# Cours de MOMI

## Licence I Math-Info

## Chapitre VI: Arithmétique dans $\mathbb{Z}$

## 1. Divisibilité.

On note $\mathbb{N}_0 = \mathbb{N} \setminus \{0\}$, de même $\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$.

### Définition 1.

*Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$. On dit que $a$ divise $b$ s'il existe $c \in \mathbb{Z}$ tel que: $b = a \times c$.*

*Autrement dit, la fraction rationnelle $\frac{b}{a}$ appartient à $\mathbb{Z}$.*

**Notation.** Lorsque $a$ divise $b$, on écrit $a \mid b$. Dans le cas contraire, on écrit $a \nmid b$

**Langage.** Lorsque $a$ divise $b$, on dit aussi:

- $a$ est un *diviseur* de $b$.
- $b$ est *divisible* par $a$.
- $b$ est un *multiple* de $a$.

**Exemples.** (1) 2 ne divise pas 1 car $\frac{1}{2} = 0,5 \notin \mathbb{Z}$.

(2) Tout entier $a$ divise 0 (car $0 = a \times 0$).

(3) Tout entier $a$ non nul est divisible par $-1, 1, -a, a$.

**Propriétés de la divisibilité.** Soient $a, b, c \in \mathbb{Z}$ avec $a \neq 0$.

(1) $a \mid b \Longrightarrow \forall\, u \in \mathbb{Z},\ a \mid bu$.

(2) $(a \mid b \ \text{ et } \ a \mid c) \Longrightarrow \forall\, u, v \in \mathbb{Z},\ a \mid bu + cv$.

(3) Si $b \neq 0$, $\quad (a \mid b \ \text{ et } \ b \mid c) \Longrightarrow a \mid c$.

(4) Si $a \mid 1$, alors $a = \pm 1$.

(5) Si $b \neq 0$, alors $(a \mid b \ \text{ et } \ b \mid a) \Longrightarrow a = \pm b$.

**Remarques.** Soit $a \in \mathbb{Z}$.

(1) Si $a \neq 0$, alors l'ensemble des diviseurs de $a$ est fini. (0 est le seul entier qui a une infinité de diviseurs).

(2) Si $a \neq 0$, alors l'ensemble $\{a \times c \mid c \in \mathbb{Z}\}$ des multiples de $a$ est infini. (0 est le seul multiple de 0).

## 2. PGCD

**Définition 2.** Soient $a, b \in \mathbb{Z}$. On dit qu'un entier $c \in \mathbb{N}_0$ est le plus grand commun diviseur de $a$ et $b$ si:

(i) $c \mid a \quad \text{et} \quad c \mid b$

(ii) $\forall\, x \in \mathbb{Z}_0,\ (x \mid a \ \text{ et } \ x \mid b) \Longrightarrow x \mid c$.

**Propriété.** Avec les mêmes notations que dans la définition précédente, l'entier $c$ vérifiant les conditions (i) et (ii) est unique.

**Preuve.** Soit $c' \in \mathbb{N}_0$ un autre entier vérifiant les conditions (i) et (ii) de la définition. Montrons que $c = c'$.

- ($c$ vérifie (i) et $c'$ vérifie (ii)) $\Longrightarrow c \mid c'$.
- ($c'$ vérifie (i) et $c$ vérifie (ii)) $\Longrightarrow c' \mid c$.

Ainsi, $c = \pm c'$ par une propriété précédente. Comme $c$ et $c'$ sont positifs, on a $c = c'$.

**Notation.** On note le plus grand commun divisieur de $a$ et $b$ par $\mathrm{pgcd}(a, b)$.

**Remarques.** (1) Si $a \neq 0$ et $a \mid b$, alors $\mathrm{pgcd}(a, b) = |a|$. En particulier, $\mathrm{pgcd}(a, 0) = |a|$.

(2) $\mathrm{pgcd}(0, 0)$ n'existe pas.

*Pour la suite, on considère* $\mathrm{pgcd}(a, b)$ *pour* $a \neq 0$ *et* $b \neq 0$.

Un résultat fondamental concernant le pgcd est le théorème suivant:

**Théorème 1.** *Soient* $a, b \in \mathbb{Z}_0$. *Alors:*

- *Le* $\mathrm{pgcd}(a, b)$ *existe.*
- *Il existe* $m, n \in \mathbb{Z}$ *tels que:* $am + bn = \mathrm{pgcd}(a, b)$.

