times 4 + 5 \times 2 = 22$ pourtant 22 n'est pas le PGCD de 3 et 5 ! ! Ce corollaire ne marche que dans un sens.

Preuve. Supposons donc que d est le PGCD de a et b. On a vu dans les propriétés du PGCD qu'on peut alors écrire $a = kd$ et $b = k'd$ avec k et k' premiers entre eux. D'après le théorème de Bézout il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $ku + k'v = 1$ en multipliant tout par d on obtient : $au + bv = d$. □

Une façon plus abstraite de présenter le théorème de Bézout est :

Corollaire 2. Soit a et b des entiers relatifs.

$$a \wedge b = 1 \Longleftrightarrow a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$$

autrement dit tout entier relatif peut s'écrire comme combinaison linéaire entière de a et de b.

Preuve. En effet si $a \wedge b = 1$ alors il existe u, v tels que $au + bv = 1$ donc $1 \in a\mathbb{Z} + b\mathbb{Z}$ et par conséquent $\mathbb{Z} \subset a\mathbb{Z}+b\mathbb{Z}$. L'autre inclusion étant triviale on a montré que $a\mathbb{Z}+b\mathbb{Z} = \mathbb{Z}$.

Réciproquement si $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ en particulier $1 \in a\mathbb{Z} + b\mathbb{Z}$ et donc il existe u, v tels que $au + bv = 1$ et par le théorème de Bézout $a \wedge b = 1$. □

Et enfin la version quelconque (pas forcément premiers entre eux) de ce corollaire :

Corollaire 3. Soit a et b des entiers relatifs. Alors :

$$d = a \wedge b \Longleftrightarrow a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

Preuve. En effet si $a \wedge b = d$ alors d'après le corollaire 1 il existe u, v tels que $au+bv = d$ donc $d \in a\mathbb{Z} + b\mathbb{Z}$ et par conséquent $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$. Pour montrer l'autre inclusion il suffit de remarquer que d est un diviseur commun de a et de b donc il divise toute combinaison linéaire entière $au + bv$ *i.e.* $d|au + bv$ quels que soient les entiers $u, v \in \mathbb{Z}$: ceci veut dire $au + bv \in d\mathbb{Z}$ pour tous $u, v \in \mathbb{Z}$ ou encore $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$.

Réciproquement si $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et montrons que $d = a \wedge b$. Puisque a et b sont dans $a\mathbb{Z} + b\mathbb{Z}$, ils sont aussi dans $d\mathbb{Z}$ *i.e.* ce sont des multiples de d ou encore d est un diviseur commun de a et b. Mais comme $\mathscr{D}_+(a; b) = \mathscr{D}_+(a \wedge b)$ on a $d|(a \wedge b)$. Or $a \wedge b$ divise (par

définition) a et b, donc divise aussi d : en effet $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ par hypothèse donc d est une combinaison linéaire entière de a et de b et on sait que tout diviseur commun de a et de b divise toute combinaison linéaire entière de a et de b. Finalement on a $d|a \wedge b$ et $a \wedge b|d$ d'où $d = a \wedge b$ car ces deux entiers sont positifs. □

Algorithme pour trouver les entiers u et v. Le théorème de Bézout assure qu'il existe des entier u et v tels que ... très bien, mais comment les trouver pratiquement ? La bonne nouvelle c'est que tout repose sur un algorithme déjà connu : l'algorithme d'Euclide. Traitons un exemple.

