Nombres premiers

1 Généralités sur les nombres premiers

Définition 1
Un nombre premier est un nombre qui possède exactement deux diviseurs positifs, 1 et lui-même.

Exemple 1
- 1 n'est pas premier.
- 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 23 ; 29 ; ⋯ sont des nombres premiers.
- Le plus grand nombre premier connu (3 janvier 2018) est $2^{77\,232\,917} - 1$.

Propriété 1
Tout entier naturel possède un diviseur premier inférieur ou égal à $\sqrt{n}$.

Propriété 2
Cet algorithme, en langage naturel, prend en entrée un entier naturel n, et détermine s'il est premier.

```
Si n = 0 ou n = 1
  « n n'est pas premier »
Sinon
  d = 2
  Tant que d ⩽ √n
    Si mod(n, d) = 0
      « n n'est pas premier »
    d = d + 1
    « n est premier »
```

$\mathrm{mod}(n, d)$ désigne le reste de la division euclidienne de n par d.

Le même algorithme en fonction Python.

```python
import math

def est_premier(n) :
    if n == 0 or n == 1 :
        return False
    else :
        d = 2
        while d <= math.sqrt(n) :
            if n % d == 0 :
                return False
            d = d+1
        return True
```

Remarque : On peut améliorer l'efficacité de cet algorithme en ne s'intéressant qu'à $d = 2$, puis ne considérer que des d impairs. Néanmoins, des tests plus puissants existent que celui-ci, considéré comme « naïf ».

Propriété 3
Il existe une infinité de nombres premiers.

Propriété 4
Pour un nombre premier p et deux entiers relatifs a et b,
si $p|ab$, alors ($p|a$ ou $p|b$) ;

2 Théorèmes sur les nombres premiers

Théorème 1 : théorème fondamental de l'arithmétique

Tout entier naturel $n \geqslant 2$ possède une **décomposition en facteurs premiers**, *i.e.*, il existe $p_1 < p_2 < \cdots < p_r$ des nombres premiers et $v_1 ; v_2 ; \cdots ; v_r$ des entiers naturels non nuls tels que

$$n = \prod_{j=1}^{r} {p_j}^{v_j} = {p_1}^{v_1} \times {p_2}^{v_2} \times \cdots \times {p_r}^{v_r}.$$

Cette décomposition est unique à l'ordre des termes près.
Le nombre v_j est appelé p_j-valuation de n.

Exemple 2

$126 = 2 \times 3^2 \times 7$.
La 3-valuation de 126 vaut 2 et la 7-valuation de 126 vaut 1.

N.B. : Une telle décomposition existe encore pour les nombres rationnels, à condition de prendre en compte le signe et que les valuations soient des entiers non nuls.

$\dfrac{175}{76} = \dfrac{5^2 \times 7}{2^2 \times 19} = 2^{-2} \times 5^2 \times 7 \times 19^{-1}$.

Propriété 5

Pour deux entiers naturels $m = \prod_{j=1}^{r} {p_j}^{v_j}$ et $n = \prod_{j=1}^{r} {p_j}^{w_j}$ donnés sous forme de décomposition de facteurs premiers,

$$m | n \Leftrightarrow \forall j \in [\![1 ; r]\!], v_j \leqslant w_j.$$

Exemple 3

$195 = 3 \times 5 \times 13$ divise $8\,775 = 3^3 \times 5^2 \times 13$.

Théorème 2 : petit théorème de Fermat

Pour un entier naturel a et un nombre premier p ne divisant pas a, on a

$$a^{p-1} \equiv 1 \pmod{p}$$

Exemple 4

Comme 17 est premier et que 15 n'est pas divisé par 17, on a $15^{16} \equiv 1 \pmod{17}$.

Propriété 6

Pour un entier naturel a et un nombre premier p, on a

$$a^p \equiv a \pmod{p}$$

Théorème 3 : théorème des nombres premiers (hors programme)

Pour $n \to +\infty$, le n-ème nombre premier est « proche » de $\dfrac{n}{\ln(n)}$, et même de $\displaystyle\int_2^n \frac{1}{\ln(x)}\,\mathrm{d}x$.