PGCD et PPCM de deux entiers naturels. Nombres premiers entre eux. Applications.

Pré-requis:
- ◇ $\mathbb{N}$ et ses propriétés.
- ◇ Relation de divisibilité dans $\mathbb{N}$ (c'est une relation d'ordre).
- ◇ Division euclidienne dans $\mathbb{N}$.
- ◇ Groupes et sous-groupes additifs de $\mathbb{Z}$: En particulier, si H est un sous-groupe de $\mathbb{Z}$, il existe un et un seul naturel n tel que $H = n\mathbb{Z}$.
- ◇ Congruences.

0.1 PGCD de deux entiers naturels.

0.1.1 Définition et propriétés.

Soient a et b deux entiers naturels.
L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, il existe donc un et un seul naturel d tel que

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Définition 0.1.1.
Ce nombre d est appelé le plus grand commun diviseur de a et b, noté $\text{pgcd}(a,b)$ ou (a,b) ou encore $a \wedge b$.

La dénomination de plus grand commun diviseur est justifiée par la proposition suivante:

Proposition 0.1.2.

$$d = \max\{c : c|a \text{ et } c|b\}.$$

Démonstration. Soit $x \in \mathbb{N}$,

$$\begin{aligned} x|a \text{ et } x|b &\Leftrightarrow a\mathbb{Z} \subset x\mathbb{Z} \text{ et } b\mathbb{Z} \subset x\mathbb{Z} \\ &\Leftrightarrow d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset x\mathbb{Z} \\ &\Leftrightarrow x|d \end{aligned}$$

De plus, $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$ donc d est un diviseur commun de a et b et tout autre diviseur commun x divise d. ■

Remarque: On vérifie immédiatement que pour tout entier m, $(m,1) = 1$ et $(m,0) = m$.
Exemples:
- ◇ $(0,5) = 5$.
- ◇ $(12,3) = 3$.

◇ $(31, 1) = 1$.

Propriétés 0.1.3.
Pour tous entiers naturels m, n, p, k on a:

1. $(m, n) = (n, m)$ (Commutativité).
2. $(m, (n, p)) = ((m, n), p)$ (associativité).
3. $(km, kn) = k(m, n)$ (homogénéité).
4. $(m, n) = (n, m - kn)$ avec $kn \leq m$.

Démonstration. 4. Soit x un élément de $m\mathbb{Z} + n\mathbb{Z}$, alors il existe $(u, v) \in \mathbb{Z}^2$ tel que $x = mu + nv = mu + nv - knu + knu = (m - kn)u + (v + ku)n$ ainsi $x \in n\mathbb{Z} + (m - kn)\mathbb{Z}$.

On montre de la même manière qu'inversement, $n\mathbb{Z} + (m - kn)\mathbb{Z} \subset n\mathbb{Z} + m\mathbb{Z}$ d'où l'égalité de ces ensembles. ■

Exercice: Sachant que $(a, b) = 1$, calculer

$$(11a + 5b, 13a + 6b).$$

Démonstration.

$$\begin{aligned} (11a + 5b, 13a + 6b) &= (11a + 5b, 2a + b) \\ &= (2a + b, a) \\ &= (a, b) \\ (11a + 5b, 13a + 6b) &= 1. \end{aligned}$$

■

0.1.2 Nombres premiers entre eux.

Définition 0.1.4.
On dit que a et b sont premiers entre eux si $(a, b) = 1$.

Exemples:
◇ 3 et 5
◇ 6 et 35

Théorème 0.1.5.
(Théorème de Bezout)
Soit $(a, b) \in \mathbb{N}^2$, a et b sont premier entre eux si, et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$au + bv = 1.$$

Démonstration. $\Rightarrow$ Si $(a, b) = 1$ alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ et donc il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$au + bv = 1.$$

$\Leftarrow$ Si $au+bv=1$, alors $1 \in a\mathbb{Z}+b\mathbb{Z}$ et donc $a\mathbb{Z}+b\mathbb{Z}=\mathbb{Z}$ d'où

$$(a,b)=1.$$

■

L'identité de Bezout permet d'algèbriser certains problèmes d'arithmétique; C'est ainsi que nous pouvons démontrer que

$$\text{si } (a,b)=(a,c)=1 \text{ alors } (a,bc)=1.$$

Démonstration. Il existe $(u,v) \in \mathbb{Z}^2$ tel que $au+bv=1$ ainsi

$$acu+bcv=c.$$

Il existe aussi $(w,t) \in \mathbb{Z}^2$ tel que $aw+ct=1$. En remplacant c par la valeur précédente, on obtient:

$$aw+acut+bcvt=1$$

c'est-à-dire

$$a(w+cut)+bc(vt)=1.$$

■

Théorème 0.1.6.
(Théorème de Gauss)
Soient a, b, c trois entiers naturels.

