

# Chapitre n° 7 : Nombres premiers

Les nombres premiers, du fil à retordre :

- Le théorème de Fermat-Wiles énonce qu'il n'existe pas de nombres entiers positifs  $x$ ,  $y$  et  $z$  tels que :  $x^n + y^n = z^n$ , dès que  $n$  est un entier strictement supérieur à 2. Pour  $n=2$ , on a les solutions entières du théorème de Pythagore (la plus simple étant  $3^2 + 4^2 = 5^2$ ). Une telle relation entre nombres entiers apparaît impossible pour un exposant supérieur à 2. Fermat prétendait avoir trouvé la démonstration. Mais c'est 350 ans plus tard et au prix d'une construction très complexe et laborieuse, que le mathématicien anglais, Andrew Wiles, a fini par en établir, en 1994, la démonstration aujourd'hui admise et validée par ses pairs.
- Pierre de Fermat émit l'hypothèse que les nombres de la forme  $2^{2^n} + 1$  sont premiers. En fait, dès  $n = 5$ , la propriété est fausse car  $2^{32} + 1$  n'est pas un nombre premier (difficile à vérifier à la main à l'époque de Fermat).

- 1742 : Tout nombre pair plus grand que 2 est la somme de deux nombres premiers (Conjecture de Goldbach binaire).

1920 : Tout entier pair assez grand est somme de deux entiers composés chacun de 9 facteurs premiers au plus (Viggo Brun).

1933 : Il existe une constante  $C$  telle que tout entier supérieur à 1 est somme de  $C$  nombres premiers au plus (Lev Šchnirel'man).

1951 : Il existe une constante  $K$  telle que tout entier pair assez grand est somme de deux nombres premiers et d'au plus  $K$  puissances de 2 (Yuri Linnik).

1966 : Tout entier pair assez grand est somme d'un nombre premier et d'un nombre ayant au plus deux facteurs premiers (Chen Jingrun).

1995 : Tout entier pair est somme de six nombres premiers au plus (Olivier Ramaré).

2012 : Tout entier impair supérieur à 1 est somme de cinq nombres premiers au plus (Terence Tao).

2014 : Tout entier impair supérieur à 1 est somme de trois nombres premiers au plus (c'était la conjecture de Goldbach ternaire, qui n'en n'est plus une depuis la démonstration par Harald Helfgott).

- Deux nombres premiers sont dits « jumeaux » lorsqu'ils sont séparés de deux unités. Ainsi les paires 3 et 5, 17 et 19 ou encore 41 et 43, 71 et 73, pour s'en tenir aux jumeaux inférieurs à 100. Mais certains peuvent être très grands : par exemple,  $2003663613 \times 2^{195000} - 1$  et  $2003663613 \times 2^{195000} + 1$ . La « conjecture des nombres premiers jumeaux » affirme qu'il existe en fait une infinité de telles paires de nombres premiers jumeaux.

Une variante forte est la conjecture de Polignac, énoncée en 1849 : « tout nombre pair est égal à la différence de deux nombres premiers consécutifs d'une infinité de manières ».

# 1 Définition et propriétés

## 1.1 Définition

### Définition 1: Nombre premier

Un nombre premier est un entier naturel qui admet exactement deux diviseurs positifs: 1 et lui-même.  
Un entier naturel non premier et supérieur à 2 est appelé un nombre composé.

#### Exemple 1:

- 1 n'est pas un nombre premier (il n'a qu'un seul diviseur). Ce n'est pas non plus un nombre composé.
- 0 n'est ni premier (il admet une infinité de diviseurs), ni composé.

Un nombre premier est donc un entier naturel supérieur **ou égal** à 2.

- Les nombres premiers inférieurs à 100 sont :

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.

- Si un entier naturel  $n \geq 2$  n'est pas premier (i.e. est composé), alors il admet un diviseur  $d$  tel que :  $2 \leq d < n$ .

Un algorithme naïf de test de primalité d'un entier  $n$  consiste à tester comme diviseurs tous les entiers qui lui sont inférieurs.

## 1.2 Critère d'arrêt ou test de primalité

### Propriété 1: Critère d'arrêt

Tout entier naturel  $n$ ,  $n \geq 2$ , admet un diviseur premier.

Si  $n$  n'est pas premier, alors il admet un diviseur premier  $p$  tel que :  $2 \leq p \leq \sqrt{n}$ .

