PGCD ET NOMBRES PREMIERS

**Partie 1 : 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 $PGCD$ de 60 et 100.

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

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

$PGCD$($a$; $b$).

Remarque :

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

Par exemple, $PGCD(–60 ;100) = PGCD(60 ;100).$

On a ainsi de façon générale : $PGCD\left(\left|a\right| ; \left|b\right|\right)=PGCD(a ;b)$.

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

a) $PGCD(a ;0)=a$

b) $PGCD(a ;1)=1$

c) Si $b$ divise $a$ alors $PGCD(a ; b)=b$

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 $PGCD$.

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 : $PGCD(a ;b) = PGCD(b ;r)$.

Démonstration :

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

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

Réciproquement, si $D$ un diviseur de $a$ et $b$ alors $D$ divise $r=a-bq$ et donc $D$ 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, $PGCD(a ;b) = PGCD(b ; r)$.

Méthode : Recherche de $PGCD$ par l'algorithme d'Euclide

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

Déterminer le $PGCD$ de 252 et 360.

**Correction**

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 $PGCD$(252 ; 360) = 36.

En effet, d'après la propriété précédente :

$PGCD$(252 ; 360) = $PGCD$(252 ; 108) = $PGCD$(108 ; 36) = $PGCD$(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".





*TP info sur tableur : L’algorithme d’Euclide*

[*http://www.maths-et-tiques.fr/telech/Euclide.pdf*](http://www.maths-et-tiques.fr/telech/Euclide.pdf)

[*http://www.maths-et-tiques.fr/telech/Euclide.ods*](http://www.maths-et-tiques.fr/telech/Euclide.ods) *(feuille de calcul OOo)*

*TP info sur tableur : L’algorithme le plus performant*

[*http://www.maths-et-tiques.fr/telech/Compa\_algo.pdf*](http://www.maths-et-tiques.fr/telech/Compa_algo.pdf)

[*http://www.maths-et-tiques.fr/telech/Compa\_algo.ods*](http://www.maths-et-tiques.fr/telech/Compa_algo.ods) *(feuille de calcul OOo)*

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 $PGCD$.

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 $r,r\_{1}$**,** $r\_{2}, r\_{3}, …$ En effet, on a successivement :

$0\leq r<b$, $0\leq r\_{1}<r$, $0\leq r\_{2}<r\_{1}$, $0\leq r\_{3}<r\_{2}$, …

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

Il existe donc un rang $k $tel que $r\_{k}\ne O$ et $r\_{k+1}=O$.

Ainsi l'ensemble des diviseurs communs de $a $et $b $est égal à l'ensemble des diviseurs communs de $r\_{k}$ 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 $PGCD$ de $a$ et $b$*.* En effet, $PGCD$($r\_{k}$ ; 0) = $r\_{k}$.

On en déduit que l'ensemble des diviseurs communs de $a$ et $b$est égal à l'ensemble des diviseurs de $r\_{k}$*.*

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 $PGCD$.

A l'aide de la calculatrice, on obtient : $PGCD$(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.

$$PGCD\left(ka ;kb\right)=k×PGCD\left(a ;b\right)$$

Démonstration :

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

$$PGCD\left(ka ;kb\right)=PGCD\left(kb ;kr\right)=PGCD\left(kr ;kr\_{1}\right)=PGCD\left(kr\_{1} ;kr\_{2}\right)=…=PGCD\left(kr\_{k} ;0\right)=kr\_{k}=k×PGCD\left(a ;b\right)$$

Exemple :

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

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

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

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

**Partie 2 : 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 $PGCD$ est égal à 1.

Exemple :

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

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

 2) 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 : $au+bv=d$*.*

Démonstration au programme :

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 $PGCD(a ;b)\leq d$ :

$PGCD(a ;b)$ divise $a$ et $b$ donc divise $d$ et donc $PGCD(a ;b)\leq d$.

