V. Arithmétique : exposé en termes "contemporains"

Propriété fondamentale des ensembles de multiples

Soit ***a*** un entier relatif et ***Mult(a)*** l'ensemble de ses multiples c'est-à-dire

$$Mult\,(a) = \{m \in Z \,/\, qu'il\ existe\ \ k \in Z \,/\, m = k.a\}$$

Cet ensemble est (sauf dans le cas de $a=0$) infini

Par exemple

Mult(2) est l'ensemble des entiers relatifs pairs

$$Mult\,(6) = \{ \ldots, -18, -12, -6, 0, 6, 12, 18, 24, \ldots\}$$

Lorsque $m \in Mult(a)$ on note $a \mid m$ qui se lit

a divise m

ou a est un diviseur de m

ou encore m est un multiple de a

Propriété fondamentale des ensembles de multiples

Propriété

On a :

1) Si m et m' sont dans $Mult\ (a)$

Alors $m-m'$ est dans $Mult\ (a)$.

2) Si m est dans $Mult(a)$ et q dans Z

Alors $q.m$ est dans $Mult\ (a)$.

Propriété fondamentale des ensembles de multiples

Les démonstrations sont assez évidentes

1) Si ***m*** et ***m'*** sont dans ***Mult (a)***

Alors ***m-m'*** est dans ***Mult (a).***

En effet ***m et m'*** dans ***Mult(a)*** signifie qu'on peut trouver deux entiers relatifs ***k et k'*** tels que ***m= k.a*** et ***m'=k'.a***

alors ***m-m'= k.a-k'.a= (k-k').a*** donc ***m-m'*** est multiple de ***a***

2) Si ***m*** est dans ***Mult(a)*** et ***q*** dans ***Z***

Alors ***q.m*** est dans ***Mult (a) .***

De même on trouve un entier relatif ***k*** tel que ***m=k.a*** donc pour un entier quelconque ***q*** on a

q.m= q.(k.a)= (q.k).a

donc ***q.m*** est un multiple de ***a.***

La propriété précédente a été qualifiée de ''fondamentale'' car elle caractérise les ensembles de multiples :

Soit ***B*** une partie non vide de ***Z*** satisfaisant les propriétés 1) et 2).

Alors il existe un entier relatif ***a*** tel que ***B=Mult (a)***

En fait il existe exactement deux entiers relatifs ***a*** tels que

B= Mult(a)

et ces deux entiers sont opposés

<u>Démonstration</u> :

0 est dans B : Comme ***B*** est non vide on trouve au moins un élément dans ***B*** soit ***b.*** Une application de 1) avec ***m=m'=b*** donne

m-m'=b-b=0 est dans ***B.***

<u>Démonstration</u> :

0 est dans *B*

Si *b* est dans *B* , *Mult (b)* est inclus dans B : Une application de 2) avec ***m=b*** donne que ***Mult(b)*** est inclus dans ***B***.

Démonstration :

0 est dans *B*

Si *b* est dans *B* , *Mult (b)* est inclus dans B :

Soit B^{+}* l'ensemble des éléments strictement positifs de *B*.

- **Si B^{+}* est vide alors *B* est réduit à *{0}* donc égal à *Mult(0).***

  En effet, si ce n'était pas le cas ***B*** contiendrait un élément non nul ***m*** et compte tenu de 1) et du fait que ***0*** est dans ***B, B*** contient également ***-m*** or parmi ***m*** et ***-m*** l'un serait alors strictement positif.

Démonstration :

0 est dans *B*

Si *b* est dans *B* , *Mult (b)* est inclus dans B :

Soit B^{+}* l'ensemble des éléments strictement positifs de *B*.

- **Si B^{+}* est vide alors *B* est réduit à *{0}* donc égal à *Mult(0).***

- **Si B^{+}* est non vide.**
  Soit **a** le plus petit élément de B^{+}* , ***Mult (a)*** est inclus dans ***B***.
  Si on n'avait pas ***B= Mult(a)*** alors on trouverait dans ***B*** un élément ***b*** qui n'est pas dans ***Mult(a)***, compte tenu de 1) on peut supposer cet élément strictement positif. Si on effectue la division entière de ***b*** par ***a*** on obtient

$$b = q.a + r \text{ avec } r \in \{0,1,...,a-1\}$$

Mais ***r*** est non nul, car sinon ***b*** serait dans ***Mult (a)***. Une application de 1) donne

$$r = b - q.a \in B$$

donc ***a*** ne serait pas le plus petit élément de B^{+}*. Donc ***B= Mult (a)***

Soit ***A*** et ***B*** deux parties de **Z** , on pose :

1) A∩B : l'ensemble des entiers qui sont à la fois dans ***A*** et dans ***B***.

