III

Arithmétique, rudiments

Contenu

I Rudiments d'arithmétique dans $\mathbb{N}$

I.1 Divisibilité

Définition I (Divisibilité dans $\mathbb{Z}$) : Soient a et b des entiers relatifs.

On dit que a *divise* b, noté $a|b$, s'il existe un entier relatif k tel que $b = ka$.

On dit alors que :

- a est *un diviseur* de b. On note $\mathscr{D}(b)$ leur ensemble.
- b est *un multiple* de a. On note $a\mathbb{Z}$ leur ensemble.

Comme a et $-a$ ont les mêmes diviseurs dans $\mathbb{Z}$, on se restreindra le plus souvent, sans le dire, à l'étude de la divisibilité dans $\mathbb{N}$. C'est le parti pris par le programme donc, à partir de maintenant, sauf remarques intéressantes, on ne considèrera plus que la divisibilité dans $\mathbb{N}$.

Exemples I :

- $3|12$ et $5\not|12$.
- L'ensemble des diviseurs de 12 est $\mathscr{D}(12) = \{1, 2, 3, 4, 6, 12\}$.
- Tous les nombres divisent 0 *i.e.* 0 est multiple de tout entier : $\mathscr{D}(0) = \mathbb{N}$.
- 0 n'est diviseur d'aucun entier (non nul) : $0\mathbb{Z} = \{0\}$.
- $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$.
- Un multiple de 2 est aussi appelé un *nombre pair*. Ceux qui ne le sont pas sont appelés *nombre impair*. L'ensemble des nombres pairs est noté $2\mathbb{N}$. (*cf* le corollaire (2.1) pour les nombres impairs)

Exercice I : On appelle *nombre parfait* tout nombre égal à la somme de ses diviseurs stricts.

Par exemple $\mathscr{D}(6) = \{1, 2, 3, 6\}$ et $6 = 1 + 2 + 3$, donc 6 est parfait.

Montrer que 28 est parfait.

Méthode 1 :
Pour les problèmes donnés sous forme additive, on essaiera de se ramener à une forme multiplicative du type $A \times B = C$, où on connaît les diviseurs de C.

Exercice 2 : Déterminer les couples $(x\,;y)$ d'entiers naturels qui vérifient $x^2 = y^2 + 21$.

Proposition 1 (Relation de divisibilité) :

1. $\forall\, a \in \mathbb{N}$, $\quad a|a$ et $1|a$. ($\ll\, a|b\,\gg$ est réflexive)
2. $\forall\, a, b \in \mathbb{N}$, $\quad \begin{cases} a|b \\ b|a \end{cases} \implies a = b.$ ($\ll\, a|b\,\gg$ est antisymétrique sur $\mathbb{N}$)
3. $\forall\, a, b, c \in \mathbb{N}$, $\quad \begin{cases} a|b \\ b|c \end{cases} \implies a|c.$ ($\ll\, a|b\,\gg$ est transitive)

La relation « $a \mathscr{R} b \iff a|b$ », réflexive, antisymétrique et transitive est appelée une relation d'ordre sur $\mathbb{N}$. C'est un ordre non total.

ATTENTION

Sur $\mathbb{Z}$, la relation $a|b$ est seulement réflexive et transitive.

On perd l'antisymétrie :

$$\forall\, a, b \in \mathbb{Z}, \quad \begin{cases} a|b \\ b|a \end{cases} \iff |a| = |b|\,.$$

Proposition 2 (Compatibilité) :

1. $\forall\, a, b, c \in \mathbb{N}$, $\forall\, m, n \in \mathbb{N}$, $\quad \begin{cases} a|b \\ a|c \end{cases} \implies a|mb + nc$ (« $a|b$ » est compatible avec les combinaisons linéaires entières)
2. $\forall\, a, b, a', b', c \in \mathbb{N}$, $\quad \begin{cases} a|b \\ a'|b' \end{cases} \implies a|bc$ et $aa'|bb'$ (« $a|b$ » est compatible avec le produit)

   En particulier, $\forall\, a, b, n \in \mathbb{N}$, $\quad a|b \implies a^n|b^n$

ATTENTION

- $\begin{cases} a|c \\ b|c \end{cases} \not\implies ab|c$:
  $2|12$ et $4|12$ mais $2 \times 4 = 8 \not| 12$.
- $a|bc \not\implies a|b$:
  $10|210 = 14 \times 15$ mais $10 \not| 14$. (et $10 \not| 15$)

Exemple 2 : Si $a \in \mathbb{Z}$ divise $3n + 2$ et $n - 3$ alors $a|11$.
En effet, a divise alors $(3n + 2) - 3(n - 3) = 11$.

