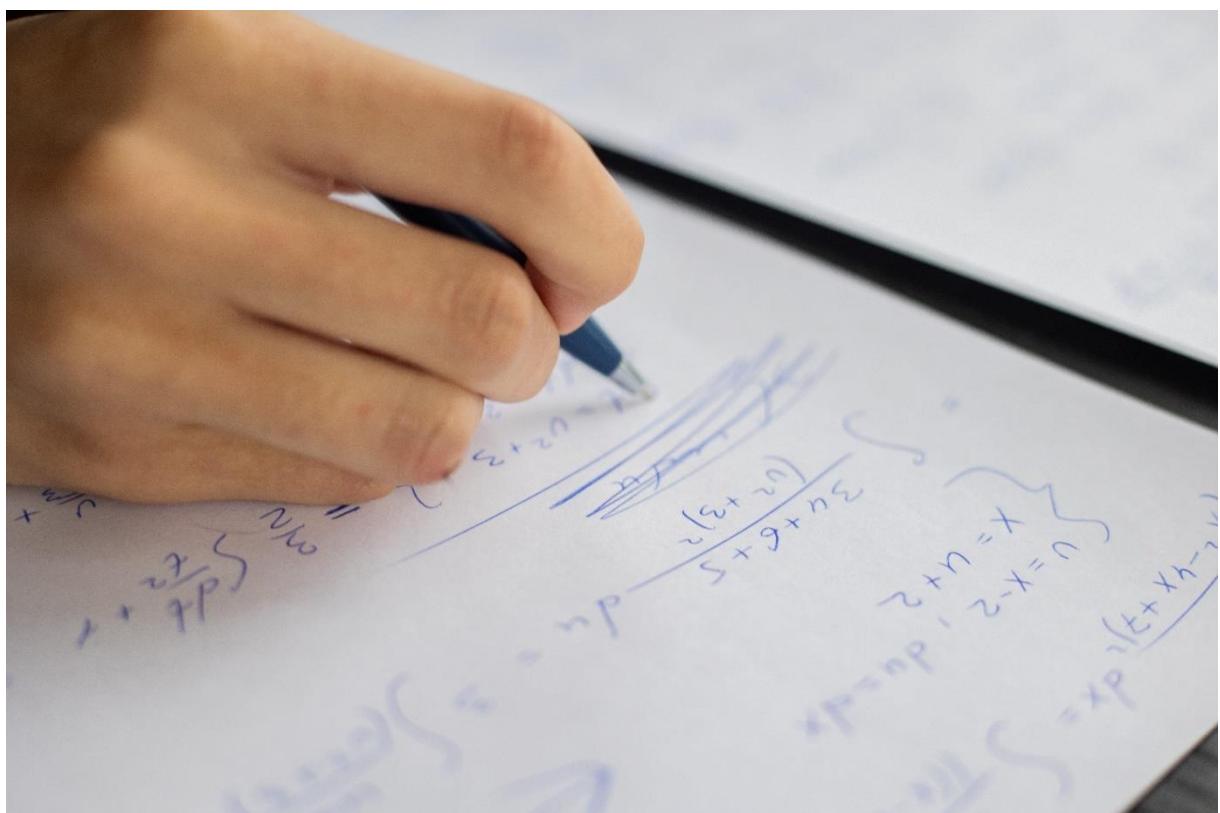


# ARITHMETIQUE

## 3. Nombre premier, PGCD

### - Cours



**Elliot LOUVEAU**

[elliot.louveau@eduservices.org](mailto:elliot.louveau@eduservices.org)



# TABLE DES MATIERES

<b>DIVISIBILITE DES ENTIERS .....</b>	<b>2</b>
Vocabulaire et formule .....	2
Exemple.....	3
Propriétés .....	3
<b>NOMBRES PREMIERS.....</b>	<b>7</b>
Définition.....	7
Exemples : .....	7
Théorème : Déterminer si un nombre est un nombre premier .....	7
Décomposition d'un nombre en produit de facteurs premiers.....	10
Théorème.....	10
En pratique : .....	10
Intérêt : Trouver la liste des diviseurs possibles .....	11
<b>PGCD DE DEUX ENTIERS NATURELS NON NULS.....</b>	<b>2</b>
Définition.....	2
Exemples .....	2
PGCD comme produit des facteurs premiers commun.....	3
PGCD avec le reste de la division euclidienne, l'algorithme d'Euclide...	5

# DIVISIBILITE DES ENTIERS

## VOCABULAIRE ET FORMULE

(revoir la règle pour multiple de 7 cf Timéo)

Soient  $a$  et  $b$  des entiers naturels.  $a$  est **divisible** par  $b$  s'il existe un **entier naturel  $k$  tel que** :  $\frac{a}{b} = k \Leftrightarrow a = k * b$ .

