

Chapitre 3 : Arithmétique

I Division d'entiers

1.1 Multiples et diviseurs d'un entier

Définition 1

Soit $(a, b) \in \mathbb{Z}^2$. On dit que a divise b si et seulement si il existe $c \in \mathbb{Z}$ tel que $b = ac$. On note $a|b$.
On dit aussi dans ce cas que a est un diviseur de b ou que b est un multiple de a .

Remarque : Soit $n \in \mathbb{Z}$.

- n est pair ssi $2|n$,
- n est impair ssi $2|n - 1$.

Proposition 1

1. $\forall a \in \mathbb{Z}, a|a$
2. $\forall a, b \in \mathbb{Z}, (a|b \text{ et } b|a) \Leftrightarrow |a| = |b|$
3. $\forall a, b, c \in \mathbb{Z}, (a|b \text{ et } b|c) \Rightarrow a|c$

Preuve. Soient $a, b, c \in \mathbb{Z}$.

1. $a = a.1$ et $1 \in \mathbb{Z}$ donc $a|a$.
2. Supposons $a|b$ et $b|a$. Alors, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $a = k_2 b$. Donc $a = k_1 k_2 a$.
Si $a = 0$, alors $b = 0$ donc $|a| = |b|$.
Sinon, $k_1 k_2 = 1$ donc $k_1 = k_2 = 1$ ou $k_1 = k_2 = -1$, donc $a = \pm b$, ainsi $|a| = |b|$.
Supposons $|a| = |b|$ alors $a = \pm b$ et $b = \pm a$ donc $a|b$ et $b|a$.
3. Supposons que $a|b$ et $b|c$. Alors, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $c = k_2 b$. Ainsi, $c = (k_2 k_1) a$ avec $k_1 k_2 \in \mathbb{Z}$.
Ainsi, a divise c .

□

Proposition 2

1. $\forall a, b, c \in \mathbb{Z}, (a|b \text{ et } a|c) \Rightarrow (\forall (p, q) \in \mathbb{Z}^2, a|(pb + qc))$
2. $\forall a, b, c, d \in \mathbb{Z}, (a|b \text{ et } c|d) \Rightarrow ac|bd$
3. $\forall a, b \in \mathbb{Z}, a|b \Rightarrow (\forall n \in \mathbb{N}, a^n|b^n)$

Remarque : Ecrire uniquement une implication ne signifie pas que la réciproque est fausse. La réciproque du troisième point est vraie mais n'est pas intéressante.

Preuve. Soient $a, b, c, d \in \mathbb{Z}$.

1. Supposons que $a|b$ et $a|c$. Alors il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $c = k_2 a$.
Soient $p, q \in \mathbb{Z}$. On a : $pb + qc = (pk_1 + qk_2)a$ avec $pk_1 + qk_2 \in \mathbb{Z}$.
Donc $a|(pb + qc)$.
2. Supposons que $a|b$ et $c|d$. Alors il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $d = k_2 c$.
D'où par produit : $bd = (k_1 a)(k_2 c) = (k_1 k_2)ac$ avec $k_1 k_2 \in \mathbb{Z}$ et donc $ac|bd$.
3. Supposons que $a|b$. Alors il existe $k_1 \in \mathbb{Z}$ tel que $b = k_1 a$.
Donc $a^n = k_1^n a^n$ avec $k_1^n \in \mathbb{Z}$, et donc $a^n|b^n$.

□

Proposition 3

Soient $a, b \in \mathbb{Z}$. Supposons que $b \neq 0$ et $a|b$, alors :

$$|a| \leq |b|.$$

Preuve. Comme $a|b$, il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Comme $b \neq 0$ alors $k \neq 0$ et comme $k \in \mathbb{Z}$, on a donc $|k| \geq 1$.

Ainsi, comme $|a| \geq 0 : |b| = |k|.|a| \geq |a|$.

□

1.2 Division euclidienne

Théorème 1

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

On dit que q est le **quotient** et r le **reste** dans la **division euclidienne** de a par b .

Remarque :

- $\mathbb{Z} \times \mathbb{N}$ est le produit cartésien de $\mathbb{Z}$ et $\mathbb{N}$, on a : $(q, r) \in \mathbb{Z} \times \mathbb{N} \Leftrightarrow (q \in \mathbb{Z} \text{ et } r \in \mathbb{N})$.
On utilise cette notation afin d'avoir un objet (le couple) qui soit unique.
- Si $a \in \mathbb{N}$, alors $q \in \mathbb{N}$.