Exercice 3 : Trouver les entiers n pour lesquels $\dfrac{n + 15}{n + 2}$ est entier.

D'une manière générale,

Méthode 2 :
Pour résoudre un problème du type $f(n)|g(n)$, on se ramène à un problème du type $h(n)|A$ où A est un entier indépendant de n.[1]

- On pourra développer une fraction en éléments simples comme à l'exercice (3).
- On pourra aussi utiliser la propriété (1.3) pour rendre le dividende indépendant de n.

Corollaire 2.1 : Les nombres impairs sont exactement les entiers de la forme $2p+1$ où $p \in \mathbb{Z}$.

Exercice 4 : Montrer que pour tout entier impair n, n^2-1 est multiple de 8.

I.2 Division euclidienne

Théorème 3 : Pour tout $(a,b) \in \mathbb{N} \times \mathbb{N}^*$, il existe un unique couple $(q,r) \in \mathbb{N}^2$ tel que :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b. \tag{III.1}$$

Lorsqu'on a obtenu cette écriture, on dit qu'on a effectué la *division euclidienne* de a par b.

Rappel ! (Vocabulaire) :

- q s'appelle le *quotient*,
- r s'appelle le *reste*,
- a s'appelle le *dividende*
- et b s'appelle le *diviseur*.

Combien de fois peut-on soustraire 7 de 83 et combien reste-t-il ?

Réponse : autant de fois que l'on veut et il reste 76 à chaque fois.

Exercice 5 : Montrer que tout entier n non divisible par 5 a un carré de la forme $5p+1$ ou $5p-1$.

Proposition 4 : Soient a et b deux entiers naturels avec b non nul.

$b|a \iff$ le reste dans la division euclidienne de a par b est nul.

Exercice 6 : Le 1er mai 2022 tombait un dimanche. Quel jour tombe le 1er mai 2023 ?

[1]. En d'autres termes, on isole la variable.

I.3 Nombres premiers

Définition 2 : Un entier naturel est dit *premier* lorsqu'il admet exactement deux diviseurs (1 et lui-même).

On note $\mathbb{P}$ l'ensemble des nombres premiers.

Exemples 3 :

- $0 \notin \mathbb{P}$: il admet une infinité de diviseurs.
- $1 \notin \mathbb{P}$: il n'admet qu'un seul diviseur.
- $2 \in \mathbb{P}$: c'est le plus petit nombre premier, et il est pair. C'est le seul nombre premier pair.
- $2^{82\,589\,933} - 1$, qui comporte près de 25 millions de chiffres en écriture décimale est le plus grand nombre premier actuellement connu.

  Il a été découvert le 7 décembre 2018 par le *Gimps* (Great Internet Mersenne Prime search)
- Une curiosité et un jeu des siècles passés, le polynôme $P(n) = n^2 - n + 41$ associé à Euler donne des nombres premiers pour n prenant les valeurs 0 à 39 mais $P(40) = 1681 = 41^2$!

Un mathématicien, un physicien, un informaticien et un littéraire sont devant un problème : montrer que tous les nombres impairs sont premiers.

Le mathématicien dit : « 3 est premier, 5 est premier, 7 est premier, 9 n'est pas premier, donc ça ne marche pas ».

Le physicien dit : « 3 est premier, 5 est premier, 7 est premier, donc en première approximation, ça marche ».

L'informaticien dit : « 3 est premier, 5 est premier, 7 est premier, 9 n'est pas premier, 9 n'est pas premier, 9 n'est pas premier, 9 n'est pas premier, …».

