Chap. 4 – Arithmétique / Division euclidienne
1. Division euclidienne

N ensemble d'entiers naturels $\mathbb{N} = \{0, 1, 2, \ldots\}$
Z ensemble d'entiers relatifs $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{N}^+$ ensemble d'entiers strictement positifs $\mathbb{N}^+ = \{1, 2, \ldots\}$

L'arithmétique est l'étude de ces ensembles
En plus de l'addition, la soustraction et la multiplication, on peut faire une quatrième opération fondamentale.

Théorème 1
Soient a et b des entiers. Si $b \neq 0$ il existe 2 entiers q et r vérifiant à la fois :

$a = bq + r,\ 0 \leq r < |b|$

Les nombres q et r sont les seuls à vérifier ces deux conditions.

Démo : *Supposons d'abord b>0. Soit E l'ensemble des entiers positifs ou nuls de la forme a – bk, avec k entier relatif. Alors E n'est pas vide car il contient toujours a si a est positif, et a – ba si a est négatif. Notons r le plus petit élément de E. D'une part r≥0, et d'autre part il existe q tel que r = a – bq. Si l'on avait b≤r le nombre r – b serait positif, et comme r – b = a – b(q+1) il serait dans l'ensemble E, ce qui est en contradiction avec la définition de r, puisque r – b < r. Par conséquent 0 ≤ r < b. Dans le cas b < 0 la division euclidienne de a par (-b) donne deux entiers q_1 et r vérifiant les conditions $a = (-b)q_1 + r$ et $0 \leq r < -b$. Si l'on pose $q = -q_1$ on a : $a = bq + r$ et $0 \leq r < |b|$*
Il reste à voir que r et q sont uniques. Supposons que R et Q vérifient les mêmes conditions. Puisque bq + r = bQ + R nous avons b(Q-q) = r – R. Si Q – q n'était pas nul le membre de gauche aurait une valeur absolue supérieure ou égale à |b|, alors que la valeur absolue du membre de droite serait strictement inférieure à |b|. Comme c'est impossible Q = q, et par conséquent r = R.
Le calcul de q et de r s'appelle la division euclidienne de a par b, le nombre q est le quotient de la division, et r est le reste.

Exemple 1
La division euclidienne de 150 par 11 donne le quotient 13 et le reste 7. La division euclidienne de –80 par 7 donne le quotient –12 et le reste 4.

Théorème 2
Si c divise a et c divise b alors tout nombre de la forme ua + vb avec u et v dans Z est divisible par c. En particulier c divise a – b et a + b

Démo : *S'il existe q1 et q2 tels que a = cq1 et b = cq2 alors ua + vb = c(uq1 + vq2) et c divise ua + vb.*

2. Nombres premiers

Un élément de $\mathbb{N}^+$ strictement supérieur à 1, qui n'a pour diviseurs dans $\mathbb{N}^+$ que 1 et lui-même, s'appelle un nombre premier. En d'autres termes un nombre premier est un élément minimal dans l'ensemble $\mathbb{N}^+$ privé de 1.

Théorème 3
Si n est un entier strictement supérieur à 1 son plus petit diviseur strictement supérieur à 1 est un nombre premier.

Démo : *L'ensemble des diviseurs de n strictement supérieurs à 1 n'est pas vide puisqu'il contient n lui-même ; notons p son plus petit élément. Si p n'était pas premier il aurait un diviseur u autre que 1 et p. Alors u diviserait n car u divise p et p divise n. Par conséquent u serait un diviseur de n plus grand que 1 et strictement inférieur à p. Comme il n'en existe pas, u n'existe pas, et p est premier.*

La liste des diviseurs d'un nombre n, ordonnée par la relation ≤, commence par 1, et finit par n ; le théorème 3 dit que le deuxième élément de cette liste est toujours un nombre premier.

Exemple 2

Quelques entiers et la liste de leur diviseurs.

1 {1}
5 {1, 5}
18 {1, 2, 3, 6, 9, 18}
100 {1, 2, 4, 5, 10, 20, 25, 50, 100}

On peut constater une certaine forme de symétrie, qui s'explique facilement. Si d est un diviseur de n il existe e tel que n = de, et ce nombre e est lui aussi un diviseur de n. Nous pouvons énoncer cette remarque sous forme de théorème.

