Les nombres premiers

Christophe ROSSIGNOL*

Année scolaire 2021/2022

Table des matières

1 Définition, premières propriétés **2**

1.1 Définition 2

1.2 Test de primalité 2

1.3 Infinité de nombres premiers 3

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

3 Petit théorème de Fermat **5**

Activités : Activité 1 page 134 [1] et activité 2 page 135 [2] [Magnard]
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. Le plus petit nombre premier est 2. Les autres nombres premiers sont impairs.
3. Dans l'ordre croissant, les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19, 23...
4. L'utilisation du crible d'Ératosthène donne les 35 nombres premiers inférieurs ou égaux à 150.

Exercices : 41, 42 page 146 [3] [Magnard]

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 : on admettra pour cette démonstration que toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Démonstration :
Si n est premier, il admet un diviseur premier : lui-même.
Si n n'est pas premier, on appelle D l'ensemble des diviseurs de n strictement supérieur à 1.
D est non vide (il contient n) et admet donc un plus petit élément p.
Si p n'est pas premier, il admet un diviseur d tel que $1 < d < p$. Ce nombre est aussi un diviseur de n, donc $d \in D$. Ce qui est impossible car p est le plus petit élément de D.
Donc p est premier et $n = p \times q$ avec $p \leq q$ (car $q \in D$). En multipliant cette inégalité par p, on obtient : $p^2 \leq pq$, soit $p^2 \leq n$ et donc $p \leq \sqrt{n}$.

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 : 1, 2 page 137 ; 24, 25 page 145 ; 40, 43, 45 page 146 [4] [Magnard]

1. Découvrir le crible d'Ératosthène.
2. Généraliser le crible d'Ératosthène par un algorithme.
3. Caractérisation des nombres premiers.
4. Nombres premiers.

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, …, 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, …, 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.

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 une puissance a^k, alors p divise a. Et, par suite, p^k divise a^k.
— Si un nombre premier p divise un produit de facteurs premiers, alors p est un de ces facteurs premiers.

Exercices : 3, 4 page 137 ; 13 page 141 ; 26, 27 page 145 et 48, 49 page 146 [5] [Magnard]

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, …, p_m et α_1, α_2, …, α_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 :

5. Théorème de Gauss appliqué aux nombres premiers.

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.

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

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.

126	2
63	3
21	3
7	7
1	

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

735	3
245	5
49	7
7	7
1	

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

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

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

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

Exercices : 5, 6 page 139 ; 28, 29, 30, 31 page 145 ; 53 page 146 [6] – 8 page 139 ; 54, 55 page 146 ; 56, 57 ; 59 page 147 [7] – 9 page 139 [8] [Magnard]

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.

340	2
170	2
85	5
17	17
1	

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 : 10, 11 page 141 ; 61, 62 page 147 [9] – 14, 15, 17, 18, 19 page 142 ; 64 page 146 ; 74, 75, 76, 78 page 148 [10] [Magnard]

6. Décomposition en facteurs premiers.
7. Applications de la décomposition en facteurs premiers.
8. Programme PYTHON.
9. Trouver les diviseurs d'un entier.
10. Déterminer un entier à partir de son nombre de diviseurs.

3 Petit théorème de Fermat

Soit p un nombre premier et a un entier naturel non multiple de p. alors $a^{p-1} \equiv 1\ (p)$
De plus, pour tout entier naturel a, $a^p \equiv a\ (p)$

Démonstration :

On considère les $p-1$ premiers multiples de a : a, $2a$, $3a$, ..., $(p-1)\,a$ et on note r_1, r_2, r_3, .., r_{p-1} les restes respectifs de leur division par p.

Ces restes sont non nuls.

En effet, si $r_i = 0$, cela signifie que ia est divisible par p premier donc soit $p \mid i$ soit $p \mid a$. Or $i < p$ donc i n'est pas divisible par p et, par hypothèse, p ne divise pas a. c'est donc impossible.

Ces restes sont tous distincts.

En effet, si $r_i = r_j$, cela signifie que $ia - ja = (i-j)\,a$ est divisible par p premier donc soit $p \mid i-j$ soit $p \mid a$. Or $i - j < p$ donc $i - j$ n'est pas divisible par p et, par hypothèse, p ne divise pas a. c'est donc impossible.

Commr il y a $p-1$ multiples de a, on obtient donc tous les restes non nuls possibles de la division par p.

On a donc :

$$a \times 2a \times 3a \times \cdots \times (p-1)\,a \equiv r_1 \times r_2 \times \cdots \times r_{p-1}\ (p) \equiv 1 \times 2 \times 3 \times \cdots \times (p-1)\ (p)$$

ce qui revient à écrire, en regroupant les termes : $(p-1)! \times a^{p-1} \equiv (p-1)!\ (p)$, c'est-à-dire $(p-1)! \times \left(a^{p-1} - 1\right) \equiv 0\ (p)$.
Donc p divise $(p-1)! \times \left(a^{p-1} - 1\right)$. Comme p est premier, on a $p \mid (p-1)!$ ou $p \mid a^{p-1} - 1$.
Comme tous les facteurs de $(p-1)!$ sont strictement inférieurs à p, aucun n'est divisible par p donc p ne divise pas $(p-1)!$.
On a donc $p \mid a^{p-1} - 1$, c'est à dire $a^{p-1} - 1 \equiv 0\ (p)$ et donc $a^{p-1} \equiv 0\ (p)$.

En multipliant cette égalité par a on obtient $a^p \equiv a\ (p)$.
Cette dernière égalité reste vraie lorsque a est un multiple de p car dans ce cas, $a \equiv 0\ (p)$ et donc $a^p \equiv 0\ (p)$.

Exemples :

- 7 est premier et 7 ne divise par 12 donc $12^6 \equiv 1\ (7)$
- 5 est premier et 5 ne divise par 8 donc $8^4 \equiv 1\ (5)$

Exercices : 12 page 141 ; 36, 37, 38 page 145 ; 66, 68, 69, 71, 72 page 147 [11] – 21 page 148 ; 80 page 148 [12] – 82 page 148 ; 84, 85 page 149 [13] – 87, 88 page 149 et 89 page 150 [14] – 93, 94 page 150 [15] – 100 page 151 [16] – 104 page 152 [17] [Magnard]

Module : TP 2 page 159 [18] [Magnard]

Références

[Magnard] Maths Tle Expertes, MAGNARD, 2020

2, 3, 4, 5

11. Utiliser le petit théorème de FERMAT.
12. Travailler modulo p avec p premier.
13. Nombres premiers et suites.
14. Divisibilité et nombres premiers.
15. Équations et nombres premiers.
16. Triplets pythagoriciens.
17. Décomposition de 40.
18. Le système RSA.