DM n°5 : Corrigé

1) $F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$
$F_1 = 2^2 + 1 = 5$
$F_2 = 2^4 + 1 = 17$
$F_3 = 2^8 + 1 = 257$
Il est clair que F_0, F_1 et F_2 sont premiers. Pour F_3, il suffit de vérifier que F_3 n'est divisible par aucun nombre premier p compris entre 2 et $\sqrt{257}$, c'est-à-dire 2, 3, 5, 7, 11 et 13. On peut s'arrêter là car $17^2 = 289$.

2) Il y a plusieurs algorithmes possibles. En voici un assez rapide.

```
def estPremier(m):
    # m sera premier si aucun nombre de 2 à la racine carrée de m ne divise m

    for k in range(2, floor(m**(1/2)) ):
        if m%k==0:  # si k divise m
            return False
    return True
```

3)

$$\begin{aligned}
&(5^4+2^4)2^{28} - \left((2^7\times 5)^4 - 1\right)\\
=&5^4 2^{28} + 2^{32} - 2^{28}5^4 + 1\\
=&2^{32}+1\\
=&F_5
\end{aligned}$$

4)

$$\begin{aligned}
(a-1)^{2m} - 1 &= \left[(a-1)^2\right]^m - 1\\
&= \left(a^2-2a+1\right)^m - 1^m\\
&= (a^2-2a+1-1)\sum_{k=0}^{m-1}(a^2-2a+1)^k 1^{m-1-k}\\
&= (a^2-2a)\sum_{k=0}^{m-1}(a^2-2a+1)^k\\
&= a(a-2)\sum_{k=0}^{m-1}(a^2-2a+1)^k
\end{aligned}$$

Or, $a-2 \in \mathbb{Z}$ et $\displaystyle\sum_{k=0}^{m-1}(a^2-2a+1)^k \in \mathbb{Z}$. On en déduit que $a \mid (a-1)^{2m} - 1$

5) $5^4 + 2^4 = 25\times 25 + 16 = 625 + 16 = 641$
$2^7 \times 5 = 128\times 5 = 640$
Ainsi, $F_5 = 641\times 2^{28} - (640^4 - 1)$. Or, 641 divise 641×2^{28} et d'autre part en posant $a = 641$, on a $(640^4-1) = (a-1)^4 - 1$.

6) On raisonne par récurrence sur $n \in \mathbb{N}$.

- Pour $n = 0$, on a $\displaystyle\prod_{k=0}^{n-1} F(k) + 2 = 1 + 2 = 3$ (un produit vide vaut 1) et par ailleurs $F_0 = 2^1 + 1 = 3$. La propriété est donc vraie pour $n = 0$.
- Hérédité : soit $n \in \mathbb{N}$. On suppose la propriété vraie au rang n. Montrons-là au rang $n+1$.

$$\begin{aligned}
\prod_{k=0}^{n} F(k) + 2 &= F(n) \prod_{k=0}^{n-1} F(k) + 2 \\
&= F(n) \times (F(n) - 2) + 2 \qquad \text{par hypothèse de récurrence} \\
&= F(n)^2 - 2F(n) + 2 \\
&= \left(2^{2^n} + 1\right)^2 - 2\left(2^{2^n} + 1\right) + 2 \\
&= \left(2^{2^n}\right)^2 + 2 \times 2^{2^n} + 1 - 2 \times 2^{2^n} - 2 + 2 \\
&= \left(2^{2^n}\right)^2 + 1 \\
&= 2^{2 \times 2^n} + 1 \\
&= 2^{2^{n+1}} + 1 \\
&= F_{n+1}
\end{aligned}$$

  La propriété est donc vraie au rang $n+1$.
- Ainsi, pour tout $n \in \mathbb{N}$, $F(n) = \displaystyle\prod_{k=0}^{n-1} F(k) + 2$.

7) Soit $m, n \in \mathbb{N}$ des entiers distincts. On pose $d = F(m) \wedge F(n)$. Montrons que $d = 1$. Quitte à échanger m et n, on peut supposer $m < n$. Alors, par ce qui précède, on a

$$F(n) = F(m) \times u + 2 \qquad \text{avec } u = \prod_{\substack{k=0 \\ k \neq m}}^{n-1} F(k)$$

Or, d divise $F(n)$ et $F(m)$ donc divise en particulier $F(n) - F(m) \times u$. Ainsi, $d \mid 2$. Comme $d \geq 0$, il n'y a que deux possibilités : $d = 1$ ou $d = 2$. Or, $F(n) = 2^{2^n} + 1$ est impair car 2^{2^n} est pair. On en déduit que $d = 2$ est impossible. Ainsi, $d = 1$. On en conclut que $F(n)$ et $F(m)$ sont premiers entre eux.