Le littéraire dit : « C'est quoi, un nombre premier ? ».

Théorème 5 (Critère d'arrêt) :

- Tout entier naturel n, $n \geqslant 2$, admet un diviseur premier.
- Si n n'est pas premier, alors il admet un diviseur premier p tel que :

$$2 \leqslant p \leqslant \sqrt{n}.$$

Exemple 4 (Comment montrer que 109 est un nombre premier) :

- On a $10 < \sqrt{109} < 11$.

  On teste donc tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.
- Des règles de divisibilité, on déduit que 109 n'est divisible ni par 2, ni par 3, ni par 5.
- Soit, on se rappelle le critère de divisibilité par 7, soit on effectue la division euclidienne de 109 par 7, on obtient :

$$109 = 7 \times 15 + 4 \implies 109 \text{ n'est pas divisible par } 7.$$

- Conclusion : comme 109 n'est pas divisible par 2, 3, 5, et 7, il est premier.

Théorème 6 : L'ensemble des nombres premiers est infini.

Crible d'Ératosthène

Pour dresser la liste des nombres premiers entre 2 et 150, la méthode du crible d'Ératosthène [2] consiste à :

1. Écrire la liste des nombres entiers de 2 à 100.
2. Éliminer successivement les multiples propres de 2, de 3, ..., puis ceux de p, où p est le premier nombre non encore éliminé [3], etc...

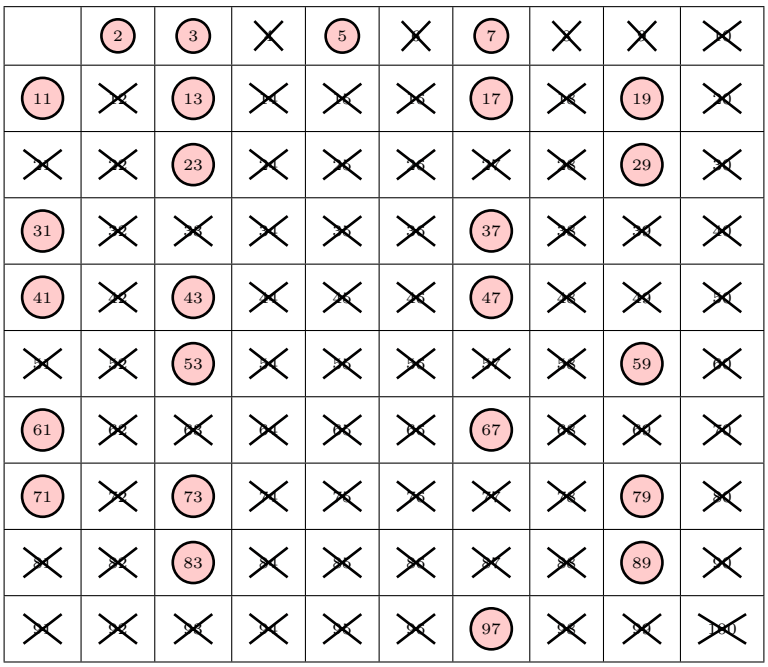

Figure III.1 – Les nombres premiers inférieurs à 100.

Les entiers barrés sont les entiers non premiers entre 2 et 100. Les entiers restant (en rouge) sont donc les nombres premiers inférieur à 100.

Un peu d'histoire : *En mathématiques, et plus précisément en théorie analytique des nombres, le théorème des nombres premiers, démontré indépendamment par Hadamard et La Vallée Poussin en 1896, est un résultat concernant la distribution asymptotique des nombres premiers.*

[1]. Connue d'Euclide himself !

[2]. **Ératosthène**, mathématicien, géographe, astronome et poète grec serait né en 276 avant J.C. à Cyrène (aujourd'hui en Libye). Il étudie quelques années à Athènes puis devient l'élève du poète grec Callimaque qui dirige la grande Bibliothèque d'Alexandrie.

