Arithmétique – nombres premiers

1. Multiples d'un entier naturel

- $\mathbb{N} = \{0,1,2,3,4,...\}$ = ensemble des entiers naturels
- $2\mathbb{N} = \{\mathbf{2}\cdot 0,\ \mathbf{2}\cdot 1,\ \mathbf{2}\cdot 2,\ \mathbf{2}\cdot 3,\ \mathbf{2}\cdot 4,...\}$
  $= \{0, 2, 4, 6, 8, ...\}$
  = ensemble des **multiples** de 2
  = ensemble des entiers naturels **pairs**
- $3\mathbb{N} = \{\mathbf{3}\cdot 0,\ \mathbf{3}\cdot 1,\ \mathbf{3}\cdot 2,\ \mathbf{3}\cdot 3,\ \mathbf{3}\cdot 4,...\}$
  $= \{0, 3, 6, 9, 12, ...\}$
  = ensemble des multiples de 3
- $4\mathbb{N} =$ ....
  = ensemble des multiples de 4
- $5\mathbb{N} =$ ....
  = ensemble ....

etc.

> ***Définition.*** Soit a un entier naturel. Un ***multiple*** de a est un entier naturel de la forme $a \cdot n$, où $n \in \mathbb{N}$. L'***ensemble des multiples*** de a est noté $a\mathbb{N}$.
>
> $$a\mathbb{N} = \left\{an \;/\; n \in \mathbb{N}\right\} \qquad \text{(définition en compréhension)}$$
> $$= \left\{0, a, 2a, 3a, 4a, ...\right\} \qquad \text{(définition en extension)}$$

Remarques.

a) L'ensemble des multiples d'un entier naturel ***non nul*** est ***infini***.

b) L'ensemble des multiples de 0 est : $0\mathbb{N} = \{0\}$.

c) Le plus petit multiple d'un entier naturel est toujours : ....

2. Diviseurs d'un entier naturel

Exemple : Au lieu de dire que 24 est un ***multiple*** de 6, on peut aussi dire que 24 ***est divisible par*** 6 ou encore que 6 est un ***diviseur*** de 24. On écrit : $6 \mid 24$ et on lit : 6 ***divise*** 24.

Définition. Soit a et b deux entiers naturels. On dit que :

$$\left.\begin{array}{l} \bullet\ a \text{ est un } \textit{diviseur} \text{ de } b \\ \bullet \text{ ou } a \textit{ divise } b \text{ (noté } a \mid b\text{)} \\ \bullet \text{ ou } b \textit{ est divisible par } a \end{array}\right\} \Leftrightarrow b \text{ est un multiple de } a.$$

Exemples :

- $3 \mid 12$
- $9 \mid 45$
- $10 \mid 80$
- $16 \mid 80$

mais :

- $6 \nmid 33$
- $7 \nmid 15$

Remarques :

a) $(\forall n \in \mathbb{N})$ $\quad 1 \mid n$ et $n \mid n$ car $n = n \cdot 1$

$n \mid 0$ car $0 = 0 \cdot n$

b) En particulier : $0 \mid 0$ mais ***attention*** : $0 \nmid n$ si n est différent de 0.

Définition. L'***ensemble des diviseurs*** d'un entier naturel a est noté Div a.
Donc : $\operatorname{Div} a = \{n \in \mathbb{N} \,/\, n \mid a\}$.

Exemples :

- $\operatorname{Div} 12 = \{1,2,3,4,6,12\}$;
- $\operatorname{Div} 25 = \{1,5,25\}$;
- $\operatorname{Div} 45 = \{1,3,5,9,15,45\}$
- $\operatorname{Div} 56 = \{1,2,4,7,8,14,28,56\}$
- $\operatorname{Div} 1 = \{1\}$;
- $\operatorname{Div} 0 = \{0,1,2,3,4,\ldots\} = \mathbb{N}$.

Pour chercher les diviseurs d'un entier naturel ***pas trop grand***, on utilise le schéma suivant :

Div 100	1	2	4	5	10
	100	50	25	20	10

Donc : $\operatorname{Div} 100 = \{1,2,4,5,10,20,25,50,100\}$

Propriétés des diviseurs et multiples

a) Ecrire en extension les ensembles suivants :

$\mathrm{Div}\,15 =$ ………………………………………………………………

$\mathrm{Div}\,45 =$ ………………………………………………………………

On remarque que : ………………………………………………………

Retenons : $a \mid b \Rightarrow \mathrm{Div}\,a \subset \mathrm{Div}\,b$

b) Ecrire en extension les ensembles suivants :

$6\mathbb{N} =$ ………………………………………………………………

$18\mathbb{N} =$ ………………………………………………………………

On remarque que : ………………………………………………………

Retenons : $a \mid b \Rightarrow b\mathbb{N} \subset a\mathbb{N}$.