Théorème 4

Dans la liste des diviseurs de n le produit de deux diviseurs placé symétriquement par rapport au milieu de la liste est égal à n.

On en déduit la propriété suivante.

Théorème 5

Un entier n ≥ 3 qui n'est divisible par aucun des nombres compris entre 2 et sqrt(n) est premier.

Théorème 6

Tout élément de N^+ supérieur ou égal à 2 est soit un nombre premier, soit un produit de nombres premiers *(démonstration par induction)*.

Ce théorème signifie qu'en multipliant ensemble les puissances des nombres premiers on obtient tous les entiers supérieurs ou égaux à 2.

Le calcul des nombres premiers dont le produit vaut n s'appelle la *décomposition en facteurs premiers* de n, et le résultat de ce calcul la *factorisation* de n.

Méthode pour décomposer un nombre en facteurs premiers

1. déterminer le plus petit diviseur de n autre que 1 ; c'est le plus petit facteur premier de n,
2. diviser n par ce facteur premier, ce qui donne m pour quotient,
3. si m > 1 recommencer à partir du 1 en remplaçant n par m.

Exemple 3

2200 2
1100 2
550 2
275 5
55 5
11 *1*
1 Le résultat de cette décomposition est $2200 = 2^3*5^2*11$

Remarque
Cette méthode s'applique sans difficulté aux entiers pas très grands. La difficulté matérielle à décomposer les grands nombres en facteurs premiers est utilisée comme rempart dans certaines méthodes de cryptographie.

Théorème 7
Il existe une infinité de nombres premiers.

Démo : *Soit $p_1, p_2, ..., p_k$ des nombres premiers, et notons p un facteur premier du nombre $n = p_1p_2...p_k + 1$. Il est différent de tous les p_i sinon, divisant à la fois n et le produit $p_1p_2...p_k$ il devrait diviser leur différence qui vaut 1, ce qui n'est pas possible. Nous avons donc un procédé permettant de rajouter à tout ensemble fini de nombres premiers des nombres premiers qui ne sont pas dans cet ensemble. Il en résulte que l'ensemble des nombres premiers n'est pas un ensemble fini.*

Exemple 4
Voyons quels nombres premiers sont obtenus quand on suit la méthode employée pour démontrer le théorème 7. Au départ l'ensemble de nombres premiers connus n'a que 2 pour élément. A chaque étape nous calculons $n = p_1p_2...p_k + 1$, nous le factorisons, et nous ajoutons ses facteurs premiers à l'ensemble des nombres premiers connus, puis nous recommençons.

nombres premiers connus	*n*	*factorisation*
{2}	*3*	*3*
{2, 3}	*7*	*7*
{2, 3, 7}	*43*	*43*
{2, 3, 7, 43}	*1807*	*13*139*
{2, 3, 7, 43, 13, 139}	*3263443*	*3263443*
{2, 3, 7, 43, 13, 139, 3263443}	*10650056950807*	*547*607*1033*31051*

3. PGCD et PPCM

Soient a et b deux éléments de N^+. Les éléments de N^+ qui divisent à la fois a et b sont tous compris entre 1 et le plus petit des deux nombres a et b ; ils forment donc un ensemble fini. Comme cet ensemble n'est pas vide, puisqu'il contient 1, il possède un plus grand élément pour la relation <=. Il est appelé le plus grand commun diviseur de a et de b, le PGCD. Il est noté $a \wedge b$

Quand deux nombres entiers ont leur PGCD égal à 1 on dit qu'ils sont premiers entre eux.

On décide aussi que le PGCD de deux éléments non nuls de Z est le PGCD de leurs valeurs absolues, et que $a \wedge 0 = a$

Exemple 5
Calculons $36 \wedge 90$ en nous servant uniquement de la définition. Nous déterminons d'abord la liste des diviseurs de 36 et de 90 ; nous en déduisons la liste de leurs diviseurs communs, et nous constatons alors que le plus grand diviseur commun à 36 et 90 est 18.
diviseurs de 36 : {1, 2, 3, 4, 6, 9, 12, 18, 36}
diviseurs de 90 : {1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90}
diviseurs communs à 36 et 90 : {1, 2, 3, 6, 9, 18}

On remarquera que l'ensemble des diviseurs communs à 36 et 90 coïncide avec l'ensemble des diviseurs de 18, leur PGCD. C'est un fait général.

