LES NOMBRES PREMIERS

I. Définition et propriétés

1. Définition

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

Conséquences
- 1 n'est pas un nombre premier (il n'a qu'un seul diviseur).
- Un nombre premier p est un entier naturel supérieur ou égal à 2, soit : $p \geq 2$.
- 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 n'est pas premier, il admet un diviseur d tel que : $2 \leq d < n$.

Remarque
Un entier naturel non premier est parfois appelé un nombre composé.

2. Critère d'arrêt ou test de primalité

Propriété - 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
- Si n est premier, il admet un diviseur premier : lui-même.
- Si n n'est pas premier, l'ensemble D des diviseurs d de n tels que : $2 \leq d < n$ n'est pas vide.
  D'après le principe du bon ordre, il admet donc un plus petit élément p.
  Si p n'était pas premier, il admettrait un diviseur d' tel que $2 \leq d' < p$ qui diviserait aussi n. Ceci est impossible car p est le plus petit élément de D. Donc p est premier.
- On a donc p premier et $n = p \times q$ avec $p \leq q$.
  En multipliant cette inégalité par p, on obtient :
  $$p^2 \leq pq \quad \Leftrightarrow \quad p^2 \leq n, \quad \text{soit} \quad p \leq \sqrt{n}$$

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.

Exercice d'application
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.

Le programme ci-dessous 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 ;

- 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, 11111 et 37589 que :
- 527 est divisible par 17
- 719 est premier ;
- 11111 est divisible par 41
- 37589 est premier.

$Saisir\ N$
$I \leftarrow 2$
$J \leftarrow 0$
$Si\ E\left(\frac{N}{I}\right) = \frac{N}{I}\ Alors$
    $afficher\ N\ "est\ divisible\ par"\ I$
    $J \leftarrow J + 1$
$I \leftarrow I + 1$
$Tant\ que\ I \leq \sqrt{N}$
    $Si\ E\left(\frac{N}{I}\right) = \frac{N}{I}\ Alors$
        $N\ "divisible\ par"\ I$
        $J \leftarrow J + 1$
    $I \leftarrow I + 2$
$Si\ J = 0\ alors$
    $Afficher\ N\ "est\ premier"$

3. Infinité des nombres premiers

Propriété
Il existe une infinité de nombres premiers.

Preuve
Cette preuve, par l'absurde ou par contradiction est celle proposée au III siècle av. J.-C., par Euclide, dans son ouvrage « Les Éléments ».
Il en existe bien évidemment d'autres.
Supposons qu'il existe un nombre fini n de nombres premiers : $p_1,\ p_2,\dots,p_i,\dots,\ p_n$.
Soit N un nombre entier non premier, supérieur à 2, tel que :

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

D'après le critère d'arrêt, N admet un diviseur premier.
Soit $p_i,\ i \in \{1,2,\dots,n\}$, ce diviseur premier.
p_i divise donc $p_1 \times p_2 \times \dots \times p_i \times \dots \times p_n$ et N.
Il divise donc la différence $N - (p_1 \times p_2 \times \dots \times p_i \times \dots \times p_n) = 1$.
Ceci est impossible car $P_i \geq 2$, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est contradictoire.

4. Crible d'Ératosthène

Algorithme - Crible d'Ératosthène
Pour dresser 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.

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

Remarques

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

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 :

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

5. Théorème de Gauss et nombres premiers

Propriété

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 :

Si p divise ab ⇔ p divise a ou p divise b

Preuve

Comme p est premier, on a : $(p, a) = p$ ou $(p, a) = 1$.

- Si $(p, a) = p$, alors p divise a.
- Si $(p, a) = 1$, alors p et a sont premiers entre eux. D'après le théorème de Gauss (voir chapitre 2), p divise b.

Remarque

En particulier, si p est premier et divise une puissance a^k, alors nécessairement p divise a. De cela découle que p^k divise a^k.

Conséquences

- 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 $p_1,p_2,,p_k$ des nombres premiers distincts et $\alpha_1,\alpha_2,,\alpha_k$ 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 l'entier n.

II. Décomposition, diviseurs d'un entier

1. Théorème fondamental de l'arithmétique

Théorème

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 2 - Décomposer un nombre en produit de facteurs premiers

Exercice d'application

Décomposer 16758 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 $16758 = 2 \times 3^2 \times 7^2 \times 19$.

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

• 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 $p_2 q_2$ et p_2 premier car, d'après le critère d'arrêt, q_1 admet un diviseur premier p_2 tel que $2p_2\sqrt{q_1}$. 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, ,q_n avec $q_3 > q_4 > \dots > q_n 2$.
Toute suite strictement décroissante dans est stationnaire à partir d'un certain rang n donc q_n est premier.

n se décompose 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, , 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 3 - Déterminer le PGCD de deux nombres à partir d'une décomposition en produit de facteurs premiers

Exercice d'application

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.

$$PGCD(126\ ;\ 735) = 3 \times 7 = 21$$

Remarque :