Par exemple : Si ***A*** est l'ensemble de nombres pairs et ***B*** celui des multiple de ***7*** , ***A∩B*** est l'ensemble des multiples de 14

A={ …., -10, -8, -6,-4,-2,0 , 2,4,6,8,10,12,14,16,….}

B= {…-21, -14,-7, 0,7,14,21,28,…..}

A∩B= { …., -14, 0, 14, 28,…}

2) A+B : l'ensemble des entiers qu'on peut obtenir comme somme d'un élément de ***A*** et d'un élément de ***B***.

Avec les ensembles précédents ***21+6= 27*** est dans ***A+B*** puisque c'est la somme d'un élément de ***A*** et d'un élément de ***B***

Propriété : Si A et B sont des ensembles de multiples

alors $A \cap B$ et $A+B$

sont aussi des ensembles de multiples.

Démonstration : Soit A et B des ensembles de multiples.

$A = Mult(a)$ et $B = Mult\ (b)$.

1 -Si m et m' sont dans $A \cap B$ alors

m et m' sont dans A et dans B donc $m-m' \in A$ et $m-m' \in B$

donc $m-m'$ est dans $A \cap B$. Donc $A \cap B$ satisfait 1).

-Si $m \in A \cap B$ et l un entier alors comme $m \in A$, $l.m \in A$,

de même $l.m \in B$ donc $l.m \in A \cap B$. Donc $A \cap B$ satisfait 2).

$A \cap B$ est donc un ensemble de multiples.

Démonstration : Soit A et B des ensembles de multiples.

$A = Mult(a)$ et $B = Mult\ (b)$.

2 - Si m et m' sont dans $A+B$ alors m et m' sont sommes d'un multiple de a et d'un multiple de b, donc de la forme

$m= qa+kb$ et $m'= q'a+k'b$.

Alors $m-m'= (q-q')a+(k-k')b$ est dans $A+B$. Donc $A+B$ satisfait 1)

- Si m est dans $A+B$ et l un entier. Comme m est de la forme

$m= q.a+k.b$ on a $l.m= q.l.a+k.l.b$ est dans $A+B$.

Donc $A+B$ satisfait 2).

$A+B$ est donc un ensemble de multiples.

Application: Soient ***a*** et ***b*** des entiers non nuls.

1) Il existe un entier ***P*** tel que
Mult(a) $\cap$ ***Mult (b) = Mult (P)***.

2) Il existe un entier ***D*** tel que
Mult(a) + ***Mult (b) = Mult (D)***.

Propriété : Soit ***a*** et ***b*** des entiers non nuls.

Soit ***P*** un entier tel que ***Mult(a)*** $\cap$ ***Mult (b) = Mult (P)***.

Alors

a) ***P*** est un multiple commun à ***a*** et ***b***

b) Si ***p*** est un multiple commun à ***a*** et ***b***, ***p*** est un multiple de ***P***.

<u>Propriété</u> : Soit ***a*** et ***b*** des entiers non nuls.

Soit ***D*** un entier tel que ***Mult(a) +Mult (b) = Mult (D).***

Alors

a) ***D*** est un diviseur commun à ***a*** et ***b***

b) Si ***d*** est un diviseur commun à ***a*** et ***b***, ***d*** est un diviseur de ***D***.

Démonstration : La première propriété est évidente.

Deuxième propriété : Soit ***a*** et ***b*** des entiers non nuls. Soit ***D*** un entier tel que ***Mult(a) +Mult (b) = Mult (D).***

L'entier ***a*** peut s'écrire ***a = 1.a+0.b*** donc est dans ***Mult(D), D*** est donc un diviseur de ***a.*** De même, ***D*** est un diviseur de ***b***.

