Nombres premiers

I] Définition et propriétés des nombres premiers :

1- Définition :

Définition : Soit $n \in \mathbb{N}$.
On dit que n est **premier** s'il possède exactement deux diviseurs distincts positifs, 1 et lui-même.

Remarques :

- 0 n'est pas premier car il possède une infinité de diviseurs.
- 1 n'est pas premier car il ne possède qu'un seul diviseur : lui-même.
- A part 2, tous les nombres premiers sont impairs .
- Il y a 25 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 et 97

2- Critère d'arrêt :

Propriété : Tout entier naturel non premier $n \geqslant 2$ possède au moins un diviseur premier p tel que $\mathbf{2 \leqslant p \leqslant \sqrt{n}}$

Démonstration : Puisque n n'est pas premier, il admet des diviseurs autres que 1 et lui-même.
Soit E l'ensemble des diviseurs de n privé de 1 et de lui-même. E n'est pas vide car n n'est pas premier.
Il existe donc un plus petit élément de E noté p.
Si p n'était pas premier, p possèderait un diviseur p' distinct de 1 et de lui-même.
Ainsi, on aurait $p' < p$ et p' divise n (car il divise p), d'où $p' \in E$.
Ceci contredit le fait que p est le plus petit élément de E, donc p est premier.
On suppose que $n = pq$ avec $p \leqslant q$ car p est le plus petit diviseur premier de n (éventuellement $q = p$).
Comme $p \leqslant q$, on a $p \times p \leqslant p \times q$. On en déduit $p2 \leqslant n$, puis $p \leqslant \sqrt{n}$.

Propriété : Soit n un entier naturel tel que $n \geqslant 2$.
Si n n'est divisible par aucun nombre premier p tel que $2 \leqslant p \leqslant \sqrt{n}$, **alors n est premier.**

Exemple : Montrer que 101 est un nombre premier. On a $10 < \sqrt{101} < 11$.
On teste tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.
D'après les règles de divisibilité, 101 n'est pas divisible par 2 (il est impair), ni par 3 (la somme de ses chiffres $1 + 0 + 1 = 2$ n'est pas un multiple de 3), ni par 5 (il ne se termine ni par 0 ni par 5).
$101 = 7 \times 14 + 3$ donc 101 n'est pas divisible par 7.
101 n'étant divisible par aucun des nombres premiers 2, 3, 5 et 7, d'après le critère d'arrêt, 101 est premier.

3- Infinité des nombres premiers :

Théorème : Il existe une infinité de nombres premiers.

Démonstration : Démontrons ce théorème par l'absurde. Supposons donc qu'il n'existe qu'un nombre fini de nombres premiers : $2 < 3 < 5 < \ldots < p$ où p serait le plus grand nombre premier.
Posons $N = 2 \times 3 \times \ldots \times p + 1$. Le nombre N est strictement supérieur à 1. Il admet donc un diviseur premier d (propriété précédente).
Comme les nombres 2, 3, 5, ..., p sont les seuls nombres premiers, d est nécessairement l'un de ces nombres. Le nombre d divise donc le produit $2 \times 3 \times \ldots \times p$.
Mais d divise également le nombre N : il divise donc leur différence, c'est-à-dire 1, ce qui signifie que que $d = 1$. Or d est premier, donc d ne peut être égal à 1 !
Il existe donc une infinité de nombres premiers.

II] Décomposition d'un entier en un produit de facteurs premiers :

1- Le théorème de décomposition :

Théorème : Tout entier naturel supérieur ou égal à 2 se décompose en produit de facteurs premiers.
On note alors $n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times ... \times p_r^{\alpha r}$ où p_1, p_2, ..., p_r sont des nombres premiers distincts et α_1, α_2, ..., α_r sont des entiers naturels non nuls.
Cette décomposition est unique à l'ordre près des facteurs.

Démonstration :

- 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 (n_k) décroissante et finie d'entiers naturels.
Ainsi, n se décompose en un produit de facteurs premiers du type :
$n = {p_1}^{\alpha_1} \times {p_2}^{\alpha_2} \times ... \times {p_r}^{\alpha_r}$.

- 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.

Exemple : On peut décomposer 300 par étapes de plusieurs manières :
$300 = 2 \times 150 = 2 \times 15 \times 10 = 2 \times 3 \times 5 \times 2 \times 5$
ou encore $300 = 3 \times 100 = 3 \times 10 \times 10 = 3 \times 2 \times 5 \times 2 \times 5$.
Dans tous les cas, la décomposition sera $300 = 2^2 \times 3 \times 5^2$.