3. Critères de divisibilité

- Un entier naturel est divisible par ***2*** s'il se termine par 0, 2, 4, 6 ou 8.
- Un entier naturel est divisible par ***3*** si la somme de ses chiffres (Quersumme) est divisible par 3.
- Un entier naturel est divisible par ***4*** si le nombre formé par ses deux derniers chiffres est divisible par 4.
- Un entier naturel est divisible par ***5*** s'il se termine par 0 ou par 5.
- Un entier naturel est divisible par ***6*** s'il est divisible par 2 et par 3.
- Un entier naturel est divisible par ***8*** si le nombre formé par les 3 derniers chiffres est divisible par 8.
- Un entier naturel est divisible par ***9*** si la somme de ses chiffres (Quersumme) est divisible par 9.
- Un entier naturel est divisible par ***10*** s'il se termine par 0.
- Un entier naturel est divisible par ***11*** ssi la ***somme alternée*** de ses chiffres est divisible par 11.

  Exemple : $11 \mid 345895$ car : $3-4+5-8+9-5=0$ et $11 \mid 0$
- Un entier naturel est divisible par ***12*** ssi il est divisible par 3 et par 4.
- Un entier naturel est divisible par ***15*** ssi il est divisible par 3 et par 5.
- Un entier naturel est divisible par ***18*** ssi il est divisible par 2 et par 9.

4. Nombres premiers. Factorisation première

> ***Définition***. Un ***nombre premier*** est un entier naturel qui a ***exactement 2 diviseurs*** : 1 et lui-même.

Nous notons $\mathbb{P}$ l'ensemble des nombres premiers.

$$\boxed{\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\}}$$

Remarques.

a) $\mathbb{P}$ est un ensemble infini.

b) Un entier >2 qui n'est pas premier est dit ***composé***.

c) 0 et 1 ne sont pas des nombres premiers !

Comment voir si un entier naturel est premier ou non ?

Exemples : a) Est-ce que 101 est premier ?

$101 = 2 \cdot 50 + 1$, donc $2 \nmid 101$

$101 = 3 \cdot 33 + 2$, donc $3 \nmid 101$

$101 = 5 \cdot 20 + 1$, donc $5 \nmid 101$

$101 = 7 \cdot 14 + 3$, donc $7 \nmid 101$

$101 = 11 \cdot 9 + 2$, donc $11 \nmid 101$.

Dans la dernière ***division euclidienne***, le quotient (=9) est pour la première fois plus petit que le diviseur (=11). C'est à ce moment qu'on peut arrêter les divisions. Pourquoi ? ……………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

On peut en conclure que 101 est premier.

b) Est-ce que 247 est premier ?

247 n'est ni divisible par 2, ni par 3 ni par 5.

$247 = 7 \cdot 35 + 2$, donc $7 \nmid 247$

$247 = 11 \cdot 22 + 5$, donc $11 \nmid 247$

$247 = 13 \cdot 19$, donc $13 \mid 247$ et 247 n'est pas premier !

Crible d'Eratosthène. C'est une méthode pratique permettant de trouver assez vite tous les nombres premiers jusqu'à un entier naturel N donné. En voici le ***principe*** :

On écrit la liste de tous les entiers de 2 jusqu'à N.

(1) On garde $p_1 = 2$ et on élimine tous les autres multiples de 2.

(2) On garde $p_2 = 3$ qui est le premier élément non éliminé après 2 et on élimine tous les autres multiples de 3.

(3) On garde $p_3 = 5$ qui est le premier élément non éliminé après 3 et on élimine tous les autres multiples de 5.

(4) On répète le procédé aussi longtemps que $p_k^2 \leq N$.

Les nombres non éliminés sont les nombres premiers $\leq N$.

Dressons par exemple la liste des nombres premiers ≤ 100 :

	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
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Voici donc la liste des nombres premiers ≤ 100 :

....

....

....

....

