

Nombres premiers

Table des matières

1	Définition et conséquences	2
1.1	Définition	2
1.2	Critère d'arrêt ou test de primalité	2
1.3	Infinité des nombres premiers	3
1.4	Crible d'Ératosthène	3
1.5	Divisibilité et nombres premiers	5
1.6	Nombres de Mersenne	5
2	Décomposition, diviseurs d'un entier	6
2.1	Théorème fondamental de l'arithmétique	6
2.2	Diviseurs d'un entier	7
2.3	Applications	8
3	Petit théorème de Fermat	9

1 Définition et conséquences

1.1 Définition

Définition 1 : Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même

Remarque :

- 1 n'est pas un nombre premier (il n'a qu'un seul diviseur)
- Un nombre premier p est un naturel supérieur ou égal à 2 soit : $p \geq 2$.
- À 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

1.2 Critère d'arrêt ou test de primalité

Théorème 1 : Tout entier naturel n tel que $n \geq 2$ admet un diviseur premier.
Si n n'est pas premier, alors il admet un diviseur premier p tel que : $2 \leq p \leq \sqrt{n}$

Démonstration :

- Si n est premier, il admet donc un diviseur premier : lui-même.
- Si n n'est pas premier, l'ensemble D des diviseurs stricts de n n'est pas vide. D'après le principe du bon ordre, D admet donc un plus petit élément p .
Si p n'était pas premier, il admettrait un diviseur strict d qui diviserait n . Ceci est impossible car p est le plus petit élément de D . Donc p est premier.
 n admet donc un diviseur premier p tel que $p \geq 2$ et $n = p \times q$ avec $p \leq q$.
En multipliant cette inégalité par p , on obtient :

$$p^2 \leq pq \Leftrightarrow p^2 \leq n \text{ soit } p \leq \sqrt{n}$$

Exemple : Montrer que 109 est un nombre premier.

$$10 < \sqrt{109} < 11.$$


On teste tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.

D'après règles de divisibilité 109 n'est divisible ni par 2, ni par 3, ni par 5.

$$109 = 7 \times 15 + 4 \text{ donc } 109 \text{ n'est donc pas divisible par } 7$$

109 non divisible par 2, 3, 5, et 7 d'après le critère d'arrêt 109 est premier.

Algorithme :

Soit la fonction Python  `prime(n)` qui détermine grâce au critère d'arrêt si le nombre est premier et s'il ne l'est pas par quel facteur premier est-il divisible.

Sans liste de nombres premiers, on teste si n est divisible par 2, puis les diviseurs impairs par ordre croissant tant que ceux-ci sont inférieurs à \sqrt{n} .

- `prime(527)` → 527 divisible par 17
- `prime(719)` → 719 premier
- 11 111 → 11 111 divisible par 41
- 37 589 → 37 589 premier

```
from math import*
def prime(n):
    i=2
    if n%i==0:
        return n, "divisible par", i
    i+=1
    while i<=sqrt(n):
        if n%i==0:
            return n, "divisible par", i
        i+=2
    return n, "premier"
```

1.3 Infinité des nombres premiers

Théorème 2 : Il existe une infinité de nombres premiers

Démonstration : Par l'absurde.

Supposons qu'il existe un nombre fini de nombres premiers : p_1, p_2, \dots, p_n .

Posons $N = p_1 \times p_2 \times \dots \times p_n + 1$

- $N \geq 2$ et $N > p_n$ donc par construction N n'est pas premier.
- D'après le critère d'arrêt, N admet un diviseur premier p_i parmi p_1, p_2, \dots, p_n .
- p_i divise donc $p_1 \times p_2 \times \dots \times p_n$ et N .
Il divise donc la différence $N - (p_1 \times p_2 \times \dots \times p_n) = 1$.
- Ceci est contradictoire car $N \geq 2$

L'hypothèse qu'il existe un nombre fini de nombres premiers est donc à rejeter.