On dit alors que  $b$  divise  $a$ , que  $b$  est un **diviseur** de  $a$  et que  $a$  est un **multiple** de  $b$ .

Autrement dit :

Soient  $a$ ,  $b$  et  $k$  des entiers naturels (nombre positif sans décimal) : Si  $a = b * k$ , On peut dire que  $a$  **est un multiple de  $b$** . On peut aussi dire que  $a$  est un **multiple de  $k$** .

Si  $a = b * k$ , alors  $\frac{a}{b} = k$  et  $\frac{a}{k} = b$

⇒ En divisant  $a$  par  $b$  ou par  $k$  on obtient un entier naturel, on peut dire que  $a$  **est divisible par  $b$**  et que  $b$  **est un diviseur de  $a$** , on peut aussi dire que  $a$  **est divisible par  $k$**  et que  $k$  **est un diviseur de  $a$**

## Exemple

$75 = 25 * 3$  ; on peut dire que

- *75 est divisible par 25 et aussi par 3,*
- *25 et 3 sont des diviseurs de 75*
- *75 est un multiple de 25 et aussi de 3*

## PROPRIETES

Rappel : **a est divisible par b** s'il existe un entier naturel  $k$  tel que

$$\frac{a}{b} = k \Leftrightarrow a = b * k.$$

### 1. Si **a est divisible par b alors tout multiple de a est divisible par b.**

Démonstration :

Un multiple de  $a$  s'écrit  $na$  avec  $n$  entier naturel.

Donc  $\frac{a}{b} = k \Leftrightarrow a = bk \Leftrightarrow na = nbk = b(nk) \Leftrightarrow \frac{na}{b} = nk$

$\Rightarrow na$  est divisible par  $b$  puisque  $nk$  est un entier.

Si  $a$  est divisible par  $b$  tous multiples de  $a$  est divisible par  $b$ .

Exemple :

Soit  $a = 12$  et  $b = 4$ .  $a$  est bien divisible par  $b$  car  $\frac{a}{b} = \frac{12}{4} = 3$  et  $3$  est un entier.

Pour reprendre la démonstration,  $k = 3, 12 = 4 * 3$

Pour trouver un multiple de  $12$ , prenons un entier au hasard :  $n = 5$

$$na = 5 * 12 = 60$$

$$a = bk \quad (b \text{ est un diviseur de } a)$$

$$nbk = 5 * 4 * 3 = 60$$

$$\frac{na}{b} = \frac{60}{4} = 15$$

$na$ , qui est un multiple de  $a$  est donc bien « divisible » par  $b$ .

## **2. Si $a$ est divisible par $b$ et si $b$ est divisible par $c$ , alors $a$ est divisible par $c$ .**

Démonstration :

$a$  est divisible par  $b$  donc il existe un entier naturel  $k$  tel que  $\frac{a}{b} = k \Leftrightarrow a = bk$

$b$  est divisible par  $c$  donc il existe un entier naturel  $k'$  tel que  $\frac{b}{c} = k' \Leftrightarrow b = ck'$

Alors  $a = bk = ck'k \Leftrightarrow \frac{a}{c} = k'k$

$a$  est donc bien divisible par  $c$  puisque  $kk'$  est un entier.

Exemple :

Soit  $a = 12$ ;  $b = 4$  et  $c = 2$

$a$  est bien divisible par  $b$ ,  $b$  est bien divisible par  $c$  et  $a$  est bien divisible par  $c$ .

