MATHEMATIQUES

soutienscolaire@monsieurtahar.com

CHAPITRE 8

Connaître le cours

1. Nombres premiers

1. Définition d'un nombre premier

Définition

Un entier naturel p est premier s'il possède exactement deux diviseurs distincts : 1 et p.

Exemples

- Le nombre 1 n'est pas premier. Il possède en effet un seul diviseur.
- Le nombre 2 est le plus petit nombre premier. 2 est le seul nombre premier pair.
- Le nombre 19 est premier car il ne possède que 1 et 19 comme diviseurs.

Théorème

DÉMO p. 167

Tout entier naturel n supérieur ou égal à 2 non premier possède un plus petit diviseur premier inférieur ou égal à $\sqrt{n}$.

Exemples

- 65 est un nombre entier non premier.

Il est divisible par 5 qui est un nombre premier inférieur ou égal à $\sqrt{65} \approx 8$.

- 4 est un nombre entier non premier.

Il est divisible par 2 qui est un nombre premier inférieur ou égal à $\sqrt{4}$.

Propriété (test de primalité)

DÉMO p. 167

Si n n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$, alors n est premier.

Exemple

On considère le nombre entier 83. $\sqrt{83} \approx 9,1$.
83 est impair donc 2 ne divise pas 83.
La somme des chiffres de 83 est égale à 11 qui n'est pas un multiple de 3 donc 3 ne divise par 83.
Le chiffre des unités de 83 n'est ni 0 ni 5 donc 5 ne divise par 83.
Enfin, 83 n'est pas divisible par 7 car $83 = 7 \times 11 + 6$.
2, 3, 5 et 7 sont les seuls nombres premiers inférieurs ou égaux à $\sqrt{83}$.
83 n'est divisible ni par 2, par 3 ni par 5 ni par 7 donc on peut affirmer que 83 est un nombre premier.

Remarque

Ce test de primalité est rapidement inefficace pour les très grandes valeurs de n car il faudrait un temps très long pour vérifier la divisibilité de n par des nombres premiers inférieurs ou égaux à $\sqrt{n}$ qui sont eux-mêmes de plus en plus grands (et donc il faudrait utiliser également un critère de primalité sur ces diviseurs).

Théorème

DÉMO p. 167

Il existe une infinité de nombres premiers et donc il n'existe pas de plus grand nombre premier.

Remarques

- En décembre 2018, le plus grand nombre premier découvert a été le nombre $2^{82\,589\,933} - 1$ qui possède presque 25 millions de chiffres.
- Il n'existe pas de formule donnant tous les nombres premiers. Certaines formules en donnent quelques-uns, comme le polynôme $n^2 + n + 41$.

Exercice résolu 1 Déterminer si un entier est premier

1 347 est-il premier ?

2 139 est-il premier ?

Solution commentée

1 $347 < 361$ et $\sqrt{361} = 19$. Donc $\sqrt{347} \leqslant 18$.
On teste la divisibilité de 347 par tous les entiers premiers inférieurs ou égaux à 17.
347 n'est pas divisible par 2, 3 et 5 en utilisant les critères de divisibilité.
On effectue les divisions euclidiennes de 347 par 7, 11, 13 et 17. On obtient :
$347 = 7 \times 49 + 4$; $347 = 11 \times 31 + 6$; $347 = 13 \times 26 + 9$ et $347 = 17 \times 20 + 7$.
347 n'est divisible par aucun nombre premier inférieur ou égal à 17.
Donc 347 est un nombre premier.

2 $119 < 121$ et $\sqrt{121} = 11$. Donc $\sqrt{119} \leqslant 10$.
On teste la divisibilité de 139 par tous les entiers premiers inférieurs ou égaux à 10.
119 n'est pas divisible par 2, 3 et 5 en utilisant les critères de divisibilité.
$119 = 7 \times 17$ donc 119 est divisible par 7.
119 n'est pas premier.