Soit ***d*** un diviseur commun à ***a*** et ***b***, alors les multiples de ***a*** sont des multiples de ***d*** et ceux de ***b*** également, autrement dit ***Mult (a)*** est inclus dans ***Mult (d)*** et ***Mult(b)*** inclus dans ***Mult (d)***. Comme ***Mult(d)*** est un ensemble de multiples ***Mult(a)+Mult(b)*** est contenu dans ***Mult(d)***, c'est-à-dire ***Mult(D)*** contenu dans ***Mult(d)*** ce qui signifie que ***d*** est un diviseur de ***D***.

Définition : Soit ***a*** et ***b*** deux entiers non nuls,

Les entiers ***P*** tels que ***Mult(a)*** ∩***Mult (b) = Mult (P)*** sont appelés des ***PPCM*** de ***a*** et de ***b.***

Les entiers ***D*** tels que ***Mult(a) +Mult (b) = Mult (D)*** sont appelés des ***PGCD*** de ***a*** et de ***b.***

Remarques :

Soit ***a*** et ***b*** deux entiers ils admettent deux ***PPCM*** et ***PGCD*** qui sont opposés. En effet, si ***Mult(a)*** ∩***Mult (b) = Mult (P)*** alors

Mult(a) ∩***Mult (b) = Mult (-P)*** donc si ***P*** est un ***PPCM*** de ***a*** et de ***b*** **,** ***-P*** également.

En effet, si ***Mult(a) +Mult (b) = Mult (D)*** alors

Mult(a) +Mult (b) = Mult (-D) donc si ***D*** est un ***PGCD*** de ***a*** et de ***b*** **,** ***-D*** également.

Parmi les deux ***PPCM*** celui qui est positif est appelé ***LE PPCM***

Parmi les deux ***PGCD*** celui qui est positif est appelé ***LE PGCD***

Théorème de Bezout : Soit ***a*** et ***b*** deux entiers non nuls.

Soit ***D*** un ***PCGD*** de ***a*** et de ***b.***
Alors il existe deux entiers ***u*** et ***v*** tels que

$$D = au+bv .$$

C'est une évidence : ***D*** est un diviseur commun de ***a*** et de ***b*** donc est dans ***Mult (a)+Mult(b).***

Définition*:* Deux entiers ayant ***1*** pour ***PGCD*** sont dit ***premiers entre eux***.

<u>Réciproque du théorème de Bezout</u> ***:*** S'il existe deux entiers ***u*** et ***v*** tels que ***1= au+bv*** alors ***a*** et ***b*** sont premiers entre eux**.**

<u>Démonstration</u> : En effet la relation ***1= au+bv*** signifie que ***1*** est un multiple du ***PGCD*** de ***a*** et ***b*** (ou que ***le PGCD*** est un diviseur de ***1***)

Théorème de Gauss-Euclide : Soit ***a, b*** et ***c*** trois entiers entiers non nuls. Si ***a|b.c*** et si ***a*** et ***b*** sont premiers entre eux, alors ***a|c.***

Démonstration : ***a*** et ***b***, étant premiers entre eux on trouve deux entiers ***u*** et ***v*** tels que ***1= a.u+b.v .*** Donc ***c=c.a.u+c.b.v.*** Comme ***a|b.c*** on trouve un entier ***k*** tel que ***b.c= k.a*** donc

$$c=c.a.u+a.k.v= a.(c.u+k.v)$$

et donc ***a|c.***

L'algorithme d'Euclide permet de calculer le (les) PCGD de deux entiers a et b donnés, mais aussi de résoudre le problème de Bezout c'est-à-dire de trouver les couples d'entiers (u,v) tel que a.u+b.v=D :

Des entiers a et b étant donnés écrivons les divisions entières successives de a par b (comme indiqué dans les "éléments")

$$a = b.q_1 + r_1 \text{ avec } r_1 \in \{0,1,...,b-1\}$$

$$b = r_1.q_2 + r_2 \text{ avec } r_2 \in \{0,1,...,r_1-1\}$$

$$r_1 = r_2.q_3 + r_3 \text{ avec } r_3 \in \{0,1,...,r_2-1\}$$

…

$$r_{n-2} = r_{n-1}.q_n + r_n \text{ avec } r_n \in \{0,1,...,r_{n-1}-1\}$$

$$r_{n-1} = r_n.q_{n+1} + 0$$

Le fait que le processus finit par fournir un reste nul provient du fait que $b > r_1 > r_2 > .... > r_n$ et que tous les restes sont des entiers positifs ou nuls.