**3. Si  $a$  et  $b$  sont divisible par  $c$ , alors  $a + b$  et  $a - b$  sont divisibles par  $c$ .**

Démonstration :

$a$  et  $b$  sont divisible par  $c$  donc il existe un entier naturel  $k$  tel que  $a = ck$  et un entier naturel  $k'$  tel que  $b = ck'$

Alors  $a + b = ck + ck' = c(k + k')$   $\Leftrightarrow \frac{a+b}{c} = k + k'$  ce qui prouve que  $a + b$  est divisible par  $c$  puisque  $k + k'$  est un entier. Idem pour  $a - b$  divisible par  $c$ .

Exemple :

Soit  $a = 15; b = 9$  et  $c = 3$ ,

$a$  est bien divisible par  $c$ ,  $b$  est bien divisible par  $c$ .

$a - b = 6$  ; qui est bien divisible par  $c$

$a + b = 24$  ; qui est bien divisible par  $c$

\_\_\_ Exercice

# NOMBRES PREMIERS

## DEFINITION

Un entier naturel est premier s'il a exactement deux diviseurs : 1 et lui-même.

### Exemples :

- *0 n'est pas premier car il possède une infinité de diviseur.*
- *1 n'est pas premier car il n'a qu'un seul diviseur : 1.*
- *2 est premier car il a exactement deux diviseurs : 1 et 2.*
- *3 est premier car il a exactement deux diviseurs : 1 et 3*
- *4 n'est pas premier car il a 3 diviseurs : 1, 2 et 4*

⚠ Les premiers nombres premiers à retenir sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

### Théorème : Déterminer si un nombre est un nombre premier

Soit  $n$  un entier naturel supérieur ou égal à 2.

**Si  $n$  n'est pas premier, alors  $n$  possède au moins un diviseur premier inférieur ou égal à  $\sqrt{n}$**

### Autrement dit :

Pour savoir si un nombre  $n$  est premier, on calcule  $\sqrt{n}$ . Si  $n$  n'est divisible par aucun des nombres premiers inférieurs ou égaux à  $\sqrt{n}$ , alors  $n$  est premier.

### **Exemples**

1) *197 est-il un nombre premier ?*

1<sup>ère</sup> étape : Je calcule  $\sqrt{197}$  pour trouver les nombres premiers inférieurs ou égaux à cette racine.

$$\sqrt{197} \approx 14,04.$$

Les nombres premiers inférieurs ou égaux à 14,04 sont 2, 3, 5, 7, 11 et 13.

2<sup>ème</sup> étape : Je vérifie si 197 est divisible par l'un de ces nombres.

D'après le théorème, si 197 est divisible par l'un de ces nombres alors il n'est pas premier.

Après vérification à la calculatrice, 197 n'est divisible par aucun d'eux. On peut donc affirmer que 197 est un nombre premier.

2) *119 est-il un nombre premier ?*

$$\sqrt{119} \approx 10,9$$

Les nombres premiers inférieurs ou égaux à 10,9 sont 2, 3, 5 et 7.

119 n'est ni divisible par 2, ni par 3 ni par 5 (cf règles ci-après) par contre  $119 / 7 = 17$ .

Donc 119 est divisible par 7, et aussi par 17, il n'est donc pas un nombre premier.

3) *813 est-il un nombre premier ?*

Soit on calcule la racine de 813 on teste si les nombres premier inférieurs sont diviseurs de 813, soit on se rappelle la règle pour savoir si un nombre est multiple de 3 :

« *Si la somme de tous les chiffres d'un nombre est multiple de 3, alors ce nombre est multiple de 3  $\Leftrightarrow$  il est divisible par 3.* »

On peut voir que 813 est multiple de 3, il n'est donc pas premier.

Pour rappel :

- *Un nombre pair ne peut pas être premier car il sera divisible au moins par 2.*
- *Un nombre qui termine par 0 ou 5 ne peut pas être premier car il sera divisible au moins par 5.*

Et pour infos :

- *Un nombre entier est divisible par 4 si le nombre formé par ses deux derniers chiffres est un multiple de 4.*
  - o *1 028 est divisible par 4 car 28 est un multiple de 4 ( $28 = 4 \times 7$ ).*
- *Un nombre entier est divisible par 9 si la somme de ses chiffres est un multiple de 9 (9 ; 18 ; 27 ; etc.).*
  - o *576 est divisible par 9 car  $5 + 7 + 6 = 18$  et  $18 = 2 \times 9$ .*

## **DECOMPOSITION D'UN NOMBRE EN PRODUIT DE FACTEURS PREMIERS**

### **Théorème**

Tout entier naturel supérieur ou égal à 2 se décompose de façon unique en un produit de facteurs premiers.

