Terminale S – Spécialité **Cours : NOMBRES PREMIERS - PPCM.**

A la fin de ce chapitre vous devez être capable de :

• savoir déterminer si un entier est premier en utilisant le nombre minimal de divisions par la suite des nombres premiers. • savoir décomposer un entier en produit de facteurs premiers. • savoir utiliser la décomposition en produits de facteurs premiers dans les problèmes de divisibilité. • connaître le PPCM de deux entiers naturels.	• savoir déterminer le PPCM et le PGCD de deux entiers naturels à partir de leur décomposition en facteurs premiers. • savoir utiliser le lien entre le PPCM et le PGCD de deux entiers naturels. • savoir utiliser une calculatrice pour déterminer la décomposition en facteurs premiers d'un entier naturel. • savoir résoudre des équations ou systèmes d'équations où interviennent le PGCD et le PPCM de deux entiers.

I. Nombres premiers.

1. Définition et exemples.

Définition 1 : On dit qu'un entier naturel n est **premier** s'il possède exactement deux diviseurs dans $\mathbb{N}$.

Cela revient à dire que l'entier naturel n est premier si ses diviseurs sont 1 et n.

Exemples :

- 0 et 1 ne sont pas premiers
- 2, 3, 5, 7 sont des nombres premiers.

Remarques :

- Ne pas confondre nombre premier et nombres premiers entre eux.
- Si p est un nombre premier et n un entier, ou bien p divise n ou bien p est premier avec n.
- Un entier naturel supérieur ou égal à 2 qui n'est pas premier est dit **composé**.

Propriétés :

1. Tout entier plus grand que 1 admet au moins un diviseur premier.
2. Tout entier naturel non premier n différent de 1 admet un diviseur premier a tel que $a \leq \sqrt{n}$.
3. Il y a une infinité de nombres premiers.

Démonstration

Propriété 1

Soit n un entier strictement supérieur à 1.

- Si n est premier, il admet lui-même comme diviseur premier.
- Si n est composé, il admet d'autres diviseurs que 1 et n ; soit p le plus petit d'entre eux. Alors p est premier ; sinon, il serait composé et il admettrait un diviseur d tel que $1 < d < p$; mais d serait alors un diviseur de n plus petit que p, ce qui est impossible. Donc, p est premier et n admet p comme diviseur premier.

Propriété 2

Soit n un entier composé strictement supérieur à 1.
n admet un diviseur d autre que 1 et n.
Alors $n = d \times d'$ avec $d' > 0$.
d est supérieur ou égal à 2.
d' est aussi supérieur ou égal à 2, car si $d' = 1$ alors on aurait $n = d$.

Supposons $d \leq d'$.
Alors $d^2 \leq dd'$, soit $d^2 \leq n$ ou encore $d \leq \sqrt{n}$.
D'après le résultat précédent, d admet au moins un diviseur premier a qui est aussi un diviseur premier de n.
Comme $a \leq d$, on en déduit que $a \leq \sqrt{n}$.

Propriété 3
Raisonnons par l'absurde en supposant qu'il existe un nombre fini d'entiers premiers $p_1, p_2, \ldots, p_n$.
Soit $N = p_1 \times p_2 \times \ldots \times p_n + 1$
N est un entier supérieur ou égal à 2, il admet donc au moins diviseur premier p_i (avec $1 \leq i \leq n$) de l'ensemble $\{ p_1 ; p_2 ; \ldots ; p_n \}$ (d'après la propriété 1).
p_i divise N et p_i divise $p_1 \times p_2 \times \ldots \times p_n$; donc p_i divise $N - p_1 \times p_2 \times \ldots \times p_n = 1$.
Donc $p_i = 1$: ce qui est impossible puisque 1 n'est pas premier.
Conclusion : l'ensemble des nombres premiers est infini.

Propriété (Test de primalité) : Soit n un entier naturel supérieur ou égal à 2.
Si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à sa racine carrée, on peut affirmer qu'il est premier.

Tester la primalité d'un entier naturel, c'est vérifier s'il est premier ou non.

Démonstration : C'est la contraposée de la propriété 2 précédente.

Exemple : 247 est-il premier ?
Comme $\sqrt{247} \approx 15{,}7$ il suffit d'examiner si 247 est divisible par 2, 3, 5, 7, 11 et 13.
Puisque 247 n'est divisible par aucun de ces entiers, alors 247 est un nombre premier.

II. Décomposition en facteurs premiers

a) Existence et unicité.

Théorème fondamental :
Tout entier naturel strictement supérieur à 1 se décompose en produit de facteurs premiers et cette décomposition est unique (à l'ordre des facteurs près).

Démonstration de l'existence

Soit n un entier naturel au moins égal à 2.

On montre l'existence d'une telle décomposition pour n.

Si n est premier, n se décompose en un seul facteur premier : lui-même.

