Nombres premiers -

Soit p premier, $a \in \mathbb{Z}^*$, on a : $p \mid a$ ou $p \wedge a = 1$

Si un nombre est premier, il est premier avec tous les nombres qu'il ne divise pas.

preuve : $p \wedge a \mid p$, or on a $p \wedge a = p$ ou $p \wedge a = 1$

donc $p \mid a$ ou $p \wedge a = 1$

Lemme de Gauss d'Euclide

Soit p premier, $n \in \mathbb{N}^*$, $x_1, \dots, x_n \in \mathbb{Z}^*$ on a

$$p \mid \prod_{i=1}^{n} x_i \iff \exists i \in [\![1, n]\!] \quad p \mid x_i$$

preuve : $\Rightarrow$

Supposons $p \mid \prod_{i=1}^{n} x_i$

Raisonnons par l'absurde et supposons $\forall i \in [\![1, n]\!] \quad p \nmid x_i$

d'après la prop précédente

$\forall i \in [\![1, n]\!] \quad p \wedge x_i = 1$

donc $p \wedge \left(\prod_{i=1}^{n} x_i \right) = 1$

mais $p \mid \prod_{i=1}^{n} x_i$, or on a alors $p = 1$ contradiction.

donc $\exists i \in [\![1, n]\!] \quad p \mid x_i$

$\Leftarrow$ clair !

Décomposition primaire

Tout élément de $\mathbb{N} \setminus \{0, 1\}$ admet une décomposition en produit de nombres premiers, unique à l'ordre près des facteurs.

preuve :

Existence : par récurrence forte sur $\mathbb{N}$

la prop est vraie pour $n=2$

Supposons que tout entier de $\{2,\dots,n\}$ se décompose en produit de nombres premiers.

- si $n+1$ est composé, alors $\exists (a,b) \in (\mathbb{N}^*)^2$ tq
$$n+1 = ab \qquad 2 \le a \le n \ , \ 2 \le b \le n$$
d'après l'hypothèse de récurrence, a et b se décomposent en produit de facteurs premiers.
$n+1 = ab$ se décompose en produit de nombres premiers.
- si $n+1$ est premier, $n+1$ se décompose en un produit d'un seul facteur, lui-même.

Unicité : par récurrence forte sur n aussi :

prop est évidente pour $n=2$

Supposons qu'il y ait unicité à l'ordre près des facteurs dans la décomposition de tout entier de $\{2,\dots,n\}$ en produit de nombres premiers.

Soient N et $N' \in \mathbb{N}^*$, $p_1 \dots p_N$ et $q_1 \dots q_{N'}$ premiers tq
$$n+1 = p_1 \dots p_N = q_1 \dots q_{N'}$$
comme p_1 est premier et $p_1 \mid q_1 \dots q_{N'}$, $\exists\, i \in [\![1, N']\!]$ tq
$$p_1 \mid q_i \quad \text{mais } q_i \text{ est premier donc } p_1 = q_i$$

En réordonnant $q_1, \dots q_{N'}$, on a $p_1 = q_1$
alors $p_2 \dots p_N = q_2 \dots q_{N'} \le n$, par hypothèse de récurrence, on a $p_2 = q_2 \dots p_N = q_{N'}$ à l'ordre près