**Preuve 1:** Soit  $n \in \mathbb{N}$  et  $n \geq 2$ .

- Si  $n$  est premier,

- Si  $n$  n'est pas premier, l'ensemble  $D$  des diviseurs  $d$  de  $n$  tels que :  $2 \leq d < n$

Si  $p$  n'était pas premier, il admettrait un diviseur  $d'$  tel que  $2 \leq d' < p$

- On a donc  $p$  premier et  $n = p \times q$  avec  $p \leq q$ . En multipliant cette inégalité par  $p$ , on obtient :

### Méthode 1 (Montrer qu'un nombre est premier):

Pour montrer qu'un naturel  $n$  est premier, on utilise la contraposée du critère d'arrêt :

« Si  $n$  n'admet pas de diviseur premier  $p$  tel que  $2 \leq p \leq \sqrt{n}$ , alors  $n$  est premier. »

Montrer que 109 est un nombre premier.

#### CORRECTION

On a  $10 < \sqrt{109} < 11$ . Donc si 109 n'est pas premier, il admet un diviseur premier inférieur à 11. On teste tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.

- Des règles de divisibilité, on déduit que 109 n'est divisible ni par 2, ni par 3, ni par 5.
- En effectuant la division euclidienne de 109 par 7, on obtient :  $109 = 7 \times 15 + 4$ . 109 n'est donc pas divisible par 7.
- Conclusion : 109 n'est pas divisible par 2, 3, 5, et 7 donc 109 est premier.

**Exemple 2:** Le programme ci-contre détermine si un nombre  $N$  est premier. N'ayant pas à notre disposition la liste des nombres premiers :

- on teste si  $N$  est divisible par 2;
- 37 589 est premier.
- puis on teste les diviseurs impairs par ordre croissant tant que ceux-ci sont inférieurs à  $\sqrt{N}$ .

On obtient alors pour les nombres 527, 719, 11 111 et 37 589 que :

- 527 est divisible par 17;
- 719 est premier;
- 11 111 est divisible par 41;

Code Python

```
1 def test_primalite(n) :
2     i = 2
3     if n%i == 0 :
4         return FALSE
5     i = i+1
6     while i <= sqrt(n):
7         if n%i == 0 :
8             return FALSE
9         i=i+2
10    return TRUE
```

### 1.3 Infinité des nombres premiers

#### Propriété 2

Il existe une infinité de nombres premiers.

#### Preuve 2:

Cette preuve, par l'absurde ou par contradiction est celle proposée au III<sup>e</sup> siècle av. J.-C., par Euclide, dans son ouvrage « *Les Éléments* ».

Il en existe bien d'autres.

Supposons qu'il existe un nombre fini  $n$  de nombres premiers :  $p_1 \leq p_2 \leq \dots \leq p_i \leq \dots \leq p_n$ .

Notons  $N$  le nombre entier défini par :

donc  $N$  est en entier composé.

D'autre part, d'après le critère d'arrêt,  $N$  admet un diviseur premier.

Notons  $i \in \{1, 2, \dots, n\}$  l'indice tel que  $p_i$  est ce diviseur premier.

Ceci est impossible car  $p_i \geq 2$ , donc l'hypothèse qu'il existe un nombre fini de nombres premiers est contradictoire.

## 1.4 Crible d'Ératosthène

**Méthode 2 (Crible d'Ératosthène):** Pour la liste des nombres premiers inférieurs ou égaux à  $N$  :

- Écrire la liste des entiers de 2 à  $N$ .

D'après le critère d'arrêt, tous les nombres composés (non premiers) plus petits que  $N$  ont un facteur premier inférieur ou égal à  $\sqrt{N}$ .

- Éliminer de la liste tous les multiples de 2 sauf 2.

Le nombre suivant non éliminé est alors premier. Ici on trouve 3.

- Éliminer de la liste tous les multiples de 3 sauf 3.

Le nombre suivant non éliminé est alors premier. Ici on trouve 5.

- Répéter l'étape ci-dessus tant qu'il existe des multiples de nombres premiers inférieurs ou égaux à  $\sqrt{N}$ .

### Remarque 1:

- ① Pour éliminer les multiples de  $a$  supérieurs à  $a$ , commencer à  $a^2$ , car les multiples inférieurs à  $a$  ont déjà été éliminés. En effet, les multiples de  $a$  inférieurs à  $a^2$  sont aussi des multiples de nombres inférieurs à  $a$ . Par exemple lorsqu'on élimine les multiples de 7, on commence à partir de 49.
- ② Si  $N = 150$ , comme  $\sqrt{150} \approx 12,25$ , alors tout nombre composé sera éliminé en tant que multiple de 2, 3, 5, 7 et 11.

**Exemple 3:** Pour  $N = 100$ , on obtient le tableau suivant. Les nombres premiers sont colorés en jaune :

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

**Remarque 2:** On appelle fonction de compte des nombres premiers, la fonction notée  $\pi(x)$  qui compte les nombres premiers inférieurs ou égaux à  $x$ .

