LES NOMBRES PREMIERS – PPCM

Extrait de Pour la Science n° 251 Septembre 1998 : La factorisation des grands nombres (Johannes Buchmann)

Le nombre 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541 *est le produit de deux nombres premiers ; lesquels ?*
Martin Gardner posa cette question aux lecteurs de Pour la Science en octobre 1977. *dans sa rubrique de «Jeux mathématiques», mais une réponse ne fut donnée que* 16 *ans plus tard : en avril* 1994, *Paul Leyland, de l'Université d'Oxford. Michael Graff, de l'Université de l'Iowa, et Derek Atkins, de l'Institut de technologie du Massachusetts, identifièrent les deux facteurs, après avoir distribué des parties de la tâche, grâce au réseau Internet, à quelque* 600 *volontaires, qui laissèrent fonctionner sur leurs ordinateurs, pendant de nombreuses nuits, le programme écrit par Arjen Lenstra, du Centre de recherches de la Société Bell Communications.*
La multiplication de deux nombres, même très grands, n'est pas compliquée : avec du papier et un crayon, on calcule le produit de deux nombres de 65 *chiffres en une heure environ ; par ordinateur, le calcul est immédiat. En revanche, l'opération inverse, c'est-à-dire l'identification des facteurs d'un produit, est très difficile, même avec les calculateurs les plus rapides. (...)*
Les opérations mathématiques telles que la multiplication et la factorisation sont à la base des systèmes cryptographiques modernes : le cryptage est rapide, mais le décryptage est quasi impossible en pratique. (...)
On ignore si la factorisation est difficile par essence ou si les mathématiciens n'ont pas encore trouvé la méthode la plus habile. Aussi la seule garantie de la sécurité des procédés de cryptage est l'ignorance d'une méthode rapide de factorisation des nombres entiers. L'étude de la factorisation date de l'Antiquité : les mathématiciens d'alors savaient déjà que chaque nombre naturel est un produit de nombres premiers, et que la décomposition en facteurs premiers est unique, à l'ordre près. Par exemple, 12 *se décompose seulement en* $2 \times 2 \times 3$. *L'étude des propriétés des nombres entiers naturels impose souvent la décomposition en facteurs premiers. (...)*

1) LES NOMBRES PREMIERS

A) DEFINITION - PROPRIETES

Définition :

Soit p un entier naturel strictement supérieur à 1.
On dit que p est un nombre premier si l'ensemble de ses diviseurs dans $\mathbb{N}$ est $\{1 ; p\}$.

Par convention, et pour des raisons de facilité, 1 n'est pas un nombre premier.

Exemple :

2 , 3 , 5 , 7 sont des nombres premiers . 4, 6, 8, 9, 10 ne sont pas des nombres premiers.

Propriétés :

Soit a un entier naturel strictement supérieur à 1.

- a possède au moins un diviseur premier.
- si a n'est pas premier, alors au moins un des diviseurs premiers de a est inférieur ou égal à $\sqrt{a}$.

Preuve :

Soit a un entier naturel strictement supérieur à 1.

- Considérons D_a l'ensemble des diviseurs de a strictement supérieurs à 1.
  D_a n'est pas vide car il contient a. D_a a donc un plus petit élément n.
  Par définition, ce plus petit élément n est un diviseur de a strictement supérieur à 1.
  Supposons que n ne soit pas premier. n possède donc un diviseur p différent de 1 et de n.
  Comme on sait que 0 ne divise pas n, on a $p > 1$.
  D'autre part p étant un diviseur de n, on sait que $|p| \leq |n|$. On a donc $1 < p < n$.
  Alors on sait que p divise n et n divise a, donc p divise a . On en déduit donc que $p \in D_a$.
  Ceci est en contradiction avec le fait que n est le plus petit élément de D_a .
  On ne peut donc pas supposer que n n'est pas premier.
  On en déduit donc que n est un diviseur premier de a et que a possède donc au moins un diviseur premier.
- Soit n un diviseur premier de a. On peut écrire $a = n \times k$ avec $k \in \mathbb{N}^*$.
  a n'est pas premier et ne peut donc pas être égal à n qui est premier . On a alors $k > 1$.
  - Si $n \leq \sqrt{a}$, alors n est bien un diviseur premier de a inférieur ou égal à $\sqrt{a}$.
  - Si $n > \sqrt{a}$, alors :
    $$n \times k > k\sqrt{a} \quad \Rightarrow \quad a > k\sqrt{a} \quad \Rightarrow \quad k < \sqrt{a} .$$
    k est donc un diviseur de a inférieur à $\sqrt{a}$.
    k étant strictement supérieur à 1, il a un diviseur premier p et on sait que $p \leq k$ donc $p \leq \sqrt{a}$.
    p étant un diviseur de k et k un diviseur de a, on en déduit que p est un diviseur de a.
    p est donc un diviseur premier de a inférieur ou égal à $\sqrt{a}$.