**Preuve.** Soit l'ensemble $M = \{ax + by \mid x, y \in \mathbb{Z}\} \subset \mathbb{Z}$.

On a $M \cap \mathbb{N}_0 \neq \emptyset$, en effet:

Si $a > 0$, alors $a = a \times 1 + b \times 0 \in M \cap \mathbb{N}_0$.

Si $a < 0$, alors $-a = a \times (-1) + b \times 0 \in M \cap \mathbb{N}_0$.

Par l'axiome du plus petit élément, l'ensemble $M \cap \mathbb{N}_0$ admet un plus petit élément, qu'on note $c$.

**Affirmation.** $\mathrm{pgcd}(a, b) = c$.

(1) $c \in M \cap \mathbb{N}_0 \Longrightarrow c \in M \Longrightarrow \exists\, m, n \in \mathbb{Z}$ tels que $c = am + bn$.

Montrons que $c$ vérifie les deux conditions de la définition du pgcd :

(2) (Pour la condition (ii)): Si $x \in \mathbb{Z}_0$ divise $a$ et $b$, alors $x$ divise $am + bn = c$.

(3) (Pour la condition (i)): On va montrer que $c$ divise $a$. La même preuve s'applique pour $b$.

Par la division Euclidienne de $a$ par $c$, il existe $q, r \in \mathbb{Z}$ tels que: $a = c \times q + r$ et $0 \leq r < c$. On va montrer que $r = 0$. En effet:

$c \in M \Longrightarrow c \times q \in M \Longrightarrow a - c \times q \in M \Longrightarrow r \in M \Longrightarrow$
$r \in M \cap \mathbb{N}$.

Si $r \neq 0$, alors on aurait $r \in M \cap \mathbb{N}_0$. Comme $r < c$, alors $c$ ne serait pas le plus petit élément de $M \cap \mathbb{N}_0$, ce qui est absurde. D'où, $r = 0$, ce qui signifie que $c$ divise $a$. □

**Remarques.** (À faire en exercice) Soient $a, b \in \mathbb{Z}_0$.

(1) Les diviseurs communs de $a$ et $b$ sont exactement les diviseurs de $\mathrm{pgcd}(a, b)$.

(2) Le $\mathrm{pgcd}(a, b)$ est le plus grand élément de l'ensemble $\{d \in \mathbb{N}_0 \mid d \text{ divise } a \text{ et } b\}$ pour l'ordre habituel $\leq$.

**Définition 3.**

*Soient $a, b \in \mathbb{Z}_0$. On dit que $a$ et $b$ sont premiers entre eux si $\mathrm{pgcd}(a, b) = 1$.*

**Corollaire 1.** (Théorème de Bézout)
*Soient $a, b \in \mathbb{Z}_0$ tels que $\mathrm{pgcd}(a, b) = 1$. Alors, il existe $m, n \in \mathbb{Z}$ tels que $am + bn = 1$.*

**Preuve.** C'est une conséquence du théorème 1. □

Réciproquement, on a:

**Lemme 1.** *Soient $a, b \in \mathbb{Z}_0$. S'il existe $m, n \in \mathbb{Z}$ tel que $am + bn = 1$, alors $\mathrm{pgcd}(a, b) = 1$.*

**Preuve.** Comme $\mathrm{pgcd}(a, b)$ divise $a$ et $b$, alors $\mathrm{pgcd}(a, b)$ divise $am + bn = 1$. Puisque $\mathrm{pgcd}(a, b) > 0$, alors $\mathrm{pgcd}(a, b) = 1$. □

**Corollaire 2.** *Soient $a, b \in \mathbb{Z}_0$. Si $\mathrm{pgcd}(a, b) = d$, alors $\mathrm{pgcd}(\frac{a}{d}, \frac{b}{d}) = 1$.*

**Preuve.** Puisque $\mathrm{pgcd}(a, b) = d$, il existe $m, n \in \mathbb{Z}$ tel que $am + bn = d$ (Théorème 1). Ainsi, $(\frac{a}{d})m + (\frac{b}{d})n = 1$. Par le lemme précédent, on a $\mathrm{pgcd}(\frac{a}{d}, \frac{b}{d}) = 1$.