On a par exemple :  $\pi(100) = 25$ ,  $\pi(200) = 46$ ,  $\pi(500) = 95$ ,  $\pi(1000) = 168$ .

Le théorème des nombres premiers (démontré indépendamment par Hadamard et La Vallée Poussin en 1896, et conjecturé par Gauss en 1793 à l'âge de 16 ans) affirme que :

## 1.5 Théorème de Gauss et nombres premiers

### Propriété 3

Un nombre premier divise un produit de facteurs si, et seulement si, il divise l'un de ces facteurs. Soit  $p$  un nombre premier et  $a, b$  deux entiers :

**Preuve 3:** Comme  $p$  est premier, on a :  $\text{PGCD}(p, a) = p$  ou  $\text{PGCD}(p, a) = 1$ .

- Si  $\text{PGCD}(p, a) = p$ , alors

- Si  $\text{PGCD}(p, a) = 1$ , alors

$p$  divise  $b$ .

**Remarque 3:** En particulier, si  $p$  est premier et divise une puissance  $a^k$ , alors nécessairement :

divise  $a^k$ .

### Corollaire 1

- Si un nombre premier  $p$  divise un produit de facteurs premiers, alors  $p$  est l'un de ces facteurs premiers.
- Si un nombre  $n$  est un carré, alors toutes les puissances des facteurs de sa décomposition en facteurs premiers sont paires.
- Soit  $p_1, p_2, \dots, p_k$  des nombres premiers distincts et  $\alpha_1, \alpha_2, \dots, \alpha_k$  des entiers naturels non nuls. Si, pour tout  $i \in \{1, 2, \dots, k\}$ ,  $p_i^{\alpha_i}$  divise un entier  $n$ , alors le produit  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  divise aussi  $n$ .

## 2 Décomposition, diviseurs d'un entier

### 2.1 Théorème fondamental de l'arithmétique

#### Théorème 4

Tout entier  $n \geq 2$  peut se décomposer de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers. Soit  $p_1, p_2, \dots, p_m$  des nombres entiers premiers distincts et  $\alpha_1, \alpha_2, \dots, \alpha_m$  des entiers naturels non nuls :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_m^{\alpha_m}$$

**Méthode 3 (Décomposer un nombre en produit de facteurs premiers):**

Décomposer 16 758 en produit de facteurs premiers.

CORRECTION

16 758	2
8 379	3
2 793	3
931	7
133	7
19	19
1	

On présente la décomposition avec une barre verticale où l'on écrit à droite, les diviseurs premiers et, à gauche, le quotient des divisions successives par ces diviseurs premiers pris dans l'ordre croissant.

On a donc  $16\,758 = 2 \times 3^2 \times 7^2 \times 19$ .

#### Preuve 4:

Soit  $n$  un entier naturel supérieur ou égal à 2.

- Si  $n$  est premier, alors  $n$  se décompose en lui-même.

Sinon  $n = p_1 \times q_1$  avec  $p_1 \leq q_1$  et  $p_1$  premier car, d'après le critère d'arrêt,  $n$  admet un diviseur premier  $p_1$  tel que  $2 \leq p_1 \leq \sqrt{n}$ .

- Si  $q_1$  est premier, alors  $n$  se décompose en  $n = p_1 \times q_1$ .

Sinon  $q_1 = p_2 \times q_2$  avec  $p_2 \leq q_2$  et  $p_2$  premier car, d'après le critère d'arrêt,  $q_1$  admet un diviseur premier  $p_2$  tel que  $2 \leq p_2 \leq \sqrt{q_1}$ . On a alors  $q_2 < q_1$ .

- Si  $q_2$  est premier, alors  $n$  se décompose en  $n = p_1 \times p_2 \times q_2$ .

Sinon on réitère le processus, obtenant  $q_3, q_4, \dots, q_n$  avec  $q_3 > q_4 > \dots > q_n \geq 2$ .

Toute suite décroissante dans  $\mathbb{N}$  est stationnaire à partir d'un certain rang  $n$ , et alors  $q_n$  est nécessairement premier (sinon on réitère le processus pour obtenir  $2 \leq q_{n+1} < q_n$ ).

$n$  se décompose alors en produit de facteurs premiers :  $n = p_1 \times p_2 \times \dots \times p_n \times q_n$ .

Les facteurs premiers  $p_1, p_2, \dots, p_n$  et  $q_n$  peuvent être éventuellement identiques. On les regroupe alors sous la forme  $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_m^{\alpha_m}$ , avec  $\alpha_1, \alpha_2, \dots, \alpha_m$  des entiers naturels non nuls.