$$\text{Si } a|bc \text{ et } (a,b)=1 \text{ alors } a|c.$$

Démonstration. $a|bc$ donc il existe $k \in \mathbb{Z}$ tel que $ka=bc$ et $(a,b)=1$ donc il existe $(u,v) \in \mathbb{Z}^2$ tel que $au+bv=1$ d'où $acu+bcv=c$ et donc

$$a(cu+kv)=c.$$

■

Lemme 0.1.7.
(Lemme d'Euclide)
Soit $(a,b,c) \in \mathbb{N}^3$ tel que $(a,b)=1$.

$$\text{Si } a|c \text{ et } b|c \text{ alors } ab|c.$$

Démonstration. $(a,b)=1$ donc il existe $(u,v) \in \mathbb{Z}^2$ tel que $au+bv=1$. Puisque $a|c$ alors il existe $k \in \mathbb{Z}$ tel que $c=ka$ et $b|c$ donc il existe $h \in \mathbb{Z}$ tel que $c=hb$, or

$$c=auc+bvc=ab(hu+kv).$$

■

0.1.3 Algorithme d'Euclide.

Lemme 0.1.8.
Si $a = bq + r$ avec a, b, q et r dans $\mathbb{N}$, alors

$$(a, b) = (b, r).$$

Démonstration.

$$\begin{aligned}(a,b) &= (bq+r, b)\\ &= (b, bq+r)\\ &= (b, bq+r-bq)\\ (a,b) &= (b,r)\end{aligned}$$

■

Ceci nous permet de construire l'algorithme d'Euclide étendu:
Soit $(a, b) \in \mathbb{N}^2$, on veut trouver $d = (a, b)$ et $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = d$.
On défini:

$$a_{n+1} = b_n,$$
$$b_{n+1} \equiv a_n [b_n],$$
$$q_{n+1} = \left\lfloor \frac{a_n}{b_n} \right\rfloor,$$
$$u_{n+1} = u'_n,$$
$$u'_{n+1} = u_n - q_{n+1} u'_n,$$
$$v_{n+1} = v'_n$$

et

$$v'_{n+1} = v_n - q_{n+1} v'_n.$$

On s'arrête lorsque $b_n = 0$.
On peut le présenter de la manière suivante:

n	a_n	b_n	q_n	u_n	u'_n	v_n	v'_n
0	a	b	$\times$	1	0	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
N	d	0	$\times$	u	$\times$	v	$\times$

Exemple: $a = 80$ et $b = 73$:

n	a_n	b_n	q_n	u_n	u'_n	v_n	v'_n
0	80	73	$\times$	1	0	0	1
1	73	7	1	0	1	1	-1
2	7	3	1	1	-10	-1	11
3	3	1	2	-10	21	11	-23
4	1	0	$\times$	21	$\times$	-23	$\times$

0.2 PPCM de deux entiers naturels.

Soit $(a,b) \in \mathbb{N}^*$, $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, il existe donc un et un seul $m \in \mathbb{N}^*$ tel que

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

Définition 0.2.1.
Ce nombre m est appelé le plus petit commun diviseur de a et de b, noté $\text{ppcm}(a,b)$ ou $a \vee b$.

La dénomination est justifiée par:

Proposition 0.2.2.

$$m = \min\{c > 0 : \ a|c \text{ et } b|c\}.$$

Démonstration. Soit $x \in \mathbb{N}^*$,

$$\begin{aligned} a|x \text{ et } b|x &\Leftrightarrow x\mathbb{Z} \subset a\mathbb{Z} \text{ et } x\mathbb{Z} \subset b\mathbb{Z} \\ &\Leftrightarrow x\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \\ &\Leftrightarrow m|x \end{aligned}$$

De plus, $m\mathbb{Z} \subset a\mathbb{Z}$ et $m\mathbb{Z} \subset b\mathbb{Z}$ donc m est un multiple de a et de b et tout autre multiple de a et de b est multiple de m. ■

Convention: Si $ab = 0$ alors $m = 0$.
Exemples:
- $3 \vee 0 = 0$.
- $13 \vee 3 = 39$.