Remarque :

Par définition, un nombre premier ne peut pas être décomposé en produit de plusieurs nombres premiers. On peut aussi dire qu'il est sa propre décomposition.

**En pratique :**

Pour décomposer un nombre en produit de facteurs premiers, **on divise le nombre par son plus petit diviseur premier, et on recommence avec le quotient obtenu jusqu'à ce qu'il soit égal à 1.**

84	2	975	3
42	2	325	5
21	3	65	5
7	7	13	13
1		1	

$$84 = 2^2 * 3 * 7$$

$$975 = 3 * 5^2 * 13$$

On peut également trouver la décomposition de manière « linéaire » :

$$430 = 2 * 215$$

*215 n'est pas divisible par 2, ni par 3, il l'est par 5 :*

$$430 = 2 * 215 = 2 * 5 * 43$$

Je n'arrive pas à trouver de diviseur à 43 rapidement, je veux savoir si 43 est un nombre premier :

$$\sqrt{43} \approx 6,56$$

43 n'est ni divisible par 2, ni par 3 ni par 5, c'est donc un nombre premier. J'ai décomposé 430 en produit de facteur premier.  $430 = 2 * 5 * 43$

## Intérêt : Trouver la liste des diviseurs possibles

La décomposition d'un nombre en produit de facteurs premiers permet d'obtenir tous ses diviseurs. En effet, d'après les propriétés sur la divisibilité des nombres entiers :

Soit  $a, b$  et  $k$  des entiers naturels,

Si  $\frac{a}{b} = k$  alors  $b$  est un diviseur de  $a$ .

$\frac{a}{b} = k \Leftrightarrow \frac{a}{k} = b$  ;  $k$  est donc aussi un diviseur de  $a$

Par extension, si  $a = b * k * x * y * \dots$  où  $b, k, x, y, \dots$  sont des entiers naturels, alors  $b, k, x, y, \dots$  ainsi que  $b * k, b * x, b * y, k * x \dots$  sont des diviseurs de  $a$ .

$\Rightarrow a = b * k * x * y * \dots \Leftrightarrow \frac{a}{b*k} = x * y * \dots \Leftrightarrow \frac{a}{b*x} = k * y * \dots$  par exemple.

En divisant  $a$  par l'une ou l'autre de toutes ces combinaisons possibles, on obtiendra toujours un nombre entier (étant donné qu'un produit de nombres entiers donne toujours un nombre entier).

## Exemples

$$\therefore 84 = 2 * 42 = 2 * 2 * 21 = 2 * 2 * 3 * 7 = 2^2 * 3 * 7$$

2, 3 et 7 sont donc des diviseurs de 84, mais aussi  $2^2$ , et aussi  $2^2 * 3$  ;  $2 * 7 \dots$

Pour être sûr de déterminer la liste complète des diviseurs de 84 nous allons mettre en place un petit algorithme :

Un diviseur de 84 s'écrit :  $2^i * 3^j * 7^k$  avec  $0 \leq i \leq 2$ ,  $0 \leq j \leq 1$ ,  $0 \leq k \leq 1$

```

Variables : i, j, k (entiers)
Début
  Pour i de 0 à 2 Faire
    Pour j de 0 à 1 Faire
      Pour k de 0 à 1 Faire
        Afficher  $2^i \times 3^j \times 7^k$ 
        FinPour
      FinPour
    FinPour
  Fin

```

**Le nombre de diviseurs possible = le nombre de boucles que l'algorithme va effectuer, soit :  $3*2*2 = 12$  diviseurs au total.**

En utilisant l'algorithme suivant, on obtient :

Premier tour de boucle : i=0, j=0, k=0

$$2^0 * 3^0 * 7^0 = 1$$

Puis i=0, j=0, k=1

$$2^0 * 3^0 * 7^1 = 7$$

Puis i=0, j=1, k=0

$$2^0 * 3^1 * 7^0 = 3$$

Puis i=0, j=1, k=1

$$2^0 * 3^1 * 7^1 = 21$$

Puis i=1, j=0, k=0

$$2^1 * 3^0 * 7^0 = 2$$

Puis i=1, j=0, k=1

$$2^1 * 3^0 * 7^1 = 14$$

...

