Fiche PGCD et PPCM

1) PGCD :

- Soit δ le PGCD de a et b : $\delta \in \mathbf{N}$ et $\delta = \text{PGCD}(a\,;b) = \text{PGCD}(|a|\,;|b|)$.

- Si $b \mid a$ alors $\text{PGCD}(a\,;b) = |b|$.

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

- Tout diviseur commun de a et b divise leur PGCD δ.

<u>- Algorithme d'Euclide :</u>

$$\left.\begin{array}{l} a = b \times q_1 + r_1 \\ b = r_1 \times q_1 + r_2 \\ r_1 = r_2 \times q_1 + r_3 \\ \text{etc...} \end{array}\right\}$$

Le PGCD est le dernier reste r_n non-nul.

- a et b sont premiers entre eux si : $\text{PGCD}(a\,;b) = 1$.

<u>- Propriété fondamentale du PGCD :</u> (Identité de Bézout)

il existe u et $v \in \mathbf{Z}$ tels que : $au + bv = \text{PGCD}(a\,;b)$. (u et v ne sont pas uniques).

<u>- Théorème de Bézout :</u> il existe u et $v \in \mathbf{Z}$ tels que : $au + bv = 1 \Leftrightarrow \text{PGCD}(a\,;b) = 1$.

(u et v ne sont pas uniques).

<u>- Théorème de Gauss :</u> a, b et $c \in \mathbf{Z}$

$$\left.\begin{array}{l} \text{si } a \mid bc \\ \text{et a et b premiers entre eux} \end{array}\right\} \text{ alors } a \mid c.$$

- Si $\delta = \text{PGCD}(a\,;b)$ alors $a = \delta \times a'$ et $b = \delta \times b'$ avec a' et b' premiers entre eux.

- Si a, b et $k \in \mathbf{Z}$ et $a + kb > 0$ alors : $\text{PGCD}(a\,;b) = \text{PGCD}(a + kb\,;b)$.

d'où le Lemme d'Euclide : $a = bq + r$ alors $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r)$ (car : $r = a - bq$).

<u>- Equation Diophantienne :</u> soit : a, b et $c \in \mathbf{Z}$ et $\delta = \text{PGCD}(a\,;b)$:

$\delta \mid c \Leftrightarrow$ « Il existe au moins une solution dans $\mathbf{Z} \times \mathbf{Z}$ à l'équation : $ax + by = c$ ».

- Si a est premier avec b, alors : $\text{PGCD}(a ; bc) = \text{PGCD}(a ; c)$.

- Si : $\left\{ \begin{array}{l} a \text{ est premier avec } b_1 \\ a \text{ est premier avec } b_2 \end{array} \right\}$ alors a est premier avec $b_1 \times b_2$.

- Si a est premier avec b, alors a^n est premier avec b^n.

- Si : $\left\{ \begin{array}{l} a_1 \text{ est premier avec } a_2 \\ \text{et } a_1 \mid b \text{ et } a_2 \mid b \end{array} \right\}$ alors $a_1 \times a_2 \mid b$.

- Si : $\left\{ \begin{array}{l} p \text{ est premier} \\ p \mid ab \end{array} \right\}$ alors $p \mid a$ ou $p \mid b$.

2) PPCM :

- Soit μ le PPCM de a et b : $\mu \in \mathbf{N}$ et $\mu = \text{PPCM}(a ; b) = \text{PPCM}(|a| ; |b|)$.

- Si $b \mid a$ alors $\text{PPCM}(a ; b) = |a|$.

- $\text{PPCM}(k \times a ; k \times b) = |k| \times \text{PPCM}(a ; b)$.

- Le PPCM μ divise tout multiple commun de a et b.

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

- Si $a \mid c$ et $b \mid d$ alors $\text{PPCM}(a ; b) \mid \text{PPCM}(c ; d)$.