Nombres premiers

Terminale S spécialité - Lycée Saint-Charles

Patrice Jacquet - www.mathxy.fr - 2015-2016

1 L'ensemble des nombres premiers

Définition 1

L'ensemble des **nombres premiers** est un sous-ensemble de $\mathbb{N}$.
Un nombre entier est dit premier s'il admet exactement deux diviseurs : 1 et lui-même

Remarque. Le nombre 1 possède un seul diviseur : 1 n'est pas premier.

Exemple. Les nombres 2, 3 et 5 sont premiers. Le nombre 4, divisible par 2, n'est pas premier.

Propriété 1

Tout nombre entier a strictement supérieur à 1 admet au moins un diviseur premier.

Preuve. On raisonne par disjonction de cas : a premier, a non premier
Si a est premier, alors le diviseur premier cherché est a.
Si a n'est pas premier.
Soit d le plus petit diviseur de a tel que $d > 1$, prouvons par l'absurde que d est premier.
Supposons donc que d n'est pas premier : il existe un entier d' diviseur de d et supérieur à 1. d' est aussi un diviseur de a. On a donc $1 < d' < d < a$, ce qui est impossible puisque d est le plus petit diviseur de a. Donc d est premier.

Propriété 2

Tout nombre entier a non premier admet un diviseur inférieur ou égal à $\sqrt{a}$.

Preuve. Soit d un diviseur de a avec $d \neq 1$ et $d \neq a$.
Il existe d' tel que $d \times d' = a$.
Si $d > \sqrt{a}$ et $d' > \sqrt{a}$, alors $d \times d' > \sqrt{a} \times \sqrt{a}$, soit $a > a$ ce qui est absurde.
Donc $d \leqslant \sqrt{a}$ ou $d' \leqslant \sqrt{a}$.

Remarque. On peut ainsi prouver qu'un nombre est premier en vérifiant qu'il n'a pas de diviseurs inférieur ou égal à $\sqrt{a}$.

Propriété 3

Il existe une infinité de nombres premiers.

Preuve. On raisonne par l'absurde (démonstration donnée par Euclide vers 300 av. J.-C.).
Supposons que l'ensemble des nombre premiers soit fini : $2; 3; 5; ...; p$.
On note P le produit de tous les nombres premiers. $P+1$ n'est pas un nombre premier et admet donc au moins un diviseur premier d.
d divise P et d divise $P+1$ donc P divise leur différence 1, ce qui est impossible. Il existe donc une infinité de nombres premiers.

2 Divisibilité par un nombre premier

Propriété 4

Si p est un nombre premier et a un entier non divisible par p, alors p et a sont premiers entre eux.

Preuve. par définition, 1 est le seul diviseur commun à a et p.

Propriété 5

p est un nombre premier
si p divise le produit ab de deux entiers, alors p divise a ou p divise b.

Preuve. Si p ne divise pas a alors p et a sont premiers entre eux. p divise ab donc d'après le théorème de Gauss p divise b.

Propriété 6

p est un nombre premier
si p divise le produit ab de deux nombres premiers, alors $p = a$ ou $p = b$.

Preuve. a et b étant premiers leurs seuls diviseurs sont 1 et eux-même. p étant différent de 1, $p = a$ ou $p = b$.

3 Théorème fondamental

Propriété 7

Un entier naturel supérieur à 1 est premier ou se décompose de manière unique en produit de nombres premiers.

Preuve. n est un entier naturel non premier.
D'après la propriété 1, n admet un diviseur premier p_1.
$n = p_1 \times q_1$. Si q_1 est premier alors n est le produit de deux nombres premiers.
Si q_1 n'est pas premier, alors q_1 admet un diviseur premier p_2, et $n = p_1 \times p_2 \times q_2$.
Tant que q_i n'est pas premier, on réitère ce processus pour construire une suite finie de nombres premiers, jusqu'au diviseur q_k premier.
Ainsi, n est le produit de facteurs premiers $p_1 \times p_2 \times ... \times p_k \times q_k$.
L'unicité de la décomposition est admise.

Exemple. $36 = 2^2 \times 3^2$ $\quad$ $92 = 2^2 \times 23$ $\quad$ $210 = 2 \times 3 \times 5 \times 7$