  Dans tous les cas on a donc trouvé un diviseur premier de a inférieur ou égal à $\sqrt{a}$.

Remarques :

- Un entier naturel strictement supérieur à 1 et qui n'est pas premier est appelé **nombre composé**.
- Pour déterminer si un nombre donné N est premier, on peut chercher s'il est divisible par un nombre premier inférieur ou égal à $\sqrt{N}$.
  - Si l'un des nombres premiers inférieurs ou égaux à $\sqrt{N}$ divise N, alors N n'est pas premier.
  - Si aucun des nombres premiers inférieurs ou égaux à $\sqrt{N}$ ne divise N, alors N est premier.

  Cette méthode nécessite de connaître la liste des nombres premiers inférieurs ou égaux à $\sqrt{N}$.

B) CRIBLE D'ERATOSTHEME

Le crible d'Eratosthène est une méthode permettant d'obtenir tous les nombres premiers inférieurs à un nombre donné.
Pour trouver par exemple tous les nombres premiers inférieurs à 100, on écrit dans un tableau tous les nombres de 1 à 100.

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
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

- On raye le nombre 1 qui n'est pas premier.
Le premier nombre non rayé est 2, il est premier.
- On raye tous les multiples de 2 supérieurs à 2.
Le premier nombre non rayé est 3, il est premier.
- On raye tous les multiples de 3 supérieurs à 3.
Le premier nombre non rayé est 5, il est premier.
- On raye tous les multiples de 5 supérieurs à 5.
Le premier nombre non rayé est 7, il est premier.
- On raye tous les multiples de 7 supérieurs à 7.
Le premier nombre non rayé est 11, il est premier.

On peut s'arrêter car $11 > \sqrt{100}$.
On a obtenu alors dans les cases non rayées, les nombres premiers inférieurs à 100.

Les nombres rayés ne sont pas premiers puisque ce sont des multiples de l'un des nombres qui précèdent.
Si un nombre N n'est pas rayé, c'est que N n'est multiple d'aucun des nombres non rayés strictement inférieurs à 11, donc N n'est multiple d'aucun nombre premier strictement inférieur à $\sqrt{N}$, donc N est premier.

C) INFINITE DES NOMBRES PREMIERS

Propriété :

Il existe dans $\mathbb{N}$ une infinité de nombres premiers.

Preuve :
Supposons que l'ensemble des nombres premiers soit un ensemble fini $\{p_1, p_2, ..., p_k\}$.
Soit $n = p_1 \times p_2 \times ... \times p_k + 1$.
n est strictement supérieur à 1, il admet donc un diviseur premier, c'est-à-dire l'un des nombres p_i.
p_i divise n et p_i divise $p_1 \times p_2 \times ... \times p_k$, donc p_i divise leur différence, c'est-à-dire 1, ce qui est absurde.

L'ensemble des nombres premiers n'est donc pas un ensemble fini.

D) DECOMPOSITION EN FACTEURS PREMIERS

Exemple :
On considère le nombre 360.
Il est divisible par 2 et on peut écrire $360 = 2 \times 180$
180 est encore divisible par 2 et on peut écrire $180 = 2 \times 90$
90 est encore divisible par 2 et on peut écrire $90 = 2 \times 45$
45 est divisible par 3 et on peut écrire $45 = 3 \times 15$
15 est divisible par 3 et on peut écrire $15 = 3 \times 5$
Finalement on obtient $360 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 = 2^3 \times 3^2 \times 5$
C'est la décomposition du nombre 360 en produit de facteurs premiers.