Factorisation première. Si l'on décompose un entier naturel ≥ 2 en ***autant de facteurs entiers*** $(\neq 1)$ ***que possible***, alors tous ces facteurs seront nécessairement des nombres premiers. On obtient ainsi la ***factorisation première (f.p.)*** ou ***décomposition en facteurs premiers*** de l'entier.

Exemples.

- $$\begin{aligned} 100 &= 4 \cdot 25 \\ &= 2 \cdot 2 \cdot 5 \cdot 5 \\ &= 2^2 \cdot 5^2 \end{aligned}$$

  C'est la factorisation première de 100.

- $$\begin{aligned} 630 &= 10 \cdot 63 \\ &= 2 \cdot 5 \cdot 7 \cdot 9 \\ &= 2 \cdot 5 \cdot 7 \cdot 3 \cdot 3 \\ &= 2 \cdot 3^2 \cdot 5 \cdot 7 \end{aligned}$$

  On range les facteurs premiers ***par ordre croissant*** !

  C'est la factorisation première de 630.

- 59 est un nombre premier, donc c'est aussi la factorisation première de 59.

> ***Théorème fondamental de l'arithmétique***. Tout entier naturel ≥ 2 admet une factorisation première ***unique*** !

Schéma pratique pour la factorisation première :

91'476	2
45'738	2
22'869	3
7'623	3
2'541	3
847	7
121	11
11	11
1	

$\Rightarrow\ 91'476 = 2^2 \cdot 3^3 \cdot 7 \cdot 11^2$

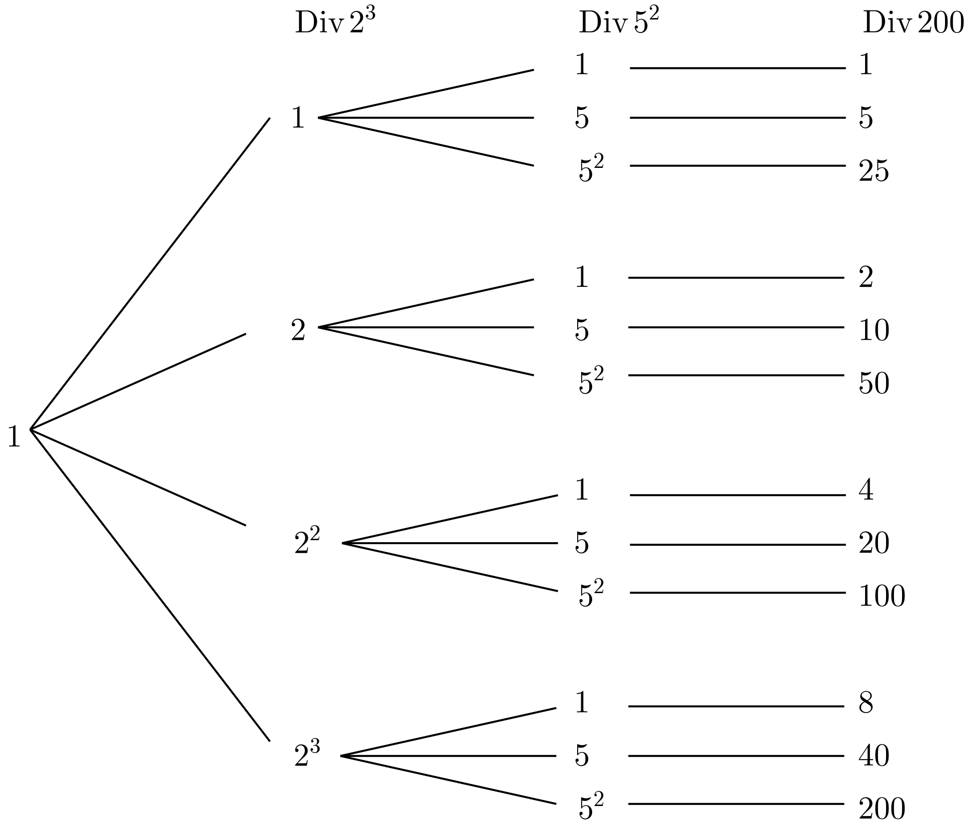
10'125	5
2'025	5
405	5
81	3
27	3
9	3
3	3
1	

$\Rightarrow 10'125 = 3^4 \cdot 5^3$

Remarque : On n'a pas besoin diviser par les facteurs premiers dans l'ordre, mais dans la factorisation première on les range par ordre croissant !

Applications. a) La factorisation première permet de ***déterminer tous les diviseurs*** d'un entier naturel l'aide d'un ***schéma en arbre***.