Ayant ainsi accès à toutes les connaissances de l'époque, Ératosthène se lance dans différents travaux qui le rendront célèbre :

- En observant la position du Soleil à Syène (Assouan aujourd'hui) puis à Alexandrie au moment du solstice d'été, il parvient à déduire avec une bonne précision la circonférence de la Terre.
- Inventeur du mot géographie, il étudie les différentes zones climatiques, les altitudes des montagnes, la répartition des continents et des océans.
- Passionné d'astronomie, il réalise un catalogue de plus de 600 étoiles et 44 constellations. Il parvient aussi à calculer l'obliquité de l'écliptique (l'inclinaison de l'axe de la Terre par rapport à son axe de rotation autour du Soleil) avec une bonne précision.
- En mathématiques il invente un procédé (le crible d'Ératosthène) permettant de trouver les nombres premiers.

Devenu aveugle, Eratosthène se laisse mourir de faim en l'an 194 av. J-C.

[3]. donc premier

```python
def eratosthene(n):
    L = [ i for i in range(2,n+1) ]
    P = [ ]

    while len(L) != 0:
        P.append(L[0])
        i = L[0]
        for k in L:
            if k % i == 0:
                del(L[L.index(k)])

    return P
```

Figure III.2 – Crible d'Ératothène

Théorème 7 : La fonction π qui à un réel x associe $\mathcal{P}(x)$ le nombre de nombres premiers inférieurs ou égaux à x, est équivalente lorsque x tend vers $+\infty$, au quotient de x par son logarithme népérien :

$$\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}.$$

Il y aurait encore beaucoup beaucoup à dire mais je m'arrête là et j'encourage les curieux à faire des recherches à partir des mots clés « théorème des nombres premiers ».

Exercice 7 : Soit $n \in \mathbb{N}$. On suppose $n \geqslant 2$.

Montrer qu'il n'existe aucun nombre premier entre $n!+2$ et $n!+n$.

Théorème 8 (Théorème fondamental de l'arithmétique) : Tout entier n supérieur à 2 admet une et une seule (à l'ordre des facteurs près) décomposition en facteurs premiers.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \text{ avec } p_i \in \mathbb{P} \text{ deux à deux distincts et } \alpha_i \in \mathbb{N}^*.$$

On l'appelle *décomposition primaire* de n et les exposants α_i s'appellent les valuations associées aux nombres premiers p_i.

Exemple 5 : Décomposons 16 758 en produit de facteurs premiers :

16758	2
8379	3
2793	3
931	7
133	7
19	19
1	

Pour décomposer un entier, on effectue des divisions successives par des nombres premiers dans l'ordre croissant.

On obtient :

$$16758 = 2 \times 3^2 \times 7^2 \times 19.$$

Exemples 6 :

- $510510 = 1001 \times 510 = (7 \times 11 \times 13) \times (2 \times 3 \times 5 \times 17) = (2)(3)(5)(7)(11)(13)(17)$
- $80000 = 8 \times 10^4 = (2)^7(5)^4$.

Corollaire 8.1 : Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\beta_p}$.

Alors :

$$a|b \iff \forall\, p \in \mathbb{P},\ \alpha_p \leqslant \beta_p.$$

Corollaire 8.2 : $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ admet $\prod_{i=1}^{k} (1+\alpha_i)$ diviseurs.

Exercice 8 : Trouver le nombre de diviseurs de 120 et déterminer tous ces diviseurs.

II PGCD ET PPCM

II.1 PGCD

Définition 3 : Soient a et b deux entiers naturels non nuls.
On appelle *PGCD de a et b*, noté $\text{pgcd}\,(a\,;b)$ ou $a \wedge b$, le plus grand diviseur commun à a et b.

Remarques :

— Comme 1 divise tous les nombres entiers $\text{pgcd}\,(a\,;b) \geqslant 1$.

De même, il est évident que si a et b sont non nuls, $\text{pgcd}\,(a\,;b) \leqslant a$ et $\text{pgcd}\,(a\,;b) \leqslant b$.

— $\text{pgcd}\,(a\,;b) = \text{pgcd}\,(b\,;a)$

— Si $a > 0$, $\text{pgcd}\,(a\,;0) = a$. Par convention, on posera $\text{pgcd}\,(0\,;0) = 0$.