Si n est composé, il admet au moins un diviseur premier p et :

$$n = p \times d_1, \text{ avec } 1 < p < n \text{ et } 1 < d_1 < n.$$

Si d_1 est premier, on a décomposé n en produits de deux facteurs.

Si d_1 est composé, on utilise le résultat précédent pour écrire que :

$d_1 = p' \times d_2$, avec p' premier, $1 < p' < d_1$ et $1 < d_2 < d_1$.

On a alors $n = p \times p' \times d_2$.

Les entiers d_1, d_2, …forment une suite strictement décroissante d'entiers naturels ; on continue le procédé jusqu'à ce que le dernier quotient obtenu soit égal à 1 : on a alors la décomposition annoncée.

On admet l'unicité de cette décomposition.

Exemple : Quelle est la décomposition en facteurs premiers de 11 400 ?

11 400	2
5700	2
2850	2
1425	3
475	5
95	5
19	19
1	

Donc $11\,400 = 2^3 \times 3 \times 5^2 \times 19$

Commentaire : Les nombres premiers sont donc les « briques » élémentaires de l'arithmétique au même titre que les atomes sont celles de la chimie.

Remarques :

- Comme dans l'exemple ci-dessus, les facteurs premiers obtenus ne sont pas nécessairement distincts. Dans la suite, nous appellerons **décomposition de n en produit de facteurs premiers** l'écriture $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ où $p_1, p_2, \ldots p_k$ sont des nombres premiers distincts et $\alpha_1, \alpha_2, \ldots \alpha_k$ des entiers naturels non nuls.
- Si des nombres premiers distincts $p_1, p_2, \ldots p_k$ divisent un entier naturel n, ce sont tous des facteurs de la décomposition en facteurs premiers de n et par suite, leur produit divise n.

b) Application à la recherche de diviseurs.

Propriété (condition de divisibilité) :
Un entier naturel d divise un entier naturel n si, et seulement si, les facteurs premiers de la décomposition en facteurs premiers de d se trouvent dans celle de n avec des exposants au moins égaux à ceux avec lesquels ils figurent dans celle de d.

Démonstration

- Supposons que d divise n.

Soit p un facteur premier de la décomposition de d, et α l'exposant de p dans cette décomposition.

Alors $n = d \times q = (p^{\alpha} a)q$, avec a et q entiers.

On a $n = p^{\alpha}(aq)$. Soit β l'exposant de p dans la décomposition en facteurs premiers de aq et γ l'exposant de p dans celle de n.

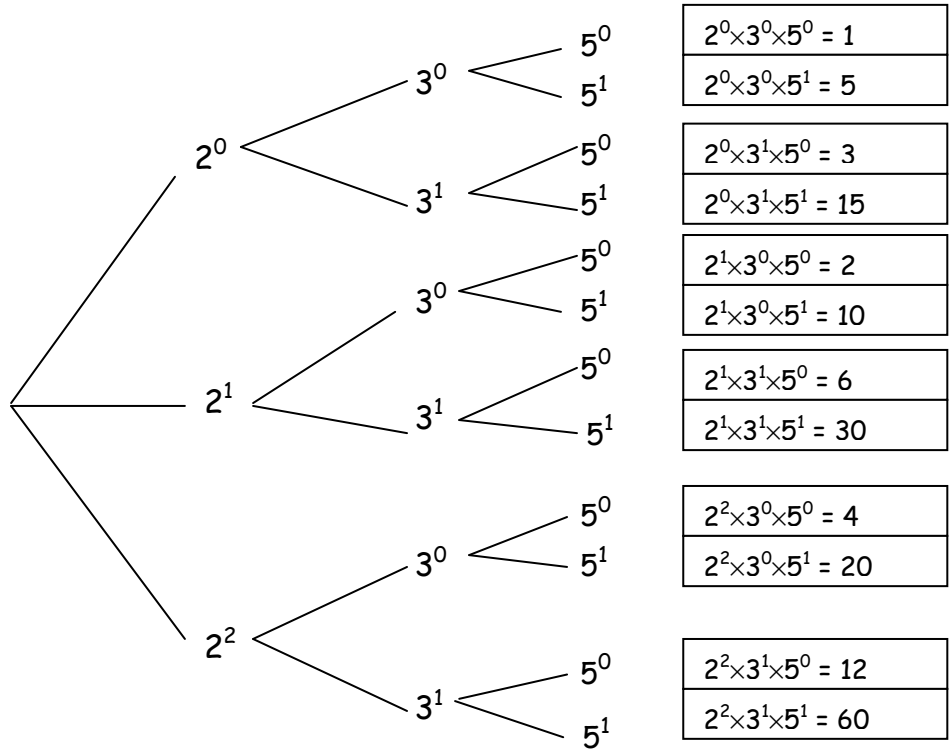
On a $\gamma = \alpha + \beta$, donc on a bien $\alpha \leq \beta$.

