

PGCD ET NOMBRES PREMIERS

Partie 1 : PGCD de deux entiers

1) Définition et propriétés

Exemple :

▶ Vidéo <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 on 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 : $PGCD(|a| ; |b|) = PGCD(a ; b)$.

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 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_apk18o

Déterminer le $PGCD$ de 252 et 360.

Correction

On applique l'algorithme d'Euclide :

$$360 = 252 \times 1 + 108$$

$$252 = 108 \times 2 + 36$$

$$108 = 36 \times 3 + 0$$

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" :

$$\begin{array}{r} \text{Pgcd}(252, 360) \\ \dots\dots\dots 36 \end{array}$$

Avec une Casio 35+ :

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

Choisir "Num" puis "⇒".

Et choisir "GCD".

$$\begin{array}{r} \text{GCD}(252, 360) \\ 36 \end{array}$$

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.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.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, \dots . En effet, on a successivement :

$$0 \leq r < b, 0 \leq r_1 < r, 0 \leq r_2 < r_1, 0 \leq r_3 < r_2, \dots$$

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

Il existe donc un rang k tel que $r_k \neq 0$ et $r_{k+1} = 0$.

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/le10FUKjEcs>

Chercher les diviseurs communs de 2 730 et 5 610 revient à chercher les diviseurs de leur $PGCD$.

A l'aide de la calculatrice, on obtient : $PGCD(2\ 730 ; 5\ 610) = 30$.

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

Donc les diviseurs communs à 2 730 et 5 610 sont 1, 2, 3, 5, 6, 10, 15 et 30.

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

$$PGCD(ka ; kb) = k \times PGCD(a ; b)$$

Démonstration :

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

$$\begin{aligned} PGCD(ka ; kb) &= PGCD(kb ; kr) = PGCD(kr ; kr_1) = PGCD(kr_1 ; kr_2) = \dots \\ &= PGCD(kr_k ; 0) = kr_k = k \times PGCD(a ; b) \end{aligned}$$

Exemple :

 Vidéo https://youtu.be/EIcXmEi_HPs

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

En effet, $420 = 2 \times 10 \times 21$ et $540 = 2 \times 10 \times 27$.

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

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>

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 :

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

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>

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 : $54 \times (-3) + 42 \times 4 = 6$.

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

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

Correction

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

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/PI4FaV5GZvc>

- a) Déterminer un inverse de 5 modulo 16.
 b) En déduire les solutions de l'équation $5x \equiv 7[16]$.

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 $5x \equiv 1[16]$.

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	...
$5x$ modulo 16	0	5	10	-1	

On peut arrêter la recherche car si $5 \times 3 \equiv -1[16]$ alors $5 \times (-3) \equiv 1[16]$.
Ainsi -3 est un inverse de 5 modulo 16.

b) $5x \equiv 7[16]$.

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

Soit : $-3 \times 5x \equiv -3 \times 7[16]$,

$-15x \equiv -21[16]$

$1x \equiv -21[16]$ car $-15 \equiv 1[16]$.

Soit encore :

$x \equiv 11[16]$

Réciproquement :

Si $x \equiv 11[16]$ alors $5 \times x \equiv 5 \times 11[16]$

$5x \equiv 55[16]$

$5x \equiv 7[16]$.

On en déduit que $x \equiv 11[16]$.

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

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 $6 \times 9 = 54$ ne divise pas 18.

Méthode : Appliquer le théorème de Gauss

 Vidéo https://youtu.be/vTqgk96T_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 : $n = 3k$, $k \in \mathbb{N}$.

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

Or, 7 et 11 sont premiers entre eux, donc, d'après le corollaire du théorème de Gauss,

$7 \times 11 = 77$ divise n .

Et donc : $n = 77k$, $k \in \mathbb{N}$.

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

 Vidéo <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 $5x + 7y = 5 \times (-4) + 7 \times 3$.

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

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 $5(x + 4) = 7(3 - y)$, on a :

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

$$5x + 20 = 7 \times 5k$$

$$x = 7k - 4$$

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

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

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

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

Soit encore : $5 \times (-48) + 7 \times 36 = 12$ 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 $x = 7k - 48$ 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 $2 \times 3 \times 5 \times \dots \times n$ de tous les nombres premiers compris entre 2 et n .

On pose alors : $M = (2 \times 3 \times 5 \times \dots \times n) + 1$.

- Si M est premier alors il existe un nombre premier plus grand que n car $(2 \times 3 \times 5 \times \dots \times n) + 1 > n$.

- 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 $2 \times 3 \times 5 \times \dots \times n$. Comme p divise également $M = (2 \times 3 \times 5 \times \dots \times n) + 1$, 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 $p \times p \leq p \times q = n$ 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 $\sqrt{391} \approx 19,8$.

