Devoir à la maison n°09 : corrigé

Solution 1

1.

$$\begin{aligned}\mathbb{U}_4 &= \{1, i, -1, -i\}\\ \mathbb{U}_6 &= \left\{1, e^{\frac{i\pi}{3}}, e^{\frac{2i\pi}{3}}, -1, e^{\frac{4i\pi}{3}}, e^{\frac{5i\pi}{3}}\right\}\\ \mathbb{U}_4 \cap \mathbb{U}_6 &= \{-1, 1\} = \mathbb{U}_2\\ \mathrm{G} &= \left\{1, e^{\frac{i\pi}{6}}, e^{\frac{i\pi}{3}}, i, e^{\frac{2i\pi}{3}}, e^{\frac{5i\pi}{6}}, -1, e^{\frac{7i\pi}{6}}, e^{\frac{4i\pi}{3}}, -i, e^{\frac{5i\pi}{3}}, e^{\frac{11i\pi}{6}}\right\} = \mathbb{U}_{12}\end{aligned}$$

Ainsi $\operatorname{card} \mathbb{U}_4 = 4$, $\operatorname{card} \mathbb{U}_6 = 6$, $\operatorname{card} \mathbb{U}_4 \cap \mathbb{U}_6 = 2$ et $\operatorname{card} \mathrm{G} = 12$.

2. Soit $z \in \mathbb{U}_{m\wedge n}$. On a donc $z^{m\wedge n} = 1$. Puisque m et n sont des multiples de $m \wedge n$, on a également $z^m = 1$ et $z^n = 1$. Donc $z \in \mathbb{U}_m \cap \mathbb{U}_n$. Ainsi $\mathbb{U}_{m\wedge n} \subset \mathbb{U}_m \cap \mathbb{U}_n$.

3. Soit $z \in \mathbb{U}_m \cap \mathbb{U}_n$. On a donc $z^m = 1$ et $z^m = 1$. D'après le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $mu + nv = m \wedge n$. Ainsi $z^{m\wedge n} = (z^m)^u (z^n)^v = 1$ et $z \in \mathbb{U}_{m\wedge n}$. Ainsi $\mathbb{U}_m \cap \mathbb{U}_n \subset \mathbb{U}_{m\wedge n}$.

4. Soit $z \in \mathrm{G}$. Il existe donc $z_1 \in \mathbb{U}_m$ et $z_2 \in \mathbb{U}_n$ tels que $z = z_1 z_2$. Dans ce cas, $z^{m\vee n} = z_1^{m\vee n} z_2^{m\vee n}$. Mais comme $m \vee n$ est un multiple de m, $z_1^{m\vee n} = 1$. De même, $m \vee n$ étant un multiple de n, $z_2^{m\vee n} = 1$. Ainsi $z^{m\vee n} = 1$ et $z \in \mathbb{U}_{m\vee n}$. Ainsi $\mathrm{G} \subset \mathbb{U}_{m\vee n}$.

5. Soit $z \in \mathbb{U}_{m\vee n}$. Par le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $um + vn = m \wedge n$. Posons $m' = \frac{m}{m\wedge n}$ et $n' = \frac{n}{m\wedge n}$. Remarquons que m' et n' sont entiers. On peut alors poser $z_1 = z^{vn'}$ et $z_2 = z^{um'}$. On a bien $z = z_1 z_2$ puisque $um' + vn' = 1$. De plus, $\frac{mn}{m\wedge n} = m \vee n$ donc $z_1^m = z^{v(m\vee n)} = 1$ et $z_2^n = z^{u(p\vee n)} = 1$. Ainsi $z = z_1 z_2$ avec $z_1 \in \mathbb{U}_m$ et $z_2 \in \mathbb{U}_n$. Donc $z \in \mathrm{G}$. Ainsi $\mathbb{U}_{m\vee n} \subset \mathrm{G}$.

Solution 2

1. **a.** Puisque $a > 1$ et $n > 0$, $a^n + 1 > 2$. Puisque $a^n + 1$ est premier et distinct de 2, il est impair. Ainsi a^n est pair et donc a est pair.

   b. On a $a^k \equiv -1\left[a^k + 1\right]$, puis $(a^k)^m \equiv -1\left[a^k + 1\right]$. Puisque m est impair, $a^{km} \equiv -1\left[a^k + 1\right]$ i.e. $a^n + 1 \equiv 0\left[a^k + 1\right]$. Ainsi $a^k + 1$ divise $a^n + 1$.
   Puisque $a^n + 1$ est premier, on en déduit que $a^k + 1 = 1$, ce qui est exclu car $a \neq 0$, ou $a^k + 1 = a^n + 1$. Puisque $a > 1$, on obtient $k = n$ et donc $m = 1$.

   c. On déduit de la question précédente que n n'admet pas de diviseur premier impair. Le seul diviseur premier de n est donc 2. Le théorème de décomposition en facteurs premiers assure alors que n est une puissance de 2.

