DEVOIR À LA MAISON N°09

- Le devoir devra être rédigé sur des copies *doubles*.
- Les copies ne devront comporter ni rature, ni renvoi, ni trace d'effaceur.
- Toute copie ne satisfaisant pas à ces exigences devra être intégralement récrite.

Exercice 1 ★★

Soient m et n des entiers naturels non nuls. On pose $\mathrm{G} = \left\{z_1z_2, (z_1, z_2) \in \mathbb{U}_m \times \mathbb{U}_n\right\}$.

1. *Dans cette question uniquement*, on pose $m = 4$ et $n = 6$. Déterminer les éléments et le cardinal de $\mathbb{U}_m$, $\mathbb{U}_n$, $\mathbb{U}_m \cap \mathbb{U}_n$ et G.
2. Montrer que $\mathbb{U}_{m \wedge n} \subset \mathbb{U}_m \cap \mathbb{U}_n$.
3. A l'aide d'une relation de Bézout entre m et n, montrer que $\mathbb{U}_m \cap \mathbb{U}_n \subset \mathbb{U}_{m \wedge n}$.
4. Montrer que $\mathrm{G} \subset \mathbb{U}_{m \vee n}$.
5. A l'aide d'une relation de Bézout entre m et n, montrer que $\mathbb{U}_{m \vee n} \subset \mathrm{G}$.

Exercice 2 ★★ **Nombres de Fermat**

1. Soient a un entier strictement supérieur à 1 et n un entier naturel non nul. On suppose que $a^n + 1$ est un nombre premier.
   a. Montrer que a est pair.
   b. Soit m un diviseur impair positif de n. Il existe alors $k \in \mathbb{N}^*$ tel que $n = km$. Montrer que $a^k + 1$ divise $a^n + 1$ puis que $m = 1$.
   c. Que peut-on en déduire sur n ?

2. On pose pour $n \in \mathbb{N}$, $\mathrm{F}_n = 2^{2^n} + 1$.
   a. Montrer que pour tout $n \in \mathbb{N}$, $\mathrm{F}_{n+1} = (\mathrm{F}_n - 1)^2 + 1$.
   b. Montrer que pour tout $n \in \mathbb{N}^*$, $\mathrm{F}_n - 2 = \prod_{k=0}^{n-1} \mathrm{F}_k$.
   c. Soit $(m, n) \in \mathbb{N}^2$ tel que $m < n$. Montrer que $\mathrm{F}_m \wedge \mathrm{F}_n = 1$.

3. Soient $n \in \mathbb{N}$ et p un nombre premier divisant F_n. On considère l'ensemble

$$\mathrm{A} = \left\{k \in \mathbb{N}^*,\ 2^k \equiv 1[p]\right\}$$

   a. Montrer que $2^{n+1} \in \mathrm{A}$.
   b. Justifier que A admet un minimum que l'on notera m.
   c. En écrivant la division euclidienne de 2^{n+1} par m, montrer que m divise 2^{n+1}.
   d. Montrer que $m = 2^{n+1}$.
   e. Justifier que $p - 1 \in \mathrm{A}$.
   f. En déduire que $p \equiv 1 \left[2^{n+1}\right]$.