2- Recherche des diviseurs :

Propriété : Soit un entier $n \geqslant 2$.
Si la décomposition en facteurs premiers de n est : $n = {p_1}^{\alpha 1} \times {p_2}^{\alpha 2} \times ... \times {p_k}^{\alpha k}$, alors les diviseurs positifs de n sont les entiers :
${p_1}^{\beta 1} \times {p_2}^{\beta 2} \times ... \times {p_k}^{\beta k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout entier i de 1 à k.

Il y a donc $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$ diviseurs positifs de n.

Exemple : $12 = 2^2 \times 3$.
$2^0 \times 3^0 = 1$; $2^1 \times 3^0 = 1$; $2^2 \times 3^0 = 4$; $2^0 \times 3 = 3$; $2^1 \times 3 = 6$ et $2^2 \times 3 = 12$.
Soit 6 diviseurs. $(2 + 1)(1 + 1) = 3 \times 2 = 6$.

III] PGCD et PPCM :

Définitions :

- Le PGCD de deux entiers est **égal au produit de leurs diviseurs premiers communs, chacun d'eux étant élevé à son plus petit exposant**.
- Le PPCM de deux entiers est **égal au produit de tous leurs diviseurs premiers des deux décompositions, chacun d'eux étant élevé à son plus grand exposant**.

Remarque : $\text{PPCM}(a ; b) = \frac{ab}{\text{PGCD}(a ; b)}$.

Exemple : Soient $a = 27\,216$ et $b = 60$.
Déterminer les décompositions en produit de facteurs premiers de a et de b, et en déduire PGCD(a ; b) et PPCM(a ; b).
$27216 = 2^4 \times 3^5 \times 7$ et $60 = 2^2 \times 3 \times 5$.
Donc : $\text{PGCD}(a ; b) = 2^2 \times 3 = 12$ et $\text{PPCM}(a ; b) = 2^4 \times 3^5 \times 5 \times 7 = 136\,080$

III] Petit théorème de Fermat :

1- La théorème :

Théorème : Soit p un nombre premier.
Pour tout entier naturel a non divisible par p, on a :

$$a^{p-1} \equiv 1[p]$$

Démonstration :

- p est un nombre premier donc il est premier avec tout entier k tel que $1 \leqslant k \leqslant p - 1$,
donc p est premier avec $(p - 1)!$.

- Soient k un entier compris entre 1 et $p - 1$, et r_k le reste de la division euclidienne de ka par p. p est premier avec k et avec a (car a n'est pas divisible par p), donc p est premier avec ka, donc p n'est pas divisible par ka, donc $r_k \neq 0$.

- Soient k' un entier compris entre 1 et $p - 1$ avec $k' \neq k$ (par exemple $k' > k$), et $r_{k'}$ le reste de la division euclidienne de $k'a$ par p. Alors $r_{k'} \neq r_k$.
En effet, si $r_{k'} = r_k$, alors $k'a \equiv ka$ [p], donc p divise $k'a - ka$, c'est-à-dire $a(k' - k)$.
Or $1 \leqslant k' - k \leqslant p - 1$, donc p est premier avec $k' - k'$ et p est premier avec a donc p ne divise pas $a(k' - k)$, donc $r_{k'} \neq r_k$.

- Pour tout entier k compris entre 1 et $p - 1$, $ka \equiv r_k$ [p], donc, par produits,
$a \times 2a \times ... \times (p - 1)a \equiv r_1 \times r_2 \times ... \times r_{p-1}$ [p].
Or les r_k sont $p - 1$ entiers distincts compris entre 1 et $p - 1$ donc $r_1 \times r_2 \times ... \times r_{p-1} = (p - 1)!$ et on a $(p - 1)!a^{p-1} \equiv (p - 1)!$ [p].
Donc p divise $(p - 1)!a^{p-1} - (p - 1)!$, c'est-à-dire p divise $(p - 1)!(a^{p-1} - 1)$.
Mais p est premier avec $(p-1)!$, donc d'après le théorème de Gauss, p divise $a^{p-1} - 1$, donc $a^{p-1} \equiv 1$ [p].

Exemple : 5 est un nombre premier et 12 est un entier naturel non divisible par 5.
Alors $12^{5-1} \equiv 1$ [5], c'est-à-dire que $12^4 - 1$ est un multiple de 5

2- Conséquence :

Propriété : Soit p un nombre premier.
Pour tout entier naturel a, on a : $\mathbf{a^p \equiv a\ [p]}$

Démonstration :
$a^p \equiv a\ [p] \Leftrightarrow$ p divise $a^p - a \Leftrightarrow$ p divise $a(a^{p-1} - 1)$.
Si a est divisible par p, alors p divise bien $a(a^{p-1} - 1)$, donc $a^p \equiv a\ [p]$.
Si a n'est pas divisible par p, alors p divise $a^{p-1} - 1$ (d'après le petit théorème de Fermat), donc p divise $a(a^{p-1} - 1)$, donc $a^p \equiv a\ [p]$.