Fiche sur les nombres premiers

I. Généralités

1°) Définition

On dit qu'un entier naturel est **premier** s'il admet exactement deux diviseurs dans $\mathbb{N}$: 1 et lui-même.

2°) Remarque

0 et 1 ne sont pas premiers.

3°) Propriété

Soit n un entier naturel tel que $n \geqslant 4$.
n non premier $\Leftrightarrow$ $n = pq$ avec $p \geqslant 2$ et $q \geqslant 2$

4°) Propriété (un test de primalité)

n est un entier naturel supérieur ou égal à 4.
Si n n'est divisible par aucun nombre premier p tel que $2 \leqslant p \leqslant \sqrt{n}$, alors n est premier.

En pratique, pour déterminer si un entier naturel n est premier, il suffit de disposer de la liste des nombres premiers p_1, p_2, …, p_k inférieurs ou égaux à $\sqrt{n}$.
Si aucun des entiers p_1, p_2, …, p_k ne divise n, alors n est premier.

5°) Propriété

L'ensemble des nombres premiers est infini.

II. Propriétés

1°) Propriété 1

Deux nombres premiers distincts sont premiers entre eux.

2°) Propriété 2

Tout nombre premier p est premier avec ses prédécesseurs entiers naturels non nuls ($p-1$, $p-2$, $p-3$ ... 2, 1).

3°) Propriété 3

Soit p un nombre premier.
Soit a un entier relatif.

- Si p divise a, alors $\text{PGCD}(a\,;\,p) = p$.
- Si p ne divise pas a, alors $\text{PGCD}(a\,;\,p) = 1$.

$$\text{PGCD}(a\,;\,p) = \begin{cases} 1 & \text{si } p \nmid a \\ p & \text{si } p \mid a \end{cases}$$

4°) Propriété 4

Soit p un nombre premier.
Soit a un entier relatif.

***p* est premier avec *a* si et seulement si *p* ne divise pas *a*.**

Corollaire :

Soit p un nombre premier.

***p* est premier avec tous les entiers qui ne sont pas multiples de *p*.**

5°) Propriété 5

Soit p un nombre premier.
Soit a et b deux entiers.

p* | *ab* ⇔ *p* | *a* ou *p* | *b

III. Décomposition en produit de facteurs premiers

1°) Théorème

Tout entier naturel supérieur ou égal à 2 est premier ou produit de nombres premiers.
Cette décomposition en produit de facteurs premiers est unique à l'ordre près des facteurs.

2°) Autre formulation

Pour tout entier naturel $n \geqslant 2$, on peut écrire $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ où :
p_1, p_2, …, p_r désignent des nombres premiers deux à deux distincts ;
α_1, α_2, … α_r désignent des entiers naturels ;
Cette écriture est unique à l'ordre près de facteurs.

Avec ces notations, l'ensemble des diviseurs premiers de *n* est $\{p_1, p_2, ..., p_r\}$.

3°) Pratique de la décomposition

IV. Condition nécessaire et suffisante de divisibilité à l'aide de la décomposition en facteurs premiers

1°) Propriété

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

b | *a* si et seulement si tout facteur premier figurant dans la décomposition de *b* figure aussi dans celle de *a* avec un exposant supérieur ou égal à celui qu'il a dans la décomposition de *b*.

2°) Diviseurs positifs d'un entier naturel à l'aide de la décomposition en facteurs premiers

n est un entier naturel dont la décomposition en facteurs premiers s'écrit $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ où

- $p_1, p_2, \ldots p_r$ sont des nombres premiers deux à deux distincts ;
- $\alpha_1, \alpha_2, \ldots \alpha_r$ sont des entiers naturels non nuls.

Les diviseurs positifs de *n* sont tous les entiers de la forme $p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$ avec $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2$, …. $0 \leqslant \beta_r \leqslant \alpha_r$.

3°) Nombre de diviseurs positifs d'un entier naturel supérieur ou égal à 2

Si $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$, les p_i étant des nombres premiers deux à deux distincts et les α_i étant des entiers naturels, le nombre de diviseurs entiers positifs de *n* est égal à $(\alpha_1 + 1) \times (\alpha_2 + 1) \times ... \times (\alpha_r + 1)$.