Preuve.

- Existence : Soit $b \in \mathbb{N}^*$.
 - Pour $a = 0$, posons $q = r = 0$. On a $a = bq + r$ et $0 \leq r < b$ donc (q, r) convient.
 - Soit $a \in \mathbb{N}$. Supposons qu'il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r$.
Alors $a + 1 = bq + r + 1$.
 - * Si $r + 1 < b$. Posons $q' = q$ et $r' = r + 1$. On a $a = bq' + r'$ et $0 \leq r' < b$ donc (q', r') convient.
 - * Si $r + 1 \geq b$, alors, comme $r < b$, on a $r = b - 1$ donc $a + 1 = bq + b = b(q + 1)$. Posons $q' = q + 1$ et $r' = 0$. On a $a = bq' + r'$ et $0 \leq r' < b$ donc (q', r') convient.
 - * Dans tous les cas, il existe un couple (q', r') qui convient.
 - Donc, par récurrence,

$$\forall a \in \mathbb{N}, \exists (q, r) \in \mathbb{Z} \times \mathbb{N}, (a = bq + r \quad \text{et} \quad 0 \leq r < b).$$

- Soit $a \in \mathbb{Z}^-$ alors $-a \in \mathbb{N}$ donc il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $(-a = bq + r \quad \text{et} \quad 0 \leq r < b)$.
On a donc $a = -bq - r = b(-q - 1) + b - r$ et $0 < b - r \leq b$.
 - * Si $b - r < b$. Posons $q' = -q - 1$ et $r' = b - r$. On a $a = bq' + r'$ et $0 \leq r' < b$ donc (q', r') convient.
 - * Si $b - r \geq b$, alors, comme $0 \leq r$, on a $r = 0$ donc $a = -bq$. Posons $q' = -q$ et $r' = 0$. On a $a = bq' + r'$ et $0 \leq r' < b$ donc (q', r') convient.
 - * Dans tous les cas, il existe un couple (q', r') qui convient.
- En conclusion :

$$\forall a \in \mathbb{Z}, \exists (q, r) \in \mathbb{Z} \times \mathbb{N}, (a = bq + r \quad \text{et} \quad 0 \leq r < b).$$

- Unicité : Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Supposons qu'il existe $(q_1, r_1), (q_2, r_2) \in \mathbb{Z} \times \mathbb{N}$ tels que

$$a = bq_1 + r_1 = bq_2 + r_2 \quad \text{et} \quad 0 \leq r_1 < b, 0 \leq r_2 < b.$$

Alors $0 = b(q_1 - q_2) + r_1 - r_2$ donc :

$$r_1 - r_2 = b(q_2 - q_1).$$

Or : $-b < r_1 - r_2 < b$ donc $-b < b(q_2 - q_1) < b$ et comme $b > 0$:

$$-1 < q_2 - q_1 < 1.$$

Or $q_2 - q_1 \in \mathbb{Z}$ donc $q_2 - q_1 = 0$ et donc $r_1 - r_2 = b \cdot 0 = 0$. Ainsi :

$$q_1 = q_2 \text{ et } r_1 = r_2.$$

D'où l'unicité. □

⇒ **Exemple 1** : Soit $n \in \mathbb{N}^*$. On suppose que le reste de la division euclidienne de n par 7 est 2. Que valent les restes des divisions euclidiennes de n^2 et n^3 par 7 ?

⇒ **Exemple 2** : Soient $n, m \in \mathbb{N}^*$. On suppose que le reste de la division euclidienne de n par m est 8 et que le reste de la division euclidienne de $2n$ par m est 5. Que vaut m ?

II pgcd

2.1 Définition

Définition 2

Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Le PGCD de a et b est le plus grand des diviseurs strictement positifs communs à a et b , il est noté $\text{pgcd}(a, b)$ ou $a \wedge b$:

$$\text{pgcd}(a, b) = a \wedge b = \max\{d \in \mathbb{N}^*, d|a \text{ et } d|b\}.$$

Proposition 4

Soient $a, b \in \mathbb{N}^*$.

$$\text{pgcd}(a, b) = a \Leftrightarrow a|b.$$

Preuve. • Si $\text{pgcd}(a, b) = a$ comme, par définition, $\text{pgcd}(a, b)|b$, on a $a|b$.
 • Si $a|b$, alors $a|a$ et $a|b$, de plus, si $n|a$ et $n|b$ alors $n \leq a$ donc : $\text{pgcd}(a, b) = a$.

