PGCD ET NOMBRES PREMIERS

I. PGCD de deux entiers

1) Définition et propriétés

Exemple :

 **Vidéo** [**https://youtu.be/sC2iPY27Ym0**](https://youtu.be/sC2iPY27Ym0)

Tous les diviseurs de 60 sont : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

Tous les diviseurs de 100 sont : 1, 2, 4, 5, 10, 20, 25, 50, 100

Les diviseurs communs à 60 et 100 sont : 1, 2, 4, 5, 10, 20

Le plus grand diviseur commun à 60 et 100 est 20. On le nomme le de 60 et 100.

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

On appelle de *a* et *b* le plus grand commun diviseur de *a* et *b* et note

(*a* ; *b*).

Remarque :

On peut étendre cette définition à des entiers relatifs. Ainsi dans le cas d'entiers négatifs, la recherche du se ramène au cas positif.

Par exemple,

On a ainsi de façon générale : .

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

a)

b)

c) Si *b* divise *a* alors

Démonstration de c :

Si *b* divise *a* alors tout diviseur de *b* est un diviseur de *a*. Donc le plus grand diviseur de *b* (qui est *b*) est un diviseur de *a*.

2) 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 .

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

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

On a : .

Démonstration :

On note respectivement *q* et *r* le quotient et le reste de la division euclidienne de *a* par *b*.

Si un diviseur de *b* et *r* alors divise *a* = *bq* + *r* et donc est un diviseur de *a* et *b*.

Réciproquement, si un diviseur de *a* et *b* alors divise *r* = *a –* *bq* et donc est un diviseur de *b* et *r*.

On en déduit que l'ensemble des diviseurs communs de *a* et *b* est égal à l'ensemble des diviseurs communs de *b* et *r.* Et donc en particulier, .

Méthode : Recherche de par l'algorithme d'Euclide

 **Vidéo** [**https://youtu.be/npG\_apkI18o**](https://youtu.be/npG_apkI18o)

Déterminer le de 252 et 360.

On applique l'algorithme d'Euclide :

360 = 252 x 1 + 108

252 = 108 x 2 + 36

108 = 36 x 3 + 0

Le dernier reste non nul est 36 donc (252 ; 360) = 36.

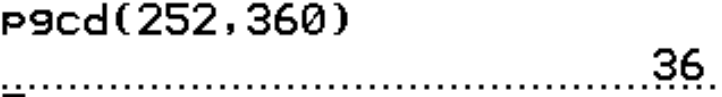
En effet, d'après la propriété précédente :

(252 ; 360) = (252 ; 108) = (108 ; 36) = (36 ; 0) = 36

Il est possible de vérifier le résultat à l'aide de la calculatrice :

Avec une TI 82/83 :

Touche "MATH" puis menu "NBRE" :



Avec une Casio 35+ :

Touche "OPTION" puis "⇨" (=touche F6).

Choisir "Num" puis "⇨".

Et choisir "GCD".

Capture d’écran 2012-06-13 à 14

Capture d’écran 2012-06-13 à 14

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

L'ensemble des diviseurs communs à *a* et *b* est l'ensemble des diviseurs de leur .

Démonstration :

On a démontré précédemment que l'ensemble des diviseurs communs de *a* et *b* est égal à l'ensemble des diviseurs communs de *b* et *r.*

En poursuivant par divisions euclidiennes successives, on obtient une liste strictement décroissante de restes **,**  En effet, on a successivement :

, , , , …

Il n'existe qu'un nombre fini d'entiers compris entre 0 et *r*.

Il existe donc un rang *k* tel que et .

Ainsi l'ensemble des diviseurs communs de *a* et *b* est égal à l'ensemble des diviseurs communs de *rk* et 0*.*

A noter qu'à ce niveau ce résultat démontre le fait que dans l'algorithme d'Euclide, le dernier reste non nul est égal au de *a* et *b.* En effet, (*rk* ; 0) = *rk*.