- Démontrons que $ d\leq PGCD(a ;b)$ :

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

Il existe un unique couple d'entiers ($q$ ; $r$) tel que $a=dq+r$avec $0\leq r<d$

On a alors :

$$r=a-dq=a-\left(au+bv\right)q=a-auq-bvq=\left(1-uq\right)a-vqb$$

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

$d\leq PGCD(a ;b)$.

On conclut que $d=PGCD(a ;b)$ et finalement, il existe deux entiers $u$ et $v$ tels que :

$au+bv$ =$ PGCD(a ;b)$.

Exemple :

 **Vidéo** [**https://youtu.be/HSrIYM8ufoE**](https://youtu.be/HSrIYM8ufoE)

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

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

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 $au+bv=1$*.*

$PGCD(a ;b)$ divise $a$ et $b$ donc divise $au+bv=1$*.*

Donc$ PGCD\left(a ;b\right)=1$. La réciproque est prouvée.

Exemple :

22 et 15 sont premiers entre eux.

On est alors assuré que l'équation $22x+15y=1$ 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 $n$, $2n+3$ et $5n+7$ sont premiers entre eux.

**Correction**

$$5\left(2n+3\right)-2\left(5n+7\right)=10n+15-10n-14=1$$

D'après le théorème de Bézout, avec les coefficients $5$ et $-2$, on peut affirmer que

$2n+3$ et $5n+7$ sont premiers entre eux.

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

Méthode : Déterminer un inverse modulo $n$

 **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 $5x≡7[16]$.

**Correction**

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

Déterminons cet inverse :

$x$ est inverse de 5 modulo 16, si $5x≡1[16]$.

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

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

Par disjonction des cas, on a :

On peut arrêter la recherche car si $5×3≡-1[16]$ alors $5×\left(-3\right)≡1\left[16\right].$

Ainsi $-3$ est un inverse de 5 modulo 16.

b) $5x≡7[16]$.

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

Soit : $-3×5x≡-3×7[16]$,

$$-15x≡-21[16]$$

$1x≡-21[16]$ car $-15≡1[16]$.

Soit encore :

$$x≡11[16]$$

Réciproquement :

Si $x≡11[16]$ alors $5×x≡5×11[16]$

$$5x≡55\left[16\right]$$

$5x≡7[16]$.

On en déduit que $x≡11\left[16\right]$.

Les entiers $x$ solutions sont tous les entiers de la forme $11+16k$, avec $k\in Z$.

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 au programme :

$a$ 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 $n$. On suppose que $5n$ est un multiple de $3$. Quelles sont les valeurs possibles pour $n$ ?

b) Soit un entier naturel $n$ multiple de $7$ et de $11$. Quelles sont les valeurs possibles pour $n$ ?

**Correction**

a) $5n$ est un multiple de $3$ donc 3 divise $5n$.

Or, $3$ et $5$ sont premiers entre eux, donc, d’après le théorème de Gauss, $3$ divise $n$.

Et donc : $n=3k$, $k\in N$.

b) $n$ est multiple de $7$ et de $11$, donc $7$ et $11$ divise $n$.

Or, $7$ et $11$ sont premiers entre eux, donc, d’après le corollaire du théorème de Gauss, $7×11=77$ divise $n$.

Et donc : $n=77k$, $k\in N$.

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

 **Vidéo** [**https://youtu.be/XpYK-F4hX24**](https://youtu.be/XpYK-F4hX24)

a) Déterminer les entiers $x$ et $y$ tels que $5x+7y=1.$

b) Déterminer les entiers $x$ et $y$ tels que $5x+7y=12$.

**Correction**

a) **SOLUTION PARTICULIÈRE :**

On a : $y=$ $\frac{1-5x}{7}$. En choisissant $x=-4$, $y$ est entier.

Ainsi, le couple $(-4 ;3)$ est une solution particulière de l'équation.

**SOLUTION GÉNÉRALE :**

- Donc $5x+7y=5×\left(-4\right)+7×3.$

Soit $5\left(x+4\right)=7(3-y)$.

$5$ divise $7(3-y)$ et $5$ et $7$ sont premiers entre eux.

D'après le théorème de Gauss, $5$ divise $3-y$.