□

2.2 Algorithme d'Euclide**Proposition 5**

Soient $a, b \in \mathbb{N}^*$. Soit r le reste de la division de a par b .
 Les entiers a et b ont les mêmes diviseurs que b et r et on a donc :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

Preuve. Soit q le quotient de la division euclidienne de a par b . On a : $a = bq + r$.

- Soit $d \in \mathbb{N}^*$ tel que $d|a$ et $d|b$ alors $d|a - bq$ donc $d|r$.
 Ainsi les diviseurs de a et b divisent b et r .
- Soit $d \in \mathbb{N}^*$ tel que $d|b$ et $d|r$ alors $d|bq + r$ donc $d|a$.
 Ainsi les diviseurs de b et r divisent a et b .
- Donc a et b ont les mêmes diviseurs que b et r .

□

Algorithme 1 (Algorithme d'Euclide)

Soient $a, b \in \mathbb{N}^*$.

- On pose $r_0 = a$ et $r_1 = b$. On a alors $\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1)$.
- Soit $k \in \mathbb{N}$, on suppose $r_k > 0$ et $r_{k+1} > 0$ construits tels que $\text{pgcd}(a, b) = \text{pgcd}(r_k, r_{k+1})$.
 Soit r_{k+2} le reste de la division euclidienne de r_k par r_{k+1} .
 On a donc $0 \leq r_{k+2} < r_{k+1}$ et :

$$\text{pgcd}(r_{k+1}, r_{k+2}) = \text{pgcd}(r_k, r_{k+1}) = \text{pgcd}(a, b).$$

De plus, si $r_{k+2} = 0$, alors $r_{k+1}|r_k$ donc $\text{pgcd}(r_k, r_{k+1}) = r_{k+1}$, ainsi :

$$\text{pgcd}(a, b) = r_{k+1}.$$

- La suite $(r_k)_{k \geq 1}$ est une suite strictement décroissante d'entiers naturels et est donc finie. Ainsi l'algorithme s'arrête et le pgcd est le dernier reste non nul.

⇔ Exemple 3 :

- Calculer $\text{pgcd}(45, 30)$.
- Calculer $\text{pgcd}(360, 105)$.

2.3 Propriétés**Proposition 6**

Soient $a, b, d \in \mathbb{N}^*$. On a :

$$(d|a \text{ et } d|b) \Leftrightarrow d|\text{pgcd}(a, b).$$

Preuve.

- Supposons que $d|\text{pgcd}(a, b)$. Comme $\text{pgcd}(a, b)|a$ et $\text{pgcd}(a, b)|b$, alors $d|a$ et $d|b$.
- Supposons que $d|a$ et $d|b$. Soit $(r_k)_{k \in \llbracket 0, N \rrbracket}$ la suite définie par l'algorithme d'Euclide avec $r_N = \text{pgcd}(a, b)$.
 Montrons que : $\forall k \in \llbracket 0, N \rrbracket, d|r_k$.
 - Pour $k = 0$, $r_k = a$ donc $d|r_k$.
 - Pour $k = 1$, $r_k = b$ donc $d|r_k$.
 - Soit $k \in \llbracket 0, N - 2 \rrbracket$. Supposons que $d|r_k$ et $d|r_{k+1}$.

- * Si $r_{k+2} = 0$, alors $d|r_{k+2}$.
- * Si $r_{k+2} \neq 0$, alors r_{k+2} est le reste de la division euclidienne de r_k par r_{k+1} donc, comme d divise r_k et r_{k+1} , alors d divise r_{k+2} .
- * Dans tous les cas : $d|r_{k+2}$.
- Donc, par récurrence finie double : $\forall k \in \llbracket 0, N \rrbracket \quad d|r_k$.
- En particulier, comme $r_N = \text{pgcd}(a, b)$, on a : $d|\text{pgcd}(a, b)$.

□

Proposition 7 : Homogénéité du PGCD

$$\forall a, b, c \in \mathbb{N}^*, \text{pgcd}(ca, cb) = c \cdot \text{pgcd}(a, b)$$

Preuve. Posons $d = \text{pgcd}(a, b)$ et $e = \text{pgcd}(ca, cb)$.