Exemple : $200 = 2^3 \cdot 5^2$.



Donc : $\operatorname{Div} 200 = \{1,2,4,5,8,10,20,25,40,50,100,200\}$.

b) La factorisation première permet de ***déterminer le nombre de diviseurs*** d'un entier ***sans les calculer tous***.

Exemple. Tous les diviseurs de 200 sont de la forme $2^p \cdot 5^q$ où $0 \leq p \leq 3$ et $0 \leq q \leq 2$. Il y a ***4 possibilités*** pour p (0,1,2, et 3) et ***3 possibilités pour q*** (0,1 et 2). Il y a donc en tout $4 \cdot 3 = 12$ diviseurs de 200.

Formule :

$$n = 2^p \cdot 3^q \cdot 5^r \cdot ... \Rightarrow \operatorname{card}(\operatorname{Div} n) = (p+1) \cdot (q+1) \cdot (r+1) \cdot ...$$

En d'autres termes : Le ***nombre de diviseurs*** d'un entier est le ***produit de tous les exposants augmentés de 1*** dans sa factorisation première.

c) La factorisation première permet de ***décider si un entier donné en divise un autre***.

Exemples. 1) Est-ce que $45 \mid 405$?

Réponse : $45 = 3^2 \cdot 5$ et $405 = 5 \cdot 81 = 3^4 \cdot 5$.

$3^2 \mid 3^4$ et $5 \mid 5$, donc $45 \mid 405$.

2) Est-ce que $56 \mid 3388$?

Réponse : $56 = 2^3 \cdot 7$ et $3388 = 2^2 \cdot 7 \cdot 11^2$

Dans 56, l'exposant de 2 est plus grand que dans 3388, donc $56 \nmid 3388$.

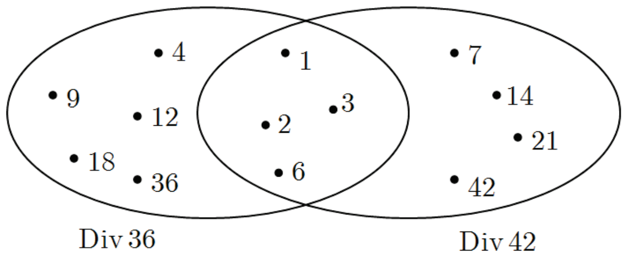
Règle : $n \mid n'$ si et seulement si les ***exposants*** des nombres premiers dans la factorisation première de n ***sont tous inférieurs ou égaux*** aux ***exposants*** des mêmes nombres premiers dans la factorisation première de n'.

5. Diviseurs communs. Pgcd

Définition. Le ***plus grand commun diviseur (pgcd)*** de deux ou plusieurs entiers naturels est leur diviseur commun le plus grand.

Exemple. $\operatorname{pgcd}(42,36) = ?$

$\mathrm{Div}42 = \{\underline{1},\underline{2},\underline{3},\underline{6},7,14,21,42\}$ et $\mathrm{Div}\,36 = \{\underline{1},\underline{2},\underline{3},4,\underline{6},9,12,18,36\}$



Donc : $\operatorname{pgcd}(42,36) = 6$.

Remarque : Les diviseurs communs de 42 et 36 sont exactement les diviseurs de 6 : $\mathrm{Div}\,42 \cap \mathrm{Div}\,36 = \mathrm{Div}\,6$.

Propriété. Les diviseurs communs de deux entiers naturels a et de b sont exactement les diviseurs de leur pgcd. En d'autres termes :

$$\mathrm{Div}\,a \cap \mathrm{Div}\,b = \mathrm{Div}\,\operatorname{pgcd}(a,b)$$

Application : simplification d'une fraction. Pour simplifier une fraction à termes entiers, on divise le numérateur et le dénominateur de cette fraction par leur pgcd. On obtient alors une fraction ***irréductible***. Par exemple :

$$\frac{42}{36} = \frac{\cancel{6} \cdot 7}{\cancel{6} \cdot 6} = \frac{7}{6}$$

Propriétés du pgcd

a) $\boxed{\text{Si } a \mid b \text{ alors } \operatorname{pgcd}(a,b) = a}$

Exemple : $\operatorname{pgcd}(17,34) = 17$.

b) ***Commutativité*** : $\boxed{\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,a)}$

Exemple : $\operatorname{pgcd}(12,15) = \operatorname{pgcd}(15,12) = 3$.

c) ***Associativité*** :

$$\boxed{\operatorname{pgcd}(a,b,c) = \operatorname{pgcd}(\operatorname{pgcd}(a,b),c) = \operatorname{pgcd}(a,\operatorname{pgcd}(b,c))}$$

Exemples :

(1) $\operatorname{pgcd}(24,40,60) = \operatorname{pgcd}(\operatorname{pgcd}(24,40),60) = \operatorname{pgcd}(8,60) = 4$,

ou bien :

$\operatorname{pgcd}(24,40,60) = \operatorname{pgcd}(24,\operatorname{pgcd}(40,60)) = \operatorname{pgcd}(24,20) = 4$.