L'existence de la décomposition est alors démontrée. L'unicité de la décomposition est admise.

#### Méthode 4 (Déterminer le PGCD à partir d'une décomposition en facteurs premiers):

##### EXERCICE

Déterminer PGCD(126 ; 735) à l'aide d'une décomposition en produit de facteurs premiers.

##### CORRECTION

- On décompose les deux nombres en produit de facteurs premiers.

126	2
63	3
21	3
7	7
1	

735	3
245	5
49	7
7	7
1	

On a donc :

$$126 = 2 \times 3^2 \times 7$$

$$735 = 3 \times 5 \times 7^2$$

- On détermine les facteurs premiers communs pour trouver le PGCD de ces deux nombres.

$$\text{PGCD}(126 ; 735) = 3 \times 7 = 21.$$

**Remarque 4:** L'algorithme d'Euclide est à préférer pour la recherche du PGCD à la méthode par

décomposition car il est plus économe en opérations :

$$\begin{aligned} 735 &= 126 \times 5 + 105 \\ 126 &= 105 \times 1 + 21 \\ 105 &= 21 \times 5 \end{aligned}$$

On obtient PGCD(735 ; 126) en trois étapes.

## 2.2 Diviseurs d'un entier

### Propriété 5

Soit un nombre  $n$  ( $n \geq 2$ ) dont la décomposition en produit de facteurs premiers est :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_m^{\alpha_m}.$$

Alors tout diviseur  $d$  de  $n$  a pour décomposition :

Le nombre  $N$  de diviseurs est alors :

### Remarque 5:

- Le nombre de diviseurs d'un entier se calcule facilement car la puissance d'un facteur premier  $p_i$  peut varier de 0 à  $\alpha_i$ , ce qui fait  $(\alpha_i + 1)$  possibilités.
- Pour qu'un entier  $n$  admette un nombre impair de diviseurs, tous les  $(\alpha_i + 1)$  doivent être impairs, donc toutes les puissances  $\alpha_i$  doivent être paires. Le nombre  $n$  est alors un carré.

### Méthode 5 (Trouver le nombre de diviseurs d'un entier):

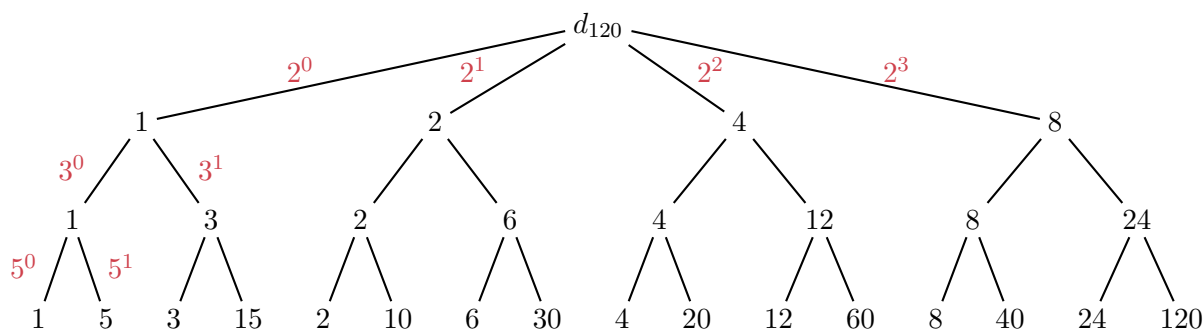
Trouver le nombre de diviseurs de 120, puis déterminer tous ses diviseurs.

CORRECTION

- On décompose 120 en facteurs premiers :  $120 = 2^3 \times 3 \times 5$ .

On alors :  $(3 + 1)(1 + 1)(1 + 1) = 4 \times 2 \times 2 = 16$ . Il y a 16 diviseurs pour 120.

- Pour déterminer tous ses diviseurs, on peut utiliser un arbre pondéré dont les coefficients sont les facteurs premiers possibles.



**Méthode 6 (Déterminer un entier conditionné par ses diviseurs):**

Un entier naturel  $n$  a 15 diviseurs. On sait de plus que  $n$  est divisible par 6 mais pas par 8.  
Déterminer cet entier  $n$ .

CORRECTION

**EXERCICE**

Déterminer le plus petit entier naturel possédant 28 diviseurs.

CORRECTION

Soit  $n$  l'entier cherché.

Trouvons toutes les décompositions de 28 en produit de facteurs supérieurs à 1.

Conclusion, le plus petit entier naturel ayant 28 diviseurs est 960.