1.4 Crible d'Ératosthène

Théorème 3 : Pour dresser la liste des nombres premiers entre 2 et n , la méthode du crible d'Ératosthène consiste à :


- écrire la liste des nombres entiers de 2 à n ;
- éliminer successivement les multiples propres^a de 2, de 3... puis ceux de p , où p est le premier nombre non encore éliminé, etc.
- D'après le critère d'arrêt, on élimine les multiples jusqu'à \sqrt{n}

^a. multiple propre de n : multiple de n distinct de n

Exemple : Dresser la liste des nombres premiers inférieurs ou égaux à 150. Les entiers éliminés (sur fond bleu dans le tableau ci après) sont les entiers non premiers entre 2 et 150. Les entiers restant (sur fond jaune) sont donc premiers.

- Pour éliminer, par exemple, les multiples propre de 7, commencer par 7^2 , car les multiples inférieurs ont déjà été éliminés.
- $12 < \sqrt{150} < 13$ et donc tout entier non premier sera éliminés en tant que multiple propre de 2, 3, 5, 7 et 11.

	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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

Algorithme : Soit la fonction Python  `crible(n)` qui donne la liste des nombres premiers inférieurs ou égaux à n ainsi que leur nombre.

```

from math import *
def crible(n):
    L=[i for i in range(n+1)]
    for i in range(2, int(floor(sqrt(n)))+1):
        if L[i]>=1:
            for k in range(2, int(floor(n/i))+1):
                L[i*k]=0
    i=0
    while i<len(L):
        if L[i]==0 or L[i]==1:
            L.remove(L[i])
        else:
            i+=1
    print(L, len(L))

```

- On détermine une liste L des nombre de 0 à n
- Pour un élément de rang i de la liste L entre le rang 2 et le rang de la partie entière de \sqrt{n} , si l'élément est différent de 0 (≥ 1) on met à 0 les éléments de L dont le rang est un multiple propre de i .
- On enlève ensuite de L tous les éléments nuls ou égaux à 1.
- On affiche L et le nombre d'éléments de L.

`crible(500) = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499] 95`

1.5 Divisibilité et nombres premiers

Théorème 4 : Théorème de Gauss et nombre premier

Un nombre premier divise un produit de facteurs s'il divise l'un de ces facteurs.

$$p \text{ divise } ab \Rightarrow p \text{ divise } a \text{ ou } p \text{ divise } b$$

Démonstration : Soit $D = \text{pgcd}(a, p)$, comme p premier alors $D = 1$ ou $D = p$

- Si $D = 1$ d'après le théorème de Gauss, p divise b
- Si $D = p$ alors p divise a

Remarque :

- Si p premier divise a^k , alors p divise a , donc p^k divise a^k avec $k \in \mathbb{N}$.
- Si p premier divise un produit de facteurs premiers, alors p est l'un de ces facteurs.

1.6 Nombres de Mersenne

Definition 2 : Soit $n \in \mathbb{N}^*$, on définit les nombres M_n par : $M_n = 2^n - 1$.

Les nombres M_n sont appelés nombre de Mersenne

1) Les 6 premiers nombres de Mersenne :

$$\begin{array}{lll} M_1 = 2 - 1 = 1 & M_2 = 4 - 1 = 3 & M_3 = 8 - 1 = 7 \\ M_4 = 16 - 1 = 15 & M_5 = 32 - 1 = 31 & M_6 = 64 - 1 = 63 \end{array}$$

2) Montrons que si n non premier alors M_n non premier.

On rappelle la factorisation standard :

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1)$$

Si n non premier, alors il existe $d > 1$ tel que : $n = dq$ avec $q > 1$.

Factorisons M_n avec la factorisation standard :

$$M_n = 2^n - 1 \stackrel{n=dq}{=} (2^d)^q - 1 = (2^d - 1)[(2^d)^{q-1} + (2^d)^{q-2} + \dots + 2^d + 1]$$

$1 < 2^d - 1 < M_n$ donc $2^d - 1$ diviseur propre de M_n et donc M_n non premier.

Si n non premier alors M_n non premier.

La contraposée donne : « si M_n premier alors n premier. »

3) Montrons que la réciproque « si n premier alors M_n premier » est fausse.

Contre-exemple :

si $n = 11$ premier alors $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ non premier.