Il existe donc un entier $k $tel que $3-y=5k$, soit : $y=3-5k$.

En substituant dans l’équation $5\left(x+4\right)=7(3-y)$, on a :

$$5\left(x+4\right)=7(3-3+5k)$$

$$5x+20=7×5k$$

$$x=7k-4$$

- Réciproquement, on vérifie que le couple $(7k-4 ;3-5k)$ est solution de l’équation $5x+7y=1$ :

$$5\left(7k-4 \right)+7\left(3-5k\right)=35k-20+21-35k=1$$

- Ainsi, les solutions sont de la forme $x=7k-4$ et $y=3-5k$, avec $k$ entier relatif.

b) On a vu que : $5×\left(-4\right)+7×3=1$ donc $5×\left(-4\right)×12+7×3×12=12$

Soit encore : $5×\left(-48\right)+7×36=12$ et donc le couple $(-48 ;36)$ 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 $x=7k-4$8 et $y=36-5k$, avec $k$ entier relatif.

**Partie 3 : 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 au programme :

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

On considère le produit $2×3×5×…×n$ de tous les nombres premiers compris entre 2 et $n$.

On pose alors : $M=\left(2×3×5×…×n\right)+1$.

* Si $M$ est premier alors il existe un nombre premier plus grand que $n$ car $\left(2×3×5×…×n\right)+1>n.$
* Si $M$ n’est pas premier :

$M$ admet donc au moins un diviseur premier $p.$

Supposons que $p$ soit compris entre 2 et $n$, alors $p$ divise $2×3×5×…×n.$ Comme $p$ divise également $M=\left(2×3×5×…×n\right)+1$, alors $p$ divise *1*. Ce qui est contradictoire. Donc $p$ est plus grand que $n$.

Il existe donc un nombre premier $p$ plus grand que $n$.

Propriété : Tout entier naturel $n$ strictement supérieur à 1 et non premier admet un diviseur premier $p$ tel que $p\leq \sqrt{n}$.

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$$\leq q$ car $p$ est le plus petit élément de *E*.

Donc $p×p\leq p×q=n$ et donc $p\leq \sqrt{n}$.

Remarque :

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

Méthode : Déterminer si un nombre est premier ou non

391 est-il premier ?

**Correction**

Pour le vérifier, on teste la divisibilité par tous les nombres premiers inférieurs à $\sqrt{391}≈19,8$.

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 $x^{n}+y^{n}=z^{n}$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 produits de 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 $n=p\_{1}^{α\_{1}}×p\_{2}^{α\_{2}}×…×p\_{r}^{α\_{r}}$ avec $p\_{1}$, $p\_{2}$, …, $p\_{r}$ nombres premiers distincts et $α\_{1}, α\_{2}$, ..., $α\_{r}$ entiers naturels non nuls.

Démonstration (difficile !) :

Existence :

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

- Sinon, le plus petit diviseur $p\_{1}$ de $n$ est premier et il existe un entier naturel $n\_{1}$ tel

que : $n=p\_{1}n\_{1}$

 - Si $n\_{1}$ est premier, l'existence est démontrée.

 - Sinon, le plus petit diviseur $p\_{2}$ de $n\_{1}$ est premier et il existe un entier naturel $n\_{2}$ tel que : $n\_{1}=p\_{2}n\_{2}$

On réitère le processus pour obtenir une suite $\left(n\_{k}\right)$ décroissante et finie d'entiers naturels.

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

$n=p\_{1}^{α\_{1}}×p\_{2}^{α\_{2}}×…×p\_{r}^{α\_{r}}$.

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 :

$k=p\_{1}p\_{2}…p\_{r}=q\_{1}q\_{2}…q\_{s}$.

Donc $p\_{1}$ divise $q\_{1}q\_{2}…q\_{s}$ et donc il existe un entier $q\_{i}$ tel que $p\_{1}$ et $q\_{i}$ ne soient pas premiers entre eux. Comme $p\_{1}$ et $q\_{i}$ sont premiers, on a $p\_{1}=q\_{i}$.