Trouver des entiers u et v dans $\mathbb{Z}$ tels que $15u + 11v = 1$. On peut bien sûr chercher «à la main» sans méthode précise en énumérant les multiples de 15 puis ceux de 11 jusqu'à ce que la différence fasse 1 : cela peut être assez long dans la pratique. Ici c'est rapide car $3 \times 15 = 45$ et $4 \times 11 = 44$. Mais cela s'avère bien plus compliqué si on cherche des entiers u et v dans $\mathbb{Z}$ tels que $258u + 145v = 1$. étudions la méthode générale :

Méthode : Ecrivons l'algorithme d'Euclide pour chercher le PGCD de 258 et 145 (dont on sait qu'il vaut 1, mais les calculs sont importants) ; on écrira ensuite chaque reste sous la forme $au + bv$. Comme le dernier reste est le PGCD (qui vaut 1) on aura une écriture de la forme $1 = au + bv$.

a	b	q	r	$r = au+bv$
258	145	1	113	$113 = a - b$
145	113	1	32	$32 = b - 113 = b - (a - b) = 2b - a$
113	32	3	17	$17 = 113 - 32\times3 = (a - b) - (2b - a)\times3 = 4a - 7b$
32	17	1	15	$15 = 32 - 17 = (2b - a) - (4a - 7b) = 9b - 5a$
17	15	1	2	$2 = 17 - 15 = (4a - 7b) - (9b - 5a) = 9a - 16b$
15	2	7	1	$1 = 15 - 2\times7 = (9b - 5a) - (9a - 16b)\times7 = -68a + 121b$

On peut vérifier qu'on a bien : $-68\times258+121\times145 = -17544+17545 = 1$. Il est évident qu'on n'aurait pas pu trouver ces coefficients aussi facilement que pour 15 et 11.

2.2 Quelques conséquences du théorème

Le théorème de Bézout permet de montrer quelques propriétés supplémentaires du PGCD.

Propriété 1. Si un entier a est premier avec b et avec c alors il est premier avec leur produit bc.

En effet, par hypothèse, et grâce au théorème de Bézout on peut écrire : $au + bv = 1$ et $au' + cv' = 1$ avec $(u, v, u', v') \in \mathbb{Z}^4$. En faisant le produit on obtient :

$$(au + bv)(au' + cv') = 1 \times 1 \Longleftrightarrow a(auu' + ucv' + bvu') + bc(vv') = 1$$

et on a une écriture de la forme $aU + bcV = 1$ ce qui prouve par le théorème de Bézout (mais dans l'autre sens) que $a \wedge bc = 1$.

Propriété 2. Si un entier a est premier avec b alors pour tous entiers naturels $n > 0$ et $p > 0$: a^n et premier avec b^p.

En effet, en prenant $c = b$ dans la proposition 1 on trouve que a est premier avec b^2. Par récurrence on établit facilement que a est premier avec b^p pour tout $p > 0$. Mais puisque b^p est premier avec a il est aussi premier avec a^2 comme on vient juste de l'expliquer. Par récurrence encore une fois on montre que b^p est premier avec a^n pour tout $n > 0$.

Propriété 3. Soit a, b deux entiers relatifs et $k \in \mathbb{Z}$ quelconque. Alors :

$$\text{PGCD}(ka; kb) = |k|\text{PGCD}(a; b)$$

On dit que c'est la *propriété multiplicative* du PGCD.

Preuve. Puisque le PGCD est invariant par changement de signe on peut déjà supposer que $k \in \mathbb{N}$ de sorte que $|k| = k$. Notons $d = a \wedge b$ et $\delta = (ka) \wedge (kb)$. On va montrer que $kd|\delta$ et que $\delta|kd$ ce qui prouvera que $kd = \delta$.

Puisque d divise a et b, kd divise ka et kb donc $kd \in \mathscr{D}_+(ka; kb) = \mathscr{D}_+(\delta)$ donc $kd|\delta$.

A l'inverse, puisque d est le PGCD de a et b il peut s'écrire (corollaire 1) $d = au + bv$ donc $kd = aku + bkv$. Mais comme δ, par définition même, divise à la fois ka et kb il divise aussi toute combinaison linéaire entière de ka et kb par exemple $aku + bkv = kd$ donc $\delta|kd$. □

Inverses d'un entier modulo n

Rappelons que si x est non nul son inverse y (que l'on note $\frac{1}{x}$) vérifie $xy = 1$. On imite cette définition en posant :

Définition 2.1 *Soit a, n des des entiers. On appelle* inverse modulo n *de a tout entier b tel que $ab \equiv 1\ [n]$.*

Et on a le résultat suivant, qui n'est qu'un corollaire du théorème de Bézout :

Théorème (inverse modulo n). L'entier a admet un inverse modulo n si et seulement s'il est premier avec n.