Finalement on obtient les 12 diviseurs de 84 qui sont, dans l'ordre croissant : 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42 et 84.

. Quantité et liste des diviseurs de 135 ?

$$135 = 3 * 45 = 3 * 3 * 15 = 3 * 3 * 3 * 5 = 3^3 * 5^1$$

Ici un diviseur de 135 s'écrit  $3^i * 5^j$  avec  $0 \leq i \leq 3$ ,  $0 \leq j \leq 1$

Donc 8 diviseurs :  $(3+1) * (1+1)$

⇒ *Liste des diviseurs de 135 :*

$$3^0 * 5^0 = 1 \quad 3^1 * 5^0 = 3 \quad 3^2 * 5^0 = 9 \quad 3^3 * 5^0 = 27$$

$$3^0 * 5^1 = 5 \quad 3^1 * 5^1 = 15 \quad 3^2 * 5^1 = 45 \quad 3^3 * 5^1 = 135$$

Dans l'ordre croissant, la liste des diviseurs de 135 est :

1, 3, 5, 9, 15, 27, 45, 135

. Quantité et liste des diviseurs de 36 ?

$$36 = 2 * 18 = 2 * 2 * 9 = 2 * 2 * 3 * 3 = 2^2 * 3^2$$

Donc  $3*3 = 9$  diviseurs à trouver.

⇒ *Liste des diviseurs de 36 :*

$$2^0 * 3^0 = 1 \quad 2^1 * 3^0 = 2 \quad 2^2 * 3^0 = 4$$

$$2^0 * 3^1 = 3 \quad 2^1 * 3^1 = 6 \quad 2^2 * 3^1 = 12$$

$$2^0 * 3^2 = 9 \quad 2^1 * 3^2 = 18 \quad 2^2 * 3^2 = 36$$

Dans l'ordre croissant, la liste des diviseurs de 36 est :

1, 2, 3, 4, 6, 9, 12, 18, 36

# PGCD DE DEUX ENTIERS NATURELS NON NULS

## DEFINITION

- Étant donné deux entiers naturels non nuls  $a$  et  $b$ , il existe un **diviseur commun** à  $a$  et à  $b$  qui **est plus grand que tous les autres**. Ce diviseur est appelé **Plus Grand Commun Diviseur** et se note  $\text{PGCD}(a; b)$ .
- Deux entiers naturels non nuls sont **premiers entre eux** si est seulement si leur PGCD est égal à 1.

## Exemples

1) Quel est le PGCD de 45 et 105 ?

Les diviseurs de 45 sont 1, 3, 5, 9, 15 et 45.

$$(45 = 3 * 15 = 3 * 3 * 5 = 3^2 * 5)$$

Ceux de 105 sont 1, 3, 5, 7, 15, 21, 35 et 105.

$$(105 = 3 * 35 = 3 * 5 * 7)$$

Les diviseurs communs à 45 et 105 sont 1, 3, 5, 15.

Le plus grand d'entre eux est 15 donc 15 est le PGCD de 45 et 105.

On écrit  $\text{PGCD}(45;105) = 15$ .

2) Quel est le PGCD de 15 et 44 ?

Les diviseurs de 15 sont 1, 3, 5 et 15.

Ceux de 44 sont 1, 2, 4, 11, 22 et 44.

Le seul diviseur commun à 15 et à 44 est 1.

Donc **PGCD(15;44) = 1**.

On dit que 15 et 44 sont **premiers entre eux**.

## **PGCD COMME PRODUIT DES FACTEURS PREMIERS COMMUN**

Soit  $a$  et  $b$  deux entiers naturels supérieurs ou égaux à 2 dont on connaît les décompositions en produits de facteurs premiers :

- S'ils n'ont pas de facteur commun, alors leur PGCD est 1 ;
- Sinon, **leur PGCD est le produit des facteurs communs** aux deux décompositions, chaque facteur étant **affecté du plus petit exposant** avec lequel il figure dans les deux décompositions.

⇒ *Cette propriété nous permet de ne pas calculer un à un tous les diviseurs pour trouver le PGCD.*

### **Exemples**

a) Quel est le  $\text{PGCD}(4950;4875)$  ?