Exercice résolu 2 Déterminer si un nombre assez grand est premier à l'aide d'un algorithme

On considère la fonction premier ci-dessous.
Expliquer pourquoi cette fonction détermine si un nombre impair est premier ou non.

```python
from math import sqrt,floor
def premier(n):
    stop=floor(sqrt(n))
    d=3
    premier=True
    while d<=stop:
        if n%d==0:
            premier=False
        d=d+2
    return premier
```

Solution commentée

On teste si l'entier n est divisible par tous les entiers impairs à partir de 3 jusqu'à l'entier le plus proche de la racine carrée de n.
Comme il n'existe pas de formule qui donne tous les nombres premiers, on teste la divisibilité par les entiers impairs car les nombres premiers sont tous impairs (sauf 2 mais on ne teste pas si un nombre pair est premier).

Exercice résolu 3 Déterminer si un nombre défini par une expression littérale peut être premier

Soit n un entier naturel supérieur ou égal à 2. Le nombre $n^2 - 1$ peut-il être premier ?

Solution commentée

$n^2 - 1 = (n+1)(n-1)$.
Si $n = 2$ alors $n - 1 = 1$ et $n + 1 = 3$ qui est premier. $n^2 - 1$ est donc premier.
Si $n > 2$, $n - 1 > 1$ donc cela veut dire que $n^2 - 1$ a au moins un diviseur strict $n - 1$. Donc $n^2 - 1$ n'est pas premier.

Connaître le cours

2. Deux théorèmes fondamentaux

1. Décomposition d'un entier en produit de facteurs premiers

Théorème

Tout nombre entier naturel n, supérieur ou égal à 2, se décompose sous la forme :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \ldots \times p_k^{\alpha_k}$$

DÉMO p. 166

où $p_1, p_2, p_3, \ldots, p_k$ sont des nombres premiers distincts rangés dans l'ordre croissant et $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k$ sont des entiers naturels non nuls.
Cette écriture porte le nom de décomposition en produit de facteurs premiers.
Elle est unique à l'ordre près des facteurs.

Exemples

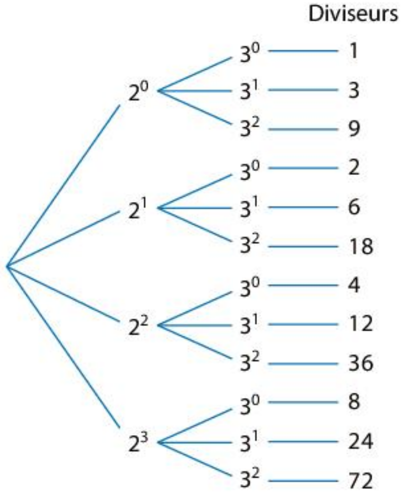
- $24 = 2^3 \times 3$
- $1178 = 2 \times 19 \times 31$
- $37 = 1 \times 37$ car 37 est un nombre premier

Remarque

En utilisant la décomposition en facteurs premiers d'un nombre entier naturel, on peut trouver l'ensemble de ses diviseurs.

Exemple

$72 = 2^3 \times 3^2$.
72 a pour diviseurs les entiers de la forme $2^a \times 3^b$ avec $0 \leqslant a \leqslant 3$ et $0 \leqslant b \leqslant 2$.
On peut visualiser l'ensemble des diviseurs de 72 par un arbre de choix.
72 a 12 diviseurs.



2. Petit théorème de Fermat

Théorème (admis)

Soit n un nombre entier.
Si p est un nombre premier ne divisant pas n, alors $n^{p-1} \equiv 1\ [p]$.

DÉMO p. 167

Conséquence

Si p est un nombre premier et n un entier, alors $n^p \equiv n\ [p]$.