L'algorithme d'Euclide est à préférer pour la recherche du $PGCD$ à la méthode par décomposition car il est plus économe en opérations :

$$735 = 126 \times 5 + 105$$
$$126 = 105 \times 1 + 21$$
$$105 = 21 \times 5$$

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

2. Diviseurs d'un entier

Propriété

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

$$n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times \ldots \times p_m^{\alpha m}$$

Alors tout diviseur d de n a pour décomposition :

$$d = p_1^{\beta 1} \times p_2^{\beta 2} \times \ldots \times p_m^{\beta m} \quad \text{avec } 0 \leq \beta_i \leq \alpha_i \text{ et } i \in \{1,2,\ldots,m\}$$

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

Remarques

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

Méthode 4 - Trouver le nombre de diviseurs d'un entier

Exercice d'application

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

Correction :

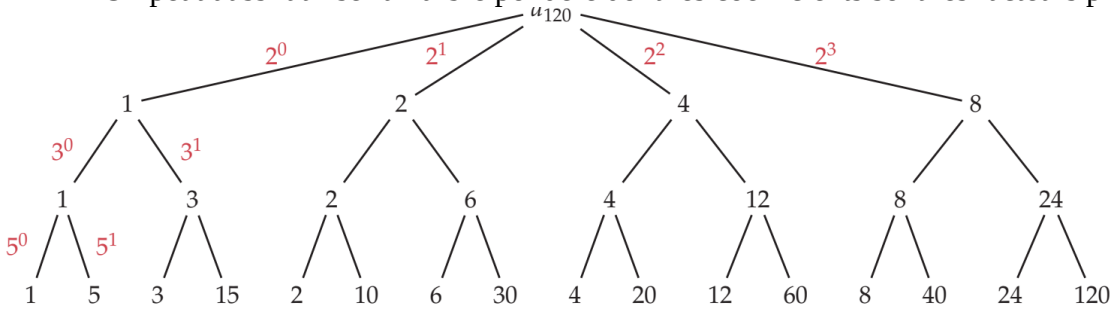
- On décompose 120 en facteurs premiers : $120 = 2^3 \times 3 \times 5$.
  On alors : $(3 + 1)(1 + 1)(1 + 1) = 4 \times 2 \times 2 = 16$. Il y a 16 diviseurs pour 120.

- Pour déterminer tous ses diviseurs, on peut utiliser un tableau à double entrée en séparant les puissances de 2 et les puissances 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

Les 16 diviseurs de 120 sont donc : $D_{120} = \{1,2,3,4,5,6,8,10,12,15,20,24,30,40,60,120\}$.

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



Méthode 5 - Déterminer un entier conditionné par ses diviseurs

Exercice d'application

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

- L'entier n a 15 diviseurs. Il faut donc connaître toutes les décompositions de 15 en facteurs supérieurs à 1. Il n'y a que deux décompositions possibles soit en un seul facteur 15, soit en deux facteurs 3×5.
- On sait que n est divisible par 6, il est donc divisible par 2 et par 3. Donc n admet au moins deux facteurs premiers. Comme 15 ne peut se décomposer en plus de deux facteurs, alors n ne peut admettre que deux facteurs premiers : 2 et 3. On a donc : $n = 2^{\alpha}3^{\beta}$.

- Comme on a $15 = 3 \times 5$ diviseurs, alors : $(1+\alpha)(1+\beta) = 3 \times 5$.

- • On trouve alors deux solutions : $\alpha = 2 \text{et} \beta = 4$ ou $\alpha = 4 \text{et} \beta = 2$.

- On sait de plus que n n'est pas divisible par $8 = 2^3$, donc α est inférieur à 3. n est donc : $n = 2^2\ 3^4 = 4 \times 81 = 324$.

Exercice d'application

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. On peut décomposer 28 en 1, 2 ou 3 facteurs : 28 ou 2×14 ou 4×7 ou $2 \times 2 \times 7$.

- En un facteur.

Le plus petit entier n est alors $n = 2^{\alpha}$ avec $\alpha + 1 = 28$, soit $\alpha = 27$.
Donc $n = 2^{27} = 134217728$.

- En deux facteurs : $28 = 2 \times 14$.

Le plus petit entier n est alors : $n = 2^{\alpha} \times 3^{\beta}$ avec $\alpha + 1 = 14$ et $\beta + 1 = 2$.
On trouve : $\alpha = 13$ et $\beta = 1$, donc $n = 2^{13} \times 3 = 24576$.

- En deux facteurs : $28 = 4 \times 7$.

Le plus petit entier n est alors : $n = 2^{\alpha} \times 3^{\beta}$ avec $\alpha + 1 = 7$ et $\beta + 1 = 4$.
On trouve : $\alpha = 6$ et $\beta = 3$, donc $n = 2^6 \times 3^3 = 1728$.

- En trois facteurs : $28 = 2 \times 2 \times 7$.

Le plus petit entier n est alors : $n = 2^{\alpha} \times 3^{\beta} \times 5^{\gamma}$ avec $\alpha + 1 = 7$,$\beta + 1 = 2$ et$\gamma + 1 = 2$.
On trouve : $\alpha = 6$, $\beta = 1$ et $\gamma = 1$, donc $n = 2^6 \times 3 \times 5 = 960$.

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