Propriétés du PGCD

1) $a \wedge b = b \wedge a$
2) $a \wedge 1 = 1$
3) $a \wedge a = a$
4) $a \wedge b = b$ ssi b divise a
5) si p est premier $a \wedge p = p$ quand p divise a et 1 quand p ne divise pas a
6) si p et q sont premiers $p \wedge q = p$ quand $p = q$ et 1 sinon

(démonstrations très faciles)

Algorithme d'Euclide

Dans l'exemple nous avons calculé un PGCD en n'utilisant que sa définition. C'est une méthode bien trop longue, parce qu'elle demande non seulement de calculer le PGCD, mais aussi de faire des décompositions en facteurs premiers, c'est qui est une autre affaire ! Voici une autre méthode plus directe et efficace qu'on appelle l'algorithme d'Euclide :

1. appeler r_{-1} le plus grand des deux nombres et r_0 le plus petit,
2. faire les divisions euclidiennes :

$$r_{-1} = r_0\, q_1 + r_1$$
$$r_0 = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\ldots\ldots\ldots\ldots$$
$$r_k = r_{k+1}\, q_{k+2} + r_{k+2}$$
$$\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1}\, q_n + r_n$$
$$r_{n-1} = r_n\, q_{n+1} + 0$$

jusqu'au moment où l'on trouve un reste nul. Alors :

a) le dernier reste non nul r_n, est u PGCD de a et deb
b) il divise chacun des r_k

Le calcul s'arrête toujours car : $r_0 > r_1 > r_2 > r_3 > \ldots \geq 0$ et on finit forcement par rencontrer le reste nul.

Soit c un diviseur commun à a et b. D'après le théorème 2 il divise $r_{-1} - r_0\, q_1$, c'est à dire r1. De même il divise $r_0 - r_1 q_2$ qui n'est autre que r_2. En descendant les équations, on montre par récurrence que c divise tous les restes jusqu'à r_n. En particulier $a \wedge b$ divise r_n ; il est donc inférieur ou égal à r_n. En sens inverse la dernière équation montre que r_n divise r_{n-1}. L'avant dernière équation montre qu'il divise r_{n-2} et de proche en proche, en remontant les équations, on prouve que r_n divise a et b.

Nous avons démontré que r_n est un diviseur commun à a et b, et que tout diviseur commun à a et b divise r_n. Par conséquent r_n est forcément le PGCD de a et b.

Au passage on a démontré que r_n divise chacun des r_k.

Exemple 6 *si a=96 et b=81, les calculs sont les suivants :*

a		*b*		*r*
96	*= 1 **	*81*	*+*	*15*

81	= 5 *	15	+	6
15	= 2 *	6	+	3
6	= 2 *	3	+	0

et le PGCD vaut 3.

Dans la démonstration précédente nous avons vu qu'un diviseur commun à a et b divise r_n. Nous avons donc démontré le résultat suivant que l'exemple 5 nous a laissé deviner.

Théorème 7

Les diviseurs communs à deux nombres sont tous les diviseurs de leur PGCD.

Théorème 8

1. Soit a, b et c trois éléments de N^+. Alors :
   7) $(ca) \wedge (cb) = c(a \wedge b)$

autrement dit, la multiplication est distributive par rapport au PGCD.

2. Si c est un diviseur commun à a et b alors :
   8) $(a/c) \wedge (b/c) = (a \wedge b)/c$
3. Si c est un diviseur commun à a et b, pour qu'il soit leur PGCD il faut et il suffit que a/c et b/c soient premiers entre eux.