Remarque

Le petit théorème de Fermat donne une condition nécessaire pour que p soit premier. On dit qu'il constitue un test de primalité.
En effet, si n est un entier tel que $1 \leqslant n < p$ et si p est premier alors $n^{p-1} \equiv 1\ [p]$.
Donc si pour tout entier n inférieur à p, n^{p-1} n'est pas congru à 1 modulo p alors p n'est pas premier.
Mais ce test n'est pas efficace pour les grandes valeurs de p.

Exercice résolu 1 Décomposer un nombre entier en produit de facteurs premiers

Décomposer en produit de facteurs premiers, les entiers suivants.

a. 30 **b.** 11 **c.** 180

Solution commentée

a. $30 = 2 \times 3 \times 5$.

b. $11 = 11$ car 11 est premier.

c. Comme 180 est un entier assez grand, on peut effectuer une série de divisions par les premiers nombres premiers.

Donc $180 = 2^2 \times 3^2 \times 5$.

180	2
90	2
45	3
15	3
5	5
1	.

Exercice résolu 2 Déterminer le nombre et la liste des diviseurs d'un entier

Déterminer la liste des diviseurs de 140.

Solution commentée

On écrit la décomposition de 140 en produit de facteurs premiers :

$$140 = 2^2 \times 5 \times 7.$$

Les diviseurs de 140 sont de la forme :

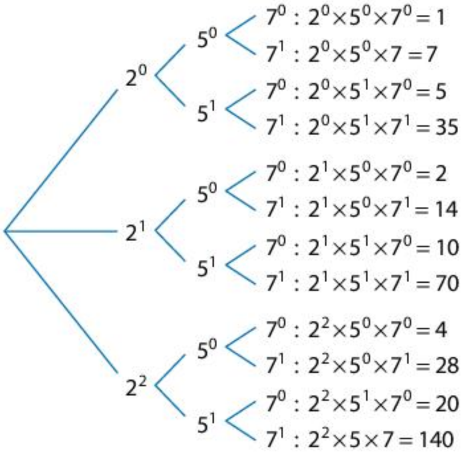
$2^\alpha \times 5^\beta \times 7^\gamma$, avec $\alpha \in \{0;1;2\}$ et $\beta, \gamma \in \{0;1\}$.

On aura donc $3 \times 2 \times 2 = 12$ diviseurs distincts.

On se sert d'un arbre (ci-contre) pour déterminer tous les diviseurs possibles.

L'ensemble des diviseurs de 140 est donc :

$\{1;2;4;5;7;10;14;20;28;35;70;140\}$.



Exercice résolu 3 Montrer une divisibilité avec le petit théorème de Fermat

Montrer que, quel que soit l'entier naturel n, $n^{13} - n$ est divisible par 26.

Solution commentée

13 étant premier, d'après la conséquence du petit théorème de Fermat, on a $n^{13} - n \equiv 0\ [13]$.

Le nombre 2 étant premier, on a de même $n^2 - n \equiv 0\ [2]$.

Or on a : $n^{13} = (n^2)^6 \times n$. On a alors : $n^2 \equiv n\ [2]$ donc $(n^2)^3 \equiv n^3\ [2]$ donc $(n^2)^6 \times n \equiv n^4\ [2]$

On en déduit que $n^{13} \equiv n^4\ [2]$. Or $n^2 \equiv n\ [2]$ donne $n^4 \equiv n^2\ [2]$ donc $n^4 \equiv n\ [2]$.

On en déduit que $n^{13} \equiv n\ [2]$.

Ainsi : $n^{13} \equiv n\ [13]$ donc il existe k entier tel que $n^{13} = n + 13k$.

De même, $n^{13} \equiv n\ [2]$ donc il existe k' entier tel que $n^{13} = n + 2k'$.

On a donc $n + 13k = n + 2k' \Leftrightarrow 13k = 2k'$. Or 2 et 13 sont premiers entre eux, donc par le théorème de Gauss, 13 divise k' soit $k' = 13k''$.

On en déduit que $n^{13} = n + 2k' = n + 2 \times 13 \times k'' = n + 26k''$. On a bien $n^{13} \equiv n\ [26]$.