Propriétés 0.2.3.
Pour tous naturels m, n, p et k, on a:

1. $m \vee n = n \vee m$ (Commutativité).
2. $m \vee (n \vee p) = (m \vee n) \vee p$ (associativité).
3. $(km) \vee (kn) = k(m \vee n)$ (homogénéité).

Théorème 0.2.4.
Soit $(a,b) \in \mathbb{N}^2$, on a:

$$\text{pgcd}(a,b) \times \text{ppcm}(a,b) = ab.$$

Démonstration. Posons $d = \text{pgcd}(a,b)$ alors $a = da_1$ et $b = db_1$ avec $(a_1,b_1) = 1$. Donc

$$\begin{aligned} d \cdot \text{ppcm}(a,b) &= d \cdot \text{ppcm}(da_1, db_1) \\ &= d^2 \cdot \text{ppcm}(a_1,b_1) \\ &= d^2 \cdot a_1 \cdot b_1 \\ &= ab. \end{aligned}$$

■

0.3 Applications.

◇ Les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont tous les éléments de la forme

$$a + n\mathbb{Z} \text{ où } (a, n) = 1.$$

On remarque que se sont aussi les générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Soit $\overline{a} = a + n\mathbb{Z}$ un élément inversible de $\mathbb{Z}/n\mathbb{Z}$, alors il existe $b \in \mathbb{Z}$ tel que $a \cdot b \equiv 1[n]$ donc il existe $k \in \mathbb{Z}$ tel que $ab = 1 + kn$ c'est-à-dire $ab - kn = 1$ et d'après le théorème de Bezout, cela implique que $(a, n) = 1$.
Si $(a, n) = 1$, alors d'après le théorème de Bezout, il existe u, v deux entiers relatifs tels que $au + nv = 1$, c'est-à-dire $au + nv \equiv 1[n]$ d'où $au \equiv 1[n]$. ■

◇ Résolution dans $\mathbb{Z}^2$ de l'équation $ax + by = c$ où a, b et c sont trois entiers donnés:
Une condition nécessaire et suffisante pour que cette équation admette une solution (x_0, y_0) est que $c = k_1 \cdot \text{pgcd}(a, b) = k_1 \cdot \delta$ et alors toute autre solution est de la forme

$$(x_0 + kb', y_0 - ka')$$

où a' et b' sont respectivement le quotient de a et b par δ et k un entier.

◇ Soient m et n deux entiers. Notons $p : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ et $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ les morphismes canoniques et

$$\begin{array}{rccc} \theta : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & x & \longmapsto & (p(x), q(x)) \end{array}$$

Théorème 0.3.1.
(Théorème Chinois)
Si $(m, n) = 1$ alors θ est surjectif et

$$\text{Ker}\theta = mn\mathbb{Z}.$$

En conséquence, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ son isomorphes.

Démonstration. Surjectivité de θ: Soit $a \in \mathbb{Z}/m\mathbb{Z}$ et $b \in \mathbb{Z}/n\mathbb{Z}$. On cherche x dans $\mathbb{Z}$ tel que

$$\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases},$$

or $(m, n) = 1$ donc il existe $(u, v) \in \mathbb{Z}^2$ tel que $mu + nv = 1$. On vérifie immédiatement que $x_0 = bmu + anv$ convient.
Kerθ est l'ensemble de tous les entiers qui sont multiples de m et n. D'après le lemme d'Euclide, puisque $(m, n) = 1$ alors ce sont tous les multiples de mn. ■

Il en résulte que $\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases}$ n'a pas d'autres solutions que les entiers de la forme $x_0 + kmn$ avec $k \in \mathbb{Z}$.

◇ L'indicatrice d'Euler: Il s'agit de la fonction φ qui a tout entier naturel n associe le nombre d'entiers naturels appartenant à $[\![1, n]\!]$ et premier avec n.
Le résultat essentiel sur φ est que si m et n sont des entiers non nuls premiers entre eux alors:

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Il suffit d'observer qu'il y a autant d'éléments inversibles dans $\mathbb{Z}/mn\mathbb{Z}$ que dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (théorème Chinois). Or les éléments inversibles de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont exactement de la forme (α, β) avec α inversible dans $\mathbb{Z}/m\mathbb{Z}$ et β inversible dans $\mathbb{Z}/n\mathbb{Z}$. Et d'après le premier point évoqué dans ce paragraphe, il y a $\varphi(n)$ éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ et $\varphi(m)$ dans $\mathbb{Z}/m\mathbb{Z}$ et $\varphi(mn)$ dans $\mathbb{Z}/mn\mathbb{Z}$. D'où le résultat.