Exemple 7 :

- $\text{pgcd}\,(24\,;18) = 6$.
- $\text{pgcd}\,(60\,;84) = 12$.
- $\text{pgcd}\,(150\,;240) = 30$.
- $\text{pgcd}\,(27\,;140) = 1$.
- $\text{pgcd}\,(6\,;72) = 6$.
- $\text{pgcd}\,(31\,;45) = 1$.
- $\text{pgcd}\,(5\,;7) = 1$.

Exercice 9 : Pour tout entier n non nul, on définit la suite $(u_n)_{n\in\mathbb{N}}$ par :

$$u_n = \frac{1}{n}\text{pgcd}\,(24\,;n)\,.$$

La suite $(u_n)_{n\in\mathbb{N}}$ est-elle convergente ?

Proposition 9 :

- $\text{pgcd}\,(a\,;a) = a$ et $\text{pgcd}\,(1\,;a) = 1$.
- Si $b|a$ alors $\text{pgcd}\,(a\,;b) = |b|$.

Théorème 10 (Fondamental) : Soient a et b deux entiers non nuls tels et un couple d'entiers $(q\,;r)$ tels que $a = bq + r$.

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

Remarques :

— Même si l'énoncé du théorème (10) fait fortement penser à la division euclidienne de a par b, il n'est nullement besoin que ce soit le cas pour que ce théorème soit vrai.
— En d'autre terme, le théorème (10) s'écrit :

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r).$$

Méthode 3 (Égalité entre deux nombres) :
Soit d et D, deux quantités. Pour montrer que $d = \mathrm{D}$, il suffit :

- de montrer successivement que $d \leqslant \mathrm{D}$ puis $\mathrm{D} \leqslant d$.
- dans le cas de nombres entiers positifs, on pourra aussi montrer que $d|\mathrm{D}$ puis $\mathrm{D}|d$.

Exercice 10 : Soient a et b deux entiers naturels non nuls. Soient $x = 7a + 5b$ et $y = 4a + 3b$.
Montrer que $\text{pgcd}\,(x\,;y) = \text{pgcd}\,(a\,;b)$.

II.2 Algorithme d'Euclide

Théorème 11 (Le pgcd est le dernier reste non nul) : Soient a et b deux naturels non nuls tels que b ne divise pas a. La suite des divisions euclidiennes suivantes finit par s'arrêter.

Le dernier reste non nul est alors le $\text{pgcd}\,(a\,;b)$.

$$\begin{array}{lll}
a \text{ par } b & a = bq_0 + r_0 & \text{avec} \quad b > r_0 \geqslant 0 \\
b \text{ par } r_0 & b = r_0 q_1 + r_1 & \text{avec} \quad r_0 > r_1 \geqslant 0 \\
r_0 \text{ par } r_1 & r_0 = r_1 q_2 + r_2 & \text{avec} \quad r_1 > r_2 \geqslant 0 \\
 & \vdots & \\
r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1} q_n + r_n & \text{avec} \quad r_{n-1} > r_n \geqslant 0 \\
r_{n-1} \text{ par } r_n & r_{n-1} = r_n q_{n+1} + 0. &
\end{array}$$

On a alors $\text{pgcd}\,(a\,;b) = r_n$.

Exemple 8 : Calculer le $\text{pgcd}\,(4539\,;1958)$. On effectue les divisions euclidiennes suivantes :

$$\begin{aligned}
4539 &= 1958 \times 2 + 623 \\
1958 &= 623 \times 3 + 89 \\
623 &= 89 \times 7 + 0
\end{aligned}$$

Conclusion : $\text{pgcd}\,(4539\,;1958) = 89$.

Exercice 11 : Calculer le pgcd de 162 et 207.

```
def pgcd(a,b) :
    while a%b != 0 :
        a, b = b, a%b
    return b
```

Figure III.3 – Algorithme d'Euclide

Théorème 12 : Soient a et b deux entiers non nuls.

Les diviseurs communs de a et b sont **exactement** les diviseurs de $\text{pgcd}(a\,;b)$:

$$d|\text{pgcd}(a\,;b) \iff \begin{cases} d|a \\ d|b \end{cases}$$

De manière équivalente : $\mathscr{D}(a\wedge b) = \mathscr{D}(a)\cap\mathscr{D}(b)$.

