PGCD - PPCM

1. DIVISEURS COMMUNS A DEUX OU PLUSIEURS NOMBRES

1.1 Définitions

Soient a, b, c, .. des entiers naturels non nuls. Un nombre d qui divise à la fois a, b, c, .. est appelé diviseur commun à ces nombres. d est au plus égal au plus petit de ces nombres.

Il y a un nombre fini de diviseurs commun à plusieurs nombres. Le plus grand de ces diviseurs est appelé le PGCD (le plus grand commun diviseur) de ces nombres.

Lorsque le PGCD est égal à 1, on dit que les nombres sont premiers entre eux.

1.2 Méthodes de calcul du PGCD

Supposons que a>b. Pour déterminer PGCD(a, b) on pourrait chercher tous les diviseurs de b qui divisent a. En b opérations au plus on obtiendrait PGCD(a, b), noté $a \wedge b$.

La méthode présentée par Euclide est plus rapide.

i - Considérons la division euclidienne de a par b :

$a = bq + r$ et $0 \leq r < b$.

Si $r = 0$ alors b divise a et PGCD(a, b) = b.

Si $r \neq 0$, alors tout diviseur commun de a et b est un diviseur de b et (a-bq) donc un diviseur commun de b et r.

Réciproquement tout diviseur commun de b et r est un diviseur commun de bq + r et b, donc diviseur commun de b et a.

On en déduit que PGCD(a, b) = PGCD(b, r).

ii - Si r divise b alors PGCD(a, b) = r.

Si r ne divise pas b alors on recommence avec b et r.

Disposition pratique :

q_i		q	q_1	q_2	q_3	. . .
	a	b	r	r_1	r_2	. . .
r_i	r	r_1	r_2	r_3		. . .

<u>Conclusion :</u>

(*Algorithme d'Euclide)* Le PGCD de deux nombres est le dernier reste non nul que l'on obtient par la méthode de divisions successives.

Exemple PGCD (315, 240)

q_i		1	3	5
	315	240	75	15
r_i	75	15	0	

Le dernier reste non nul est 15 donc le PGCD de 315 et 240 est 15.

1.3 Propriétés du PGCD

- PGCD (a, b) = PGCD (b, a)

-Si on multiplie (ou si l'on divise) plusieurs nombres par un même nombre, le PGCD est multiplié (ou divisé) par ce nombre.
Exemple : PGCD (300, 216) = 12 alors PGCD (1800, 1296) = 6 x PGCD (300, 216) = 72

PGCD (ka ; kb) = k.PGCD (a ; b)

- Les diviseurs communs à plusieurs nombres divisent leur PGCD.
Si c | a et c | b alors c | PGCD (a , b)

- Pour qu'un diviseur commun à plusieurs nombres soit le PGCD de ces nombres, il faut et il suffit que leurs quotients par le diviseur commun considéré soient premiers entre eux.
Soient a , b de IN* et d de IN* tel que il existe a' et b' de IN* a = da' , b = db' alors d = PGCD(a,b) si et seulement si PGCD(a',b')=1

- L'ensemble des diviseurs communs à plusieurs entiers est le même quand on remplace deux de ces nombres par leur PGCD.

- Pour déterminer le PGCD de plusieurs entiers on peut remplacer deux entiers par leur PGCD.

- Si c divise ab et PGCD (a ; c)= 1 alors c divise b (Théorème de Gauss)

Il résulte de la propriété multiplicative du PGCD et du théorème de Gauss que si a et b sont premiers entre eux, alors a^n et b^p (n et p dans IN) le sont aussi.

- Si PGCD (a ; b) =1 et PGCD (a ; c) = 1 alors PGCD (a ; bc) =1

- Si PGCD (a ; b) = d alors il existe des entiers u et v tels que d = au + bv

PGCD (a, b) =1 si et seulement si, il existe u, v $\in$ Z tels que au + bv = 1. (Identité de Bézout)

2. PPCM

2.1 Définitions

Un nombre M divisible par des entiers a, b est appelé multiple commun à ces entiers.
• Le produit ab est l'un de ces multiples communs. Comme tout multiple de M est un multiple commun, il existe une infinité de multiple communs à plusieurs entiers.
•M est au moins égal au plus grand des nombres a, b.

•Parmi tous les multiples communs, il en existe un, inférieur à tous les autres, que l'on appelle le PPCM (ou plus petit commun multiple). On note PPCM(a , b) ou $a \vee b$.

2.2 Recherche des multiples communs à deux entiers

Soit M un multiple commun à deux entiers a et b. Il existe deux entiers p et q tels que
M = pa et M = qb donc pa = qb .
Soit d le PGCD de a et b , il existe a' et b' tels que a = d.a' et b = d.b' avec a' et b' premiers entre eux. Comme pa = qb, on a pda' = qdb ' i.e pa' = qb'.
b' divise qb' donc b divise pa' et d'après le théorème d Gauss b' divise p (car b' et a' premiers entre eux)
Il existe donc un entier k tel que p = b'k.
Et puisque M = pa, on a M = ab'k = da'b'k.

Une condition nécessaire pour que M soit divisible par a et b est qu'il soit divisible par d a' b' .

C'est une condition suffisante.

Le PPCM s'obtient en prenant k = 1 et le PPCM (a ; b) = m = d a' b ' .
D'où : d m = da' db' = ab.
On a donc :

PGCD (a ; b) . PPCM (a ; b) = a.b

2.3 Propriétés :

- Si PPCM (a; b) = m alors il existe u et v tels que m = au = bv.

- PPCM (ka ; kb) = k.PPCM (a ; b)

- PGCD (a ; b) = 1 si et seulement si PPCM (a ; b) = ab.

- Pour déterminer le PPCM de plusieurs entiers on peut remplacer deux entiers par leur PPCM.