**Corollaire 3.** (Théorème de Gauss)
*Soient $a, b, c \in \mathbb{Z}_0$ tels que $a \mid bc$ et $\mathrm{pgcd}(a, b) = 1$. Alors, $a \mid c$.*

**Preuve.** Puisque $\mathrm{pgcd}(a, b) = 1$, il existe $m, n \in \mathbb{Z}$ tels que $am + bn = 1$ (Théorème de Bézout). Ainsi, $acm + bcn = c$. Comme $a \mid bc$, alors $a \mid bcn$. Par conséquent, $a \mid amc + bnc = c$. □

## 3. Nombres premiers

### Définition 4.

*Soit $p \in \mathbb{N}$ avec $p \neq 0$ et $p \neq 1$. On dit que $p$ est un nombre premier si ses seuls diviseurs sont $-1$, $1$, $-p$ et $p$.* (c'est-à-dire, 1 et $p$ sont les seuls diviseurs positifs de $p$.)

**Exemple.** (1) $2, 3, 5, 7$ sont des nombres premiers.

(2) 4 n'est pas un nombre premier car $\pm 1$, $\pm 2$ et $\pm 4$ sont les diviseurs de 4.

**Remarques.**

(1) Soient $p$ et $q$ deux nombres premiers. Si $p$ divise $q$, alors $p = q$. En effet, $p$ divise $q$ implique que $p \in \{\pm 1, \pm q\}$ car $q$ est premier. Comme $p > 1$, alors $p = q$.

(2) Soient $a \in \mathbb{Z}_0$ et $p$ un nombre premier. Si $p$ ne divise pas $a$, alors $\mathrm{pgcd}(a, p) = 1$.

Posons $d = \mathrm{pgcd}(a, p)$. Puisque $d \mid p$ et $d > 0$, alors $d \in \{1, p\}$. Comme $d$ divise $a$ mais $p$ ne divise pas $a$, alors $d = 1$.

(3) (Exo) Soit $p \in \mathbb{N}$ avec $p \neq 0$ et $p \neq 1$. On a les équivalences suivantes:

$$p \text{ n'est pas premier} \iff \exists\, u \in \mathbb{N} \text{ tel que } 1 < u < p \text{ et } u \mid p$$

**Proposition 1.** (Lemme d'Euclide)

*Soient $p$ un nombre premier et $a, b \in \mathbb{Z}$. Alors,*
$p \mid ab \implies (p \mid a \text{ ou } p \mid b)$.

**Preuve.** Supposons $p \mid ab$. Montrons $p \mid a$ ou $p \mid b$.

– Si $p$ divise $a$, alors c'est bon.

– Si $p$ ne divise pas $a$, alors $\mathrm{pgcd}(a, p) = 1$ (par le remarque précédente). Puisque $p$ divise $ab$, on déduit par le théorème de Gauss que $p$ divise $b$. □

**Crible d'Eratosthène.** Le crible d'Eratosthène consiste à déterminer les nombres premiers inférieurs à un entier donné $N$.

Le procédé est comme suit:

(1) On écrit tous les entiers $1, 2, \cdots, N$.

(2) On barre 1.

(3) On itère: "on entoure le suivant et on barre ses multiples", jusqu'à avoir barré ou entouré tous les entiers écrits.

**Résultat:** Les entiers $\leq N$ qui sont entourés sont des nombres premiers.

**Exemple.** Donner les nombres premiers $\leq 40$.

On écrit les entiers naturels $1, 2, 3, \cdots, 40$, puis on applique le procédé ci-dessus pour avoir:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ~~1~~ | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| ~~21~~ | ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ |
| 31 | ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ |

**Conclusion.** Les nombres premiers inférieurs à 40 sont: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.

**Théorème 2.** (Théorème fondamental de l'arithmétique)

*Soit $a \in \mathbb{N}$ avec $a \geq 2$. Alors:*

*(1) Il existe des nombres premiers $p_1 > \cdots > p_r$ et des entiers $m_1, \cdots, m_r \in \mathbb{N}_0$ tels que:*

$$a = p_1^{m_1} \times \cdots \times p_r^{m_r}.$$

*(2) La décomposition dans (1) est unique, c'est-à-dire, si on a une autre décomposition $a = q_1^{n_1} \times \cdots \times q_s^{n_s}$ où $q_1 > \cdots > q_s$ sont des nombres premiers et $n_1, \cdots, n_s \in \mathbb{N}_0$, alors:*

$$\begin{cases} r = s \\ p_1 = q_1, \cdots, p_r = q_r \\ m_1 = n_1, \cdots, m_r = n_r. \end{cases}$$

**Preuve.** On procède en deux étapes.

**1. Existence de la décomposition.** On va procéder par récurrence sur $a$ en utilisant le deuxième principe.

Pour tout $a \geq 2$ un entier, soit $P(a)$ la propriété: *Il existe des nombres premiers* $p_1, \cdots, p_r$ *deux à deux distincts, et des entiers* $m_1, \cdots, m_r \in \mathbb{N}_0$ *tels que:* $a = p_1^{m_1} \times \cdots \times p_r^{m_r}$.