Le dernier reste non nul est un ***PGCD*** de ***a*** et ***b,*** cela a déjà été vu lors de l'étude du livre VII des éléments.

.

Une ré-écriture astucieuse de l'algorithme permet de trouver une solution du problème de Bezout.

$a = bq_1 + r_1$ avec $r_1 \in \{0,1,...,b-1\}$ donc $r_1 = a - bq_1$

$b = r_1 q_2 + r_2$ avec $r_2 \in \{0,1,...,r_1-1\}$ donc $r_2 = b - q_2 r_1$

$r_1 = r_2 q_3 + r_3$ avec $r_3 \in \{0,1,...,r_2-1\}$ donc $r_3 = r_1 - q_3 r_2$

…

$r_{n-2} = r_{n-1}.q_n + r_n$ avec $r_n \in \{0,1,...,r_{n-1}-1\}$ donc $r_n = r_{n-2} - q_n.r_{n-1}$

$r_{n-1} = r_n . q_{n+1} + 0.$

On a vu que $r_n = D$ est **PGCD** de a et b. Donc $D = r_{n-2} - q_n.r_{n-1}$ en remplaçant successivement les différents restes apparaissant dans le second membre par les expressions des restes à l'aide des quotients et reste précédents on obtient une expression de D sous la forme voulue.

Si on traite, par exemple, le cas de $a = 562$ et $b = 224$

On a

$a = b.2 + 114$ ($q_1 = 2$, $r_1 = 114$) donc $r_1 = a - b.q_1 = a - 2.b$

$b = 114.1 + 110$ ($q_2 = 1$, $r_2 = 110$) donc $r_2 = b - q_2 r_1 = b - 114.1$

$114 = 110.1 + 4$ ($q_3 = 1$, $r_3 = 4$) donc $r_3 = r_1 - q_3 r_2 = 114 - 110.1$

$110 = 4.27 + 2$ ($q_4 = 27$, $r_4 = 2$) donc $r_4 = r_2 - q_2 r_3 = 110 - 4.27$

$4 = 2.2 + 0$ ($q_5 = 2$, $r_5 = 0$)

Le dernier reste non nul est $r_4 = 2$ c'est le ***PCGD*** de ***562*** et ***224***.

Résolution partielle du problème de Bezout

$r_4 = 110 - 4.27 = 110 - r_3 . 27 = 110 - (114 - 110)\ 27$

$= 110\ (1+27) - 114 . 27 = r_2 . 28 - 114 . 27$

$= (b - 114) . 28 - 114 . 27 = b . 28 + 114\ (-28 - 27)$

$= b . 28 - r_1 . 55 = b . 28 - (a - b . 2)\ 55 = b . (28 + 2 . 55) - a . 55$

$= b . 138 - a\ 55.$

Ce qui donne finalement la relation

$$2 = 224 . 138 - 562 . 55$$

Donc $(u_0, v_0) = (138, -55)$ satisfait $PGCD\ (562, 224) = 224\ u + 562\ v$

Le couple (u_0,v_0) solution du problème de Bezout ainsi obtenu n'est *a priori* pas l'unique solution de ce problème. Supposons que (u,v) soit une solution. On a alors simultanément

$$a.u_0 + b.v_0 = D \quad \text{et} \quad a.u+b.v=D$$

Donc par différence on obtient

$$a.(u_0-u)+b.(v_0-v)=0$$

donc $$a.(u_0-u)= b.(v-v_0)\ .$$

Par ailleurs a et b sont des multiples de D, précisément

$$a = a'.D \quad \text{et} \quad b= b'.D,$$

on a a' et b' premiers entre eux puisque en simplifiant par D la relation $a.u_0+b.v_0=D$ il vient $a'.u_0+b'.v_0=1$, qui entraine que a' et b' sont premiers entre eux (réciproque du théorème de Bezout).
On obtient, par simplification de $a.(u_0-u)= b.(v-v_0)$
la relation $$a'.(u_0-u)= b'.(v-v_0)$$

Donc a' est un diviseur de $b'.(v-v_0)$ comme a' et b' sont premiers entre eux, a' est donc un diviseur de $v-v_0$: il existe un entier k tel que

$$v-v_0= k.a' \text{ (donc } v= v_0+k.a')$$

par substitution dans (1) on obtient

$$a' .(u_0-u) = b'.k.a‘$$

d'où $u= u_0-k.b'$.

