

# EXAMEN: Formule Note = 1 + 5 \* NbPts / 35

Cours du 16.11.2020  
lundi, 16 novembre 2020 18:39

**Définition:** On appelle le "Plus Grand Diviseur Commun" (PGCD)  
De deux nombres  $a$  et  $b$  par  
 **$PGCD(a,b)$**

**QUESTION:** Comment calculer le PGCD ???

**Réponse :** passer par la factorisation en nombres premiers

NOTE : on va supposer  $a \geq b$

EXEMPLE: calculez le PGCD (168, 32)

Méthode 1 : FACTORISATION

$$32 = \underline{2} \cdot \underline{2} \cdot \underline{2} \cdot \underline{2} \cdot \underline{2} = 2^5$$
$$168 = 2 \cdot 84 = 2 \cdot 2 \cdot 42 = 2 \cdot 2 \cdot 2 \cdot 21 = \underline{2} \cdot \underline{2} \cdot \underline{2} \cdot 3 \cdot 7$$

$$PGCD = \underline{2} \cdot \underline{2} \cdot \underline{2} = 8$$

32 est divisible par 8

168 est divisible par 8

IMPORTANT: "a divisible par b" signifie que le RESTE de  $a / b = 0$

↳ EN NOMBRES ENTIERS!

$$\begin{array}{r|l} a & b \\ \hline \boxed{r=0} & a \end{array}$$

$$\frac{a}{b} \in \mathbb{Z}$$

$$\boxed{r=0} \mid 9$$

$$\frac{a}{b} \in \mathbb{Z}$$

### Algorithme d'Euclide:

Entrée :  $a, b \in \mathbb{Z}$  ( $a \geq b$ )

Sortie : PGCD( $a, b$ )

Poser,  $r = a \bmod b$

TANT QUE  $r \neq 0$  faire

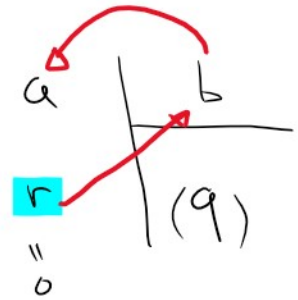
$a \leftarrow b$

$b \leftarrow r$

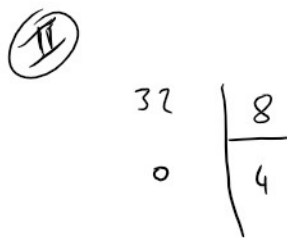
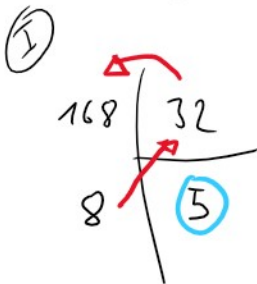
$r = a \bmod b$

FIN

PGCD( $a, b$ ) =  $b$



Exemple : PGCD(168, 32)



$$168 : 32 = \underline{5,25} \Rightarrow 168 = \underline{5,25} \cdot 32 \in [0,1[$$

$$= \underline{5} \cdot 32 + \overbrace{0,25 \cdot 32} \in [0,31]$$

Exercice : Calculez PGCD(770,168)

770 - 4 \cdot 168

...

...

$$\begin{array}{r|l} 770 & 168 \\ 98 & 4 \end{array}$$

$$\begin{array}{r|l} 168 & 98 \\ 70 & 1 \end{array}$$

$$\begin{array}{r|l} 98 & 70 \\ 28 & 1 \end{array}$$

$$\begin{array}{r|l} 70 & 28 \\ 14 & 2 \end{array}$$

$$\begin{array}{r|l} 28 & 14 \\ 0 & 2 \\ \hline \end{array}$$

$$\text{PGCD}(770, 168) = 14$$

STOP



Le calcul de la factorisation en nombres premiers est "fastidieux".

L'algorithme d'Euclide est dans la classe d'algorithmes la plus performante.