1. Décomposer 4950 et 4875 en produits de facteurs communs.
2. Trouver les facteurs communs
3. En déduire le PGCD avec la propriété ci-dessus.

$$\begin{aligned} 4950 &= 2 \cdot 2475 = 2 \cdot 3 \cdot 875 = 2 \cdot 3 \cdot 3 \cdot 275 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 55 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 11 \\ &= \mathbf{2 \cdot 3^2 \cdot 5^2 \cdot 11} \end{aligned}$$

$$4875 = 3 * 1625 = 3 * 5 * 325 = 3 * 5 * 5 * 65 = 3 * 5 * 5 * 5 * 13$$
$$= \mathbf{3 * 5^3 * 13}$$

Le PGCD est le produit des facteurs communs aux deux décompositions, chaque facteur étant affecté du plus petit exposant avec lequel il figure dans les deux décompositions.

Les facteurs communs des deux décompositions sont 3 et 5.

3 figure avec les exposants 2 et 1, on garde le plus petit, c'est-à-dire 1.  
5 figure avec les exposants 2 et 3, on garde le plus petit, c'est-à-dire 2.

$$\text{Donc PGCD}(4950 ; 4875) = \mathbf{3 * 5^2 = 75}$$

b) Quel est le PGCD des nombres  $a$  et  $b$  se décomposant tel que  
 $a = 2^4 * 3 * 5^2 * 7 * 19$  et  $b = 2^3 * 3^2 * 7^2 * 17$  ?

Facteurs communs : 2, 3, et 7

$$\begin{aligned} \text{PGCD}(a; b) &= \text{produit des facteurs commun avec le plus petit exposant} \\ &= 2^3 * 3 * 7 = 168 \end{aligned}$$

## **PGCD AVEC LE RESTE DE LA DIVISION EUCLIDIENNE, L'ALGORITHME D'EUCLIDE.**

Soient  $a$  et  $b$  deux entiers naturels non nuls tel que  $a > b$ .

Soit  $r$  le reste de la division euclidienne de  $a$  par  $b$ .

Alors  $\text{PGCD}(a; b) = \text{PGCD}(b ; r)$

Par extension : soit  $r'$  le reste de la division euclidienne de  $b$  par  $r$ .

**$\text{PGCD}(a; b) = \text{PGCD}(b ; r) = \text{PGCD}(r; r')$  et ainsi de suite.**

Cette propriété permet d'avoir une autre méthode pour chercher un PGCD. **Pour trouver le PGCD il suffit de répéter l'opération jusqu'à trouver un reste nul.**

L'avantage de cette propriété est qu'elle est algorithmique, donc programmable. Elle est connue sous le nom d'algorithme d'Euclide.

### **Exemples**

#### **1) Quel est le PGCD(420;182) ?**

*Il s'agit d'écrire la division euclidienne de 420 par 182 puis du quotient et du reste trouvé et ainsi de suite jusqu'à obtenir un reste égal à 0. Le PGCD est le dernier reste non nul trouvé.*

$420 = 182 * 2 + 56$  ; Donc, d'après le théorème :

$$\text{PGCD}(420;182) = \text{PGCD}(182;56)$$

car 56 est le reste de la division euclidienne de 420 par 182.

$$182 = 56 * 3 + 14$$

$$\text{PGCD}(182;56) = \text{PGCD}(56;14)$$

$$56 = 14 * 4 + 0$$

$$\text{PGCD}(182;56) = \text{PGCD}(56;14) = 14$$

car 14 est le reste de la division euclidienne de 56 par 14 et que Le reste de la division euclidienne de 56 par 14 est 0.

$$\text{PGCD}(420;182) = \text{PGCD}(182;56) = \text{PGCD}(56;14) = 14$$

2) Quel est le PGCD(1422;381) ?

$$1422 = 381 * 3 + 279$$

$$381 = 279 * 1 + 102$$

$$279 = 102 * 2 + 75$$

$$102 = 75 * 1 + 27$$

$$75 = 27 * 2 + 21$$

$$27 = 21 * 1 + 6$$

$$21 = 6 * 3 + 3$$

$$6 = 3 * 2 + 0$$

$$\Rightarrow \text{PGCD}(1422;381) = 3$$