Les nombres premiers

Christophe ROSSIGNOL*

Année scolaire 2018/2019

Table des matières

1 Définition, premières propriétés **2**

1.1 Définition 2

1.2 Test de primalité 2

1.3 Infinité de nombres premiers 2

1.4 Divisibilité par un nombre premier 3

2 Décomposition en facteurs premiers **3**

2.1 Théorème fondamental de l'arithmétique 3

2.2 Diviseur d'un entier 4

Activité : Problème 2 page 77 [1] [TransMath],
en utilisant *le crible d'*ÉRATOSTHÈNE sur feuille polycopiée.

Dans tout ce chapitre, on n'utilisera que des nombres entiers naturels. Lorsque l'on parlera de diviseurs d'un entier naturel, il s'agira de ses diviseurs positifs.

1 Définition, premières propriétés

1.1 Définition

Définition : Un nombre entier naturel est dit premier s'il a exactement deux diviseurs distincts : 1 et lui-même.
Un entier naturel non premier (autre que 1) est dit composé.

Exemples :

1. Attention ! 1 n'est pas un nombre premier car il n'a qu'un seul diviseur.
2. Dans l'ordre croissant, les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19, 23...

Exercices : 1, 2, 4 page 84 [2] [TransMath]

1.2 Test de primalité

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

Remarque : Pour montrer qu'un nombre *est* premier, il suffit donc d'utiliser la contraposée de cette propriété, c'est-à-dire :
Si $n \geq 2$ n'admet aucun diviseur premier p avec $2 \leq p \leq \sqrt{n}$, alors n est un nombre premier.

Exemple : Montrer que 109 est un nombre premier.
On a $\sqrt{109} \simeq 10,4$. Il suffit de voir si 109 a un diviseur premier compris entre 2 et 10, c'est-à-dire un diviseur parmi 2, 3, 5 et 7.
$109 = 54 \times 2 + 1$ donc 109 n'est pas divisible par 2.
$109 = 36 \times 3 + 1$ donc 109 n'est pas divisible par 3.
$109 = 20 \times 5 + 9$ donc 109 n'est pas divisible par 5.
$109 = 15 \times 7 + 4$ donc 109 n'est pas divisible par 7.
Le nombre 109 est donc un nombre premier.

Exercices : 37, 39, 41 page 96 [3] [TransMath]

1.3 Infinité de nombres premiers

Propriété : Il existe une infinité de nombres premiers.

Démonstration :
On va raisonner par l'absurde en supposant qu'il y ait un nombre fini de nombres premiers.
On note ces nombres $p_1, p_2, \ldots, p_n$.
On note $N = 1 + p_1 \times p_2 \times \cdots \times p_n$.
Le nombre N est strictement supérieur à 1, donc il admet un diviseur premier, noté d.
Comme il n'y a qu'un nombre fini de nombres premiers, d est l'un des nombres $p_1, p_2, \ldots, p_n$ et donc, d divise $p_1 \times p_2 \times \cdots \times p_n$.
Par suite, d divise $N - p_1 \times p_2 \times \cdots \times p_n = 1$. Donc $d = 1$.
Ce qui est impossible car 1 n'est pas un nombre premier.
l'hypothèse de départ est donc fausse. Il y a donc une infinité de nombres premiers.

1. Trouver les premiers nombres premiers
2. Caractérisation des nombres premiers.
3. Nombres premiers.

Remarque : Cette démonstration par l'absurde est exigible. Elle a été proposé au III^e siècle avant J.-C., par EUCLIDE, dans son ouvrage « *Les Éléments* ».

1.4 Divisibilité par un nombre premier

Propriété 1 : Soient a un entier naturel non nul et p un nombre premier.
Si a n'est pas divisible par p alors p et a sont premiers entre eux.

Remarques :

1. C'est une application directe du fait qu'un nombre premier a exactement deux diviseurs : 1 et lui-même. Si a n'est pas divisible par p, le seul diviseur commun à a et p est 1.
2. On en déduit donc une forme plus forte du théorème de GAUSS pour les nombres premiers.