Le preuve est importante car elle explique comment trouver un inverse modulo n :

Preuve. Puisque a et n sont premiers entre eux il existe d'après le théorème de Bézout deux entiers u et v tels que $au + nv = 1$. Puisque $nv \equiv 0\ [n]$ on a $au \equiv 1\ [n]$ et u est un inverse modulo n de a. □

On comprend donc que pour trouver un inverse modulo n de a il faut trouver l'entier u donc pratiquer un algorithme d'Euclide.

Exemple. Trouver l'inverse de 145 modulo 258. On a vu auparavant qu'une relation de Bézout entre ces deux nombres était $-68 \times 258 + 121 \times 145 = 1$ donc 121 est un inverse de 145 modulo 258.

Conséquence : équations $ax \equiv b\ [n]$. Cette équation (d'inconnue $x \in \mathbb{Z}$) admet des solutions si a admet un inverse modulo n, autrement dit si a est premier avec n. Si u est un tel inverse alors $x \equiv ub\ [n]$ c'est-à-dire :

$$x = uv + kn$$

où $k \in \mathbb{Z}$ est quelconque.

Réciproquement si a n'est pas inversible modulo n cela veut dire que a n'est pas premier avec n : dans ce cas $a \wedge n = d > 1$ et on peut écrire $a = da'$, $n = dn'$ avec $a' \wedge n' = 1$. On a alors

$$ax \equiv b\ [n] \Longleftrightarrow a'dx = b + kn'd\ (k \in \mathbb{Z})$$

et donc $b = d(a'x - kn')$. Si jamais b n'est pas un multiple de d l'équation est impossible. Sinon on peut écrire $b = b'd$ et en simplifiant par d on trouve :

$$a'x = b' + kn'\ (k \in \mathbb{Z}) \equiv a'x \equiv b'\ [n]$$

qui a des solutions puisque a' est premier avec n'. Au bilan :

Théorème (équation $ax \equiv b\ [n]$). L'équation $ax \equiv b\ [n]$:

1. admet une infinité de solutions si a est premier avec n. Si u est un inverse modulo n de a ces solutions sont les entiers $ub + kn$ où $k \in \mathbb{Z}$.
2. n'admet pas de solution si a n'est pas premier avec n ET si b n'est pas un multiple du PGCD de a et n.
3. admet une infinité de solutions si a n'est pas premier avec b mais que que b est un multiple du PGCD de a et b.

On remarquera, puisque b est un multiple de 1 que l'équation $ax \equiv b\ [n]$ admet donc une infinité de solutions si et seulement si b est un multiple de $a \wedge n$. Dans le cas 3 il faut diviser toute l'équation (n y compris) par le PGCD de a et b pour se ramener en 1.

Exemple. Résoudre $145x \equiv 3\ [258]$. On sait que 145 est premier avec 258 et que 121 est un inverse modulo 258 de 145. Donc $x \equiv 121 \times 3\ [258]$ autrement dit les solutions sont les entiers de la forme $363 + 258k$ avec $k \in \mathbb{Z}$.

3 Le théorème de Gauss et conséquences

Le théorème de Gauss se déduit aisément du théorème de Bézout et a plusieurs conséquences importantes : sur les congruences et sur la résolution d'équations diophantiennes importantes au programme : les *équations de Bézout*. Le théorème de Gauss est un résultat de divisibilité :

Théorème (de Gauss). Soit a, b, c trois entiers relatifs. Si a divise bc et que a est premier avec b alors a divise c.