(i) Initialisation: $P(2)$ est vraie car $2 = 2^1$ et 2 est premier (on prend $p_1 = 2$ et $n_1 = 1$).

(ii) Hérédité: Supposons $a > 2$ et que $P(u)$ soit vraie pour tout $u$ vérifiant $2 \leq u < a$. Montrons que $P(a)$ est vraie.

• Si $a$ est premier, alors $P(a)$ est vraie car $a = a^1$ et $a$ est premier (on prend $p_1 = a$ et $n_1 = 1$).

• Si $a$ n'est pas premier, alors il existe deux entiers $u$ et $v$ tels que: $a = u \times v$, $1 < u < a$ et $1 < v < a$. Puisque $P(u)$ et $P(v)$ sont vraies, on déduit que $P(a)$ est vraie.

**2. Unicité de la décomposition.** On va procéder par récurrence sur $a$ en utilisant le deuxième principe.

Pour tout entier $a \geq 2$, soit $Q(a)$ la propriété: *La décomposition de a en facteurs premiers est unique comme énoncé dans l'assertion (2) du théorème.*

(i) Initialisation: La décomposition $2 = 2^1$ est unique puisque tout premier divisant 2 est égal à 2. Ainsi, $Q(2)$ est vraie.

(ii) Hérédité: Supposons $a > 2$ et que $Q(u)$ soit vraie pour tout entier $u$ vérifiant $2 \leq u < a$. Montrons que $Q(a)$ est vraie. Supposons qu'on ait:

$$a = p_1^{m_1} \times \cdots \times p_r^{m_r} = q_1^{n_1} \times \cdots \times q_s^{n_s} \quad (*)$$

où $p_1 > \cdots > p_r$ et $q_1 > \cdots > q_s$ sont des nombres premiers, et $m_1, \cdots, m_r, n_1, \cdots, n_s \in \mathbb{N}_0$.

Notre but est de montrer que $r = s$, et $p_i = q_i$, $m_i = n_i$ pour tout $1 \leq i \leq r$.

On a

$$\begin{aligned} p_1 \mid a &\Longrightarrow p_1 \mid q_1^{n_1} \times \cdots \times q_s^{n_s} \\ &\Longrightarrow \exists\, 1 \leq i \leq s \text{ tel que } p_1 \mid q_i \quad \text{(Lemme d'Euclide)} \\ &\Longrightarrow \exists\, 1 \leq i \leq s \text{ tel que } p_1 = q_i \text{ (car } p_1 \text{ et } q_i \text{ sont premiers)} \\ &\Longrightarrow p_1 \leq q_1 \quad (\text{car } q_i \leq q_1). \end{aligned}$$

De même, puisque $q_1 \mid a$ on déduit que $q_1 \leq p_1$. Ainsi, $p_1 = q_1$. Par conséquent, l'égalité $(*)$ ci-dessus implique

$$\frac{a}{p_1} = p_1^{m_1-1} \times p_2^{m_2} \times \cdots \times p_r^{m_r} = p_1^{n_1-1} \times q_2^{n_2} \times \cdots \times q_s^{n_s} \quad (**)$$

• Si $m_1 = 1$, alors nécessairement $n_1 = 1$. Comme $\frac{a}{p_1} < a$, on applique l'hypothèse de récurrence à $(**)$ pour avoir:

$$\begin{cases} r - 1 = s - 1 \Longrightarrow r = s \\ p_2 = q_2,\ m_2 = n_2 \\ \quad \vdots \\ p_r = q_r,\ m_r = n_r. \end{cases}$$

• Si $m_1 > 1$, alors nécessairement $n_1 > 1$. Comme $\frac{a}{p_1} < a$, on applique l'hypothèse de récurrence à $(**)$ pour avoir:

$$\begin{cases} r = s \\ m_1 - 1 = n_1 - 1 \implies m_1 = n_1 \\ p_2 = q_2,\ m_2 = n_2 \\ \quad \vdots \\ p_r = q_r,\ m_r = n_r. \end{cases}$$