Lien entre le PGCD et le PPCM (Plus Petit Commun Multiple)

$$32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$$

$$168 = 2 \cdot 84 = 2 \cdot 2 \cdot 42 = 2 \cdot 2 \cdot 2 \cdot 21 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7$$

$$\text{PGCD}(a,b) = \text{Produit des facteurs "Communs"} = 2 \cdot 2 \cdot 2 = 8$$

$$\text{PPCM}(a,b) = \text{Produit des facteurs "restants"} = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 = 672$$

PROPRIETE REMARQUABLE :

$$\text{PGCD}(a,b) \cdot \text{PPCM}(a,b) = a \cdot b$$

$$8 \cdot 672 = 32 \cdot 168 = 5376$$

Donc, pour le calculer le PPCM on dispose d'un algo.

Efficace : on calcule  $a \cdot b$ , puis  $\text{PGCD}(a,b)$  avec Euclide, et

finalement

$$\text{PPCM}(a, b) = \frac{a \times b}{\text{PGCD}(a, b)}$$

PAS BESOIN de passer par la factorisation !!!!

**Exercice : (série 5 sur le site du cours)**

Prouvez que si  $\text{PGCD}(a, b) = 1$ , alors  
 $\text{PGCD}(a \cdot b, c) = \text{PGCD}(a, c) \cdot \text{PGCD}(b, c)$

$\otimes$   $a = a_1 \cdot a_2 \cdot \dots \cdot a_n$   
 $= \prod_{i=1}^n a_i$

PREUVE:

$a = a_1 \cdot a_2 \cdot \dots \cdot a_N$   $\otimes$  (facteurs premiers)  $\rightarrow \Rightarrow \mathbb{Z}$   
 $b = b_1 \cdot b_2 \cdot \dots \cdot b_M$  il n'y jamais le même entre  $a_i$  et  $b_j$   $i=1, \dots, N$   $j=1, \dots, M$   
Par le théorème fond. de l'Arithmétique.

① Comme  $\text{PGCD}(a, b) = 1$ , alors AUCUN des  $a_i = b_j$  (sinon  $\text{PGCD}(a, b) \geq 2$  !!!!)

②  $\text{PGCD}(a \cdot b, c) =$  Facteurs communs de  $a \cdot b$  et  $c$

$c = c_1 \cdot c_2 \cdot \dots \cdot c_M$  sont à la fois dans  $c_1, \dots, c_M$   
et  $a_1, \dots, a_N$  et  $b_1, \dots, b_M$

③ Comme aucun des  $a_i$  et  $b_j$  ne sont les mêmes, alors SOIT le facteur du PGCD est un facteur commun de  $a$  et  $c$ , soit un facteur commun de  $b$  et  $c$  (de manière exclusive)

④ Il suffit alors de regrouper les facteurs communs de  $a$  et  $c \Rightarrow \text{PGCD}(a, c)$ , et de même pour les fact. communs de  $b$  et  $c \Rightarrow \text{PGCD}(b, c)$

$$\text{PGCD}(a \cdot b, c) = x_1 \cdot x_2 \cdot x_3 \cdot \dots = \text{PGCD}(a, c) \cdot \text{PGCD}(b, c)$$

⑤

Je devrais encore prouver que TOUS les facteurs du PGCD(a,c) et PGCD(b,c) sont dans le PGCD(a\*b, c)... TRIVIAL car s'il y a un facteur commun entre a et c (ou a et b), ce sera forcément aussi un facteur commun de a\*b et c !

CQFD.

### Théorème de Bachet-Bézout: (XVIIe s.)

Soient a,b deux entiers relatifs ( $a, b \in \mathbb{Z}^*$ ) alors il existe deux entiers relatifs x et y  $\in \mathbb{Z}$  tels que

$$a \cdot \underline{x} + b \cdot \underline{y} = \text{PGCD}(a, b)$$

x et y sont appelés les "**coefficients de Bézout**".

#### EXEMPLE:

PGCD(168, 32) = 8. Trouvez les coefficients de Bézout !

Trouvez x et y (DANS  $\mathbb{Z}$ ) tels que

$$168 * x + 32 * y = 8.$$

$$168 \cdot 1 - 32 \cdot 5 = 168 - 160 = 8 \quad \text{PGCD}(168, 32)$$

Y en a-t-il d'autres ? OUI, il y en a une INFINITE !!!!