Def: Pour $a \in \mathbb{Z}$, on pose

$$pgcd(a, 0) = |a|$$

et

$$ppcm(a, 0) = 0$$

Théorème de Bezout: Soient $a, b \in \mathbb{Z}$. Alors il existe $u, v \in \mathbb{Z}$ tq $ua + vb = pgcd(a, b)$

Rque: L'algorithme d'Euclide étendu (voir la démonstration) permet de calculer efficacement un couple $(u, v) \in \mathbb{Z}^2$ tq $ua + vb = pgcd(a, b)$

Démonstration:

- Quitte à remplacer u par $-u$ et/ou v par $-v$, on peut supposer $a, b \geq 0$.
- Quitte à échanger a et b, on peut supposer que $a \geq b$. Ecrivons la division euclidienne

$$a = b \cdot q_1 + r_1 \quad (1)$$

Si $r_1 = 0$, alors b divise a et on a

$$pgcd(a, b) = b = \underbrace{0}_{u} \cdot a + \underbrace{1}_{v} \cdot b$$

Si $r_1 \neq 0$, alors on écrit la division euclidienne

$$b = r_1 \cdot q_2 + r_2 \quad (2)$$

Si $r_2 = 0$, alors b est divisible par r_1 et on a:

$$\begin{aligned} pgcd(a,b) &= pgcd(b, r_1) \\ &= r_1 \\ &\underset{(1)}{=} a - q_1 b \\ &= \underbrace{1}_{u} a + \underbrace{(-q_1)}_{v} b \end{aligned}$$

Si $r_2 \neq 0$, alors on écrit la division euclidienne

$$r_1 = r_2 q_3 + r_3 \quad (3)$$

Si $r_3 = 0$, alors r_2 divise r_1 et on a

$$\begin{aligned} pgcd(a,b) &= pgcd(b, r_2) \\ &= pgcd(r_1, r_2) = r_2 \\ &= r_2 \underset{(2)}{=} b - r_1 q_2 \underset{(1)}{=} b - (a - b q_1) \cdot q_2 \\ &= \underbrace{(-1)}_{=u} a + \underbrace{(1 + q_1 q_2)}_{=v} b \end{aligned}$$

Si $r_3 \neq 0$, on effectue la division euclidienne de r_2 par r_3 etc

Ce processus doit s'arrêter à $r_k = 0$ pour un $k \geq 0$ car $r_1, r_2, r_3 \ldots$ forment une suite strictement décroissante d'entiers ≥ 0.

Exemple 21 : Considérons $a = 21$ et $b = 15$

Calculons :

pgcd (21, 15) par l'algo Euclidienne :

$$21 = 1 \cdot 15 + 6 \quad (1)$$
$$15 = 2 \cdot 6 + \boxed{3} \quad (2)$$
$$6 = 2 \cdot 3 + 0 \quad (3)$$

Le dernier reste non nulle est 3

Donc pgcd(21, 15) = 3

Cherchons $u, v \in \mathbb{Z}$ tq $u \cdot 21 + v \cdot 15 = 3$

$$3 \underset{(2)}{=} 15 - 2 \cdot 6$$
$$\underset{(1)}{=} 15 - 2 \times (21 - 1 \cdot 15)$$
$$= \underbrace{(-2)}_{=u} 21 + \underbrace{3}_{=v} \cdot 15$$

Prop 22 : Soient $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tq $ua + vb = 1$

Démonstration : "$\Rightarrow$" Si a et b sont premiers entre eux, on a $\text{pgcd}(a, b) = 1$. Donc il existe $u, v \in \mathbb{Z}$ par le Théorème de Bézout

"$\Leftarrow$" $d = \text{pgcd}(a, b)$ divise a et b. Mais alors il divise aussi $ua + vb = 1$

$\uparrow \mathbb{Z}$ $\quad$ $\uparrow \mathbb{Z}$

Donc $d = 1$ et $\text{pgcd}(a, b) = 1$

⚠ Ce prop n'est pas vraie si $ua + vb = d$ pour un $d > 1$!

