Les nombres premiers

I Définition, test de primalité

Définition 1
On dit qu'un entier naturel p est premier s'il admet exactement deux diviseurs entiers naturels distinscts : 1 et p. L'ensemble des nombres premiers sera noté $\mathbb{P}$.

Propriété 1
Soit n un entier naturel, $n \geqslant 2$.
1) n admet au moins un diviseur premier. 2) n n'est pas premier s'il admet un entier naturel p premier tel que $2 \leqslant p \leqslant \sqrt{n}$.

Preuve :
1) Soit n un entier naturel, si n est premier alors n admet un diviseur premier n.
Si n est non premier, n admet des diviseurs supérieur à 2. Notons p le plus petit diviseur supérieur ou égal à 2. p est premier sinon il ne serait pas le plus petit.
En effet, si p est non premier alors $p = dd'$ avec $p \geqslant d \geqslant 2$ et on a d qui divise n.
2) n est non premier donc il admet un diviseur premier p (on prend le plus petit diviseur). Il existe ainsi a tel que $n = pa$ avec $a \geqslant p$. Donc, $ap \geqslant p^2$ et ainsi $n \geqslant p^2$. On a donc $p \leqslant \sqrt{n}$. ■

Propriété 2 (Test de primalité)
Un nombre p est premier s'il n'est divisible par aucun nombre premier inférieur à $\sqrt{p}$.

II L'ensemble des nombres premiers

Théorème 1
Il existe une infinité de nombres premiers.

Preuve :

Par l'absurde,
Supposons qu'il existe un nombre fini de nombres premiers : $p_1, \ldots, p_n$.
Notons $N = p_1 \times p_2 \times \cdots \times p_n + 1$, N admet un diviseur premier p_i.
De plus p_i divise $p_1 \times p_2 \times \cdots \times p_n$ donc p_i divise $N - p_1 \times p_2 \times \cdots \times p_n$ et ainsi p_i divise 1 ce qui est impossible. L'ensemble des nombres premiers est donc infini. ■

III Théorème fondamental

Théorème 2
Tout entier n $(n > 1)$ peut être décomposer de façon unique en produit de nombres premiers sous la forme :
$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$

Preuve :
On admet l'unicité.
Existance :
Si n est premier, le théorème est démontré.
Si n n'est pas premier, n admet un diviseur premier p_1 et on a $n = p_1 a_1$.
Si a_1 est premier, le théorème est démontré sinon a_1 admet un diviseur premier p_2 et on a $a_1 = p_2 a_2$.
On recommence avec a_2, la suite (a_k) est décroissante et minorée par 1 et on a $a_1 > a_2 > \cdots$.
1 est atteint par cette suite. D'où l'existance. ■

Théorème 3
Soit n un entier naturel $(n > 1)$, dont la décomposition en facteur premier est $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, et d un entier naturel.
d est un diviseur de n si et seulement si d est de la forme $d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$,
avec $0 \leqslant \beta_i \leqslant \alpha_i$.

Théorème 4
Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, le nombre de diviseur de n est
$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.