Feuille d'exercices 11: Corrigé de deux exercices.

Exercice 11.12 :

1°) Il existe $(n,m) \in \mathbb{N}^{*2}$ tel que $x^n = 0$ et $y^m = 0$.

- x et y commutent, donc $(xy)^n = x^n y^n = 0$. Ainsi xy est nilpotent.
- x et y commutent, donc on peut appliquer la formule du binôme de Newton.

Ainsi $(x+y)^{n+m-1} = \displaystyle\sum_{k=0}^{n+m-1} \binom{n+m-1}{k} x^k y^{n+m-1-k}$.

Soit $k \in \{0, \dots, n+m-1\}$.

$\diamond$ Si $k \geq n$, alors $x^k = x^n x^{k-n} = 0$, donc $\binom{n+m-1}{k} x^k y^{n+m-1-k} = 0$.

$\diamond$ Sinon, $k < n$ et $n+m-1-k > m-1$, donc $y^{n+m-1-k} = 0$ et on a encore $\binom{n+m-1}{k} x^k y^{n+m-1-k} = 0$.

Ainsi $(x+y)^{n+m-1} = 0$, ce qui prouve que $x+y$ est nilpotent.

2°) **a)** Soit $x \in \mathbb{Z}/n\mathbb{Z}$. Il existe $a \in \mathbb{Z}$ tel que $x = \overline{a}$.
Supposons que x est nilpotent. Alors il existe $m \in \mathbb{N}^*$ tel que $x^m = 0$. Ainsi, $n \mid a^m$.
Pour tout $i \in \mathbb{N}_k$, $p_i \mid n$, donc $p_i \mid a^m$. Ceci impose que le nombre premier p_i est présent dans la décomposition primaire de a^m, donc c'est aussi le cas pour la décomposition primaire de a. Ainsi, p_i divise a, pour tout $i \in \mathbb{N}_k$. Or pour $i, j \in \mathbb{N}_k$ avec $i \neq j$, p_i et p_j sont premiers entre eux, donc d'après le cours d'arithmétique, a est un multiple de $p = \displaystyle\prod_{i=1}^{k} p_i$. Réciproquement, supposons que p divise a. Posons $\alpha = \max_{1 \leq i \leq k} \alpha_i$. Alors p^α divise a^α, mais n divise p^α, donc $x^\alpha = 0$ et x est nilpotent.
En conclusion, on a montré que l'ensemble des éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ est $\overline{p}(\mathbb{Z}/n\mathbb{Z})$. Il s'agit de l'idéal engendré par $\overline{p}$.

b) On note encore $n = \displaystyle\prod_{i=1}^{k} p_i^{\alpha_i}$ la décomposition en facteurs premiers de n.

- Supposons que $k \geq 2$. Alors $\overline{p}_1$ n'est pas nilpotent. Cependant, p_1 et n ne sont pas premiers entre eux, donc $\overline{p}_1$ est un diviseur de 0.

En passant à la contraposée, on a montré que, si tout diviseur de 0 est nilpotent, k est égal à 1.

• Réciproquement, supposons que $k = 1$. Soit $a \in \mathbb{Z}$ tel que $\overline{a}$ est un diviseur de 0. a et $n = p_1^{\alpha_1}$ ne sont pas premier entre eux, donc p_1 divise a. Ainsi, a^{α_1} est un multiple de n, ce qui prouve que $\overline{a}$ est nilpotent.
En conclusion, la condition nécessaire et suffisante cherchée est que n soit une puissance d'un nombre premier.

Exercice 11.13 :

Notons $n = \prod_{i=1}^{k} p_i^{v_i}$ la décomposition de n en produit de nombres premiers. Ainsi, pour tout $i \in \mathbb{N}_k$, $p_i \in \mathbb{P}$ et $v_i \in \mathbb{N}^*$. On sait que $\varphi(n) = \prod_{i=1}^{k}(p_i^{v_i} - p_i^{v_i-1})$.
Supposons que $\varphi(n) \mid n$. Ainsi, il existe $d \in \mathbb{N}^*$ tel que $n = d\varphi(n)$. Alors, en simplifiant par $\prod_{i=1}^{k} p_i^{v_i-1}$, on obtient que (1) : $\prod_{i=1}^{k} p_i = d\prod_{i=1}^{k}(p_i - 1)$.
Si $n = 1$, alors $\varphi(n) = 1$ et n convient.
Supposons maintenant que $n \geq 2$. Alors $k \geq 1$.
Si 2 ne divise pas n, alors pour tout $i \in \mathbb{N}_k$, p_i est impair, donc $\prod_{i=1}^{k}(p_i - 1)$ est pair alors que $\prod_{i=1}^{k} p_i$ est impair. La relation (1) est alors fausse, donc n n'est pas solution.
Ainsi, 2 intervient dans la décomposition de n en produit de nombres premiers. Cette dernière peut donc s'écrire $n = 2^v \prod_{i=1}^{k-1} p_i^{v_i}$, où pour tout $i \in \mathbb{N}_{k-1}$, p_i est un nombre premier impair. (1) devient alors $2\prod_{i=1}^{k-1} p_i = d\prod_{i=1}^{k-1}(p_i - 1)$.
Si $k \geq 3$, alors $d\prod_{i=1}^{k-1}(p_i - 1)$ est un multiple de 4, ce qui n'est pas le cas de $2\prod_{i=1}^{k-1} p_i$, donc n n'est pas solution. Supposons maintenant que $k \leq 2$.
Si $k = 1$, alors $n = 2^v$ et $\varphi(n) = 2^{v-1}$ divise bien n.
Supposons enfin que $k = 2$. Alors $n = 2^v p_1^{k_1}$. Alors (1) devient : $2p_1 = d(p_1 - 1)$. Ainsi, $(p_1 - 1) \mid 2p_1$, or $p_1 - (p_1 - 1) = 1$, donc d'après l'identité de Bezout, $p_1 \wedge (p_1 - 1) = 1$. Alors, d'après le lemme de Gauss, $(p_1 - 1) \mid 2$, or $p_1 - 1 \geq 2$, donc $p_1 - 1 = 2$, puis $p_1 = 3$.
Alors $n = 2^v 3^{k_1}$ avec $k_1 \geq 1$. On vérifie dans ce cas que $\varphi(n) = 2^{v-1}3^{k_1}(1 - \frac{1}{3}) = 2^v 3^{k_1-1}$ divise n.
En conclusion, n est un multiple de $\varphi(n)$ si et seulement si il est de la forme $2^v 3^w$ avec $v, w \in \mathbb{N}$ et $v \neq 0$ lorsque $w \geq 1$.