On en déduit que l'ensemble des diviseurs communs de *a* et *b* est égal à l'ensemble des diviseurs de *rk.*

Exemple :

 **Vidéo** [**https://youtu.be/leI0FUKjEcs**](https://youtu.be/leI0FUKjEcs)

Chercher les diviseurs communs de 2730 et 5610 revient à chercher les diviseurs de leur .

A l'aide de la calculatrice, on obtient : (2730 ; 5610) = 30.

Les diviseurs de 30 sont 1, 2, 3, 5, 6, 10, 15 et 30.

Donc les diviseurs communs à 2730 et 5610 sont 1, 2, 3, 5, 6, 10, 15 et 30.

Propriété : Soit *a*, *b* et *k* des entiers naturels non nuls.

Démonstration :

En appliquant l'algorithme d'Euclide, on obtient successivement :

Exemple :

 **Vidéo** [**https://youtu.be/EIcXmEi\_HPs**](https://youtu.be/EIcXmEi_HPs)

Chercher le de 420 et 540 revient à chercher le de 21 et 27.

En effet, 420 = 2 x 10 x 21 et 540 = 2 x 10 x 27.

Or (21 ; 27) = 3 donc (420 ; 540) = 2 x 10 x 3 = 60.

II. Théorème de Bézout et théorème de Gauss

1) Nombres premiers entre eux

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

On dit que *a* et *b* sont **premiers entre eux** lorsque leur est égal à 1.

Exemple :

 **Vidéo** [**https://youtu.be/Rno1eANN7aY**](https://youtu.be/Rno1eANN7aY)

42 et 55 sont premiers entre eux en effet (42 ; 55) = 1.

2) Théorème de Bézout

Propriété (Identité de Bézout) : Soit *a* et *b* deux entiers naturels non nuls et *d* leur .

Il existe deux entiers relatifs *u* et *v* tels que : *au* + *bv* = *d.*

Démonstration :

On appelle *E* l'ensemble des entiers strictement positifs de la forme *am* + *bn* avec *m* et *n* entiers relatifs.

*a* et *–a*  appartiennent par exemple à *E* donc *E* est non vide et *E* contient un plus petit élément strictement positif noté *d*.

- Démontrons que :

divise *a* et *b* donc divise *d* et donc .

- Démontrons que :

On effectue la division euclidienne de *a* par *d* :

Il existe un unique couple d'entiers (*q* ; *r*) tel que *a* = *dq* + *r* avec

On a alors :

Donc *r* est un élément de *E* plus petit que *d* ce qui est contradictoire et donc *r* = 0.

On en déduit que *d* divise *a*. On montre de même que *d* divise *b* et donc

.

On conclut que et finalement, il existe deux entiers *u* et *v* tels que :

*au* + *bv* =.

Exemple :

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

Il existe donc deux entiers *u* et *v* tels que : 54*u* + 42*v* = 6.

Le couple (*–*3 ; 4) convient. En effet : 54 x (*–*3) + 42 x 4 = 6.

Théorème de Bézout : Soit *a* et *b* deux entiers naturels non nuls.

*a* et *b* sont premiers entre eux si, et seulement si, il existe deux entiers relatifs *u* et *v* tels que *au* + *bv* = 1*.*

Démonstration :

- Si *a* et *b* sont premiers entre eux alors le résultat est immédiat d'après l'identité de Bézout.

- Supposons qu'il existe deux entiers relatifs *u* et *v* tels que *au* + *bv* = 1*.*

divise *a* et *b* donc divise *au* + *bv* = 1*.*

Donc. La réciproque est prouvée.

Exemple :

22 et 15 sont premiers entre eux.

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

Méthode : Démontrer que deux entiers sont premiers entre eux

 **Vidéo** [**https://youtu.be/oJuQv8guLJk**](https://youtu.be/oJuQv8guLJk)

Démontrer que pour tout entier naturel , et sont premiers entre eux.

D'après le théorème de Bézout, avec les coefficients et , on peut affirmer que

et sont premiers entre eux.

Propriété : Un entier admet un inverse modulo , si et sont premiers entre eux.

Méthode : Déterminer un inverse modulo

 **Vidéo** [**https://youtu.be/Pl4FaV5GZvc**](https://youtu.be/Pl4FaV5GZvc)

a) Déterminer un inverse de 5 modulo 16.

b) En déduire les solutions de l’équation .

a) 5 et 16 sont premiers entre eux, donc 5 admet un inverse modulo 16.