V. PGCD et PPCM à l'aide de la décomposition en facteurs premiers

1°) Formules

On considère deux entiers naturels *a* et *b* tels que $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$ où :
$p_1, p_2, \ldots, p_r$ désignent des nombres premiers deux à deux distincts ;
$\alpha_1, \alpha_2, \ldots \alpha_r$ désignent des entiers naturels ;
$\beta_1, \beta_2, \ldots \beta_r$ désignent des entiers naturels.

Attention, certains entiers parmi les α_i ou les β_i peuvent être nuls.

$\text{PGCD}(a ; b) = p_1^{\gamma_1} \times p_2^{\gamma_2} \times ... \times p_r^{\gamma_r}$ en posant $\gamma_i = \min(\alpha_i ; \beta_i)$ pour tout entier *i* tel que $1 \leqslant i \leqslant r$.
$\text{PPCM}(a ; b) = p_1^{\delta_1} \times p_2^{\delta_2} \times ... \times p_r^{\delta_r}$ en posant $\delta_i = \max(\alpha_i ; \beta_i)$ pour tout entier *i* tel que $1 \leqslant i \leqslant r$.

Le PPCM de *a* et *b* est égal au produit des facteurs premiers intervenant dans les deux décompositions de *a* et *b*, chacun étant élevé au plus grand exposant avec lequel il figure dans la décomposition de *a* et *b*.

3°) Décomposition en facteurs premiers et nombres premiers entre eux

• Propriété [condition nécessaire et suffisante pour que deux entiers naturels supérieurs ou égaux à 2 soient premiers entre eux] :

Deux entiers supérieurs ou égaux à 2 sont premiers entre eux si et seulement si leurs décompositions en facteurs premiers font intervenir des nombres premiers différents.

• Formulation équivalente 1 :

Deux entiers supérieurs ou égaux à 2 sont premiers entre eux si et seulement si aucun facteur premier qui intervient dans la décomposition de l'un n'intervient dans la décomposition de l'autre.

• Formulation équivalente 2 :

Deux entiers supérieurs ou égaux à 2 sont premiers entre eux si et seulement si ils n'admettent aucun un diviseur premier commun.

• Conséquence :

Deux entiers supérieurs ou égaux à 2 ne sont pas premiers entre eux si et seulement si ils admettent un diviseur premier commun.

• Généralisation :

Des entiers naturels supérieurs ou égaux à 2 (en nombre fini) sont premiers entre eux dans leur ensemble si et seulement si ils n'ont aucun diviseur premier commun.

4°) Retour sur la détermination du PGCD de deux entiers naturels à partir de leur décomposition en facteurs premiers

On considère deux entiers naturels a et b supérieurs ou égaux à 2.

1er cas : a et b n'ont aucun facteur premier commun
Dans ce cas, le PGCD de a et b est égal à 1.

2e cas : a et b ont au moins un facteur premier commun
Dans ce cas, le PGCD de a et b est égal au produit des facteurs premiers communs aux décompositions de a et b, chacun étant élevé au plus petit exposant avec lequel il figure dans la décomposition de a et b.

Autrement dit, pour déterminer le PGCD de deux entiers naturels supérieurs ou égaux à 2 :

- On effectue leurs décompositions en facteurs premiers.

- On regarde s'il y a des facteurs premiers qui apparaissent dans les deux décompositions.

- Si oui : on écrit les facteurs premiers communs ;
  on leur affecte le plus petit exposant qui apparaît dans les deux décompositions ;
  on effectue le produit.

- Si non : on écrit directement que le PGCD vaut 1.

VI. Petit théorème de Fermat

1°) Petit théorème de Fermat

p est un nombre premier et a est un entier non divisible par p.
Alors $a^{p-1}-1$ est divisible par p c'est-à-dire $a^{p-1} \equiv 1 \pmod{p}$.

2°) Corollaire du petit théorème de Fermat

p est un nombre premier.
$\forall a \in \mathbb{Z} \qquad a^p \equiv a \pmod{p}$

VII. Condition nécessaire et suffisante pour qu'un entier naturel supérieur ou égal à 2 soit un carré parfait ou un cube parfait à partir de sa décomposition en facteurs premiers

• Un entier naturel supérieur ou égal à 2 est un carré parfait si et seulement si tous les exposants de sa décomposition en facteurs premiers sont pairs.

• Un entier naturel supérieur ou égal à 2 est un cube parfait si et seulement si tous les exposants de sa décomposition en facteurs premiers sont des multiples de 3.

On peut généraliser à d'autres exposants.