PGCD ET NOMBRES PREMIERS

1. *PGCD de deux entiers*
	1. *Définition et propriétés*

**Exemple :**

Tous les diviseurs de 60 sont :…………………………………………………………..

Tous les diviseurs de 100 sont :…………………………………………………………

Les diviseurs communs à 60 et 100 sont : …………………………………….

Le plus grand diviseur commun à 60 et 100 est ………... On le nomme le ………………….. de 60 et 100.

**Définition**

Soit *a* et *b* deux entiers relatifs non nuls.

L’ensemble des diviseurs communs à $a$ et $b$ admet un plus grand diviseur $d$, appelé plus grand commun diviseur.

On le note …………………..

Démonstration :

…..

**Propriétés**

Soit *a* et *b* deux entiers relatifs non nuls.

1. $PGCD\left(a , b\right)= ……………………..$
2. $PGCD\left(a , b\right)= ……………………..$
3. $PGCD\left(a ; 0\right)= ………$car $………………………………….$.
4. PGCD(*a* ; 1) = .........
5. Si *b* divise *a* alors $PGCD\left(a ; b\right)= ……………$
6. Pour tout entier naturel $k$, on a: $PGCD\left(ka , kb\right)= …………………….$

**Exemples
1** PGCD(30 , 75) = …………………….

**2** PGCD(– 24 , – 18) = …………………………..
**3** PGCD(82 , 0) = ……………………..
**4** PGCD(30 , 5) = ……………………………….
**5** PGCD(240 , 180) = ……………………………..

**Définition - Nombres premiers entre eux**

Soit *a*, $b$ deux entiers relatifs non tous nuls.

On dit que $a$ et $b$ sont premiers entre eux si, et seulement s$i………………………………$

**Exemples**

PGCD(15 , 8) =…… donc 15 et 8 sont…………………………...

PGCD(a , 1) = ……. donc l’entier 1 est …………………………...

**Remarques**

* Il ne faut pas confondre nombres premiers entre eux et nombres premiers.

Les nombres 15 et 8 sont premiers entre eux mais ni l’un ni l’autre ne sont premiers.

En revanche, deux nombres premiers sont premiers entre eux.

* Une fraction irréductible q s’écrit comme le rapport de deux entiers premiers entre eux :

$$q=\frac{a}{b} avec a\in Z , b\in N^{\*} et PGCD\left(a , b\right)=1$$

**Livre page 109**









* 1. *Algorithme d'Euclide*



C’est avec *Euclide d'Alexandrie*(-320? ; -260?), que les théories sur les nombres premiers se mettent en place.

 Dans « *Les éléments* » (livres VII, VIII, IX), il donne des définitions, des propriétés et démontre certaines affirmations du passé, comme l’existence d’une infinité de nombres premiers.

« Les nombres premiers sont en quantité plus grande que toute quantité proposée de nombres premiers ».

Il présente aussi la décomposition en facteurs premiers liée à la notion de PGCD.

**Théorème Algorithme d’Euclide**

Soit $a$ et $b$ deux entiers naturels non nuls tels que $b$ ne divise pas $a$.

La suite des divisions euclidiennes du diviseur par le reste de la division précédente finit par s’arrêter.

Le dernier reste non nul est alors le $PGCD$ de $a$ et de $b$.

Division de a par b : $a = bq\_{0} + r\_{0}$ avec $b> r\_{0} ⩾0$

Division de b par r0 : $b = r\_{0}q\_{1} + r\_{1}$ avec $r\_{0}>r\_{1}⩾0$

Division de $r\_{0}$ par $r\_{1} $: $r\_{0} = r\_{1}q\_{2} + r\_{2}$ avec $r\_{1}>r\_{2}⩾0$

⋮ ⋮ ⋮

Division de $r\_{n-2}$ par $r\_{n-1} $: $r\_{n-2}=r\_{n-1}q\_{n}+r\_{n}$ avec $r\_{n–1}>r\_{n}⩾0$

Division de $r\_{n-1}$ par $r\_{n} $: $r\_{n–1} =r\_{n} q\_{n+1}+0$ on a alors : $PGCD(a , b)=r$







1. *Théorème de Bézout et théorème de Gauss*
	1. *Théorème de Bézout*

**Propriété (Identité de Bézout)**

Soit *a* et *b* deux entiers naturels non nuls et *d* leur PGCD.

Il existe deux entiers relatifs *u* et *v* tels que *……………………..*

**Démonstration :**

……

Exemple :

On a par exemple : PGCD(54 ; 42) = 6.

Il existe donc deux entiers *u* et *v* tels que : …………………………..

Le couple …………. convient. En effet : …………………………….

**Théorème de Bézout**

Soit *a* et *b* deux entiers naturels non nuls.

*a* et *b* sont premiers entre eux si, et seulement si, ……………………………………………………………..