Preuve. Par hypothèse a et b sont premiers entre eux, donc par le théorème de Bézout $au + bv = 1$ avec u, v dans $\mathbb{Z}$. On suppose aussi dans les hypothèses que a divise bc donc $bc = ka$ avec $k \in \mathbb{Z}$. On a donc en multipliant par c dans l'égalité de Bézout :

$$auc + bvc = c \Longleftrightarrow auc + v(ka) = c \Longleftrightarrow aK = c$$

avec $K = uc + vk \in \mathbb{Z}$. Donc $a|c$. □

3.1 Simplifications dans les congruences.

En terme de congruences le théorème de Gauss eut s'écrire formellement ainsi :

Théorème (de Gauss, version congruence). Supposons que l'on ait une congruence entre entiers relatifs de la forme :

$$ax \equiv bx\ [n]$$

Si x est premier avec n alors on peut simplifier par x : $a \equiv b\ [n]$.

Preuve. La congruence $ax \equiv bx\ [n]$ est équivalente à $(a-b)x \equiv 0\ [n]$ ce qui signifie encore «n divise $(a-b)x$». Puisque x est premier avec n le théorème de Gauss affirme que n divise $a-b$ ce qui s'écrit aussi $a-b \equiv 0\ [n]$

ou encore $a \equiv b\ [n]$. □

Une autre preuve consiste à utiliser la notion d'inverse modulo n (écrire la démonstration). On a donc la règle qui nous manquait pour pouvoir simplifier dans des congruences (cf. chapitre 1).

3.2 Les équations de Bézout

Ce qui suit concerne la résolution des équations diophantiennes dites de Bézout :

Théorème (Equation de Bézout réduite). Soit a, b deux entiers relatifs. l'équation diophiantienne :

$$ax + by = 1$$

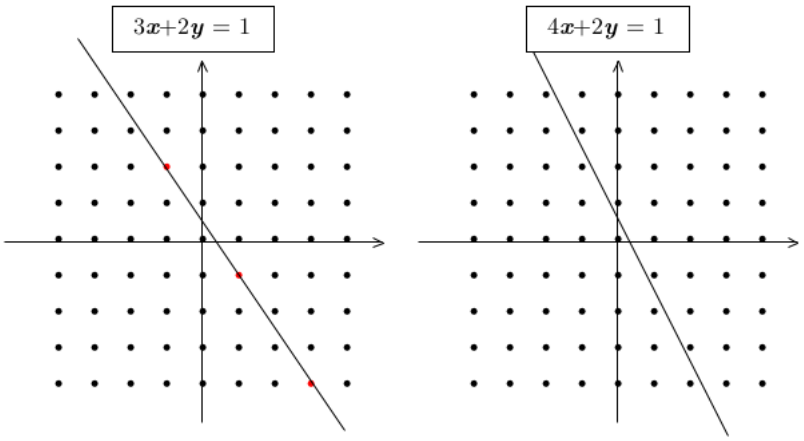
d'inconnue $(x, y) \in \mathbb{Z}^2$ admet :

1. aucune solution si a et b ne sont pas premiers entre eux,
2. une infinité de solutions si a et b sont premiers entre eux et ces solutions sont toutes de la forme :

$$x = bk + x_0, \qquad y = -ak + y_0$$

où $k \in \mathbb{Z}$ quelconque et où $(x_0; y_0)$ est une solution particulière de l'équation $ax + by = 1$.

Interprétation géométrique. Les solutions sont donc les couples $(bk + x_0; -ak + y_0)$ $(k \in \mathbb{Z})$ ils sont donc situés sur la droite passant par le point $M_0(x_0; y_0)$ et de vecteur directeur $\vec{u}(b; -a)$. Cette droite a pour équation cartésienne $ax + by = 1$. Les solutions sont donc les couples coordonnées des points de cette droite qui ont des coordonnées entières.



