1. Si m divise n, alors il existe un entier $q \in \mathbb{N}^*$ tel que

$$n = q.m$$

et par conséquent

$$X^n - 1 = X^{qm} - 1 = (X^m - 1)(X^{(q-1)m} + \cdots + X^m + 1)$$

donc $(X^m - 1)$ divise $(X^n - 1)$.

✍ *Une expresion de la forme*

$$X^n - 1 = X^n - 1^n$$

doit impérativement faire penser à la formule de la somme géométrique :

$$a^n - b^n = (a - b) \cdot \left(\sum_{k=0}^{n-1} a^k b^{n-k} \right)$$

qui est vraie dans tout anneau pourvu que a et b commutent.

2. Réciproquement, si $(X^m - 1)$ divise $(X^n - 1)$, alors toute racine m-ième de l'unité est aussi une racine n-ième de l'unité et en particulier

$$\left(\exp \frac{2i\pi}{m} \right)^n = 1$$

c'est-à-dire

$$\exp \frac{2imn\pi}{n} = 1$$

donc $2imn\pi/n$ est un multiple entier de $2i\pi$. Autrement dit, n divise m !

✍ *On doit savoir que l'application*

$$\left[t \mapsto e^{it} \right]$$

est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$ et que le noyau de ce morphisme est le sous-groupe discret $2\pi\mathbb{Z}$.