360	2
180	2
90	2
45	3
15	3
5	5
1	

Propriété :

Soit n un entier supérieur ou égal à 2.
n peut se décomposer sous la forme : $n = p_1^{\alpha 1} p_2^{\alpha 2} \dots p_k^{\alpha k}$
où $p_1 , p_2 , ... , p_k$ sont des nombres premiers tels que $p_1 < p_2 < \dots < p_k$ et $\alpha_1 , \alpha_2 , ... , \alpha_k$ des entiers naturels non nuls.
Cette décomposition est appelée **décomposition de *n* en produit de facteurs premiers**.
On admet que cette décomposition est unique.

Preuve :
On considère pour $n \geq 2$ la propriété P(n) : "tout entier q tel que $2 \leq q \leq n$ peut se décomposer en produit de facteurs premiers."
Démontrons par récurrence que cette propriété est vraie pour tout entier $n \geq 2$.

- 2 peut se décomposer sous la forme $2 = 2^1$. La propriété P(2) est donc vraie.
- Supposons que P(n) est vraie pour un entier n donné, $n \geq 2$.
  Alors pour tout entier q tel que $2 \leq q \leq n$, q peut se décomposer en produit de facteurs premiers.

  Démontrons que la propriété P(n+1) est vraie.
  Soit q un entier tel que $2 \leq q \leq n + 1$
  - Si $2 \leq q \leq n$, q peut se décomposer en produit de facteurs premiers puisque P(n) est vraie.
  - Si $q = n + 1$, alors on peut envisager deux cas :
    - Si $n + 1$ est premier, alors on peut écrire $n + 1 = (n + 1)^1$ et la décomposition est immédiate.
    - Si $n + 1$ n'est pas premier, alors $n + 1$ a un diviseur premier p tel que $1 < p < n + 1$, donc $2 \leq p \leq n$.
      On peut alors écrire $(n + 1) = p\, q$ avec q entier tel que $2 \leq q \leq n$.
      Comme P(n) est vraie et que $2 \leq q \leq n$ on sait que l'on peut décomposer q en facteurs premiers.

On obtient alors une décomposition de $p \times q$ en facteurs premiers, c'est-à-dire une décomposition de $n + 1$ en facteurs premiers.

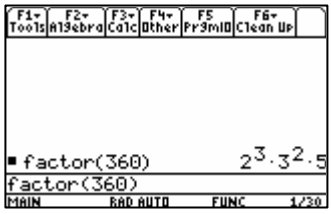
On a donc démontré que P(n+1) est vraie.

On en déduit que P(n) est vraie pour tout entier $n \geq 2$ et en particulier que tout entier $n \geq 2$ peut se décomposer en produit de facteurs premiers.

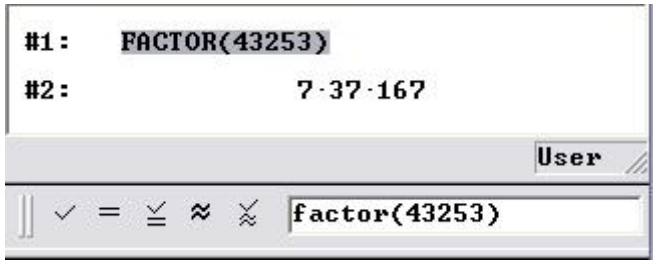
Remarques :

- Du fait de l'unicité de le décomposition, si n a pour décomposition en produit de facteurs premiers $n = p_1^{\alpha 1} p_2^{\alpha 2} \dots p_k^{\alpha k}$ alors tout diviseur premier de n est l'un des nombres $p_1, p_2, \dots, p_k$
- Certaines calculatrices et certains logiciels permettent d'obtenir la décomposition d'un nombre en produit de facteurs premiers :

Calculatrice TI 89



Logiciel Dérive



E) ENSEMBLE DES DIVISEURS

Exemple :

Dans IN l'ensemble des diviseurs de 200 est {1 ; 2 ; 4 ; 5 ; 8 ; 10 ; 20 ; 25 ; 40 ; 50 ; 100 ; 200}

On peut retrouver ce résultat à partir de la décomposition de 200 en produit de facteurs premiers.

En effet cette décomposition est $200 = 2^3 \times 5^2$

On peut alors vérifier que les diviseurs de 200 sont les nombres s'écrivant sous la forme $2^{\beta 1} 5^{\beta 2}$ avec $0 \leq \beta_1 \leq 3$ et $0 \leq \beta_2 \leq 2$.