Lemme 23 : Soient $a, b \in \mathbb{Z}$ et soit c un diviseur commun de a et b. Alors c **divise** $\text{pgcd}(a, b)$!

Rque : Par def de $\text{pgcd}(a, b)$, on on $|c| \leq \text{pgcd}(a, b)$

L'affirmation du lemme est plus forte !

Démonstration du Lemme : Par le Théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tq $ua + vb = pgcd(a,b)$
Si c divise a et b, il divise aussi
$$ua + vb = pgcd(a,b)$$ ✓

Lemme 24 : Soient $a, b, c \in \mathbb{Z}$. Alors
$$pgcd(ca, cb) = |c| \cdot pgcd(a,b)$$

Démonstration : Exercice ! ✓

Lemme de Gauss (= Lemme 25) : Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{Z}$ un diviseur du produit ab. Si c est premier avec a, alors c divise b

Démonstration : On suppose $pgcd(a,c) = 1$
Alors par le Théorème de Bézout et existe
$$u, v \in \mathbb{Z} \text{ tq } ua + vc = 1$$
Multiplions des deux côtés par b :
$$uab + vcb = b$$
Comme c divise ab, il divise uab. Clairement c divise vcd
Donc c divise $uab + vcb = b$. ✓

Lemme d'Euclide (= Lem26) : Soient $a, b \in \mathbb{Z}$ et p un nombre premier. Si p divise le produit ab, alors p divise a ou p divise b (ou les 2!)

Dem : Supposons que p ne divise pas a. Il faut montrer que p divise b. Comme p est premiers et ne divise pas a, il est premier avec a. Par le lemme de Gauss p divise b ✓

Lemme 28 : Soient $a, b \in \mathbb{Z}$. Alors on a

$$pgcd(a,b)\ ppcm(a,b) = |ab|$$

En particulier, si a et b sont premiers entre eux, on a

$$ppcm(a,b) = |ab|$$

Dém : Soient $d = pgcd(a,b)$ et m un multiple commun de a et b

On pose $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$

Alors a' et b' sont premiers entre eux

Comme m est multiple commun de a et b, il existe $k, l \in \mathbb{Z}$ tq

$m = ka$ et $n = lb$. Or $a = a'd$ et $b = b'd$

Donc
$$m = ka = ka'd$$
$$n = \ell b = \ell b'd$$

En divisant par d, on trouve que $ka' = \ell b'$
Comme a' et b' sont premiers entre eux, par le lemme de Gauss, a' doit diviser ℓ
Disons $\ell = q.a'$ pour un $q \in \mathbb{Z}$
Donc le multiple commun n est forcément de la forme

$$n = \ell b'd = qa'b'd$$

pour un $q \in \mathbb{Z}$. Clairement le plus petit entier positif de cette forme est

$$|a'b'd| = \left|\frac{ab}{d}\right| = \frac{|ab|}{pgcd(a,b)} \checkmark$$

Rque : la dem montre que si m est un multiple commun de a et b alors m est un **multiple** de $ppcm(a,b)$ (et pas seulement $|m| \geq ppcm(a,b)$)

6. Théorème fondamental de l'arithmétique

Théorème fond de l'arithmétique (= Thm 3©):
Soit $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, p_4, p_5, ...
la liste complète des nombres premiers (distincts 2à2)

pour tout entier $N \geq 1$, il existe une unique suite

$m_1, m_2, m_3, \ldots$
d'entiers ≥ 0 tels que

$$N = p_1^{m_1} p_2^{m_2} p_3^{m} \cdots$$

Dém: Existence : Procédons par récurrence sur N. Si $N = 1$, la suite constante $m_i = 0$, $\forall i$

Supposons que $N > 1$

Premier cas: N est premier. Alors

$N = p_k$ pour un k et on pose $m_i = 0$ pour $i \neq k$ et