Ainsi, le théorème est démontré. □

**Remarque.** Lorsque $a \in \mathbb{Z}$ avec $a \leq -2$, alors il existe des nombres premiers $p_1 > \cdots > p_r$ et des entiers $m_1, \cdots, m_r \in \mathbb{N}_0$ uniques tels que:

$$a = -p_1^{m_1} \times \cdots \times p_r^{m_r}.$$

**Corollaire 4.**

*Soit $a = p_1^{m_1} \times \cdots \times p_r^{m_r}$ avec $p_1, \cdots, p_r$ des nombres premiers deux à deux distincts, et $m_1, \cdots, m_r \in \mathbb{N}_0$. Alors, le nombre de diviseurs positifs de $a$ est*

$$(m_1 + 1) \times \cdots \times (m_r + 1).$$

**Preuve.** Soit $u \in \mathbb{N}_0$ un diviseur de $a$. Par l'unicité de la décomposition en facteurs premiers, on a $u = p_1^{n_1} \times \cdots \times p_r^{n_r}$ avec $0 \leq n_i \leq m_i$ pour tout $i = 1, \cdots, r$. Ainsi, il y a $(m_1 + 1) \times \cdots \times (m_r + 1)$ entiers naturels diviseurs de $a$. □

**Exemples.** (1) Soient $p$ un nombre premier et $n \in \mathbb{N}_0$. Les diviseurs positifs de $p^n$ sont les entiers $p^k$ avec $0 \leq k \leq n$:

$$1 = p^0, p = p^1, \cdots, p^n$$

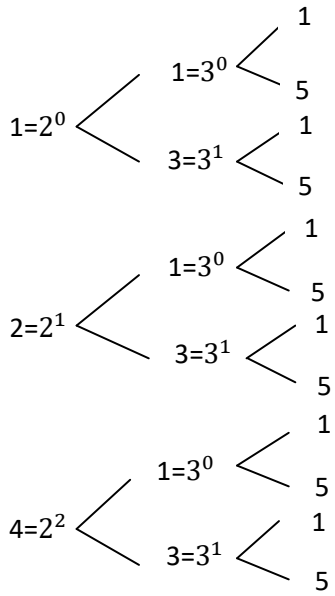
.

(2) Donner les diviseurs positifs de 60.

– On commence par décomposer 60 en facteurs premiers:
$60 = 2 \times 30 = 2 \times 2 \times 15 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3^1 \times 5^1$.

– Ensuite on introduit l'arbre des diviseurs:

On place les diviseurs de $2^2$ dans une colonne, ensuite on ramifie dans une deuxième colonne chacun de ces diviseurs selon les diviseurs de $3^1$, et ainsi de suite.




On trouve les diviseurs de 60 en parcourant toutes les branches:

$$1 \times 1 \times 1 = 1$$
$$1 \times 1 \times 5 = 5$$
$$1 \times 3 \times 1 = 3$$
$$\vdots$$
$$4 \times 3 \times 5 = 60.$$

Les diviseurs de 60 sont: $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$, qui sont en nombre de $(2+1) \times (1+1) \times (1+1) = 12$.

**Proposition 2.** *Il y a une infinité de nombres premiers.*

**Preuve.** Supposons que l'ensemble des nombres premiers soit fini dont les éléments sont $p_1, \cdots, p_n$. Soit $N = p_1 \times p_2 \times \cdots \times p_n + 1$. Puisque $N > 1$, il existe $p$ un nombre premier qui divise $N$. Ainsi, $p = p_i$ pour un certain $1 \leq i \leq n$. Comme $p = p_i$ divise $N - 1$ et $N$, alors $p = p_i$ divise $N - (N - 1) = 1$, ce qui est absurde. □

## 4. Procédés de calcul de pgcd

### 1. Méthode utilisant l'algorithme d'Euclide

La méthode est basée sur le lemme suivant:

**Lemme 2.** *Soient $a, b \in \mathbb{Z}_0$ et $q, r \in \mathbb{Z}$ tels que: $a = b \times q + r$. On a:*

*(1) Si $r = 0$, alors $\mathrm{pgcd}(a, b) = |b|$.*

*(2) Si $r \neq 0$, alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.*
*($q$ et $r$ ne sont pas nécessairement le quotient et le reste de la division Euclidienne de $a$ par $b$.)*