Remarque : Dans la pratique, pour trouver un grand nombre premier, on peut utiliser un nombre de Mersenne avec n premier mais l'on doit cependant tester si M_n est premier car la réciproque 3) n'est pas vraie.

Actuellement le plus grand nombre de Mersenne premier est $M_{82\,589\,933}$ trouvé en 2018 qui possède 24 862 048 chiffres.

2 Décomposition, diviseurs d'un entier

2.1 Théorème fondamental de l'arithmétique

Théorème 5 : Tout entier $n \geq 2$, peut se décomposer de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers. Soit m nombres premiers distincts p_1, p_2, \dots, p_m et m entiers naturels $\alpha_1, \alpha_2, \dots, \alpha_m$, alors

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

Démonstration : Montrons par récurrence que tout entier $n \geq 2$ admet une décomposition en facteurs premiers.

Initialisation : $n = 2$. L'entier 2 étant premier, il se décompose en lui-même. La proposition est initialisée.

Hérédité : soit $n \geq 2$, on suppose que tout entier jusqu'à n se décompose en facteurs premiers (hypothèse de récurrence).

Montrons qu'il en est de même pour $n + 1$.

- Soit $n + 1$ est premier, il se décompose alors en lui-même.
- Soit $n + 1$ est composé, il admet alors un diviseur strict $d \geq 2$. On a alors $n + 1 = dq$ avec $d \leq n$ et $q \leq n$, les facteurs d et q d'après l'hypothèse de récurrence se décomposent en facteurs premiers et donc par produit $n + 1$ aussi.

La proposition est héréditaire.

Conclusion : par initialisation et hérédité, tout entier $n \geq 2$ admet une décomposition en facteurs premiers.

Remarque :


- Lorsque, dans un raisonnement par récurrence, on suppose, dans l'hérédité, la proposition vraie jusqu'au rang n , on dit que la récurrence est forte.
- Pour montrer l'unicité à l'ordre des facteurs près, on utilise également une récurrence forte. On admettra l'unicité de cette décomposition.

Exemple : Décomposons 16 758 en produit de facteur premier

$$\begin{array}{r|l} 16\ 758 & 2 \\ 8\ 379 & 3 \\ 2\ 793 & 3 \\ 931 & 7 \\ 133 & 7 \\ 19 & 19 \\ 1 & \end{array}$$

Pour décomposer un entier, on effectue des divisions successives par des nombres premiers dans l'ordre croissant.

on a donc $16\ 758 = 2 \times 3^2 \times 7^2 \times 19$

Algorithme : Soit la fonction Python  `decomposition(n)` qui donne la décomposition en facteurs premiers du nombre $n \geq 2$.

On teste si d est un diviseur de n en commençant par 2 puis les nombres impairs dans l'ordre croissant en appliquant le critère d'arrêt $d \leq \sqrt{n}$. On réinitialise n en prenant le quotient n/d . Le dernier nombre qui ne vérifie par le critère d'arrêt est alors premier et on le rajoute à la liste des diviseurs.

`decomposition(16758) = [2, 3, 3, 7, 7, 19]`
`decomposition(77 986 545) = [3, 5, 7, 13, 19, 31, 97]`

```
def decomposition(n):
    d=2
    c=1
    L=[]
    while d<=sqrt(n):
        if n%d==0:
            L.append(d)
            n=int(n/d)
        else:
            d=d+c
            c=2
    L.append(n)
    return L
```

Application : Calculer $\text{pgcd}(126, 735)$ à l'aide de décompositions.

126	2	735	3
63	3	245	5
21	3	49	7
7	7	7	7
1		1	

$126 = 2 \times 3^2 \times 7$
 $735 = 3 \times 5 \times 7^2$
 $\text{pgcd}(126, 735) = 3 \times 7 = 21$

2.2 Diviseurs d'un entier

Théorème 6 : Soit $n \geq 2$ dont la décomposition en facteurs premiers est :

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

Alors tout diviseurs d de n a pour décomposition :

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_m^{\beta_m} \text{ avec } 0 \leq \beta_i \leq \alpha_i \text{ et } i \in \llbracket 1, m \rrbracket$$