Démo : *Après avoir calculé le PGCD de a et de b par l'algorithme d'Euclide multiplions toutes les équations par c, ce qui donne :*

$$cr_{-1} = cr_0\, q_1 + cr_1$$
$$cr_0 = cr_1 q_2 + cr_2$$
$$cr_1 = cr_2 q_3 + cr_3$$
$$\ldots\ldots\ldots\ldots$$
$$cr_k = cr_{k+1}\, q_{k+2} + cr_{k+2}$$
$$\ldots\ldots\ldots\ldots$$
$$cr_{n-2} = cr_{n-1}\, q_n + cr_n$$
$$cr_{n-1} = cr_n\, q_{n+1} + 0$$

Chaque ligne représente une division euclidienne, car : $cr_0 > cr_1 > cr_2 > \ldots \geq 0$ donc ce calcul n'est autre que l'algorithme d'Euclide appliqué à ca et cb. Il en résulte que le cr_n est le PGCD de ca et de cb. L'affirmation 2 se déduit immédiatement de 1. En effet $c[(a/c) \wedge (b/c)] = a \wedge b$ d'après 7, et il suffit de diviser les deux membres par c pour obtenir 8. Pour démontrer 3 posons $c = (a \wedge b)$; alors $1 = (a/c) \wedge (b/c)$ d'après 8, et a/c et b/c sont premiers entre eux. Réciproquement si a/c et b/c sont premiers entre eux nous avons $1 = (a/c) \wedge (b/c)$ et 8 montre que $c = a \wedge b$.

Dans la pratique l'affirmation 3 de théorème 8 est souvent utilisée de façon suivante : étant donnés deux nombres a et b, si l'on note c leur PGCD, il existe deux entiers A et B premiers entre eux tels que a = cA et b = cB.

Théorème 9

Quels que soient a, b, c et d dans N^+, $a \wedge b$ divise $(ac) \wedge (bd)$.

Démo : *Tout diviseur de a divise ac et tout diviseur de b divise bd. Par conséquent les diviseurs communs à a et b sont des diviseurs communs à ac et bd. En particulier le PGCD de a et de b est un diviseur commun à ac et bd, et d'après le théorème 7 il divise $(ac) \wedge (bd)$.*

Théorème 10 (appelé lemme de Gauss)

Soit a, b et c trois éléments de N^+.

1) si $a \wedge b = 1$, et si a divise bc, alors a divise c,
2) si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$,
3) si $a \wedge b = 1$, alors $a \wedge bc = a \wedge c$

Démo :

1) *Puisque $a \wedge b = 1$ la relation 7 donne $(ca) \wedge (cb) = c$, et puisque par hypothèse a est un diviseur commun à ac et bc il divise c, leur PGCD.*
2) *Faisons la démonstration par l'absurde en supposant que $a \wedge (bc)$ n'est pas égal à 1. Il possède alors au moins un diviseur premier, p. Ce nombre premier divise a et ne divise pas b, sinon il diviserait $a \wedge b$ qui vaut 1. Alors $p \wedge b = 1$, parce que p est premier, et qu'il ne divise pas b. Comme p divise bc la propriété 1 montre que p divise c. Mais p divisant à la fois a et c devrait diviser $a \wedge c$ qui vaut 1. Il y a donc une contradiction si l'on suppose $a \wedge (bc)$ différent de 1.*
3) *Posons $d = a \wedge c$. Alors, d'après le théorème 8, $a \wedge b$ est multiple de $(a/d) \wedge b$, qui vaut donc 1. Comme $(a/d) \wedge (c/d) = 1$, la propriété 2 donne $(a/d) \wedge [b(c/d)] = 1$, et en multipliant les deux membres par d on obtient $a \wedge (bc) = d = a \wedge c$.*

Théorème 11

Soit p un nombre premier. S'il divise le produit $a_1a_2\ldots a_n$ alors il divise au moins l'un des a_i.

Démo : *Supposons que p ne divise aucun des a_i. D'après 5 on a toujours $p \wedge a_i = 1$, et l'affirmation 2 du théorème 10 montre que $p \wedge (a_1a_2) = 1$ puis, par récurrence, que $p \wedge (a_1a_2\ldots a_n) = 1$, ce qui prouve que p ne divise pas $a_1a_2\ldots a_n$.*

Utiliserons ce théorème pour démontrer l'unicité de la décomposition en facteurs premiers.

Théorème 12

A condition de ne pas tenir compte de l'ordre des facteurs il existe une seule façon d'écrire u nombre entier comme produit des nombres premiers.

Démo : *Supposons qu'on ait deux décompositions en facteurs premiers :*

$$n = p_1p_2\ldots p_n = q_1q_2\ldots q_m$$

Comme p_1 divise le produit $q_1q_2\ldots q_m$, il divise un des q_i, et, quitte à changer leur ordre, nous pouvons supposer que c'est q_1. Puisque les diviseurs de q_1 est 1 et q_1, on a nécessairement $p_1=q_1$, et après simplification il vient $p_2\ldots p_n = q_2\ldots q_m$. Par récurrence on obtient ainsi l'égalité des p_i et q_i.