2. **a.** Soit $n \in \mathbb{N}$.
$$\mathrm{F}_{n+1} - 1 = 2^{2^{n+1}} = \left(2^{2^n}\right)^2 = (\mathrm{F}_n - 1)^2$$

   b. On raisonne par récurrence. On a bien $\mathrm{F}_1 - 2 = 3 = \mathrm{F}_0$. Supposons qu'il existe $n \in \mathbb{N}^*$ tel que $\mathrm{F}_{n+1} = (\mathrm{F}_n - 1)^2 + 1$. Alors, d'après la question précédente
$$\mathrm{F}_{n+1} - 2 = (\mathrm{F}_n - 1)^2 - 1 = \mathrm{F}_n(\mathrm{F}_n - 2) = \mathrm{F}_n \prod_{k=0}^{n-1} \mathrm{F}_k = \prod_{k=0}^{n} \mathrm{F}_k$$
   Par récurrence, $\mathrm{F}_n - 2 = \prod_{k=0}^{n-1} \mathrm{F}_k$ pour tout $n \in \mathbb{N}^*$.

   c. On a $n \in \mathbb{N}^*$ et on peut appliquer la question précédente. Ainsi $\mathrm{F}_n - 2 = \prod_{k=0}^{n-1} \mathrm{F}_k$ ou encore $\mathrm{F}_n - \prod_{k=0}^{n-1} \mathrm{F}_k = 2$. D'une part, $\mathrm{F}_m \wedge \mathrm{F}_n$ divise F_n et, d'autre part, $\mathrm{F}_m \wedge \mathrm{F}_n$ divise F_m donc $\prod_{k=0}^{n-1} \mathrm{F}_k$ puisque $m < n$. Ainsi $\mathrm{F}_m \wedge \mathrm{F}_n$ divise 2. Par ailleurs, F_n est impair donc $\mathrm{F}_m \wedge \mathrm{F}_n = 1$.

3. **a.** Puisque p divise F_n, $2^{2^n} \equiv -1[p]$. En élevant au carré, $2^{2^{n+1}} \equiv 1[p]$ donc $2^{n+1} \in \mathrm{A}$.

b. A est une partie non vide (d'après la question précédente) de $\mathbb{N}^*$: elle admet donc un minimum.

c. Notons q et r le quotient et le reste de la division euclidienne de 2^{n+1} par m. On a donc $2^{n+1} = qm + r$ avec $0 \leq r < m$. De plus, $q \in \mathbb{N}$ puisque 2^{n+1} et m sont positifs. Ainsi $2^{2^{n+1}} = (2^m)^q \cdot 2^r$. Or $m \in \mathrm{A}$ donc $2^m \equiv 1[p]$ puis $(2^m)^q \equiv 1[p]$. Finalement $2^{2^{n+1}} \equiv 2^r[p]$. Or $2^{n+1} \in \mathrm{A}$ donc $2^r \equiv 1[p]$. Si on avait $r > 0$, on aurait $r \in \mathrm{A}$ et $r < m$, ce qui est impossible car $m = \min \mathrm{A}$. Ainsi $r = 0$ de sorte que m divise 2^{n+1}.

d. Il s'ensuit que m est une puissance de 2. Il existe donc un entier naturel $q \leq n+1$ tel que $m = 2^q$. Supposons $q \leq n$. Puisque $2^{2^q} \equiv 1[p]$, on obtient en élevant à la puissance 2^{n-q}, $2^{2^n} \equiv 1[p]$. Or p divise F_n donc $2^{2^n} \equiv -1[p]$. Ainsi $2 \equiv 0[p]$ i.e. p divise 2. Puisque p est premier, on aurait $p = 2$, ce qui est impossible car F_n est impair.

e. Puisque F_n est impair, $p \neq 2$ et donc p est impair. En particulier, 2 est premier avec p. D'après le petit théorème de Fermat, $2^{p-1} \equiv 1[p]$ et $p - 1 \in \mathrm{A}$.

f. En écrivant à nouveau la division euclidienne de $p-1$ par m, la minimalité de m montre que m divise $p-1$ i.e. $p \equiv 1[m]$. Puisque $m = 2^{n+1}$, $p \equiv 1\left[2^{n+1}\right]$.