Déterminons cet inverse :

est inverse de 5 modulo 16, si .

Or *x* est nécessairement congru à l'un des entiers 0, 1, 2, 3, … ou 15 modulo 16.

Par disjonction des cas, on a :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *x* modulo 16 | 0 | 1 | 2 | 3 | … |
| 5*x* modulo 16 | 0 | 5 | 10 | –1 |  |

On peut arrêter la recherche car si alors

Ainsi est un inverse de 5 modulo 16.

b) .

Pour « se débarrasser » du facteur 5, on va multiplier les deux membres par un inverse de 5 :

Soit : ,

car .

Soit encore :

Réciproquement :

Si alors

.

On en déduit que .

Les entiers solutions sont tous les entiers de la forme , avec .

3) 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 *a* divise *c*.

Démonstration :

*a* divise *bc* donc il existe un entier *k* tel que *bc* = *ka*.

*a* et *b* sont premiers entre eux donc il existe deux entiers relatifs *u* et *v* tels que :

*au* + *bv* = 1*.*

Soit : *acu* + *bcv* = *c* soit encore *acu* + *kav* = *c*

Et donc *a*(*cu* + *kv*)= *c*

On en déduit que *a* divise *c*.

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

Si *a* et *b* divisent *c* et si *a* et *b* sont premiers entre eux alors *ab* divise *c*.

Démonstration :

*a* et *b* divisent *c* donc il existe deux entiers *k* et *k'* tel que *c* = *ka* = *k'b*.

Et donc *a* divise *k'b*.

*a* et *b* sont premiers entre eux donc d'après le théorème de Gauss, *a* divise *k'*.

Il existe donc un entier *k''* tel que *k'* = *ak''*.

Comme *c* = *k'b*, on a *c* = *ak''b* = *k''ab*

Et donc *ab* divise *c*.

Exemple :

6 et 11 divisent 660,

6 et 11 sont premiers entre eux,

donc 66 divise 660.

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 x 9 = 54 ne divise pas 18.

Méthode : Appliquer le théorème de Gauss

 **Vidéo** [**https://youtu.be/vTqqk96T\_Fo**](https://youtu.be/vTqqk96T_Fo)

a) Soit un entier naturel . On suppose que est un multiple de . Quelles sont les valeurs possibles pour  ?

b) Soit un entier naturel multiple de et de . Quelles sont les valeurs possibles pour  ?

a) est un multiple de donc 3 divise .

Or, et sont premiers entre eux, donc, d’après le théorème de Gauss, divise .

Et donc : , .

b) est multiple de et de , donc et divise .

Or, et sont premiers entre eux, donc, d’après le corollaire du théorème de Gauss, divise .

Et donc : , .

Méthode : Résoudre une équation diophantienne (du type *ax* + *by* = *c*)

 **Vidéo** [**https://youtu.be/0rbKnNjT3fY**](https://youtu.be/0rbKnNjT3fY)

a) Déterminer les entiers et tels que

b) Déterminer les entiers et tels que .

a) On a : . En choisissant , est entier.

Ainsi, le couple est une solution particulière de l'équation.

Donc

Soit .

divise et et sont premiers entre eux.

D'après le théorème de Gauss, divise .

On prouve de même que divise .

Il existe donc deux entiers et tels que et .

Réciproquement, on remplace dans l'équation soit :

et donc .

Ainsi, les solutions sont de la forme et , avec entier quelconque.

b) On a vu que : donc

Soit encore : et donc le couple est une solution particulière de l'équation.

En appliquant la même méthode qu'à la question a, on prouve que les solutions sont de la forme 8 et , avec entier quelconque.

II. Nombres premiers



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 : L’ensemble des nombres premiers est infini.

Démonstration :

Soit un nombre premier quelconque. Nous allons démontrer qu’il existe un nombre premier qui lui est plus grand.

On considère le produit de tous les nombres premiers compris entre 2 et .

On pose alors : .