Propriété :

Soit n un entier supérieur ou égal à 2, dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha 1} p_2^{\alpha 2} \dots p_k^{\alpha k}$

L'ensemble des diviseurs naturels de n est l'ensemble des entiers d s'écrivant sous la forme $d = p_1^{\beta 1} p_2^{\beta 2} \dots p_k^{\beta k}$

où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1$, $0 \leq \beta_2 \leq \alpha_2$, ... , $0 \leq \beta_k \leq \alpha_k$.

Preuve :

n est un entier supérieur ou égal à 2, dont la décomposition en produit de facteurs premiers est : $n = p_1^{\alpha 1} p_2^{\alpha 2} \dots p_k^{\alpha k}$

- Considérons un entier d s'écrivant sous la forme $d = p_1^{\beta 1} p_2^{\beta 2} \dots p_k^{\beta k}$

où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1$, $0 \leq \beta_2 \leq \alpha_2$, ... , $0 \leq \beta_k \leq \alpha_k$.

On peut alors écrire $n = p_1^{\alpha 1} p_2^{\alpha 2} \dots p_k^{\alpha k} = (p_1^{\beta 1} p_2^{\beta 2} \dots p_k^{\beta k}) \times (p_1^{\alpha 1 - \beta 1} p_2^{\alpha 2 - \beta 2} \dots p_k^{\alpha k - \beta k})$

Donc $n = d \times q$ avec $q = p_1^{\alpha 1 - \beta 1} p_2^{\alpha 2 - \beta 2} \dots p_k^{\alpha k - \beta k}$

On sait que $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1$, $0 \leq \beta_2 \leq \alpha_2$, ... , $0 \leq \beta_k \leq \alpha_k$.

Donc $\alpha_1 - \beta_1$; $\alpha_2 - \beta_2$; ... ; $\alpha_k - \beta_k$ sont des entiers naturels.

Par conséquent q est un entier naturel et d est donc un diviseur de n.

- Considérons un entier d diviseur de n.

- Si $d = 1$, d peut s'écrire sous la forme $d = p_1^{\beta 1} p_2^{\beta 2} \dots p_k^{\beta k}$ avec $\beta_1 = \beta_2 = \dots = \beta_k = 0$
- Si $d > 1$, soit $d = q_1^{\gamma 1} q_2^{\gamma 2} \dots q_r^{\gamma r}$ la décomposition de d en produit de facteurs premiers.

  Alors $q_1, q_2, \dots, q_r$ sont des diviseurs premiers de d, donc ce sont des diviseurs premiers de n, donc ce sont certains des nombres $p_1, p_2, \dots, p_k$.

  On peut donc écrire $d = p_1^{\beta 1} p_2^{\beta 2} \dots p_k^{\beta k}$ où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels .

  (Si le nombre p_i n'apparaît pas dans la décomposition de d, on aura $\beta_i = 0$)

Démontrons que l'on a alors que $\beta_1 \leq \alpha_1$

On sait que d divise n, et $p_1^{\beta 1}$ divise d , donc $p_1^{\beta 1}$ divise n , donc $p_1^{\beta 1}$ divise $p_1^{\alpha 1} p_2^{\alpha 2} \dots p_k^{\alpha k}$.

Si β_1 était strictement supérieur à α_1, alors $p_1^{\beta 1 - \alpha 1}$ diviserait $p_2^{\alpha 2} \dots p_k^{\alpha k}$ donc p_1 diviserait $p_2^{\alpha 2} \dots p_k^{\alpha k}$, ce qui n'est pas possible puisque p_1 n'est pas l'un des nombres $p_2, \dots, p_k$.

On a donc $\beta_1 \leq \alpha_1$. De même on peut justifier que $\beta_2 \leq \alpha_2$, ... , $\beta_k \leq \alpha_k$.

Donc d s'écrit sous la forme $d = p_1^{\beta 1} p_2^{\beta 2} \dots p_k^{\beta k}$ où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1$, $0 \leq \beta_2 \leq \alpha_2$, ... , $0 \leq \beta_k \leq \alpha_k$

Remarque :

Si n a pour décomposition en produit de facteurs premiers $n = p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots p_k^{\alpha k}$,

le nombre de diviseurs naturels de n est alors $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \ldots \times (\alpha_k + 1)$.

