DM n°5 : Les nombres de Fermat

On s'intéresse aux *nombres de Fermat*, définis pour tout $n \in \mathbb{N}$ par $F_n = 2^{2^n} + 1$, à ne pas confondre avec $(2^2)^n + 1$ qui vaut $4^n + 1$. Le mathématicien Fermat a conjecturé que chacun de ces nombres était premier. Voyons cela...

1) Calculer F_0, F_1, F_2 et F_3 et vérifier qu'ils sont premiers. Pour F_3, écrire une condition suffisante à vérifier pour s'assurer qu'il soit premier.
2) Écrire une fonction `estPremier` (en Python) qui prend en argument un entier naturel $m \geq 2$ et retourne `True` si m est premier, `False` sinon.

Grâce à `estPremier`, on pourra vérifier (par ordinateur) que F_4 est premier.

3) Vérifier (sans faire de calcul poussé !) que $F_5 = (5^4 + 2^4)2^{28} - \left((2^7 \times 5)^4 - 1\right)$.
4) Soit $a \in \mathbb{N}$ et $m \in \mathbb{N}$. Montrer que a divise $(a-1)^{2m} - 1$.
5) Calculer $5^4 + 2^4$ et $2^7 \times 5$. Déduire des questions précédentes que F_5 n'est pas premier.
6) Montrer que $F(n) = \prod_{k=0}^{n-1} F(k) + 2$.
7) En déduire que pour tous entiers $m, n \in \mathbb{N}$ avec $m \neq n$, les entiers $F(m)$ et $F(n)$ sont premiers entre eux.

C'est Euler qui réfuta de la sorte la conjecture de Fermat. Mais une autre conjecture la remplace : parmi les nombres de Fermat, seuls les nombres de F_0 à F_4 seraient des nombres premiers. Jusqu'à présent, cette conjecture n'a pas été mise en défaut, car on a pu vérifier que les nombres F_5 à F_{32} ne sont pas premiers. La puissance de calcul actuelle est cependant insuffisante pour aller plus loin... En effet $F_{32} \approx 10^{1\,000\,000\,000}$...