Réciproquement, un couple de la forme $(u_0-k.b', v_0+k.a')$ avec k un entier satisfait la relation de Bezout puisque

$$a.(u_0-kb')+ b.(v_0+ka')= a.u_0-a.k.b'+b.v_0-b.k.a'$$

$$=(a.u_0+b.v_0) + a'.D.k.b'-b'.D.k.a'$$

$$= a.u_0+b.v_0=D.$$

Si on reprend l'exemple précédent le couple $(u_0,v_0)= (138, -55)$ est solution du problème de Bezout $2=224\,u+562\,v$.

Supposons que ***(u,v)*** en soit une autre solution. On a alors simultanément

$$224 \cdot 138 + 562 \cdot (-55) = 2 \quad (a) \qquad \text{et} \qquad 224 \cdot u + 562 \cdot v = 2$$

Par différence on obtient $224 \cdot (138-u) + 562 \cdot (-55-v) = 0$

donc $224(138-u) = 562(55+v) \qquad (b)$

Par ailleurs,

$$224 = 112 \cdot 2 \qquad \text{et} \qquad 562 = 281.2,$$

En simplifiant par ***2*** la relation ***(b)***, on obtient <la relation

$$112.(138-u) = 281.(55+v) \ (c).$$

Donc $112 \mid 281.(55+v)$, mais comme ***112*** et ***281*** sont premiers entre eux

$$112 \mid v+55 :$$

Il existe un entier ***k*** tel que $v+55 = k112$ (donc $v = -55+112.k$).

Par substitution dans ***(c)***

on obtient ***112. (138-u) = 281. k .112*** d'où ***u= 138-281. k***.

Réciproquement, un couple de la forme ***(138-281. k, -55+112.k)*** avec ***k*** un entier satisfait la relation de Bezout puisque

$$224(138-281k)+562(-55+112.k)$$

$$= 224 . 138-224 . k . 281+562. (-55)+562 . k.112$$

$$= (224 . 138+562. (-55)) -2.112 . k . 281+2.281 . k.112$$

$$= 224 . 138+562. (-55)=2.$$

Donc l'ensemble des solutions du problème de Bezout

$$2=224 .u+562. v$$

est l'ensemble des couples (138-281. k, -55+112.k) avec k un entier quelconque.

Le problème de Bezout est lié à un problème très ancien : le "lemme Chinois" : Le comptage des effectifs d'une armée était un problème de gestion des armées extrêmement important dans la Chine ancienne. Le procédé employé par les officiers était le suivant : On demandait aux soldats de se ranger une première fois en rang par $\boldsymbol{P}$ on ne comptait que le nombre $\boldsymbol{n_P}$ des soldats en excès (ceux qui ne pouvaient pas se ranger), on leur ordonnait ensuite de se ranger par rangée de $\boldsymbol{Q}$, une nouvelle fois on comptait le nombre $\boldsymbol{n_Q}$ des soldats en excès.

Les officiers disposaient de tables où ils pouvaient lire le nombre de soldats présents. (Le procédé peut sembler idiot puisque l'on pourrait par exemple compter le nombre de rangées de $\boldsymbol{P}$ soldats multiplier ce nombre par $\boldsymbol{P}$ puis ajouter les soldats en excès, mais n'oublions pas que durant toute l'antiquité la multiplication était seulement dominée par une toute petite minorité de personne et certainement pas par les officiers subalternes chargés du comptage). Il existait des variantes locales sur les valeurs de $\boldsymbol{P}$ et $\boldsymbol{Q}$.

Si on mets en équation le problème de l'officier chinois.

Soit X le nombre de soldats. Lorsqu'ils se rangent en rang par P il reste n_P soldats qui ne trouvent pas de place donc il existe un entier K (le nombre de rang) tel que

$$X = K.P + n_P \quad (p)$$

De même il existe un entiers L tel que

$$X = L.Q + n_Q \quad (q).$$

On a par différence entre les relations (p) et (q)

$$0 = K.P - L.Q + n_P - n_Q$$

Donc $$n_P - n_Q = L.Q - K.P \in Mult(Q) + Mult(P).$$

donc on a nécessairement $n_P - n_Q$ multiple du $PGCD$ de P et Q. (si cela n'a pas lieu c'est que les soldats n'ont pas exécuté les ordres correctement).