En effet tout diviseur naturel peut s'écrire $p_1^{\beta 1}\, p_2^{\beta 2} \ldots p_k^{\beta k}$ et chaque nombre β_i peut prendre les $(\alpha_i + 1)$ valeurs de 0 à α_i .

La décomposition de 200 en produit de facteurs premiers est : $200 = 2^3 \times 5^2$.
Ceci permet de dire que le nombre de diviseurs naturels de 200 est : $(3 + 1) \times (2 + 1) = 4 \times 3 = 12$.

2) PLUS PETIT COMMUN MULTIPLE : PPCM

A) DEFINITION

Exemple :

Pour effectuer le calcul $\frac{65}{18\,372} - \frac{21}{15\,310}$, on peut réduire les fractions au même dénominateur . En l'absence d'autre méthode, on écrit

$$\frac{65}{18\,372} - \frac{21}{15\,310} = \frac{65 \times 15\,310}{18\,372 \times 15\,310} - \frac{21 \times 18\,372}{15\,310 \times 18\,372} = \frac{995\,150}{281\,275\,320} - \frac{385\,812}{281\,275\,320} = \frac{609\,338}{281\,275\,320}$$

On simplifie ensuite $\frac{609\,338}{281\,275\,320}$ en cherchant par exemple le PGCD de 609 338 et de 281 275 320 et on obtient $\frac{199}{91\,860}$.

Si on avait pu prévoir que 91 860 était un multiple commun à 18 372 et à 15 310 (et même que c'était le plus petit multiple commun), les calculs en auraient été simplifiés.
En effet 91 860 étant égal à $18\,372 \times 5$ et à $15\,310 \times 6$, on aurait pu écrire

$$\frac{65}{18\,372} - \frac{21}{15\,310} = \frac{65 \times 5}{18\,372 \times 5} - \frac{21 \times 6}{15\,310 \times 6} = \frac{325}{91\,860} - \frac{126}{91\,860} = \frac{199}{91\,860}$$

La recherche des multiples communs à deux nombres présente donc un intérêt certain pour le calcul.

Propriété-définition :

Soit a et b deux entiers naturels non nuls.
L'ensemble des multiples strictement positifs communs à a et b possède un plus petit élément.
Ce plus petit élément est appelé "plus petit commun multiple" de a et b. On le note PPCM(a ; b).

Preuve :

a et b étant deux entiers naturels non nuls, ils ont au moins un multiple commun strictement positif qui est le produit ab.
L'ensemble des multiples strictement positifs communs à a et b n'est donc pas vide
Cet ensemble, qui est une partie de $\mathbb{N}$ a donc un plus petit élément.
Ce plus petit élément est noté PPCM(a,b).

Remarques :

- PPCM(a ; b) = PPCM(b ; a).
- Si b est multiple de a, PPCM(a , b) = b
- a étant un entier naturel, l'ensemble des multiples de a est égal à l'ensemble des multiples de $-a$.
  On pourra étendre, si besoin est, la notion de PPCM à des nombres entiers relatifs.
  On dira par exemple que PPCM(-15 ; 12) = PPCM(15 ; 12) = 60

B) PROPRIETES

Propriétés :

Soit a et b deux entiers naturels non nuls.

- PGCD(a ; b) divise PPCM(a ; b)
- PGCD(a ; b) × PPCM(a ; b) = $a \times b$
- Si a et b sont premiers entre eux, on a PPCM(a ; b) = $a \times b$
- Si k est un entier naturel non nul, on a PPCM(ka ; kb) = k PPCM(a ; b) (homogénéité)

Preuve :

a et b sont deux entiers naturels non nuls.

- PPCM(a ; b) est un multiple de a , et a est un multiple de PGCD(a ; b)
  Donc PPCM(a ; b) est un multiple de PGCD(a ; b)
  c'est-à-dire PGCD(a ; b) divise PPCM(a ; b)
- Notons D = PGCD(a ; b)
  On peut écrire $a = Da'$ et $b = Db'$ avec a' et b' deux entiers naturels (non nuls) premiers entre eux.
  On a alors $ab = Da' \times Db' = D(a'Db')$

  Posons $p = a'Db'$ on a $p \in \mathbb{N}^*$. On a alors :
  - $p = (a'D)\, b' = ab'$ donc p est multiple de a .
  - $p = a'(Db') = a'b$ donc p est multiple de b .

  p est donc un multiple (strictement positif) commun à a et à b.