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.

$$600 = 6 \times 100 = 6 \times 10^2 = 2 \times 3 \times 2^2 \times 5^2 = 2^3 \times 3 \times 5^2$$

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 $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ avec p_1, p_2, \dots, p_r nombres premiers distincts et $\alpha_1, \alpha_2, \dots, \alpha_r$ 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

$$\text{que : } n = p_1 n_1$$

- 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 (n_k) décroissante et finie d'entiers naturels.

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

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}.$$

Unicité : On effectue une démonstration par récurrence

- Initialisation : Trivial pour $n = 2$.

- Hérité :

- 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 :

$$k = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s.$$

Donc p_1 divise $q_1 q_2 \dots q_s$ 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 :

$$l = p_2 p_3 \dots p_r = q_1 q_2 \dots q_{i-1} q_{i+1} \dots q_s$$

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 $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ la décomposition en produit de facteurs premiers d'un entier naturel n strictement supérieur à 1.

Tout diviseur de n admet une décomposition en produit de facteurs premiers de la forme $p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq r$.

Démonstration :

- $p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_r^{\beta_r}$ divise $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$

- Réciproquement, soit d un diviseur de $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$.

Donc tout facteur premier de d divise n et est donc égal à p_1, p_2, \dots ou p_r .

Par extension, on en déduit que d peut s'écrire $p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$.

Exemple :

 **Vidéo** <https://youtu.be/1WMQ-iH7-7c>

$$600 = 2^3 \times 3 \times 5^2$$

Donc $2^2 \times 3^0 \times 5^1 = 20$ est un diviseur de 600.

Méthode : Déterminer un *PGCD* ou un *PPCM**

 **Vidéo** <https://youtu.be/2bIK1KkQ1k0>

* Plus Petit Commun Multiple

- Décomposer 17 640 et 411 600 en produits de facteurs premiers.
- En déduire le *PGCD* et le *PPCM** de ces deux nombres.

Correction

$$\text{a) } 17\,640 = 2 \times 8\,820$$

$$= 2^2 \times 4\,410$$

$$= 2^3 \times 2\,205$$

$$= 2^3 \times 3 \times 735$$

$$= 2^3 \times 3^2 \times 245$$

$$= 2^3 \times 3^2 \times 5 \times 49$$

$$= 2^3 \times 3^2 \times 5 \times 7^2$$

$$411\,600 = 2 \times 205\,800$$

$$= 2^2 \times 102\,900$$

$$= 2^3 \times 51\,450$$

$$= 2^4 \times 25\,725$$

$$= 2^4 \times 3 \times 8\,575$$

$$= 2^4 \times 3 \times 5 \times 1\,715$$

$$= 2^4 \times 3 \times 5^2 \times 343$$

$$= 2^4 \times 3 \times 5^2 \times 7 \times 49$$

$$= 2^4 \times 3 \times 5^2 \times 7^3$$

b) Le *PGCD* de 17 640 et 411 600 est donc $2^3 \times 3 \times 5 \times 7^2 = 5\,880$

Le *PPCM* de 17 640 et 411 600 est donc $2^4 \times 3^2 \times 5^2 \times 7^3 = 1\,234\,800$

Méthode : Déterminer tous les diviseurs d'un entier

 Vidéo <https://youtu.be/k0rhi8fwdjs>

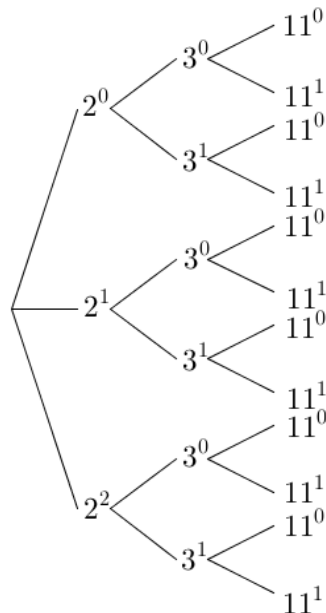
Déterminer tous les diviseurs de 132.

Correction

On décompose 132 en produit de facteurs premiers :

$$132 = 2 \times 66 = 2 \times 2 \times 33 = 2^2 \times 3 \times 11$$

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, $2^1 \times 3^0 \times 11^1 = 22$ 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 $(2 + 1) \times (1 + 1) \times (1 + 1) = 12$ diviseurs.

3) Petit théorème de Fermat

Théorème : Si p est un nombre premier et si a est un entier non divisible par p , alors $a^{p-1} - 1$ est divisible par p .

Corollaire : Si p est un nombre premier et si a est un entier, alors $a^p - a$ est divisible par p .

Méthode : Appliquer le petit théorème de Fermat

 Vidéo <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 :

$$3^{7-1} - 1 \equiv 0[7]$$

$$3^6 \equiv 1[7]$$

Soit encore : $(3^6)^n \equiv 1^n[7]$

$$3^{6n} \equiv 1[7]$$

$$3^{6n} - 1 \equiv 0[7]$$

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