**Preuve.** Voir TD (Exercice 6.11). □

**Algorithme:** *Soient* $a, b \in \mathbb{Z}_0$. *Donner* $\mathrm{pgcd}(a, b)$.

On va se servir du lemme précédent pour trouver le $\mathrm{pgcd}(a, b)$. Sans perdre de généralités, on peut supposer $a \geq b > 0$ (car $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(-a, b) = \mathrm{pgcd}(a, -b) = \mathrm{pgcd}(-a, -b)$.)

On effectue la D. E. de $a$ par $b$:

$a = bq_1 + r_1$ avec $0 \leq r_1 < b$.

- Si $r_1 = 0$, alors $\mathrm{pgcd}(a, b) = b$ par le lemme précédent.
- Si $r_1 \neq 0$, alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1)$ $\quad (\star)$.

On effectue la D. E. de $b$ par $r_1$:

$b = r_1 q_2 + r_2$ avec $0 \leq r_2 < r_1$.

- Si $r_2 = 0$, alors $\mathrm{pgcd}(b, r_1) = r_1$. Ainsi, $\mathrm{pgcd}(a, b) = r_1$.
- Si $r_2 \neq 0$, alors $\mathrm{pgcd}(b, r_1) = \mathrm{pgcd}(r_1, r_2)$. Ainsi, par $(\star)$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_1, r_2)$.

On effectue la D. E. de $r_1$ par $r_2$:

$r_1 = r_2 q_3 + r_3$ avec $0 \leq r_3 < r_2$. On discute suivant que $r_3$ est nul ou non.

Ainsi de suite, en continuant les divisions Euclidiennes successives, on construit une suite de restes vérifiant $0 \leq \cdots r_3 < r_2 < r_1 < b$. On finira par avoir un reste nul. Soit $r_n$ le plus petit reste non nul. On récapitule alors:

$$
\begin{array}{ll}
a = bq_1 + r_1 & pgcd(a,b) = pgcd(b,r_1) \\
b = r_1 q_2 + r_2 & pgcd(b,r_1) = pgcd(r_1,r_2) \\
r_1 = r_2\, q_3 + r_3 & pgcd(r_1,r_2) = pgcd(r_2,r_3) \\
\vdots & \vdots \\
\vdots & \vdots \\
r_{n-2} = r_{n-1}\, q_n + r_n & pgcd(r_{n-2},r_{n-1}) = pgcd(r_{n-1},r_n) \\
r_{n-1} = r_n\, q_{n+1} + 0 & pgcd(r_{n-1},\, r_n) = r_n
\end{array}
$$

En conclusion, lorsque $a \geq b > 0$ et $b$ ne divise pas $a$, alors $\mathrm{pgcd}(a,b)$ est le dernier reste non nul des divisions Euclidiennes successives de l'algorithme ci-dessus.

**Exercice.** Soient $a = 125$ et $b = 35$.

(1) Calculer le $\mathrm{pgcd}(a, b)$.

(2) Trouver deux entiers $m, n \in \mathbb{Z}$ tels que:

$$125m + 35n = \mathrm{pgcd}(125, 35).$$

(1) Puisque 35 ne divise pas 125, on effectue les divisions Euclidiennes successives jusqu'à avoir un reste nul:

(R1): $125 = 35 \times 3 + 20 \longrightarrow \operatorname{pgcd}(125, 35) = \operatorname{pgcd}(35, 20).$

(R2): $35 = 20 \times 1 + 15 \longrightarrow \operatorname{pgcd}(35, 20) = \operatorname{pgcd}(20, 15).$

(R3): $20 = 15 \times 1 + 5 \longrightarrow \operatorname{pgcd}(20, 15) = \operatorname{pgcd}(15, 5).$

(R4): $15 = 5 \times 3 + 0 \longrightarrow \operatorname{pgcd}(15, 5) = 5.$

Donc, par l'algorithme donné précédemment, $\operatorname{pgcd}(125, 35) = 5$.