- On a $d|a$ et $d|b$, donc $cd|ca$ et $cd|cb$. Ainsi : $cd|\text{pgcd}(ca, cb) = e$.
Donc il existe $k \in \mathbb{N}^*$ tel que : $e = kcd$.
- $e|ca$ donc $kcd|ca$, ainsi $kd|a$. De même, $kd|b$ donc $kd|\text{pgcd}(a, b) = d$.
Ainsi $k|1$ donc $k = 1$.
- On a donc :

$$\text{pgcd}(ca, cb) = e = kcd = cd = c \cdot \text{pgcd}(a, b).$$

□

⇔ **Exemple 4 :** Soient $a, b, c \in \mathbb{N}^*$ tels que $\text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$. Montrer que :

$$\text{pgcd}(a, bc) = 1.$$

Corollaire 1

$$\mathbb{Q} = \left\{ \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N}^*, \text{pgcd}(p, q) = 1 \right\}.$$

Preuve.

- Par définition : $\left\{ \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N}^*, \text{pgcd}(p, q) = 1 \right\} \subset \mathbb{Q}$.
- Soit $r \in \mathbb{Q}$. Il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $r = \frac{p}{q}$.
Posons $d = \text{pgcd}(p, q)$. Il existe $p' \in \mathbb{Z}$ et $q' \in \mathbb{N}^*$ tels que : $p = dp'$ et $q = dq'$. On a alors :

$$r = \frac{dp'}{dq'} = \frac{p'}{q'} \text{ et } \text{pgcd}(p', q') = \frac{\text{pgcd}(p, q)}{d} = 1.$$

Donc :

$$\mathbb{Q} \subset \left\{ \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N}^*, \text{pgcd}(p, q) = 1 \right\}.$$

- Ainsi :

$$\mathbb{Q} = \left\{ \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N}^*, \text{pgcd}(p, q) = 1 \right\}.$$

□

III ppcm

3.1 Définition

Définition 3

Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Le PPCM de a et b est le plus petit des multiples strictement positifs communs à a et b , il est noté $\text{ppcm}(a, b)$ ou $a \vee b$:

$$\text{ppcm}(a, b) = a \vee b = \min\{m \in \mathbb{N}^*, a|m \text{ et } b|m\}.$$

Proposition 8

Soient $a, b \in \mathbb{N}^*$.

$$\text{ppcm}(a, b) = a \Leftrightarrow b|a.$$

Preuve.

- Si $\text{ppcm}(a, b) = a$ comme, par définition, $b|\text{ppcm}(a, b)$, on a $b|a$.
- Si $b|a$, alors $a|a$ et $b|a$, de plus, si $a|m$ et $b|m$ alors $a \leq m$ donc : $\text{ppcm}(a, b) = a$.

□

3.2 Propriétés

Proposition 9

Soient $a, b, m \in \mathbb{N}^*$. On a :

$$(a|m \text{ et } b|m) \iff \text{ppcm}(a, b)|m.$$

Preuve.

- Supposons $\text{ppcm}(a, b)|m$. Comme $a|\text{ppcm}(a, b)$ et $b|\text{ppcm}(a, b)$, on a :

$$a|m \text{ et } b|m.$$

- Supposons $a|m$ et $b|m$. Soient q (resp. r) le quotient (resp. le reste) de la division euclidienne de m par $\text{ppcm}(a, b)$.
On a : $m = q \cdot \text{ppcm}(a, b) + r$ donc $r = m - q \cdot \text{ppcm}(a, b)$. De plus $a|m$ et $a|\text{ppcm}(a, b)$ donc $a|r$ et de même $b|r$. Ainsi r est un multiple commun de a et b .
De plus, $0 \leq r < \text{ppcm}(a, b)$ donc, par définition du ppcm , $r = 0$. Ainsi :

$$\text{ppcm}(a, b)|m.$$

□

Proposition 10

Soient $a, b \in \mathbb{N}^*$, on a :