Afin d'indiquer une autre façon de calculer les PGCD, nous allons présenter les décompositions en facteurs premiers sous forme d'un produit infini de facteurs. Par exemple, au lieu d'écrire $2200 = 2^3*3^0*5^2*7^0*11^1*13^0*17^0*19^0*23^0\ldots$
Dans cette expression tous les nombres premiers sont présents, mais ceux qui ne divisent pas 2200 ont l'exposant 0. en fait tous les facteurs, sauf quelques-uns au début, sont égaux à 1, ce qui donne un sens au produit.
Nous noterons $v_p(n)$ l'exposant du nombre premier p dans cette représentation du nombre n ; dans notre exemple $v_5(2200) = 2$, et $v_{83}(2200) = 0$. Le fait que la décomposition en facteurs premiers soit unique revient à dire que n est caractérisé par la liste des exposants $v_p(n)$. Bien évidemment nous avons :

9) $v_p(ab) = v_p(a) + v_p(b)$.

Théorème 13
Pour que b divise a il faut et il suffit que $v_p(b) \leq v_p(a)$ quel que soit le nombre premier p.

Démo : *Supposons d'abord $v_p(b) \leq v_p(a)$ quel que soit p. Alors la différence $v_p(a) - v_p(b) \geq 0$, et elle vaut presque toujours 0, car les $v_p(a)$ et $v_p(b)$ sont nuls, sauf un nombre fini d'entre eux. Par conséquent il existe un entier c tel que $v_p(c) = v_p(a) - v_p(b)$ quel que soit p. Nous avons $v_p(bc) = v_p(b) + v_p(c)$, et l'unicité de la décomposition en facteurs premiers montre que a = bc, ce qui fait que b divise a.*
Réciproquement si b divise a il existe c tel que a = bc. Alors $v_p(a) = v_p(b) + v_p(c)$ d'après 9, et puisque les nombres qui figurent dans cette égalité sont tous positifs, nous avons bien $v_p(b) \leq v_p(a)$.
Jusqu'ici nous avons seulement défini le PGCD de deux entiers, mais il est facile de généraliser à trois ou plus.
Soient $a_1, a_2, \ldots, a_n$ des nombres entiers non tous nuls. L'ensemble de leurs diviseurs communs positifs n'est pas vide puisqu'il contient 1, et il est fini car tous sont compris entre 1 et $\inf(a_1, a_2, \ldots, a_n)$. Il possède donc un plus grand élément qu'on appelle le PGCD de $a_1, a_2, \ldots, a_n$, et qu'on note : $a_1 \wedge a_2 \wedge \ldots \wedge a_n$
Théorème 14
Soient $a_1, a_2, \ldots, a_n$ des éléments de N^+. Alors
propriété 10 : $v_p(a_1 \wedge a_2 \wedge \ldots \wedge a_n) = \inf [(v_p(a_1), v_p(a_2), \ldots, v_p(a_n)]$
Démo : *Soit c l'entier défini par : $v_p(c) = \inf [(v_p(a_1), v_p(a_2), \ldots, v_p(a_n)]$. D'après le théorème 13 c'est un diviseur commun à $a_1, a_2, \ldots, a_n$. Réciproquement, si d est un diviseur commun à $a_1, a_2, \ldots, a_n$ ce théorème montre que $v_p(d) \leq \inf [(v_p(a_1), v_p(a_2), \ldots, v_p(a_n)] = v_p(c)$. par conséquent d divise c, qui est donc le PGCD de $a_1, a_2, \ldots, a_n$.*
Le théorème 14 donne une nouvelle façon de calculer le PGCD de deux entiers
Exemple 7. *Pour calculer $980 \wedge 76050$ écrivons*

$$980 = 2^2 * 3^0 * 5^1 * 7^2 * 11^0 * 13^0 * 17^0 * 19^0 * 23^0 \ldots$$
$$76050 = 2^1 * 3^1 * 5^2 * 7^0 * 11^0 * 13^2 * 17^0 * 19^0 * 23^0 \ldots$$