(2) L'associativité peut être généralisé au calcul du pgcd de plusieurs entiers naturels :

$$\begin{aligned}\operatorname{pgcd}\big(98,42,84,63\big) &= \operatorname{pgcd}\big(98,\operatorname{pgcd}\big(42,84\big),63\big)\\ &= \operatorname{pgcd}\big(98,42,63\big)\\ &= \operatorname{pgcd}\big(98,\operatorname{pgcd}\big(42,63\big)\big)\\ &= \operatorname{pgcd}\big(98,7\big) = 7\end{aligned}$$

d) ***Distributivité de la multiplication par rapport au pgcd*** :

$$\boxed{\operatorname{pgcd}(a \cdot b, a \cdot c) = a \cdot \operatorname{pgcd}(b,c)}$$

Exemple : $\operatorname{pgcd}(270,300) = 10 \cdot \operatorname{pgcd}(27,30) = 10 \cdot 3 = 30$

Calcul du pgcd à l'aide de la factorisation première

Exemple : $\operatorname{pgcd}(17640, 30800) = ?$

17'640	2
8'820	2
4'410	2
2'205	3
735	3
245	5
49	7
7	7
1	

30'800	2
15'400	2
7'700	2
3'850	2
1'925	5
385	5
77	7
11	11
1	

$17'640 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$

$30'800 = 2^4 \cdot 5^2 \cdot 7 \cdot 11$

Donc : $\operatorname{pgcd}(17'640, 30'800) = 2^3 \cdot 5 \cdot 7 = 280$

Règle : Le pgcd de plusieurs entiers naturels est le produit de leurs ***diviseurs premiers communs***, affectés chacun du ***plus petit des exposants*** apparaissant dans les factorisations premières respectives.

Définition. Deux entiers naturels a et b sont dits ***premiers entre eux*** si leur seul diviseur commun est 1, c.-à-d. si $\operatorname{pgcd}(a,b) = 1$.

Exemples :

(1) $16 = 2^4$ et $25 = 5^2$ sont premiers entre eux car $\operatorname{pgcd}(16,25) = 1$.

(2) $35 = 5 \cdot 7$ et $12 = 2^2 \cdot 3$ sont premiers entre eux car $\operatorname{pgcd}(35,12) = 1$.

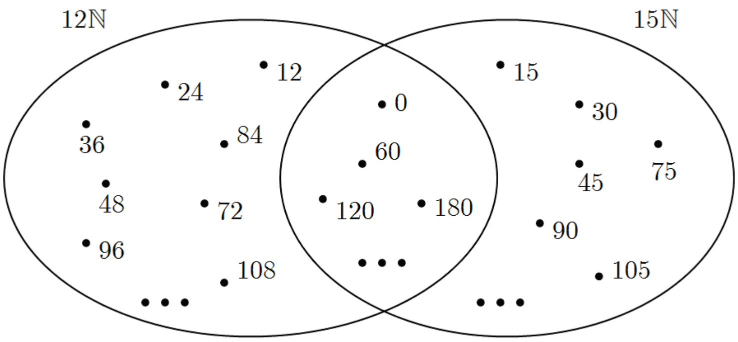
6. Multiples communs. Ppcm

Définition. Le ***plus petit commun multiple (ppcm)*** de plusieurs naturels est leur multiple commun ***le plus petit*** et ***non nul***.

Exemple. $\operatorname{ppcm}(12,15) = ?$

$12\mathbb{N} = \{\underline{0}, 12, 24, 36, 48, \underline{60}, 72, 84, 96, 108, \underline{120}, \ldots\}$ et

$15\mathbb{N} = \{\underline{0}, 15, 30, 45, \underline{60}, 75, 90, 105, \underline{120}, \ldots\}$



Donc : $\operatorname{ppcm}(12,15) = 60$.