Le nombre $l=$ $\frac{k}{p\_{1}}$ est inférieur à $k$ et on a :

$$l=p\_{2}p\_{3}…p\_{r}=q\_{1}q\_{2}…q\_{i-1}q\_{i+1}…q\_{r}$$

$l$ 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 $p\_{1}^{α\_{1}}×p\_{2}^{α\_{2}}×…×p\_{r}^{α\_{r}}$ 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 $p\_{1}^{β\_{1}}×p\_{2}^{β\_{2}}×…×p\_{r}^{β\_{r}}$ avec $0\leq β\_{i}\leq α\_{i}$ pour tout $1\leq i\leq r$.

Démonstration :

- $p\_{1}^{β\_{1}}×p\_{2}^{β\_{2}}×…×p\_{r}^{β\_{r}}$ divise $p\_{1}^{α\_{1}}×p\_{2}^{α\_{2}}×…×p\_{r}^{α\_{r}}$

- Réciproquement, soit $d$ un diviseur de $n=p\_{1}^{α\_{1}}×p\_{2}^{α\_{2}}×…×p\_{r}^{α\_{r}}$.

Donc tout facteur premier de $d$ divise $n$ et est donc égal à $p\_{1}$, $p\_{2}$, … ou $p\_{r}$.

Par extension, on en déduit que $d$ peut s'écrire $p\_{1}^{β\_{1}}×p\_{2}^{β\_{2}}×…×p\_{r}^{β\_{r}}$

avec $0\leq β\_{i}\leq α\_{i}$.

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 $PGCD$ ou un $PPCM$\*

 **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 $PGCD$ et le $PPCM$\* de ces deux nombres.

**Correction**

a) 17 640 = 2 $×$ 8820 411 600 = 2 $×$ 205 800

 = 22 $×$ 4410 = 22 $×$ 102 900

 = 23 $×$ 2205 = 23 $×$ 51 450

 = 23 $×$ 3 $×$ 735 = 24 $×$ 25 725

 = 23 $×$ 32 $×$ 245 = 24 $×$ 3 $×$ 8575

 = 23 $×$ 32 $×$ 5 $×$ 49 = 24 $×$ 3 $×$ 5 $×$ 1715

 = 23 $×$ 32 $×$ 5 $×$ 72 = 24 $×$ 3 $×$ 52 $×$ 343

 = 24 $×$ 3 $×$ 52 $×$ 7 $×$ 49

 = 24 $×$ 3 $×$ 52 $×$ 73

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

Le $PPCM$ de 17 640 et 411 600 est donc 24 $×$ 32 $×$ 52 $×$ 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.

**Correction**

On décompose 132 en produit de facteurs premiers :

132 = 2 $×$ 66 = 2 $×$ 2 $×$ 33 = 22 $×$ 3 $×$ 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 $×$ 30 $×$ 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) $×$ (1 + 1) $×$ (1 + 1) = 12 diviseurs.

3) Petit théorème de Fermat

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

$a^{p–1}-1$ est divisible par $p$.

Corollaire : Si $p$ est un [nombre premier](https://fr.wikipedia.org/wiki/Nombre_premier) et si $a$ est un [entier](https://fr.wikipedia.org/wiki/Entier_relatif), alors $a^{p}-a$ est divisible par $p$.

Méthode : Appliquer le petit théorème de Fermat

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

Démontrer que pour tout entier naturel $n$, 7 divise $3^{6n}-1$.

**Correction**

7 est un nombre premier et 7 est premier avec 3. Donc, d’après le petit théorème de Fermat, on a : 7 divise $3^{7–1}-1$, soit :

$$3^{7–1}-1≡0\left[7\right]$$

$$3^{6}≡1\left[7\right]$$

Soit encore : $\left(3^{6}\right)^{n}≡1^{n}\left[7\right]$

$$3^{6n}≡1\left[7\right]$$

$$3^{6n}-1≡0\left[7\right]$$

Et donc, 7 divise $3^{6n}-1$.

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)