* Si est premier alors il existe un nombre premier plus grand que car
* Si n’est pas premier :

admet donc au moins un diviseur premier

Supposons que soit compris entre 2 et , alors divise Comme divise également , alors divise *1*. Ce qui est contradictoire. Donc est plus grand que .

Il existe donc un nombre premier plus grand que .

Propriété : Tout entier naturel strictement supérieur à 1 et non premier admet un diviseur premier tel que .

Démonstration :

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

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

On peut écrire que avec  car est le plus petit élément de *E*.

Donc et donc .

Remarque :

Pour savoir si un nombre 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 a fallu attendre trois siècles et demi pour qu’en 1995, un anglais, *Andrew Wiles*, en vienne à bout et empoche récompenses et célébrité.

2) 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 , , …, nombres premiers distincts et , ..., entiers naturels non nuls.

Démonstration (difficile !) :

Existence :

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

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

que :

- Si est premier, l'existence est démontrée.

- Sinon, le plus petit diviseur de est premier et il existe un entier naturel tel que :

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

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

.

Unicité : On effectue une démonstration par récurrence

* Initialisation : Trivial pour .
* 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 : La décomposition de *k* en produit de facteurs premiers est unique.

Supposons qu'il existe deux décompositions distinctes :

.

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

Le nombre est inférieur à 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 et héréditaire à partir de ce rang. D'après le principe de récurrence, elle est vraie pour tout entier naturel .

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

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

Démonstration :

- divise

- Réciproquement, soit un diviseur de .

Donc tout facteur premier de divise et est donc égal à , , … ou .

Par extension, on en déduit que peut s'écrire

avec .

Exemple :

 **Vidéo** [**https://youtu.be/1WMQ-iH7-7c**](https://youtu.be/1WMQ-iH7-7c)

600 = 23 x 3 x 52

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

Méthode : Déterminer un ou un \*

 **Vidéo** [**https://youtu.be/2bIK1KkQ1k0**](https://youtu.be/2bIK1KkQ1k0)

*\* Plus Petit Commun Multiple*

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

b) En déduire le et le \* 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 de 17 640 et 411 600 est donc 23 x 3 x 5 x 72 = 5880

Le 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

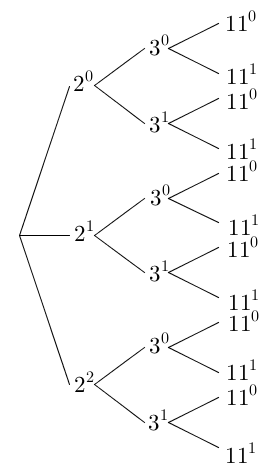
 **Vidéo** [**https://youtu.be/k0rhj8fwdjs**](https://youtu.be/k0rhj8fwdjs)

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 diviseurs 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.

3) Petit théorème de Fermat

Théorème : Si  est un [nombre premier](https://fr.wikipedia.org/wiki/Nombre_premier) et si  est un [entier](https://fr.wikipedia.org/wiki/Entier_relatif) non [divisible](https://fr.wikipedia.org/wiki/Divisible) par , alors  est divisible par .

Corollaire : Si  est un [nombre premier](https://fr.wikipedia.org/wiki/Nombre_premier) et si  est un [entier](https://fr.wikipedia.org/wiki/Entier_relatif), alors  est divisible par .

Méthode : Appliquer le petit théorème de Fermat

 **Vidéo** [**https://youtu.be/dMLtO6mB5yI**](https://youtu.be/dMLtO6mB5yI)

Démontrer que pour tout entier naturel , 7 divise .

7 est un nombre premier et 7 est premier avec 3. Donc, d’après le petit théorème de Fermat, on a :

7 divise , soit :

Soit encore :

Et donc, 7 divise .



Hors du cadre de la classe, aucune reproduction, même partielle, autres que celles prévues à l'article L 122-5 du code de la propriété intellectuelle, ne peut être faite de ce site sans l'autorisation expresse de l'auteur.

[*www.maths-et-tiques.fr/index.php/mentions-legales*](http://www.maths-et-tiques.fr/index.php/mentions-legales)