Interrogation 1 : corrigé

Exercice 1

On a :

$$\begin{aligned}\left(\frac{53}{89}\right) &= \left(\frac{89}{53}\right) && \text{car } 89 \equiv 1 \pmod 4\\ &= \left(\frac{36}{53}\right) && \text{car } 89 \equiv 36 \pmod{53}\\ &= \left(\frac{6^2}{53}\right)\\ &= 1.\end{aligned}$$

Exercice 2

Question 1

Si $n \geq 2$, on a

$$\begin{aligned}F_n &= 2^{2^n} + 1\\ &= 2^{4\cdot 2^{n-2}} + 1\\ &= 16^{2^{n-2}} + 1\\ &\equiv 1^{2^{n-2}} + 1 \pmod 5\\ &\equiv 2 \pmod 5.\end{aligned}$$

Question 2

Si $n \geq 2$, on a

$$\begin{aligned}\left(\frac{F_n}{5}\right) &= \left(\frac{2}{5}\right) && \text{car } F_n \equiv 2 \pmod 5\\ &= -1 && \text{car } 5 \equiv -1 \pmod 8.\end{aligned}$$

Pour $n = 0$, on a $F_0 = 2^{2^0} + 1 = 3$, donc $\left(\frac{F_0}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{-2}{5}\right) = -1$.

Pour $n = 1$, on a $F_1 = 2^{2^1} + 1 = 5$, donc $\left(\frac{F_1}{5}\right) = \left(\frac{5}{5}\right) = 0$.

Comme F_n est impair et $5 \equiv 1 \pmod 4$, on a $\left(\frac{F_n}{5}\right) = \left(\frac{5}{F_n}\right)$ pour tout $n \in \mathbb{N}$, donc $\left(\frac{5}{F_n}\right) = \begin{cases}0 \text{ si } n = 1\\ -1 \text{ sinon.}\end{cases}$

Question 3

Si F_n est premier, on a $5^{2^{2^n-1}} = 5^{\frac{F_n-1}{2}} \equiv \begin{cases}0 & \text{si } F_n \mid 5\\ 1 & \text{si } F_n \nmid 5 \text{ et 5 est un carré modulo } F_n\\ -1 & \text{si 5 n'est pas un carré modulo } F_n\end{cases} \pmod{F_n}$,

donc $5^{2^{2^n-1}} \equiv \left(\frac{5}{F_n}\right) \pmod{F_n}$, et en particulier $5^{2^{2^n-1}} \equiv -1 \pmod{F_n}$ si $n \neq 1$, d'après la question 2.

Question 4

On a $5^{2^{2^n-1}} \equiv -1 \pmod{F_n}$ et $p \mid F_n$, par hypothèse, donc $5^{2^{2^n-1}} \equiv -1 \pmod{p}$, donc $5^{2^{2^n}} \equiv \left(5^{2^{2^n-1}}\right)^2 \equiv (-1)^2 \equiv 1 \pmod{p}$, donc $e \mid 2^{2^n}$. Or on a $5^{2^{2^n-1}} \not\equiv 1 \pmod{p}$, donc $e \nmid 2^{2^n-1}$.

Question 5

D'après la question 4, on a $e \mid 2^{2^n}$ et $e \nmid 2^{2^n-1}$. Comme $e \mid 2^{2^n}$, l'entier e est une puissance de 2, et plus précisément $e = 2^k$ pour un entier $k \in \{0,1,\dots,2^n\}$. Comme $e \nmid 2^{2^n-1}$, on a $k > 2^n - 1$, donc $k = 2^n$, donc $e = 2^{2^n}$.

Question 6

Comme e est l'ordre d'un élément du groupe $\mathbb{F}_p^\times$, et $\left|\mathbb{F}_p^\times\right| = p - 1$, on a $e \mid (p-1)$, donc $2^{2^n} \mid (p-1)$. Comme p est premier, on a $p - 1 \geq 1$, or $2^{2^n} \mid (p-1)$, donc $p - 1 \geq 2^{2^n}$, donc $p \geq 2^{2^n} + 1 = F_n$.

Question 7

Si F_n est premier, alors $n = 1$ ou $5^{2^{2^n-1}} \equiv -1 \pmod{F_n}$ d'après la question 3.

Si $n = 1$, alors $F_n = 5$ donc F_n est premier.

Si $5^{2^{2^n-1}} \equiv -1 \pmod{F_n}$, soit p un diviseur premier de F_n, alors :

- $p \leq F_n$ car $p \mid F_n$,
- $p \geq F_n$ d'après la question 6,

donc $p = F_n$, donc F_n est premier.

Donc F_n est premier si et seulement si $n = 1$ ou $5^{2^{2^n-1}} \equiv -1 \pmod{F_n}$.