NOMBRES PREMIERS

Jean Chanzy

Université de Paris-Sud *

1 Définitions et exemples :

Définition 1.1. *Un entier naturel p est dit « **premier** » s'il admet exactement deux diviseurs dans $\mathbb{N}$: 1 et p lui-même.*

Exemples et contre-exemples :

1. *0 n'est pas premier car il a une infinité de diviseurs.*
2. *1 n'est pas premier car il n'a qu'un seul diviseur dans $\mathbb{N}$: 1 lui-même.*
3. *2 est le premier nombre premier, et le plus petit. C'est le seul nombre entier naturel premier qui soit pair.*
4. *$3; 5; 7; 11; 13; 17; 19; \ldots$ sont premiers.*

Définition 1.2. *Deux entiers naturels a et b sont dits « **premiers entre eux** » s'ils n'ont en commun que 1 comme diviseur.*

Remarques :

1. NE PAS CONFONDRE « **PREMIER** » avec « **PREMIERS ENTRE EUX** »
2. Si p est un nombre premier et $n \in \mathbb{N}$, alors ou $p|n$ ou p est premier avec n.
3. Un entier naturel $n \geq 2$, non premier, est dit « **composé** ».

♣

2 Propriétés des nombres premiers :

Théorème *Soit $n \in \mathbb{N}$, $n \geq 2$.*

1. *n admet au moins un diviseur premier.*
2. *Si n n'est pas premier, il admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$.*
3. *Il y a une infinité de nombres premiers.*

Démonstration :

1. $n \geq 2$.
   - Si n est premier, il est divisible par lui-même.
   - Si n n'est pas premier, il admet d'autres diviseurs que 1 et n. Soit p le plus petit d'entre eux. Alors p est premier, sinon il admettrait un diviseur d tel que $1 \leq d \leq p$. d serait alors un diviseur de n plus petit que p, ce qui est absurde.
2. Soit n un entier naturel non premier ($n > 1$). n admet au moins un diviseur d autre que 1 et n. Il existe donc $q \in \mathbb{N}^*$ tel que $n = dq$. $d \geq 2$, $q \geq 2$, sinon $q = 1$ et $n = d$. Supposons $d \leq q$, alors $d^2 \leq dq$ et $d^2 \leq n$. Donc $d \leq \sqrt{n}$. D'autre part, d'après la première partie du théorème, d admet au moins un diviseur premier a qui est également un diviseur premier de n, et $a \leq d \leq \sqrt{n}$.

*Université de Paris-Sud,Bâtiment 425;F-91405 Orsay Cedex

3. Supposons qu'il existe un nombre fini de nombres premiers. Soient p le plus grand d'entre eux et N le produit de tous les nombres premiers entre 2 et p : $N = 2 \times 3 \times \ldots \times p$. Soit $N' = N + 1$. Le reste de la division euclidienne de N' par $2, 3, 5, \ldots$, ou p est 1, donc N' n'est divisible par aucun des nombres premiers $2, 3, 5, \ldots, p$. Si N' est premier, il est supérieur à p, ce qui est absurde. Si N' n'est pas premier, il a au moins un diviseur premier qui est supérieur à p, ce qui est encore absurde. Donc il y a une infinité de nombres premiers.

□

3 Crible d'Ératosthène :

Proposition ;Test de primalité d'un nombre entier : *Si un entier naturel n n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$, alors n est premier.*

Ce test de primalité permet de concevoir le crible d'Ératosthène, qui donne la liste de tous les nombres premiers compris entre deux nombres entiers donnés :

1	(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

On vérifie les règles suivantes :

1. Pour obtenir tous les nombres premiers entre 1 et 50, on prend le premier nombre premier, c'est-à-dire 2, on barre tous les multiples de 2, puis le nombre premier suivant et on barre tous ses multiples, et ainsi de suite...
2. Quand on arrive à un nombre premier p, le premier nombre suivant non premier à barrer est p^2.
3. Quand on a barré tous les nombres multiples des nombres premiers entre 1 et 50, les nombres non barrés sont les nombres premiers entre 1 et 50. Ce sont les nombres qui sont entourés.

4 Décomposition en nombres premiers :

Théorème *Tout entier naturel supérieur à 1 se décompose en un produit de nombres premiers et cette décomposition est unique, à l'ordre des facteurs près.*

Démonstration : Soit $n \in \mathbb{N}$, $n \geq 2$. Si n est premier, il se décompose en un seul facteur premier : lui-même.

Si n n'est pas premier, il admet au moins un diviseur premier p et $n = p \times d_1$, avec $1 < p < n$ et $1 < d_1 < n$. Si d_1 est premier, on a décomposé n en produit de deux facteurs premiers. Si d_1 n'est pas premier, on recommence et on écrit $d_1 = p' \times d_2$,etc..., jusqu'à ce que le dernier quotient obtenu soit 1. On admet l'unicité. □

Corollaire *Un entier naturel d divise un entier naturel n si et seulement si les nombres premiers de sa décomposition en facteurs premiers figurent dans celle de n avec des exposants inférieurs ou égaux à ceux de la décomposition de n.*

Démonstration : Supposons que $d \in \mathbb{N}$ divise $n \in \mathbb{N}$. Soient p un nombre premier de la décomposition de d et α son exposant dans cette décomposition. Alors $n = d \times q = (p^\alpha d_1)q$, avec $a \in \mathbb{N}$ et $q \in \mathbb{N}$, et $n = p^\alpha(aq)$. Si β est l'exposant de p dans la décomposition de aq, et γ l'exposant de p dans la décomposition de n, on a alors $\gamma = \alpha + \beta$, donc $\alpha \leq \gamma$. Réciproquement, si $n = p_1^{\gamma_1} \times p_2^{\gamma_2} \times \ldots p_r^{\gamma_r}$ et $d = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots p_r^{\alpha_r}$, avec $0 \leq \alpha_1 \leq \gamma_1$, $0 \leq \alpha_2 \leq \gamma_2$,..., $0 \leq \alpha_r \leq \gamma_r$, alors $d|n$ car on peut écrire $n = p_1^{\gamma_1 - \alpha_1} \times p_2^{\gamma_2 - \alpha_2} \times \ldots p_r^{\gamma_r - \alpha_r} \times d$. □