Soit D le $PGCD$ de P et Q, on a $P = P' .D$ et $Q= Q'.D.$

On a $X= K'.P' + n_P$ et $X= L'.Q' + n_Q$

Avec $K' = KD$ et $L' = LD.$ Ici on a de plus P' et Q' premiers entre eux

C'est d'ailleurs avec des valeurs de P et Q premiers entre eux qu'opéraient les chinois.

On suppose dans la suite que ***P*** et ***Q*** sont premiers entre eux. On peut trouver deux entiers ***u*** et ***v*** tels que $u.P+ v.Q=1$.

Alors $u.P\ .n_Q = (1-v.Q)\ n_Q = n_Q – v.\ Q.n_Q$

Et $v.Q\ .n_P = (1-u.P)\ n_P = n_P – u.\ P.n_P$

En sommant il vient

$u.P.n_Q + v.Q.n_P = n_Q + (-v.n_Q+v.n_P)Q$ ***(le reste de la division par Q vaut n_Q)***

Et

$u.P.n_Q+ v.Q.n_P= n_P+ (u.n_Q – u.n_P).P$ ***(le reste de la division par P vaut n_p)***

Donc le nombre $S_0= u.P.n_Q+ v.Q.n_P$ est **une** solution du problème chinois.

Supposons que S soit une autre solution du problème chinois alors on a simultanément existence de quatre entiers K_0, L_0, K et L tels que

$$S_0 = K_0.P + n_P,\ S = K.P + n_P,\ S_0 = L_0.Q + n_Q \text{ et } S = L.Q + n_Q$$

Par différence on obtient

$$S_0 - S = (K_0 - K).P \text{ et } S_0 - S = (L_0 - L).Q$$

Donc $S_0 - S$ doit être un multiple commun de P et Q et donc doit être un multiple du ***PPCM*** de P et Q. Mais P et Q sont premiers entre eux donc leur ***PPCM*** vaut leur produit [(1)]

Donc il existe un entier M tel que $S = S_0 + MPQ$.

---

(1) Ceci sera montré plus loin.

Réciproquement si $S = S_0 + MPQ$ comme $S_0 = KP + n_P$ on a

$S = KP + n_P + MPQ$ donc S est bien de la forme $S = KP + n_P$

De même S est de la forme $S = LQ + nQ$.

Finalement

les solutions du problème chinois sont les entiers de la forme $S = u.P.nQ + v.Q.nP + MPQ$ avec M un entier quelconque

Dans le cas où ***P*** et ***Q*** sont assez grand, la différence entre deux solutions successives du problème chinois est suffisamment grande pour que, pratiquement, il ne reste qu'une solution vraisemblable, c'est ce fait qu'utilisaient les officiers Chinois.

Supposons que les soldats se soient rangé par **437 = 23.19** puis par **899= 29.31** (les deux entiers **437** et **899** sont premiers entre eux, Une solution du problème de Bezout est **1= 35. 899+ (-72).437**

Si dans le premier rangement il reste **245** soldats non rangés et que dans le second il reste **123** soldats alors a un multiple de **437.899= 393 863** près le nombre de soldats vaut **2 768 955** parmi les valeurs possibles du nombre de soldats on trouve **11 914** . (la solution suivante est 405777 sans doute plus grande que n'importe quelle armée de l'époque !)

La décomposition en produit de nombres premiers fournit une seconde méthode de calcul des PGCD et PPCM

On a vu que tous les nombres entiers naturels se décomposent en produit de nombres premiers, précisément si N est un entier naturel il existe une famille de nombres premiers $p_1<p_2<....<p_k$ et une famille d'entiers strictement positifs $n_1, n_2, ..., n_k$ tels que

$$N= p_1^{n_1}.p_2^{n_2}..... p_k^{n_k}$$

Cette décomposition est unique.

