Pour tout entier $n \in \mathbb{N}$, on pose

$$F_n = 2^{2^n}.$$

1. *Calculer F_0 et démontrer que*

$$\forall\, n \in \mathbb{N}^*, \quad F_n = 2 + \prod_{k=0}^{n-1} F_k.$$

2. *On suppose que m et n sont deux entiers naturels distincts. Démontrer que*

$$F_m \wedge F_n = 1.$$

3. *En déduire que l'ensemble des nombres premiers est infini.*

1. Il est clair que $F_0 = 2^1 + 1 = 3$ et que $F_1 = 2^2 + 1 = 5$. On a donc

$$F_1 = 2 + F_0.$$

✍ *Par convention, un produit indexé par $0 \leqslant k \leqslant -1$ est égal à 1, donc la relation demandée est vraie aussi pour $n = 0$.*

Supposons que la formule demandée soit vraie pour un entier $n \in \mathbb{N}^*$. Alors

$$F_{n+1} - 1 = 2^{2^{n+1}} = 2^{2.2^n} = (2^{2^n})^2 = (F_n - 1)^2.$$

On en déduit que

$$F_{n+1} = 1 + (F_n - 1)^2 \overset{HR}{=} 1 + \left(1 + \prod_{k=0}^{n-1} F_k\right)^2 = 2 + 2\prod_{k=1}^{n-1} F_k + \left(\prod_{k=0}^{n-1} F_k\right)^2 = 2 + \left(\prod_{k=1}^{n-1} F_k\right)\left(2 + \prod_{k=0}^{n-1} F_k\right)$$

$$\overset{HR}{=} 2 + \left(\prod_{k=0}^{n-1} F_k\right) F_n = 2 + \prod_{k=0}^{n} F_k$$

et la formule est établie par récurrence.

2. Soient $0 \leqslant m < n$. On a donc $0 \leqslant m \leqslant n-1$ et, d'après la question précédente,

$$F_n - \left(\prod_{\substack{0 \leqslant k \leqslant n-1 \\ k \neq m}} F_k\right) F_m = 2.$$

On déduit du Théorème de Bézout que le pgcd $F_m \wedge F_n$ divise 2, alors que ce pgcd est impair.

✍ *La relation de Bézout nous assure que le pgcd $d = a \wedge b$ divise tous les entiers de la forme $au + bv$, quel que soit $(u, v) \in \mathbb{Z}^2$.*

❧ *Les deux entiers F_m et F_n sont impairs, donc aucun des deux n'est divisible par 2 et leur pgcd est donc impair.*

On a donc bien démontré que

$$\forall\, 0 \leqslant m < n, \qquad F_m \wedge F_n = 1.$$

3. On a démontré que $(F_n)_{n\in\mathbb{N}}$ était une famille infinie d'entiers deux à deux premiers entre eux.

❧ Supposons qu'il n'existe qu'un nombre *fini* de nombres premiers : $p_1, \ldots, p_d$. Chaque entier admet une, et une seule, décomposition en produit de facteurs premiers, donc

$$\forall\, n \in \mathbb{N},\ \exists\, (\alpha_{n,1}, \ldots, \alpha_{n,d}) \in \mathbb{N}^d, \qquad n = \prod_{k=1}^{d} p_k^{\alpha_{n,k}}.$$

Si deux entiers m et n sont premiers entre eux, chaque facteur premier p_k apparaît au plus une fois avec une valuation non nulle dans la décomposition de ces deux entiers :

$$\forall\, m \neq n,\ \forall\, 1 \leqslant k \leqslant d, \quad \alpha_{m,k}\alpha_{n,k} = 0.$$

Par conséquent, une famille d'entiers deux à deux premiers entre eux contient au plus d entiers distincts.

❧ On a démontré par l'absurde qu'il existe une infinité de nombres premiers.