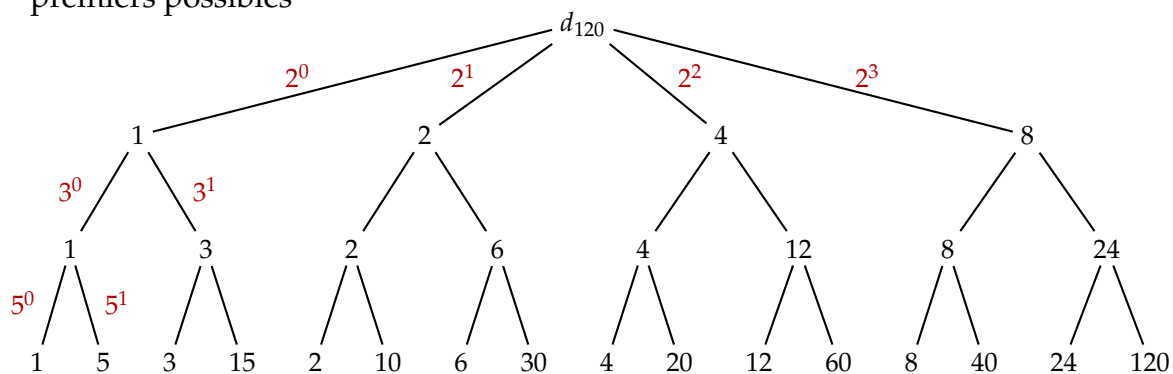
Le nombre de diviseurs N est alors : $N = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$

Exemple : Déterminer le nombre de diviseurs de 120 et tous ses diviseurs.

- On décompose 120 en facteurs premiers : $120 = 2^3 \times 3 \times 5$
 On alors : $(3 + 1)(1 + 1)(1 + 1) = 4 \times 2 \times 2 = 16$
 120 a donc 16 diviseurs.
- Pour déterminer tous ces diviseurs, on peut utiliser un tableau double entrée en séparant les puissance de 2 et les puissance de 3 et 5. On obtient alors :

×	2^0	2^1	2^2	2^3
$3^0 5^0$	1	2	4	8
$3^1 5^0$	3	6	12	24
$3^0 5^1$	5	10	20	40
$3^1 5^1$	15	30	60	120

- On peut aussi utiliser un arbre pondéré dont les coefficients sont les facteurs premiers possibles



- Les diviseurs de 120 sont : $D_{120} = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$.

2.3 Applications

1) 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 .

- L'entier n a 15 diviseurs. L'entier 15 ne possède qu'une décomposition en facteurs supérieurs à 1 : $15 = 3 \times 5$. L'entier n n'a que deux facteurs premiers.
- n est divisible par 6 donc divisible par 2 et 3. Les facteurs premiers de n sont 2 et 3. On a donc : $n = 2^\alpha 3^\beta$ avec $(1 + \alpha)(1 + \beta) = 3 \times 5$

$$\begin{cases} 1 + \alpha = 3 \\ 1 + \beta = 5 \end{cases} \text{ ou } \begin{cases} 1 + \alpha = 5 \\ 1 + \beta = 3 \end{cases} \Leftrightarrow \begin{cases} \alpha = 2 \\ \beta = 4 \end{cases} \text{ ou } \begin{cases} \alpha = 4 \\ \beta = 2 \end{cases}$$

- n n'est pas divisible par $8 = 2^3$, donc $\alpha < 3$. L'entier cherché n est donc :

$$n = 2^2 3^4 = 4 \times 81 = 324$$

2) Déterminer le plus petit entier naturel possédant 28 diviseurs.

