DEMONSTRATION

L'ENSEMBLE DES NOMBRES PREMIERS EST INFINI

Le théorème fondamental de l'arithmétique nous permet d'écrire que $\forall\, n \in \mathbb{N}$ avec $n \geq 2$, $\exists\, (p_1 ; p_2 ; p_3 \ldots . p_m) \in P^m$ et $\exists\, (\alpha_1 ; \alpha_2 ; \alpha_3 \ldots . \alpha_m) \in \mathbb{N}^m$ tel que :

$n = p_1^{\alpha 1} * p_2^{\alpha 2} * p_3^{\alpha 3} * \ldots . * p_m^{\alpha m}$ avec P l'ensemble des nombres premiers,

On va alors prendre l'entier n de la forme :

$n = p_1 * p_2 * p_3 * \ldots . * p_m$

avec $p_1 = 2$; $p_2 = 3$; $p_3 = 5$ .... et p_m nombre premier aussi grand que l'on peut,

On a $p_1 < p_2 < p_3 < \ldots . < p_m$ classés par ordre croissant autrement dit : p_{i-1} et p_i sont des nombres premiers successifs ($2 \leq i \leq m$).

On pose P_n l'ensemble suivant :

$P_n = \{ p_1 ; p_2 ; p_3 ; \ldots . ; p_{m-1} ; p_m \}$.

On va énoncer la supposition suivante :

S : << Il n'y a pas de nombre premier entre p_m et n >>

On a : $p_1 < p_2 < p_3 < \ldots . < p_{m-1} < p_m$ donc $-p_m < -p_{m-1} < \ldots . < -p_3 < -p_2 < -p_1$.

$\Rightarrow\ n-p_m < n-p_{m-1} < \ldots . < n-p_3 < n-p_2 < n-p_1 < n$.

Or p_m divise n et p_m divise p_m donc p_m divise $n-p_m$

$\Rightarrow\ p_m < n-p_m$ ($n-p_m \neq p_m$, $n \neq 2*p_m$ n>>>)

On obtient alors :

$p_1 < p_2 < p_3 < \ldots . < p_m < n-p_m < n-p_{m-1} < \ldots . < n-p_3 < n-p_2 < n-p_1 < n$

d'où $\forall$ i entre 1 et m :

$p_m < n-p_m \leq n-p_i < n$

ou $p_m < n-p_i < n \quad \forall\, p_i \in P_n$,

Donc $n-p_i$ n'est pas premier puisqu'on a supposé qu'il n'y a pas de nombre premier entre p_m et n, il est donc décomposable en facteurs premiers et n'a pas de diviseurs premiers entre p_m et n : c'est une conséquence de S,

En appliquant le théorème fondamental de l'arithmétique à $n-p_i$ alors celui-ci peut s'écrire sous la forme suivante :

$n-p_i = p_1^{a1} * p_2^{a2} * p_3^{a3} *\ldots* p_i^{ai} * \ldots * p_m^{am}$ avec $a_i \in \mathbb{N}$ et i de 1 à m,

Prenons un p_j de P_n qui divise $n-p_i$, comme p_j divise n et p_j divise $n-p_i$ alors p_j divise p_i d'où $p_j = p_i$ ($p_j \in P_n$ donc $\neq$ de 1),

Donc $n-p_i$ va s'écrire sous la forme :

$\mathbf{n-p_i = p_i^{ai} \quad \forall\, p_i \in P_n \Rightarrow n = p_i^{ai} + p_i}$,

On aura alors :

$\mathbf{n = 2^{a1} + 2 = 3^{a2} + 3 = 5^{a3} + 5 = \ldots = p_{m-1}^{am-1} + p_{m-1} = p_m^{am} + p_m}$,

Si on prend par exemple les deux termes suivants :

$5^a + 5 = 11^b + 11$ avec $(a,b) \in \mathbb{N}^2$,

On remarque que le chiffre des unités de 11^b se termine toujours par 1 et si on lui ajoute le chiffre des unités du nombre 11 on aura toujours 2 comme chiffre d'unité du nombre $11^b + 11 \quad \forall\, b \in \mathbb{N}$, or le nombre $5^a + 5$ est un multiple de 5 (avec $a \geq 1$ car pour a=0 , $5^0 + 5 = 6 = 11^b + 11$ n'a pas de solution dans $\mathbb{N}$),

Donc le chiffre des unités du nombre $5^a + 5$ est 0 ou 5 (critère de divisibilité par 5) dans ce cas de $5^a + 5$, c'est 5 différent de 2 de $11^b + 11$,

Alors l'équation $5^a + 5 = 11^b + 11$ n'a pas de solution dans $\mathbb{N}$, autrement dit n n'existe pas,

C'est donc une contradiction car l'entier naturel $n = p_1 * p_2 * p_3 * \ldots * p_m$ existe bel et bien,

Ce qui nous permet de conclure que la supposition S est fausse,

Pour pallier à cette contradiction il doit bien exister au moins un nombre premier p_{m+i} entre p_m et n avec $i \geq 1$ et qui divise au moins un $n-p_i$ car nous avons aussi $p_m < n-p_i < n$) mais ne divise pas n,

Ce que nous traduirons comme ceci :

$\exists\ p_{m+i}\ (i \geq 1)$ nombre premier entre p_m et n et $\exists\ p_k \in P_n$ tel que p_{m+i} divise $n-p_k$ $(p_{m+i} < n-p_k < n)$, ,

$n-p_k$ s'écrira alors de la manière suivante :

$n-p_k = p_k^{ak} * p_{m+i}^{am+i} \Rightarrow n = p_k^{ak} * p_{m+i}^{am+i} + p_k$ avec $a_k \geq 1$ et $a_{m+i} \geq 1$,

c'est-à-dire que nous aurons des $p_i \in P_n$ tel que : $n = p_i^{ai} + p_i$ et nous aurons aussi des $p_j \in P_n$ tel que $n = p_j^{aj} * p_{m+i}^{am+i} + p_j$,

Par la suite, nous allons prendre l'entier naturel n_1 égal à :

$n_1 = p_1 * p_2 * p_3 * \ldots * p_m * p_{m+1}$ avec p_{m+1} le nombre premier successif à p_m,

On voit bien que $n_1 > n$, on va alors appliquer à n_1 le même raisonnement qu'on a appliqué à n, on conclura qu'il existe bel et bien au moins un nombre premier $\mathbf{p_{m+1+i}}$ ($i \geq 1$) tel que :

$P_{m+1} < p_{m+1+i} < n_1$ et p_{m+1+i} divise au moins un $n_1 - p_k$ $(1 \leq k \leq m+1)$

.... et ainsi de suite de façon illimitée pour les p_{m+i} ,

Ce qui montre que le nombre d'entiers premiers est infini,

Conclusion :

L'ensemble P des nombres premiers est infini