Propriété 2 : Soient a et b deux entiers naturels non nuls et p un nombre premier.
p divise le produit ab si et seulement si p divise a ou p divise b.

Remarque : Cela entraîne les conséquences suivantes :
— Si un nombre premier p divise un produit de facteurs premiers, alors p est un de ces facteurs premiers.
— Si un nombre premier p divise une puissance a^k, alors p divise a. Et, par suite, p^k divise a^k.

Exercices : 3 page 84 ; 23 page 90 : 65 page 97 et 67, 69 page 98 [4] – 71, 72 page 99 [5] –82, 83, 85 page 101 [6] [TransMath]

2 Décomposition en facteurs premiers

2.1 Théorème fondamental de l'arithmétique

Théorème : Tout entier $n \geq 2$ se décompose de façon unique (à l'ordre près des facteurs) en produit de facteurs premiers.
Il existe donc des nombres premiers distincts $p_1, p_2, \ldots, p_m$ et $\alpha_1, \alpha_2, \ldots, \alpha_m$ des entiers naturels non nuls tels que :

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

Exemples :

1. Décomposer 16 758 en produit de facteurs premiers.

Méthode :
On détermine le plus petit nombre premier divisant 16 758, puis on continue avec les quotients successifs, jusqu'à ce que le nombre obtenu soit un nombre premier.

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

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

2. À l'aide de la décomposition en produit de facteurs premiers des nombres 126 et 735, déterminer leur PGCD.

$$\begin{array}{r|l} 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

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

$$\begin{array}{r|l} 735 & 3 \\ 245 & 5 \\ 49 & 7 \\ 7 & 7 \\ 1 & \end{array}$$

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

Le PGCD de 126 et 735 est la plus grande partie commune de ces décompositions, donc :

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

4. Divisibilité des nombres premiers.
5. PGCD et nombres premiers
6. Type BAC.

Remarque : Cette méthode de détermination du PGCD est en général moins efficace que l'algorithme d'EUCLIDE.

Exercices : 6, 7 page 87[7] – 11, 12, 14, 16, 17 page 88[8] – 46 page 96[9] — 22 page 90 et 56, 57 page 97[10] [TransMath]

2.2 Diviseur d'un entier

Propriété : Soit n un entier ($n \geq 2$) 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 admet une décomposition de la forme :

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_m^{\beta_m} \quad \text{avec } 0 \leq \beta_i \leq \alpha_i$$

En particulier, le nombre de diviseur de n est $N = (\alpha_1 + 1) \times (\alpha_2 + 1) \times \cdots \times (\alpha_m + 1)$

Exemple : Déterminer le nombre de diviseurs de 340, puis l'ensemble de ces diviseurs.

$$\begin{array}{r|l}
340 & 2 \\
170 & 2 \\
85 & 5 \\
17 & 17 \\
1 &
\end{array} \quad \text{donc}$$

$340 = 2^2 \times 5 \times 17$

340 a donc $3 \times 2 \times 2 = 12$ diviseurs.

Liste des diviseurs :

$2^0 \times 5^0 \times 17^0 = 1$
$2^0 \times 5^0 \times 17^1 = 17$
$2^0 \times 5^1 \times 17^0 = 5$
$2^0 \times 5^1 \times 17^1 = 85$
$2^1 \times 5^0 \times 17^0 = 2$
$2^1 \times 5^0 \times 17^1 = 34$
$2^1 \times 5^1 \times 17^0 = 10$
$2^1 \times 5^1 \times 17^1 = 170$
$2^2 \times 5^0 \times 17^0 = 4$
$2^2 \times 5^0 \times 17^1 = 68$
$2^2 \times 5^1 \times 17^0 = 20$
$2^2 \times 5^1 \times 17^1 = 340$

Exercices : 9, 10 page 87[11] [TransMath]

Références

[TransMath] TransMATH Term S Spécialité, programme 2012 (NATHAN)

2, 3, 4

7. Décomposition en facteurs premiers.
8. Utilisation de la décomposition en facteurs premiers
9. Algorithmique.
10. Résolutions d'équations.
11. Ensemble des diviseurs