- Réciproquement, soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ et $d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ avec :

$$0 \leq \beta_i \leq \alpha_i \text{ pour } i \in [1 ; r].$$

Alors, d divise n, car on peut écrire : $n = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \ldots\ldots p_r^{\alpha_r - \beta_r} \times d$

Exemple : On se propose de déterminer tous les diviseurs positifs de 60.
Nous allons utiliser sa décomposition en produit de facteurs premiers : $60 = 2^2 \times 3 \times 5$. Les diviseurs positifs de 60 sont les entiers de la forme $2^a \times 3^b \times 5^c$ avec $0 \leq a \leq 2$; $0 \leq b \leq 1$ et $0 \leq c \leq 1$.
Pour déterminer tous les cas possibles, nous utiliserons un arbre :



Les diviseurs positifs de 60 sont donc 1 – 2 – 3 – 4 – 5 – 6 – 10 - 12 -15 – 20 - 30 – 60.
On en déduit également le nombre de diviseurs positifs de 60 : $(2 + 1) \times (1 + 1) \times (1 + 1) = 12$.

De façon plus générale, si la décomposition en facteurs premiers de l'entier naturel n est de la forme :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

Alors, le nombre de diviseurs positifs de n est : $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \ldots \times (\alpha_k + 1)$.

III. Plus Petit Commun Multiple de deux entiers

Propriété et Définition *:* Soit a et b deux entiers relatifs non nuls. L'ensemble des multiples communs strictement positifs à a et b admet un plus petit élément m, noté m = PPCM(a ;b) et appelé plus petit multiple commun à a et b.

Exemples :

- Les multiples strictement positifs de 9 sont : 9 ;18 ;27 ;36 ; …..
- Les multiples strictement positifs de 12 sont : 12 ;24 ;36 ;48 ;…..

Donc PPCM(9 ; 12) = 36

Remarques :

- PPCM(a ; b) = PPCM(b ; a) = PPCM($|a|$; $|b|$) donc on se ramènera en général à a et b positifs.
- Si a est un entier naturel non nuls, PPCM(1 ; a) = a
- Si a et b sont deux entiers naturels non nuls tels que b divise a alors PPCM(a ; b) =a

Propriété *:* Soit a et b deux entiers relatifs non nuls. Les multiples communs à a et b sont les multiples de PPCM(a ;b)

Propriété *:* Soit a et b deux entiers relatifs non nuls. Pour tout $k \in \mathbb{Z}^*$,

$$PPCM(ka ;kb) = |k| \times PPCM(a ;b).$$

IV. Déterminer un PGCD, un PPCM.

a) PGCD, PPCM et décomposition.

Propriété (décomposition en facteurs premiers du PGCD et du PPCM) *:*

Soit a et b deux entiers supérieurs ou égaux à 2.

- PGCD(a ; b) est égal au produit des facteurs premiers communs aux deux nombres, chacun étant affecté du plus petit exposant avec lequel il figure dans leurs deux décompositions.
- PPCM(a ;b) est égal au produit des facteurs premiers figurant dans l'une ou l'autre de leurs décompositions, chacun étant affecté de son exposant s'il n'apparaît que dans l'une des deux décompositions ou du plus grand des deux exposants s'il apparaît dans les deux.

Exemples *:*

- Calculons PGCD(1 008 ; 540) par cette méthode.

$1\,008 = 2^4 \times 3^2 \times 7$ et $540 = 2^2 \times 3^3 \times 5$ donc PGCD(1 008 ; 540) = $2^2 \times 3^2 = 36$

- Déterminons par cette méthode PPCM(1 008 ; 540).

$1\,008 = 2^4 \times 3^2 \times 7$ et $540 = 2^2 \times 3^3 \times 5$ donc PPCM(1 008 ; 540) = $2^4 \times 3^3 \times 5 \times 7 = 15120$

b) Relation entre PGCD et PPCM.

Propriétés *:*

1. Soit a' et b' deux entiers premiers entre eux, alors PPCM(a' ;b') = |a'b'|.
2. Soit a et b deux entiers relatifs non nuls, alors on a :

$$PGCD(a ;b) \times PPCM(a ;b) = |a| \times |b|.$$

Démonstration du 2

Comme PPCM(a ;b) = PPCM(|a| ;|b|), on se limite à a et b entiers naturels.

Soit δ = PGCD(a ;b) et μ = PPCM(a ;b).

On a alors a= $\delta a'$ et b = $\delta b'$ avec a' et b' premiers entre eux.

On a donc PPCM(a' ;b') = a'b'

μ = PPCM($\delta a'$; $\delta b'$) = $\delta \times$PPCM(a' ; b') = $\delta \times a' \times b'$

Ainsi $\delta\mu = \delta^2 \times a' \times b' = \delta \times a' \times \delta \times b' = ab$