



1 Un entier naturel n est premier lorsqu'il possède exactement deux diviseurs positifs : 1 et lui-même. Pour savoir si n est premier, il suffit de tester s'il est divisible par des entiers compris entre 2 et \sqrt{n} .

Cela permet de :

- ✓ déterminer si l'entier n est un nombre premier ou non ;
- ✓ trouver un diviseur de n afin de déterminer ensuite une factorisation de l'entier n .

2 Le crible d'Eratosthène permet de connaître l'ensemble des nombres premiers inférieurs ou égaux à un entier n . Cela permet de :

- ✓ savoir facilement si un nombre inférieur ou égal à n est premier ou non ;
- ✓ savoir quels sont les diviseurs premiers potentiels d'un nombre n et faciliter ainsi les tests de primalité.

3 Tout entier naturel supérieur ou égal à 2 se décompose de façon unique en produit de nombres premiers.

Cela permet de :

- ✓ déterminer l'ensemble des diviseurs d'un entier, en les énumérant à l'aide d'un arbre ;
- ✓ déterminer le nombre de diviseurs, en regardant uniquement les exposants apparaissant dans la décomposition ;
- ✓ déterminer le PGCD de deux entiers.

4 Le petit théorème de Fermat : si p est un nombre premier et si a est un entier non divisible par p , alors $a^{p-1} \equiv 1 [p]$. Cela permet de :

- ✓ calculer des puissances modulo p en simplifiant les calculs.

CARTE MENTALE

n est un entier supérieur ou égal à 2.

NOMBRES PREMIERS

Test de primalité pour savoir si un entier est premier ou non (on teste les diviseurs entre 1 et \sqrt{n})

Si n est premier

On peut utiliser le petit théorème de Fermat pour simplifier des calculs modulo n : si p est un nombre premier et a un entier non divisible par p , alors $a^{p-1} \equiv 1 [p]$

Si n n'est pas premier, on peut le décomposer en produit de facteurs premiers (la décomposition est unique à l'ordre des facteurs près)

$$n = p_1^{a_1} \times \dots \times p_k^{a_k}$$

Déterminer le nombre de diviseurs de n : $(a_1+1)(a_2+1)\dots(a_k+1)$

Déterminer l'ensemble des diviseurs de n en utilisant un arbre

Déterminer des PGCD (favoriser toutefois l'algorithme d'Euclide)