Proposition 13 : Pour tout entier naturel k non nul, $\text{pgcd}(ka\,;kb) = k\times\text{pgcd}(a\,;b)$.

Exemple 9 :

- $\text{pgcd}(800\,;500) = \text{pgcd}(100\times 8\,;100\times 5) = 100\times\text{pgcd}(8\,;5) = 100$.
- $\text{pgcd}(36\,;24) = \text{pgcd}(12\times 3\,;12\times 2) = 12\times\text{pgcd}(3\,;2) = 12$.

Proposition 14 : Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\beta_p}$.

Alors,

$$a\wedge b = \prod_{p\in\mathbb{P}} p^{\min(\alpha_p,\beta_p)}.$$

Exemples 10 :

- $510510\wedge 80000 = (2)(3)(5)(7)(11)(13)(17)\wedge(2)^7(5)^4 = (2)(5) = 10$.
- $9100\wedge 1848 = (2)^2(5)^2(7)(13)\wedge(2)^3(3)(7)(11) = (2)^2(7) = 28$.

Exercice 12 : Déterminer le PGCD de 1960 et de 34300.

II.3 PPCM

Définition 4 : Soient a et b deux entiers naturels non nuls.

On appelle *PPCM de a et b*, noté $\text{ppcm}(a\,;b)$ ou $a\vee b$, le plus petit multiple commun de a et b.

Remarques :

— Le seul multiple de 0 est 0 donc, pour tout entier a, $\text{ppcm}(a\,;0) = 0$.

— Comme tous les entiers sont multiples de 1, $\text{ppcm}(a\,;b)\geqslant 1$.

De même, il est évident que si a et b sont non nuls, $\text{ppcm}(a\,;b)\geqslant a$ et $\text{ppcm}(a\,;b)\geqslant b$.

— $\text{ppcm}(a\,;b) = \text{ppcm}(b\,;a)$.

Exemple 11 :

- $\text{ppcm}(18\,;12) = 36$.
- $\text{ppcm}(24\,;40) = 120$.
- $\text{ppcm}(11\,;17) = 11\times 17 = 187$.
- $\text{ppcm}(19\,;5) = 19\times 5 = 195$.

Proposition 15 : Soient a et b deux entiers naturels non nuls.

- $\text{ppcm}(a\,;a) = a$ et $\text{ppcm}(1\,;a) = a$.
- Si $b|a$ alors $\text{ppcm}(a\,;b) = a$.

Théorème 16 : Soient a et b deux entiers non nuls.

Les multiples communs de a et b sont **exactement** les multiples de $\text{ppcm}(a\,;b)$:

$$\text{ppcm}(a\,;b)\,|m \iff \begin{cases} a|m \\ b|m \end{cases}$$

De manière équivalente : $(a \vee b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Théorème 17 : Soient a et b deux entiers naturels.

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

Remarque : La notion de PPCM peut aisément s'étendre aux entiers relatifs en prenant comme définition, le plus petit multiple de $|a|$ et $|b|$. Dans ce cas, on aurait également :

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

Exemple 12 : Le PGCD de 42 et 60 est 6. Si on note m leur PPCM, alors $6m = 42 \times 60$ d'où $m = 420$.

Exercice 13 : Déterminer $m = 44100 \vee 36036$.

Corollaire 17.1 : Si k est un entier naturel : $\text{ppcm}(ka\,;kb) = k \times \text{ppcm}(a\,;b)$.

Proposition 18 : Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\beta_p}$.

Alors,

$$a \vee b = \prod_{p\in\mathbb{P}} p^{\max(\alpha_p,\beta_p)}.$$

Méthode 4 (Trouver un PPCM) :

Pour des entiers a et b pas « trop grands », une méthode enfantine mais souvent suffisante est de décomposer a et b en facteurs premiers.

Le ppcm de a et b est alors égal au produit de tous les facteurs premiers de a et b pris avec l'exposant le plus grand apparaissant dans les décompositions.

Exercice 14 : Déterminer $\text{ppcm}(240\,;756)$.