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

Preuve. Posons $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$. Alors, il existe $\alpha, \beta, \gamma, \delta \in \mathbb{N}$ tels que :

$$a = \alpha d, b = \beta d, m = \gamma a, m = \delta b.$$

- $\alpha \beta d = \beta a = \alpha b$ donc $a|\alpha \beta d$ et $b|\alpha \beta d$, ainsi $m|\alpha \beta d$. Donc, il existe $k \in \mathbb{N}$ tel que : $mk = \alpha \beta d$.
- $mk = \gamma ak = a\beta$ donc $\beta = \gamma k$, donc $k|\beta$.
- $mk = \delta bk = b\alpha$ donc $\alpha = \delta k$, donc $k|\alpha$.
- Ainsi $k|\text{pgcd}(\alpha, \beta)$. Or $\text{pgcd}(a, b) = d = \text{pgcd}(\alpha d, \beta d) = d \cdot \text{pgcd}(\alpha, \beta)$. Donc : $\text{pgcd}(\alpha, \beta) = 1$, ainsi $k = 1$.
- D'où $m = \alpha \beta d$, ainsi $md = \alpha d \beta d = ab$.

□

⇔ **Exemple 5 :** Soit $n \in \mathbb{N}^*$. Calculer $\text{pgcd}(n, 2n+1)$ et $\text{ppcm}(n, 2n+1)$.

IV Nombres premiers

4.1 Ensemble des nombres premiers

Définition 4

Un nombre $p \in \mathbb{N}$ est dit premier ssi $p \geq 2$ et :

$$\forall d \in \mathbb{N}^*, d|p \Rightarrow (d = 1 \text{ ou } d = p),$$

c'est-à-dire les seuls diviseurs de p sont 1 et lui-même.

Proposition 11

Tout nombre entier $n \geq 2$ possède au moins un diviseur premier.

Preuve. On le montre par récurrence forte sur $n \geq 2$.

- Pour $n = 2$, la propriété est vraie puisque 2 est premier.
- Soit $n \geq 2$, supposons que tout nombre premier $k \in \llbracket 2, n \rrbracket$ admet au moins un diviseur premier.
 - Si $n+1$ est premier, le résultat est établi.
 - Sinon il existe $d \in \mathbb{N}$ tels que $d|(n+1)$ avec $2 \leq d \leq n$. On applique l'hypothèse de récurrence à d : il existe donc p premier tel que $p|d$. Ainsi comme $d|(n+1)$, on a $p|(n+1)$.Ceci prouve la propriété au rang $n+1$.
- Ainsi, tout entier naturel $n \geq 2$ admet au moins un diviseur premier.

□

Proposition 12

L'ensemble des nombres premiers est infini.

Preuve.

Supposons que l'ensemble des nombres premiers soit fini. Notons $\{p_1, \dots, p_N\}$ l'ensemble des nombres premiers, avec $N \in \mathbb{N}^*$. Posons $n = p_1 \prod p_N + 1$. Alors $n \geq 2$ donc n admet un diviseur premier. Ainsi, il existe $k \in \llbracket 1, N \rrbracket$ tel que $p_k | n$.

Or $p_k | p_1 \prod p_N$ donc $p_k | n - p_1 \prod p_N$ c'est-à-dire $p_k | 1$ donc $p_k = 1$ ce qui est absurde.

Donc l'ensemble des nombres premiers est infini. $\square$

4.2 Décomposition en facteurs premiers**Théorème 2**

Tout entier supérieur ou égal à 2 admet une décomposition en produit de nombres premiers, unique à l'ordre des facteurs près. Autrement dit, si $n \in \mathbb{N}$ et $n \geq 2$, alors il existe $r \in \mathbb{N}^*$, des nombres premiers deux à deux distincts $p_1, \dots, p_r$, et des entiers naturels non nuls $\alpha_1, \dots, \alpha_r$ tels que $n = p_1^{\alpha_1} \dots p_r^{\alpha_r} = \prod_{i=1}^r p_i^{\alpha_i}$.