Lorsque $N = p_1^{n_1}.p_2^{n_2}..... p_k^{n_k}$ où $p_1<p_2<....<p_k$ est une famille de nombres premiers et $n_1, n_2, ..., n_k$ est une famille d'entiers strictement positifs, alors les diviseurs de N sont les entiers dont la décomposition est de la forme

$$p_1^{s_1}.p_2^{s_2}..... p_k^{s_k}$$

Où $s_1, s_2, ... , s_k$ sont des entiers naturels tels que $0 \leq s_i \leq n_i$. Les multiples de N sont les entiers pour lesquels la décomposition contient au moins les facteurs $p_1^{n_1}.p_2^{n_2}..... p_k^{n_k}$.

Par exemple, $12 = 2^2.3^1$, ($p_1=2$, $n_1=2$, $p_2=3$,$n_2=1$)
ses diviseurs positifs sont

$1= 2^0.3^0$, $3= 2^0.3^1$, $2= 2^1.3^0$, $6= 2^1.3^1$, $4= 2^2.3^0$ et $12= 2^2.3^1$

Lorsque $N = p_1^{n_1}.p_2^{n_2}..... p_k^{n_k}$ et $M = q_1^{m_1}.q_2^{m_2}..... q_l^{m_l}$

Où $p_1<p_2<....<p_k$ et $q_1<q_2<....<q_l$ sont des familles de nombres premiers, $n_1,n_2,...,n_k$ et $m_1,m_2,...,m_l$ des familles d'entiers strictement positifs, alors quitte à rajouter des facteurs de la forme $q_u^{\,0}$ dans la décomposition de N et des facteurs de la forme $p_t^{\,0}$ dans celle de M on peut supposer que les deux familles intervenant dans les décompositions de N et M sont les mêmes, autrement dit

$$N = r_1^{n_1}.r_2^{n_2}..... r_s^{n_s} \quad \text{et} \quad M = r_1^{m_1}.r_2^{m_2}..... r_s^{m_s}$$

avec $r_1<r_2<....<r_s$ est une famille de nombres premiers, $n_1,n_2,...,n_s$ et $m_1,m_2,...,m_{ls}$ des familles d'entiers positifs **ou nuls.**

Lorsque

$$N = r_1^{n_1}.r_2^{n_2}..... r_s^{n_s} \quad \text{et} \quad M = r_1^{m_1}.r_2^{m_2}..... r_s^{m_s}$$

avec $r_1 < r_2 < .... < r_s$ est une famille de nombres premiers, $n_1, n_2, ..., n_s$ et $m_1, m_2, ..., m_s$ des familles d'entiers positifs ou nuls. D'après la remarque faite sur l'ensemble des diviseurs d'un entier en fonction de sa décomposition le plus grand diviseur commun de ces deux entiers est

$$r_1^{i_1}.r_2^{i_2}..... r_s^{i_s} \quad \text{où} \quad i_l = Inf\ (n_l, m_l)$$

et le plus petit multiple commun est

$$r_1^{s_1}.r_2^{s_2}..... r_s^{s_s} \quad \text{où} \quad s_l = Sup\ (n_l, m_l)$$

Par exemple

$$12 = 2^2.3^1.7^0 \quad \text{et} \quad 21 = 2^0.3^1.7^1$$

le plus grand diviseur commun de ces deux entiers est

$$3 = 2^0.3^1.7^0$$

et le plus petit multiple commun est

$$84 = 2^2.3^1.7^1$$

$$N = r_1^{n_1}.r_2^{n_2}..... r_s^{n_s} \quad \text{et} \quad M = r_1^{m_1}.r_2^{m_2}..... r_s^{m_s}$$

avec $r_1<r_2<....<r_l$ est une famille de nombres premiers, $n_1, n_2, ..., n_k$ et $m_1, m_2, ..., m_l$ des familles d'entiers positifs ou nuls.

Le plus grand diviseur commun de ces deux entiers est

$$r_1^{i_1}.r_2^{i_2}..... r_s^{i_s} \quad \text{où} \quad i_l = Inf\ (n_l, m_l)$$

et le plus petit multiple commun est

$$r_1^{s_1}.r_2^{s_2}..... r_s^{s_s} \quad \text{où} \quad s_l = Sup\ (n_l, m_l)$$

On a $s_l + i_l = Inf\ (n_l, m_l) + Sup\ (n_l, m_l) = n_l + m_l$

Donc le produit du pgcd et du ppcm de N et M vaut $N.M$