Remarque : Les multiples communs de 12 et 15 sont exactement les multiples de 60 : $12\mathbb{N} \cap 15\mathbb{N} = 60\mathbb{N}$.

Propriété. Les multiples communs de deux entiers naturels a et de b sont exactement les multiples de leur ppcm. En d'autres termes :

$$a\mathbb{N} \cap b\mathbb{N} = \operatorname{ppcm}(a,b)\,\mathbb{N}$$

Application : dénominateur commun. Lorsqu'on additionne ou soustrait des fractions à termes entiers, on prend comme dénominateur commun le ppcm des dénominateurs.

Exemple :

$$\frac{7}{12}+\frac{4}{15}=\frac{35}{60}+\frac{16}{60}=\frac{51}{60}$$

Propriétés du ppcm

a) $\boxed{\text{Si } a \mid b \text{ alors } \operatorname{ppcm}(a,b)=b}$

Exemple : $\operatorname{ppcm}(15,90)=90$.

b) $\boxed{\text{Si } a \text{ et } b \text{ sont premiers entre eux alors } \operatorname{ppcm}(a,b)=a\cdot b}$

Exemple : $\operatorname{ppcm}(6,35)=6\cdot 35=210$.

c) ***Commutativité*** :

$$\boxed{\operatorname{ppcm}(a,b)=\operatorname{ppcm}(b,a)}$$

Exemple : $\operatorname{ppcm}(12,15)=\operatorname{ppcm}(15,12)=60$.

d) ***Associativité*** :

$$\boxed{\operatorname{ppcm}(a,b,c)=\operatorname{ppcm}(\operatorname{ppcm}(a,b),c)=\operatorname{ppcm}(a,\operatorname{ppcm}(b,c))}$$

Exemples :

(1) $\operatorname{ppcm}(2,6,15)=\operatorname{ppcm}(\operatorname{ppcm}(2,6),15)=\operatorname{ppcm}(6,15)=30$,

ou bien :

$\operatorname{ppcm}(2,6,15)=\operatorname{ppcm}(2,\operatorname{ppcm}(6,15))=\operatorname{ppcm}(2,30)=30$.

(2) L'associativité peut être généralisé au calcul du ppcm de plusieurs entiers naturels :

$$\begin{aligned}\operatorname{ppcm}\big(5,6,7,8,9\big)&=\operatorname{ppcm}\big(\operatorname{ppcm}\big(5,7,8\big),\operatorname{ppcm}\big(6,9\big)\big)\\&=\operatorname{ppcm}\big(280,18\big)\\&=2\cdot\operatorname{ppcm}\big(140,9\big)\\&=2\cdot 140\cdot 9=2'520\end{aligned}$$

Dans la dernière ligne on a utilisé la :

e) ***Distributivité de la multiplication par rapport au ppcm*** :

$$\boxed{\operatorname{ppcm}(a\cdot b,a\cdot c)=a\cdot\operatorname{ppcm}(b,c)}$$

Exemple : $\operatorname{ppcm}(350,450)=50\cdot\operatorname{ppcm}(7,9)=50\cdot 63=3'150$;

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

Le produit de deux entiers naturels non nuls est égal au produit de leur pgcd par leur ppcm.

La propriété s'explique aisément si l'on part des factorisations premières des deux entiers.

Exemple : $a = 2^5 \cdot 3 \cdot 5^2$ et $b = 2^4 \cdot 3^2 \cdot 7$

Alors : $\text{pgcd}(a,b) = 2^4 \cdot 3$ et $\text{ppcm}(a,b) = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7$.

La formule est vérifiée puisque les facteurs qui n'apparaissent pas dans le pgcd apparaissent dans le ppcm et vice-versa.

Calcul du ppcm à l'aide de la factorisation première

Exemple : $\text{ppcm}(1960,1232) = ?$

1960	2		1232	2
980	2		616	2
490	2		308	2
245	5		154	2
49	7		77	7
7	7		11	11
1			1	

$1960 = 2^3 \cdot 5 \cdot 7^2$ $\qquad$ $1232 = 2^4 \cdot 7 \cdot 11$

Donc : $\text{ppcm}(1960,1232) = 2^4 \cdot 5 \cdot 7^2 \cdot 11 = 43'120$

Règle : Le ppcm de plusieurs entiers naturels est le produit de tous les ***diviseurs premiers*** apparaissant dans les factorisations premières respectives, chacun étant affecté du ***plus grand des exposants***.