**Démonstration :**

……

Exemple :

22 et 15 sont premiers entre eux.

On est alors assuré que l'équation ……………………….. admet un couple solution d'entiers.

Méthode : Démontrer que deux entiers sont premiers entre eux

Démontrer que pour tout entier naturel *n*, 2*n* + 3 et 5*n* + 7 sont premiers entre eux.

**Corollaire de Bézout**

 L’équation $ax+by=c$ admet des solutions entières si, et seulement si, $c$ est un multiple du $PGCD(a,b)$.

**Démonstration :**

……

Exemple :

* L’équation $4x+9y=2$ admet des solutions car….
* L’équation $9x-15y=2$ n’admet pas de solution car….
	1. *Théorème de Gauss*

**Théorème de Gauss**

Soit *a*, *b* et *c* trois entiers naturels non nuls.

Si *a* divise *bc* et si *a* et *b* sont premiers entre eux alors *……………………*

**Démonstration :**

…..

**Corollaire**

Soit *a*, *b* et *c* trois entiers naturels non nuls.

Si *a* et *b* divise *c* et si *a* et *b* sont premiers entre eux alors *…………………………*

**Démonstration :**

…..

Exemple :

6 et 11 divisent 660,

6 et 11 sont premiers entre eux,

donc ………………………..

Remarque :

Intuitivement, on pourrait croire que la condition "*a* et *b* sont premiers entre eux" est inutile.

Prenons un contre-exemple :

6 et 9 divisent 18,

6 et 9 ne sont pas premiers entre eux,

et 6 $×$ 9 = 54 ne divise pas 18.





1. *Nombres premiers*

*Problème 4 : Trouver les premiers nombres premiers (livre page 77)*



Les plus anciennes traces des nombres premiers ont été trouvées près du lac *Edouard* au *Zaïre* sur un os (de plus de 20000 ans), l’os d’*Ishango*, recouvert d’entailles marquant les nombres premiers 11, 13, 17 et 19.

Est-ce ici l’ébauche d’une table de nombres premiers ou cette correspondance est-elle due au hasard ?

* 1. *Définition et propriétés*

**Définition**

Un nombre entier naturel est premier s'il possède exactement deux diviseurs positifs distincts 1 et lui-même.

Exemples et contre-exemples :

* 2, 3, 5, 7 sont des nombres premiers.
* 6 n'est pas un nombre premier car divisible par 2 et 3.
* 1 n'est pas un nombre premier car il ne possède qu'un seul diviseur positif.

Liste des nombres premiers inférieurs à 100 :

**2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97**

**Propriété**

Tout entier naturel *n* strictement supérieur à 1 et non premier admet un diviseur premier *p* tel que .

**Démonstration :**

Soit *E* l'ensemble des diviseurs de *n* autre que 1 et *n*. Cet ensemble est non vide car *n* n'est pas premier donc *E* admet un plus petit élément noté *p*.

*p* est premier car dans le cas contraire, *p* admettrait un diviseur autre que 1 et *p*. Ce diviseur serait plus petit que *p* et diviserait également *n* ce qui contredit le fait que *p* est le plus petit élément de *E*.

On peut écrire que *n* = *pq* avec *p* < *q* car *p* est le plus petit élément de *E*.

Donc $p×p<pq=n$ et donc $<\sqrt{n}$ .

Remarque :

Pour savoir si un nombre *n* est premier ou non, la recherche de diviseurs peut s'arrêter au dernier entier premier inférieur à .

Méthode : Déterminer si un nombre est premier ou non

391 est-il premier ?

Pour le vérifier, on teste la divisibilité par tous les nombres premiers inférieurs à .

Soit : 2, 3, 5, 7, 11, 13, 17 et 19.

Les critères de divisibilités connus en classe du collège permettent de vérifier facilement que 391 n'est pas divisible par 2, 3 et 5.

En vérifiant par calcul pour 7, 11, 13 et 17, on constate que 391 : 17 = 23.

On en déduit que 391 n'est pas premier.

*Pierre de Fermat* (1601 ; 1665) est l’auteur de la plus célèbre conjecture des mathématiques :

« L’équation *xn + yn = zn*n’a pas de solution avec *x*, *y*, *z* > 0 et *n* > 2 ».

*Fermat*prétendait en détenir une preuve étonnante, mais il inscrivit dans la marge d’un ouvrage de *Diophante d'Alexandrie* ne pas avoir assez de place pour la rédiger !!!

Il fallut attendre trois siècles et demi pour qu’en 1995, un anglais, *Andrew Wiles*, en vienne à bout et empoche récompenses et célébrité.

* 1. *Décomposition en facteurs premiers*

Exemple :

On veut décomposer 600 en produit de facteurs premiers.