⇨ **Exemple 6 :** Soient $a, b \in \mathbb{N}^*$. On suppose que $\text{pgcd}(a, b) = 1$. Montrer que :

$$\forall n, m \in \mathbb{N}^*, \text{pgcd}(a^n, b^m) = 1.$$

Proposition 13

Soient $a, b \in \mathbb{N} \setminus \{0, 1\}$ tels que $a = p_1^{\alpha_1} \dots p_r^{\alpha_r} = \prod_{i=1}^r p_i^{\alpha_i}$ et $b = p_1^{\beta_1} \dots p_r^{\beta_r} = \prod_{i=1}^r p_i^{\beta_i}$ où $p_1, p_2, \dots, p_r$ sont des nombres premiers distincts deux à deux, et $\alpha_1, \dots, \alpha_r \in \mathbb{N}$, $\beta_1, \dots, \beta_r \in \mathbb{N}$ (éventuellement nuls pour tenir compte d'un nombre premier qui pourrait ne diviser qu'un seul des deux entiers a ou b). Alors :

$$\begin{aligned} \text{pgcd}(a, b) &= p_1^{\min(\alpha_1, \beta_1)} \dots p_r^{\min(\alpha_r, \beta_r)} = \prod_{i=1}^r p_i^{\min(\alpha_i, \beta_i)} \\ \text{ppcm}(a, b) &= p_1^{\max(\alpha_1, \beta_1)} \dots p_r^{\max(\alpha_r, \beta_r)} = \prod_{i=1}^r p_i^{\max(\alpha_i, \beta_i)} \end{aligned}$$

Preuve.

- Posons $d = \prod_{i=1}^r p_i^{\min(\alpha_i, \beta_i)}$.
 - Pour tout $i \in \llbracket 1, r \rrbracket$, $\min(\alpha_i, \beta_i) \leq \alpha_i$. Donc : $a = \prod_{i=1}^r p_i^{\alpha_i - \min(\alpha_i, \beta_i) + \min(\alpha_i, \beta_i)} = d \cdot \prod_{i=1}^r p_i^{\alpha_i - \min(\alpha_i, \beta_i)}$.
Ainsi, $d | a$ et, de même, $d | b$.
 - Posons $\alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$. On a $\alpha, \beta \in \mathbb{N}^*$ et : $\alpha = \prod_{i=1}^r p_i^{\alpha_i - \min(\alpha_i, \beta_i)}$ et $\beta = \prod_{i=1}^r p_i^{\beta_i - \min(\alpha_i, \beta_i)}$.
Soit $i \in \llbracket 1, r \rrbracket$, on a : $\alpha_i - \min(\alpha_i, \beta_i) = 0$ ou $\beta_i - \min(\alpha_i, \beta_i) = 0$ ainsi $p_i \nmid \alpha$ ou $p_i \nmid \beta$.
Ainsi α et β n'ont pas de facteur premier commun donc $\text{pgcd}(\alpha, \beta) = 1$.
 - Donc :

$$\text{pgcd}(a, b) = \text{pgcd}(d\alpha, d\beta) = d \text{pgcd}(\alpha, \beta) = d.$$

- On a : $\text{pgcd}(a, b) \text{ppcm}(a, b) = ab = \prod_{i=1}^r p_i^{\alpha_i + \beta_i}$.

$$\text{D'où } \text{ppcm}(a, b) = \prod_{i=1}^r p_i^{\min(\alpha_i, \beta_i)} = \prod_{i=1}^r p_i^{\alpha_i + \beta_i}.$$

$$\text{Ainsi, } \text{ppcm}(a, b) = \prod_{i=1}^r p_i^{\alpha_i + \beta_i - \min(\alpha_i, \beta_i)}.$$

Soit $i \in \llbracket 1, r \rrbracket$, on a : $\alpha_i + \beta_i - \min(\alpha_i, \beta_i) = \max(\alpha_i, \beta_i)$. En effet :

- Si $\alpha_i \geq \beta_i$. Alors, $\min(\alpha_i, \beta_i) = \beta_i$ et $\max(\alpha_i, \beta_i) = \alpha_i$.
Ainsi, $\alpha_i + \beta_i - \min(\alpha_i, \beta_i) = \alpha_i + \beta_i - \beta_i = \alpha_i = \max(\alpha_i, \beta_i)$.
- Si $\alpha_i < \beta_i$. Alors, $\min(\alpha_i, \beta_i) = \alpha_i$ et $\max(\alpha_i, \beta_i) = \beta_i$.
Ainsi, $\alpha_i + \beta_i - \min(\alpha_i, \beta_i) = \alpha_i + \beta_i - \alpha_i = \beta_i = \max(\alpha_i, \beta_i)$.

$\square$

⇨ **Exemple 7 :** Déterminer les entiers naturels non nuls b tels que $\text{ppcm}(28, b) = 140$.