La droite rencontre le réseau $\mathbb{Z}^2$: par exemple en (1 ; -1), en (-1 ; 2), etc.

La droite ne rencontre pas le réseau $\mathbb{Z}^2$.

On note $\mathbb{Z}^2$ l'ensemble des couples d'entiers relatifs : graphiquement $\mathbb{Z}^2$ est un *réseau* du plan $\mathbb{R}^2$ (comme un quadrillage de points). La résolution de $ax + by = 1$ consiste à savoir si la droite d'équation $ax + by = 1$ rencontre ou non ce réseau. Il se peut, si a et b ne sont pas premiers entre eux que la droite «passe au travers» du réseau et ne le rencontre jamais !

Preuve. Si $a \wedge b \neq 1$ alors 1 ne peut pas s'écrire $au + bv$ (d'après le théorème de Bézout). Ainsi l'équation $ax + by = 1$ n'a pas de solution.

Si $a \wedge b = 1$ il existe d'après le théorème de Bézout un couple d'entiers relatifs (x_0, y_0) tel que $ax_0 + by_0 = 1$. Par différence l'équation à résoudre devient :

$$a(x - x_0) + b(y - y_0) = 0 \Longleftrightarrow a(x - x_0) = b(y_0 - y)$$

Ainsi b divise $a(x - x_0)$, mais comme a et b sont premiers entre eux, on applique le théorème de Gauss pour en déduire que b divise $x - x_0$: il existe donc $k \in \mathbb{Z}$ tel que $x - x_0 = bk$. En reportant dans l'équation précédente on a : $abk = b(y_0 - y)$. On peut simplifier par b car on peut le supposer non nul (s'il est nul, cela veut dire que $a = 1$ et l'équation $x = 1$ est... facile à résoudre !). On a donc $ak = y_0 - y$ d'où $y = -ak + y_0$.

Réciproquement il s'agit de montrer que les solutions trouvées conviennent toutes. On a en effet, quel que soit $k \in \mathbb{Z}$:

$$a(bk + x_0) + b(-ak + y_0) = abk - abk + ax_0 + by_0 = 1$$

puisque $(x_0; y_0)$ est une solution particulière. Ainsi toutes les solutions sont convenables. □

On peut alors résoudre l'équation de Bézout générale :

Corollaire (Equation de Bézout générale). Soit a, b, c trois entiers relatifs. l'équation diophiantienne :

$$ax + by = c$$

d'inconnue $(x, y) \in \mathbb{Z}^2$ admet :

1. aucune solution si c n'est pas un multiple de $a \wedge b$,
2. une infinité de solutions si c n'est pas un multiple de $a \wedge b$ et ces solutions sont toutes de la forme :

$$x = bk + x_0, \qquad y = -ak + y_0$$

où $k \in \mathbb{Z}$ quelconque et où $(x_0; y_0)$ est une solution particulière de l'équation $ax + by = c$.

Preuve. Notons $d = a \wedge b$. On sait que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, or s'il existe une solution de $ax + by = c$ on a donc $c \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ donc c est forcément un multiple de d.

Supposons donc qu'il en soit ainsi et écrivons $c = kd$ avec $k \in \mathbb{Z}$. Comme $(x_0; y_0)$ est solution particulière, on a $ax_0 + by_0 = c$ et par différence :

$$a(x - x_0) + b(y - y_0) = 0$$

Ecrivons aussi $a = a'd$, $b = b'd$ avec $a' \wedge b' = 1$. On a donc :

$$a'd(x - x_0) + b'd(y - y_0) = 0 \Longrightarrow a'(x - x_0) + b'(y - y_0) = 0$$

On procède exactement comme dans le cas de l'équation réduite. □

Exemple 1. Résoudre dans $\mathbb{Z}^2$ l'équation $5x - 7y = 1$. C'est une équation de Bézout réduite qui a des solutions puis que 5 et 7 sont premiers entre eux.