600 = 6 x 100 = 6 x 102 = 2 x 3 x 22 x 52 = 23 x 3 x 52

En effet, 2, 3 et 5 sont des nombres premiers.

**Propriété**

Tout entier naturel *n* strictement supérieur à 1 se décompose en produit de facteurs premiers.

Cette décomposition est unique à l'ordre près des facteurs.

On note  avec *p1*, *p2*, …, *pr* nombres premiers distincts et  entiers naturels non nuls.

**Démonstration :**

Existence :

- Si *n* est premier, l'existence est démontrée.

- Sinon, le plus petit diviseur *p1* de *n* est premier et il existe un entier naturel *n1* tel

que : *n* = *p1n1*.

 - Si *n1* est premier, l'existence est démontrée.

 - Sinon, le plus petit diviseur *p2* de *n1* est premier et il existe un entier naturel *n2* tel que : *n1* = *p2n2*.

On réitère le processus pour obtenir une suite  décroissante et finie d'entiers naturels.

Ainsi, *n* se décompose en un produit de facteurs premiers du type : .

Unicité : On effectue une démonstration par récurrence

* Initialisation : Trivial pour *n* = 2.
* Hérédité :

 - Hypothèse de récurrence :

 Supposons qu'il existe un entier *k* strictement supérieur à 1, tel que la propriété soit vraie pour tout entier strictement inférieur à *k* :

La décomposition de tout entier strictement inférieur à *k* en produit de facteurs premiers est unique.

 - Démontrons que : La propriété est vraie au rang *k* : La décomposition de *k* en produit de facteurs premiers est unique.

Supposons qu'il existe deux décompositions distinctes :



Donc *p1* divise  et donc il existe un entier *qi* tel que *p1* et *qi* ne soient pas premiers entre eux. Comme *p1* et *qi* sont premiers, on a *p1* = *qi*.

Le nombre  est inférieur à *k* et on a :



*l* qui est inférieur à *k* admet donc deux décompositions distinctes ce qui est contradictoire avec l'hypothèse de récurrence.

* Conclusion :

La propriété est vraie pour *n* = 2 et héréditaire à partir de ce rang. D'après le principe de récurrence, elle est vraie pour tout entier naturel *n*.

**Propriété**

Soit la décomposition en produit de facteurs premiers d'un entier naturel *n* non nul.

Tout diviseur de *n* admet une décomposition en produit de facteurs premiers de la forme  avec  pour tout .

**Démonstration :**

-  divise 

- Réciproquement, soit *d* un diviseur de .

Donc tout facteur premier de *d* divise *n* et est donc égal à *p1*, *p2*, … ou *pr*.

Par extension, on en déduit que *d* peut s'écrire  avec .

Exemple :

600 = 23 x 3 x 52

Donc 22 x 30 x 51 = 20 est un diviseur de 600.

Méthode : Déterminer un PGCD ou un PPCM\*

*\* Plus Petit Commun Multiple*

a) Décomposer 17 640 et 411 600 en produits de facteurs premiers.

b) En déduire le PGCD et le PPCM (plus petit multiple commun) de ces deux nombres.

a) 17 640 = 2 x 8820 411 600 = 2 x 205 800

 = 22 x 4410 = 22 x 102 900

 = 23 x 2205 = 23 x 51 450

 = 23 x 3 x 735 = 24 x 25 725

 = 23 x 32 x 245 = 24 x 3 x 8575

 = 23 x 32 x 5 x 49 = 24 x 3 x 5 x 1715

 = 23 x 32 x 5 x 72 = 24 x 3 x 52 x 343

 = 24 x 3 x 52 x 7 x 49

 = 24 x 3 x 52 x 73

b) Le PGCD de 17 640 et 411 600 est donc 23 x 3 x 5 x 72 = 5880

Le PPCM de 17 640 et 411 600 est donc 24 x 32 x 52 x 73 = 1 234 800

Méthode : Déterminer tous les diviseurs d'un entier

Déterminer tous les diviseurs de 132.

On décompose 132 en produit de facteurs premiers :

132 = 2 x 66 = 2 x 2 x 33 = 22 x 3 x 11

On construit un arbre donnant tous les cas possibles :

 

En parcourant tous les chemins possibles de l'arbre, on obtient tous les diviseurs de 132.

Ainsi par exemple, 21 x 30 x 111 = 22 est un diviseur de 132.

L'ensemble des diviseur de 132 est : 1, 2, 3, 4, 6, 11, 12, 22, 33, 44, 66, 132.

Remarque : La décomposition permet également de déterminer le nombre de diviseurs d'un entier. Il s'agit du produit des exposants augmentés de 1 des facteurs premiers. Cela correspond au produit des branches de chaque niveau de l'arbre.

Ainsi 132 possède (2 + 1) x (1 + 1) x (1 + 1) = 12 diviseurs.