  Démontrons que p est le PPCM de a et b.
  Soit M un multiple strictement positif de a et de b.
  On peut écrire $M = ka$ et $M = k'b$ avec $k \in \mathbb{N}^*$ et $k' \in \mathbb{N}^*$
  On a alors : $ka = k'b \Leftrightarrow kDa' = k'Db' \Leftrightarrow ka' = k'b'$

a' et b' étant premiers entre eux, on en déduit que a' divise k' et b' divise k (théorème de Gauss)
On peut alors écrire $k' = a'q'$ et $k = b'q$ avec $q \in \mathbb{N}^*$ et $q' \in \mathbb{N}^*$
On a alors : $M = ka = b'qa = q(ab') = qp$.

M est donc multiple de p, M étant strictement positif, on en déduit que $M \geq p$.
Donc p est le plus petit multiple strictement positif de a et de b.
Donc $p = PPCM(a ; b)$

On a alors par définition de p : $p = a'Db'$ donc $D \times p = Da'Db' = a \times b$
et par conséquent $PGCD(a ; b) \times PPCM(a ; b) = a \times b$

- Si a et b sont premiers entre eux, on a $PGCD(a ; b) = 1$
  La relation précédente permet alors de conclure que $PPCM(a ; b) = a \times b$
- Si k est un entier naturel non nul, on sait que : $PGCD(ka ; kb) = k\,PGCD(a ; b)$
  On a alors : $PPCM(ka ; kb) \times PGCD(ka ; kb) = ka \times kb \Leftrightarrow PPCM(ka ; kb) \times k\,PGCD(a ; b) = k^2\,a\,b$
  $\Leftrightarrow PPCM(ka ; kb) \times k\,PGCD(a ; b) = k^2\,PPCM(a ; b) \times PGCD(a ; b)$
  $\Leftrightarrow PPCM(ka ; kb) = k\,PPCM(a ; b)$

Propriété :

Soit a et b deux entiers naturels non nuls.
L'ensemble des multiples communs à a et à b est l'ensemble des multiples de leur PPCM.

Preuve :
Il est immédiat que si M est multiple de $PPCM(a ; b)$, alors M est multiple de a et de b.
Donc l'ensemble des multiples de $PPCM(a ; b)$ est contenu dans l'ensemble des multiples communs à a et b.

Réciproquement soit M un multiple commun à a et de b.
Notons $D = PGCD(a ; b)$
On sait que l'on peut écrire $a = Da'$ et $b = Db'$ avec a' et b' premiers entre eux . On a alors :
$PPCM(a ; b) \times PGCD(a ; b) = ab \Leftrightarrow PPCM(a ; b) \times D = Da'Db' \Leftrightarrow PPCM(a ; b) = a'Db'$
M étant multiple de a, on peut écrire $M = ka = kDa'$ $k \in \mathbb{Z}$
M étant multiple de b, on peut écrire $M = qb = qDb'$ $q \in \mathbb{Z}$
Donc $ka' = qb'$ avec a' et b' premier entre eux.
Donc a' divise q et b' divise k (Théorème de Gauss)
On peut alors écrire $q = a'q'$ et $k = b'k'$ avec $q' \in \mathbb{Z}$ et $k' \in \mathbb{Z}$
Alors $M = kDa' = b'k'Da' = k'a'Db' = k\,PPCM(a ; b)$
k étant un entier, on en déduit que M est un multiple de $PPCM(a ; b)$.
Donc l'ensemble des multiples communs à a et b est contenu dans l'ensemble des multiples de $PPCM(a ; b)$.

On a donc démontré que l'ensemble des multiples communs à a et à b est l'ensemble des multiples de leur PPCM.

3) PGCD, PPCM ET DECOMPOSITION

Exemple :

L'algorithme d'Euclide permet de justifier que $PGCD(1500 ; 4725) = 75$.
On sait que $PGCD(1500 ; 4725) \times PPCM(1500 ; 4725) = 1500 \times 4725$.
On peut en déduire que $PPCM(1500 ; 4725) = 94500$.
Ce résultat peut être obtenu à partir de la décomposition des nombres en facteurs premiers.
On a $1500 = 2^2 \times 3 \times 5^3$ et $4725 = 3^3 \times 5^2 \times 7$
Si on écrit la décomposition en utilisant les mêmes facteurs premiers pour les deux nombres et en autorisant l'utilisation d'exposants nuls, on peut écrire :
$1500 = 2^2 \times 3^1 \times 5^3 \times 7^0$ et $4725 = 2^0 \times 3^3 \times 5^2 \times 7^1$
On peut alors remarquer que le nombre obtenu en prenant les exposants les plus petits est :
$2^0 \times 3^1 \times 5^2 \times 7^0 = 75 = PGCD(1500 ; 4725)$
et le nombre obtenu en prenant les exposants les plus grands est :
$2^2 \times 3^3 \times 5^3 \times 7^1 = 94500 = PPCM(1500 ; 4725)$