(2) Pour trouver deux entiers $m, n \in \mathbb{Z}$ tels que $125m + 35n = 5$, on remonte les divisions précédentes de la ligne (R3) donnant le $\mathrm{pgcd}$ à la ligne (R1) comme suit:

$$\begin{aligned} 5 &= 20 - 15 && \text{(d'après } (R3)) \\ &= 20 - (35 - 20) && \text{(d'après } (R2)) \\ &= 20 \times 2 - 35 \\ &= (125 - 35 \times 3) \times 2 - 35 && \text{(d'après } (R1)) \\ &= 125 \times 2 + 35 \times (-7). \end{aligned}$$

Donc, on peut prendre $m = 2$ et $n = -7$.

Le couple $(2, -7)$ n'est pas unique. Par exmple, le couple $(9, -32)$ convient aussi: $125 \times 9 + 35 \times (-32) = 5$.

## 2. Méthode utilisant les soustractions successives.

**Lemme.**

*Soient* $a, b \in \mathbb{N}_0$ *avec* $a \geq b$. *Alors,* $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a - b, b)$.

**Preuve.** À faire en exercice. □

**Exercice.** Retrouver $\mathrm{pgcd}(125, 35)$ en utilisant cette méthode.

## 3. Méthode utilisant la décomposition en facteurs premiers

Cette méthode est basée sur la proposition suivante:

### Proposition 3.

*Soient $a, b \in \mathbb{N}_0$. Supposons que $a = p_1^{m_1} \times \cdots \times p_r^{m_r}$ et $b = p_1^{n_1} \times \cdots \times p_r^{n_r}$, où $p_1, \cdots, p_r$ sont des nombres premiers deux à deux distincts, et $m_1, \cdots, m_r, n_1, \cdots, n_r \in \mathbb{N}$. Alors*

$$\mathrm{pgcd}(a, b) = p_1^{\min(m_1, n_1)} \times \cdots \times p_r^{\min(m_r, n_r)}$$

*où $\min(m_i, n_i)$ est le minimum des entiers $m_i, n_i$ pour tout $1 \leq i \leq r$.*

**Preuve.** À faire en exercice (utiliser l'unicité de la décomposition en facteurs premiers, et le fait que $p_i^{\min(m_i, n_i)}$ divise $p_i^{m_i}$ et $p_i^{n_i}$ pour tout $1 \leq i \leq r$. □

**Exemple.** Soient $a = 125$ et $b = 35$. Donner $\mathrm{pgcd}(125, 35)$.

On a $125 = 5^3$ et $35 = 5 \times 7$. Ce qu'on écrit

$$\begin{cases} 125 = 5^3 \times 7^0 \\ 35 = 5^1 \times 7^1. \end{cases}$$

Donc, on a

$$\begin{aligned} \mathrm{pgcd}(125, 35) &= 5^{\min(3,1)} \times 7^{\min(0,1)} \\ &= 5^1 \times 7^0 = 5. \end{aligned}$$

## 5. PPCM

**Définition 5.** *Soient $a, b \in \mathbb{Z}_0$. On dit qu'un entier $c \in \mathbb{N}_0$ est le plus petit commun multiple de $a$ et $b$ si:*

(i) $a \mid c \quad et \quad b \mid c$

(ii) $\forall x \in \mathbb{Z}_0, (a \mid x \ \ et \ \ b \mid x) \implies c \mid x.$

**Propriété.** L'entier $c$ vérifiant les conditions (i) and (ii) de la définition précédente est unique. Pour cela, on procède comme pour l'unicité du $\mathrm{pgcd}$.

**Notation.** On note le plus petit commun multiple de $a$ et $b$ par $\mathrm{ppcm}(a, b)$.

**Remarque.** Pour tout $a \in \mathbb{Z}$, le $\mathrm{ppcm}(a, 0)$ n'existe pas. Donc, on ne considère que le $\mathrm{ppcm}(a, b)$ avec $a \neq 0$ et $b \neq 0$.

**Proposition 3.** *Soient $a, b \in \mathbb{Z}_0$. Le $\mathrm{ppcm}(a, b)$ existe et vérifie*

$$\mathrm{ppcm}(a, b) = \frac{|a| \times |b|}{\mathrm{pgcd}(a, b)}.$$

**Preuve.** Posons $d = \mathrm{pgcd}(a, b)$. On peut supposer $a > 0$ et $b > 0$. On a $\mathrm{pgcd}(\frac{a}{d}, \frac{b}{d}) = 1$ (Corollaire 2).