D'après le théorème 14 :

$$980 \wedge 76050 = 2^1 * 3^0 * 5^1 * 7^0 * 11^0 * 13^0 * 17^0 * 19^0 * 23^0 \ldots$$

Ce qui donne $980 \wedge 76050 = 10$.
Cette façon de procéder ne peut s'appliquer qu'aux entiers déjà décomposés ou faciles à décomposer. Pour les autres, l'algorithme d'Euclide est bien plus efficace.
D'après le théorème 14 le calcul de PGCD est une opération associative :
propriété 11 : $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.
donc, pour calculer le PGCD de plusieurs nombres on peut employer l'algorithme d'Euclide de façon répétitive.
Soit $a_1, a_2, \ldots, a_n$ des éléments de N^+. L'ensemble de leurs multiples communs n'est pas vide puisqu'il contient leur produit. Comme toute partie non vide de N^+ il possède un plus petit élément ; on l'appelle le plus petit commun multiple (PPCM) de $a_1, a_2, \ldots, a_n$, et on le note $a_1 \vee a_2 \vee \ldots \vee a_n$.
Théorème 15
Soit $a_1, a_2, \ldots, a_n$ des éléments de N^+. Alors
propriété 12 : $v_p(a_1 \vee a_2 \vee \ldots \vee a_n) = \sup[v_p(a_1), v_p(a2), \ldots, v_p(a_n)]$
et les multiples communs à $a_1, a_2, \ldots, a_n$ sont tous les multiples de leur PPCM.
Dans le cas particulier où les entiers $a_1, a_2, \ldots, a_n$ sont premiers entre eux deux à deux leur PPCM est égal à leur produit.

Démo : *Soit M l'entier défini par : $v_p(M) = sup[v_p(a_1), v_p(a2), ..., v_p(a_n)]$. D'après le théorème 15 c'est un multiple commun à $a_1, a_2, ..., a_n$. Si m est un autre multiple commun à $a_1, a_2, ..., a_n$ d'après ce même théorème $v_p(m) \geq sup[v_p(a_1), v_p(a_2), ..., v_p(a_n)] = v_p(M)$, et M divise m, qui est donc plus grand que lui. Par conséquent M est le PPCM de $a_1, a_2, ..., a_n$ et il divise tous les multiples communs à $a_1, a_2, ..., a_n$. Comme tous les multiples de M sont des multiples communs à $a_1, a_2, ..., a_n$ la deuxième affirmation est démontrée. Enfin si les $a_1, a_2, ..., a_n$ sont premiers entre eux deux à deux, pour p fixé un seul des nombres $v_p(a_i)$ n'est pas nul, et le plus grand d'entre eux est égal à leur somme.*

Il résulte de ce théorème que le calcul du PPCM est associatif :
$a \vee (b \vee c) = (a \vee b) \vee c$
On peut donc calculer $a_1 \vee a_2 \vee \ldots \vee a_n$ en calculant d'abord M1, le PPCM de a_1 et a_2, puis M2, le PPCM de M1 et a_3, etc. Il suffit donc de savoir calculer le PPCM de deux nombres pour être capable de calculer tous les PPCM.

Pour calculer $a \vee b$ avec la propriété 12 il faut d'abord décomposer a et b en facteurs premiers ce qui demande trop de calculs en général. Il est préférable d'utiliser l'algorithme d'Euclide en se servant de la formule suivante :

Théorème 16

Le PGCD et le PPCM de deux nombres a et b sont liés par
propriété 14 : $ab = (a \vee b)(a \wedge b)$

Démo : *D'abord $v_p(ab) = v_p(a) + v_p(b)$. Alors si on note c le membre de droite de 14 nous avons*
$v_p(c) = inf[v_p(a), v_p(b)] + sup[v_p(a), v_p(b)] = v_p(a) + v_p(b) = v_p(ab)$ quel que soit p, ce qui prouve que ab = c, d'après l'unicité de la décomposition en facteurs premiers.

Méthode pour calculer le PPCM de a et de b

1) calculer $a \wedge b$ par l'algorithme d'Euclide,
2) diviser l'un des deux nombres par $a \wedge b$,
3) multiplier le quotient par l'autre nombre

Exemple 8.
$15 \wedge 20 = 5$
20/5 = 4
*15 * 4 = 60*