Soit n l'entier cherché. Les décompositions de 28 en facteurs supérieurs à 1 sont : 28 , 2×14 , 4×7 , $2 \times 2 \times 7$

- 28 en 1 facteur : le plus petit entier n est $n = 2^\alpha$ avec $\alpha + 1 = 28 \Leftrightarrow \alpha = 27$

$$n = 2^{27} = 134\,217\,728$$

- 28 en 2×14 : le plus petit entier n est alors

$$n = 2^\alpha \times 3^\beta \text{ avec } \alpha + 1 = 14 \text{ et } \beta + 1 = 2 \Leftrightarrow \alpha = 13 \text{ et } \beta = 1$$

$$n = 2^{13} \times 3 = 24\,576$$

- 28 en 4×7 : le plus petit entier n est alors

$$n = 2^\alpha \times 3^\beta \text{ avec } \alpha + 1 = 7 \text{ et } \beta + 1 = 4 \Leftrightarrow \alpha = 6 \text{ et } \beta = 3$$

$$n = 2^6 \times 3^3 = 1\,728$$

- 28 en $2 \times 2 \times 7$: le plus petit entier n est alors

$$n = 2^\alpha \times 3^\beta \times 5^\gamma \text{ avec } \alpha + 1 = 7, \beta + 1 = \gamma + 1 = 2 \Leftrightarrow \alpha = 6, \beta = \gamma = 1$$

$$n = 2^6 \times 3 \times 5 = 960$$

Le plus petit entier naturel ayant 28 diviseurs est 960

3 Petit théorème de Fermat

Théorème 7 : Soit p premier et $a \in \mathbb{N}$ non multiple de p alors : $a^{p-1} \equiv 1 (p)$
De plus pour tout $a \in \mathbb{N}$, on a : $a^p \equiv a (p)$

Démonstration : Soit les $(p-1)$ premiers multiples de a : $a, 2a, 3a, \dots, (p-1)a$.
et leurs restes dans division par p : $r_1, r_2, r_3, \dots, r_{p-1}$.

- Ces restes sont deux à deux distinct.

En effet s'il existait deux restes identiques soit $r_i = r_j$ avec $i > j$, alors :

$$ia - ja \equiv r_i - r_j (p) \Leftrightarrow a(i-j) \equiv 0 (p)$$

donc $(i-j)a$ serait multiple de p , qui d'après le théorème de Gauss appliqué aux nombres premiers, impliquerait a ou $(i-j)$ multiples de p , ce qui est impossible.

- Ces restes sont tous différents et comme il y a $(p-1)$ multiples, on trouve tous les restes non nul possibles dans division par p .
- On a alors : $r_1 \times r_2 \times \dots \times r_{p-1} = 1 \times 2 \times 3 \times \dots \times (p-1) = (p-1)!$
- Le produit des $(p-1)$ multiples vérifie alors :

$$\begin{aligned} a \times 2a \times 3a \times \dots \times (p-1)a &\equiv (p-1)! (p) \\ (p-1)! a^{p-1} &\equiv (p-1)! (p) \\ (p-1)! (a^{p-1} - 1) &\equiv 0 (p) \end{aligned}$$

$(p-1)!$ est premier avec p car tous les facteurs de $(p-1)!$ sont inférieurs à p , d'après le théorème de Gauss $a^{p-1} - 1$ est alors un multiple de p .

On a donc : $a^{p-1} - 1 \equiv 0 (p) \Leftrightarrow a^{p-1} \equiv 1 (p)$.

- En multipliant par a , on obtient : $a^p \equiv a (p)$.

Cette égalité reste vraie si a est multiple de p car alors $a \equiv 0(p)$.

Remarque : Dans la suite, on parlera du théorème de Fermat pour le petit théorème de Fermat.

Exemple :

- $4^{12} \equiv 1 (13)$ car 13 est premier et 4 non multiple de 13.
- 7 est premier et 3 non multiple de 7, donc, d'après le théorème de Fermat, on a : $3^6 \equiv 1 \pmod{7} \xrightarrow{\uparrow n} 3^{6n} \equiv 1^n \equiv 1 (7) \Leftrightarrow 3^{6n} - 1 \equiv 0 (7)$
donc $3^{6n} - 1$ est divisible par 7 pour tout $n \in \mathbb{N}$.

⚠ La réciproque du théorème de Fermat est fautive. On peut avoir $a^{p-1} \equiv 1 (p)$ sans pour cela avoir p premier pour a premier avec p . Cette égalité n'est pas un critère de primalité.

Contre-exemple : $2^{10} = 1024 = 341 \times 3 + 1$ donc $2^{10} \equiv 1 (341)$.

On a alors : $2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 (341)$ et $341 = 11 \times 31$ non premier.