**But:** Montrer que $\frac{a \times b}{d}$ vérifie les deux conditions du $\mathrm{ppcm}$.

(i) Puisque $\frac{a \times b}{d} = a \times \frac{b}{d} = \frac{a}{d} \times b$, alors $\frac{a \times b}{d}$ est un multiple commun de $a$ est $b$.

(ii) Soit $\alpha \in \mathbb{Z}$ multiple de $a$ et $b$. Montrons que $\frac{a \times b}{d}$ divise $\alpha$.

Il existe $u, v \in \mathbb{Z}$ tels que:

$$\alpha = a \times u = b \times v.$$

Ainsi, $\frac{a}{d} \times u = \frac{b}{d} \times v$. Comme $\mathrm{pgcd}(\frac{a}{d}, \frac{b}{d}) = 1$, on obtient par le théorème de Gauss que $\frac{a}{d}$ divise $v$. Soit $\beta \in \mathbb{Z}$ tel que $v = \frac{a}{d} \times \beta$. Alors, on obtient

$$\alpha = \frac{a \times b}{d} \times \beta.$$

D'où $\frac{a \times b}{d}$ divise $\alpha$. □

**Remarque.** *Soient $a, b \in \mathbb{Z}_0$. Alors:*

*(1) Les multiples communs à $a$ et $b$ sont exactement les multiples de $\mathrm{ppcm}(a, b)$.*

*(2) $\mathrm{ppcm}(a, b)$ est le plus petit entier de $\{x \in \mathbb{N}_0 \mid x$ multiple de $a$ et $b\}$ au sens de l'ordre habituel $\leq$.*

Le ppcm se calucle aussi en utilisant les décompositions en facteurs premiers:

**Proposition 4.**

*Soient $a, b \in \mathbb{N}_0$. Supposons que $a = p_1^{m_1} \times \cdots \times p_r^{m_r}$ et $b = p_1^{n_1} \times \cdots \times p_r^{n_r}$, où $p_1, \cdots, p_r$ sont des nombres premiers deux à deux distincts, et $m_1, \cdots, m_r, n_1, \cdots, n_r \in \mathbb{N}$. Alors*

$$\mathrm{ppcm}(a, b) = p_1^{\max(m_1, n_1)} \times \cdots \times p_r^{\max(m_r, n_r)}$$

*où $\max(m_i, n_i)$ est le maximum des entiers $m_i, n_i$ pour tout $1 \leq i \leq r$.*

**Preuve.** Pour tout $i \in \{1, \cdots, r\}$, on a

$$m_i + n_i = \min(m_i, n_i) + \max(m_i, n_i).$$

Ainsi

$$\begin{aligned}
a \times b &= p_1^{m_1} \times \cdots \times p_r^{m_r} \times p_1^{n_1} \times \cdots \times p_r^{n_r} \\
&= p_1^{m_1+n_1} \times \cdots \times p_r^{m_r+n_r} \\
&= p_1^{\min(m_1,n_1)+\max(m_1,n_1)} \times \cdots \times p_r^{\min(m_r,n_r)+\max(m_r,n_r)} \\
&= p_1^{\min(m_1,n_1)} \times \cdots \times p_r^{\min(m_r,n_r)} \times p_1^{\max(m_1,n_1)} \times \cdots \times p_r^{\max(m_r,n_r)} \\
&= \operatorname{pgcd}(a, b) \times p_1^{\max(m_1,n_1)} \times \cdots \times p_r^{\max(m_r,n_r)}.
\end{aligned}$$

Puisque $\operatorname{ppcm}(a, b) = \frac{a \times b}{\operatorname{pgcd}(a,b)}$, on déduit que

$\operatorname{ppcm}(a, b) = p_1^{\max(m_1,n_1)} \times \cdots \times p_r^{\max(m_r,n_r)}$. □

**Exemple.** Soient $a = 125$ et $b = 35$.

(1) On a déjà vu que $\mathrm{pgcd}(a, b) = 5$. Donc

$$\mathrm{ppcm}(a, b) = \frac{125 \times 35}{5} = 875.$$

(2) Utilisation de la décomposition en facteurs premiers:

$$125 = 5^3 \text{ et } 35 = 5 \times 7.$$

Donc

$$125 = 5^3 \times 7^0 \text{ et } 35 = 5^1 \times 7^1.$$

Ainsi, $\mathrm{ppcm}(a, b) = 5^{\max(3,1)} \times 7^{\max(0,1)} = 5^3 \times 7^1 = 875.$