

Montrons que pour tout $n \in \mathbb{N}^*$, il existe $m \in \mathbb{N}$ tel que $n/2^m + m$.

Par l'absurde, soit n **minimal** tel que n ne divise aucun des $2^m + m$.

Ecrivons $n = 2^\alpha \cdot N$ avec $\alpha \geq 0$ et N impair.

Comme $2^\alpha/2^{2^\alpha} + 2^\alpha, N \geq 3$.

Soit $\beta =$ ordre de 2 dans $(\mathbb{Z}/N\mathbb{Z})^*$. Alors $\beta < N \leq n$.

Par définition de n , on peut trouver $m \in \mathbb{N}$ pour lequel $n - \beta/2^m + m$.

Si $m < \alpha$, alors $\alpha > 0$ et $2^{\alpha-1} + \alpha - 1 \geq 2^m + m \geq n - \beta = 2^\alpha N - \beta$

d'où $\alpha + \beta - 1 \geq 2^{\alpha-1} \cdot (2N - 1)$

puis $\alpha + N - 1 \geq 2^{\alpha-1} \cdot (2N - 1)$ ce qui est clairement impossible.

Donc $m \geq \alpha$.

Ainsi, pour tout $k \in \mathbb{N}$, $2^{k\beta} = 1 \pmod{N}$ donc $N/2^{k\beta} - 1$ et

$n/2^m \cdot N/2^{m+k\beta} - 2^m$ soit $2^{m+k\beta} = 2^m \pmod{n}$.

Soit alors $\gamma \in \mathbb{N}$ tel que $2^m + m = \gamma(n - \beta)$.

On a $\underline{2^{m+\gamma\beta} + m + \gamma\beta} = 2^m + m + \gamma\beta = \underline{0 \pmod{n}}$ ce qui contredit la définition de n .