Il est facile de trouver une solution particulière (inutile de l'algorithme d'Euclide pour cela). En effet $10 \times 5 = 50$ et $7 \times 7 = 49$ donc $(10; 7)$ est une solution particulière. Ecrivons donc :

$$\begin{cases} 5x - 7y &= 1 \\ 5 \times 10 - 7 \times 7 &= 1 \end{cases}$$

et faisons la différence : $5(x-10)-7(y-7)=0$ ce qui donne : $5(x-10)=7(y-7)$. Ainsi 5 divise $7(y-7)$ mais comme 5 est premier avec 7, le théorème de Gauss assure que 5 divise en fait $y-7$: il existe donc $k\in\mathbb{Z}$ tel que $y-7=5k$. En reportant dans l'équation précédente il vient $5(x-10)=7\times 5k$ d'où $x-10=7k$. Finalement les solutions possibles sont les couples $(7k+10;5k+7)$ où $k\in\mathbb{Z}$. Réciproquement tous ces couples sont solutions car :

$$5(7k+10)-7(5k+7)=50-49=1$$

On a donc trouvé toutes les solutions de l'équation proposée.

Exemple 2. Résoudre dans $\mathbb{Z}^2$ l'équation $12x+8y=20$. C'est une équation de Bézout générale qui a des solutions puis que $12\wedge 8=4$ et que 20 est un multiple de 4.

On peut tout de suite simplifier l'équation par 4 : $3x+2y=5$. Il est facile de trouver une solution particulière (inutile de l'algorithme d'Euclide pour cela). En effet $(1;1)$ est une solution. On a donc :

$$\begin{cases} 3x+2y &= 5\\ 3\times 1+2\times 1 &= 5\end{cases}$$

et faisons la différence : $3(x-1)+2(y-1)=0$ ce qui donne : $3(x-1)=2(1-y)$. Ainsi 3 divise $2(1-y)$ mais comme 3 est premier avec 2, le théorème de Gauss assure que 3 divise en fait $1-y$: il existe donc $k\in\mathbb{Z}$ tel que $1-y=3k$. En reportant dans l'équation précédente il vient $3(x-1)=2\times 3k$ d'où $x-1=2k$. Finalement les solutions possibles sont les couples $(2k+1;-3k+1)$ où $k\in\mathbb{Z}$. Réciproquement tous ces couples sont solutions car :

$$3(2k+1)+2(-3k+1)=3+2=5$$

On a donc trouvé toutes les solutions de l'équation proposée.

4 P.P.C.M. de deux entiers

Reste maintenant à étudier rapidement la notion duale du PGCD : le PPCM. Rappelons qu'on note $a\mathbb{Z}$ l'ensemble des multiples de l'entier a. Ainsi l'ensemble des multiples communs à a et b est $a\mathbb{Z}\cap b\mathbb{Z}$. Cet ensemble n'est pas vide car ab lui appartient. Parmi les positifs il y en a forcément un qui est le plus petit :

Définition 4.1 *Soit a et b deux entiers non nuls. On appelle plus petit commun multiple de a et b le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$. On le note :*

$$\text{ppcm}(a;b) \quad ou \quad \text{PPCM}(a;b) \quad ou \quad a \vee b$$

Il est évident que $a \vee b = v \vee a$.

Convention. Quel que soit a on a posera $a \vee 0 = 0$. Ceci est en accord avec le théorème fondamental qui va suivre.

Théorème. Soit a, b deux entiers relatifs et m leur PPCM. Alors :

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$

autrement dit : tout multiple commun à a et b est un multiple de m.

Cette propriété est à rapprocher de celle vérifiée par le PGCD : $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. En fait dans un cours de supérieur, c'est grâce à ces deux propriétés que l'on définit le PGCD et le PPCM. Pourquoi ? parce que cette définition peut se généraliser à d'autres anneaux que $\mathbb{Z}$ (anneaux dits *principaux*). On peut même définir une notion de PGCD et de PPCM dans des anneaux pas forcément principaux (anneaux dits *factoriels*) grâce à la décomposition en facteurs premiers (cf. chapitre 3).