Propriété :

Soit a et b deux entiers naturels supérieurs ou égaux à 2, se décomposant sous la forme :

$$a = p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots p_k^{\alpha k} \quad \text{et} \quad b = p_1^{\beta 1}\, p_2^{\beta 2} \ldots p_k^{\beta k}$$

où $p_1, p_2, \ldots, p_k$ sont des nombres premiers , $\alpha_1, \alpha_2, \ldots, \alpha_k$ et $\beta_1, \beta_2, \ldots, \beta_k$ des entiers naturels éventuellement nuls.
Pour chaque valeur de i entre 1 et k, on pose $\delta_i = \text{minimum}(\alpha_i, \beta_i)$ et $\gamma_i = \text{maximum}(\alpha_i, \beta_i)$.

Alors $PGCD(a ; b) = p_1^{\delta 1}\, p_2^{\delta 2} \ldots p_k^{\delta k}$ et $PPCM(a ; b) = p_1^{\gamma 1}\, p_2^{\gamma 2} \ldots p_k^{\gamma k}$

Preuve :

- Tous les diviseurs de a sont de la forme $d = p_1^{\theta 1} p_2^{\theta 2} \dots p_k^{\theta k}$ où $\theta_1, \theta_2, \dots, \theta_k$ sont des entiers naturels tels que
$0 \le \theta_1 \le \alpha_1$, $0 \le \theta_2 \le \alpha_2$, ... , $0 \le \theta_k \le \alpha_k$.

- Tous les diviseurs de b sont de la forme $D = p_1^{\sigma 1} p_2^{\sigma 2} \dots p_k^{\sigma k}$ où $\sigma_1, \sigma_2, \dots, \sigma_k$ sont des entiers naturels tels que
$0 \le \sigma_1 \le \beta_1$, $0 \le \sigma_2 \le \beta_2$, ... , $0 \le \sigma_k \le \beta_k$.

- Les diviseurs communs à a et b sont alors de la forme $p_1^{\pi 1} p_2^{\pi 2} \dots p_k^{\pi k}$ où $\pi_1, \pi_2, \dots, \pi_k$ sont des entiers naturels tels que
$0 \le \pi_1 \le \alpha_1$, $0 \le \pi_2 \le \alpha_2$, ... , $0 \le \pi_k \le \alpha_k$ et $0 \le \pi_1 \le \beta_1$, $0 \le \pi_2 \le \beta_2$, ... , $0 \le \pi_k \le \beta_k$

On en déduit donc que
$0 \le \pi_1 \le \delta_1$, $0 \le \pi_2 \le \delta_2$, ... , $0 \le \pi_k \le \delta_k$.

Le PGCD de a et b sera obtenu pour des exposants égaux aux plus grandes valeurs possibles des π_i , c'est-à-dire pour des exposants égaux aux δ_i .

On a donc $\text{PGCD}(a ; b) = p_1^{\delta 1} p_2^{\delta 2} \dots p_k^{\delta k}$.

Sachant que $\text{PGCD}(a ; b) \times \text{PPCM}(a ; b) = ab$

On obtient $\text{PPCM}(a ; b) = p_1^{\alpha 1 + \beta 1 - \delta 1} p_2^{\alpha 2 + \beta 2 - \delta 2} \dots p_k^{\alpha k + \beta k - \delta k}$

D'autre part on a $\alpha_i + \beta_i = \text{minimum}(\alpha_i , \beta_i) + \text{maximum}(\alpha_i , \beta_i) = \delta_i + \gamma_i$

donc $\alpha_i + \beta_i - \delta_i = \gamma_i$

et on en déduit $\text{PPCM}(a ; b) = p_1^{\gamma 1} p_2^{\gamma 2} \dots p_k^{\gamma k}$