Preuve. Remarquons déjà que $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$ est une inclusion évidente : si $M \in m\mathbb{Z}$ alors $M = mk$ avec $k \in \mathbb{Z}$ et M est un multiple commun de a et b puisqu'il en est ainsi de m.

Il nous faut donc démontrer l'autre inclusion : $a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$. Soit donc $M \in a\mathbb{Z} \cap b\mathbb{Z}$. La division euclidienne de M par m donne : $M = mq + r$ avec $0 \leqslant r < m$. Oui mais alors $r = M - mq$ est un multiple commun à a et b puisque c'est le cas de M et de m (donc de mq), donc $r \in (a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}$ est plus petit strictement que m : comme m est par définition le plus petit élément de $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^*$ on a forcément $r = 0$. Donc $M = mq \in m\mathbb{Z}$. □

On peut alors en déduire la propriété bien pratique suivante :

Théorème (du complément). Soit a, b deux entiers naturels (donc positifs). Alors :

$$\text{PGCD}(a;b) \times \text{PPCM}(a;b) = a \times b$$

Ainsi, dès qu'on a trouvé le PGCD de a et de b on a immédiatement le PPCM puisque ce dernier vaut $\frac{ab}{\text{PGCD}(a;b)}$. Si les entiers a et b ne sont pas positifs, il convient de ne pas oublier les valeurs absolues car un PGCD et

un PPCM sont toujours positifs, eux.

Preuve. Si jamais l'un des deux entiers est nul, le PPCM est nul est la relation est vraie. Nous écartons ce cas par la suite.

Soit $d = a \wedge b$ et $m = a \vee b$. On sait que $a = a'd$ et $b = b'd$ avec a', b' premiers entre eux. Intéressons-nous alors à l'entier $a'b'd$. Cet entier peut s'écrire ab' ou bien encore ba' : ceci prouve que $a'b'd$ est un multiple commun de a et b c'est donc un multiple de m d'après le théorème fondamental ci-dessus. On a donc $m|a'b'd$.

Réciproquement montrons que $a'b'd|m$. Puisque m est un multiple commun de a et b écrivons $m = ax$ et $m = by$ avec $x, y \in \mathbb{N}$. L'égalité $ax = by$ devient donc $a'dx = b'dy$ et puisque d est non nul (car a et b sont non nuls par hypothèse) on a donc $a'x = b'y$. Puisque a' est premier avec b' le théorème de Gauss assure que a' divise y (et aussi que b' divise x mais on n'en a pas besoin ici) : on a donc $y = ka'$ avec $k \in \mathbb{Z}$. Donc $m = by = bka' = b'dka'$ ce qui prouve bien que $a'b'd|m$.

Au bilan on a $a'b'd|m$ et $m|a'b'd$, comme il s'agit d'entiers positifs on en déduit que $a'b'd = m$. En multipliant par d on trouve alors $a'db'd = md$ *i.e.* $ab = md$ ce qui était demandé. □

En corollaire on peut montrer que le PPCM possède tout comme le PGCD la propriété multiplicative :

Corollaire. Soit a, b deux entiers relatifs et $k \in \mathbb{Z}$ quelconque. Alors :

$$\text{PPCM}(ka; kb) = |k|\text{PPCM}(a; b)$$

Preuve. Pour simplifier on peut supposer k positif car le signe ne change pas le PPCM. Il suffit alors d'écrire :

$$\begin{aligned} \text{PPCM}(ka; kb) &= \frac{kakb}{\text{PGCD}(ka; kb)} \\ &= \frac{kakb}{k\text{PGCD}(a; b)} \\ &= k\frac{ab}{\text{PGCD}(a; b)} \\ &= k\text{PPCM}(a; b) \end{aligned}$$

□