Exercice 1 Mines Telecom 2019 : Autre méthode : s'intéresser aux racines (racine de l'unité, qui sont toutes simples...)

Soit $n, m \in \mathbb{N}^*$ tel que $n < m$

($\Leftarrow$) Si $n \mid m$ alors on a $q \in \mathbb{N}^*$ tel que $m = nq$

d'où $X^m - 1 = X^{nq} - 1 = (X^n)^q - 1^q$

$= (X^n - 1)\underbrace{(X^{n(q-1)} + \dots + X^n + 1)}_{\in \mathbb{R}[X]}$

Ainsi $X^n - 1$ divise $X^m - 1$ ✓

($\Rightarrow$) Si $X^n - 1$ divise $X^m - 1$

alors on a $Q \in \mathbb{R}[X]$ avec $0 \leqslant \deg Q < m$

tel que $X^m - 1 = (X^n - 1)Q$ ✓

On écrit la division euclidienne de m par n.

$m = nq + r$ avec $q \in \mathbb{N}^*$ et $0 \leqslant r < n$

D'où $X^m - 1 = X^{nq+r} - 1$

$= X^r(X^{nq} - 1) + X^r - 1$ ✓

d'où $X^r(X^{nq} - 1) + X^r - 1 = (X^n - 1)Q$

et $(X^n - 1)X^r(X^{n(q-1)} + \dots + X^n + 1) + X^r - 1 = (X^n - 1)Q$

Par unicité des coefficients polynomiaux : Non c'est l'unicité de la division euclidienne.

$Q = X^r(X^{n(q-1)} + \dots + X^n + 1)$ et $X^r - 1 = 0$

d'où $X^r = 1$ donc $r = 0$

donc $m = nq$ et $n \mid m$ ✓

Ainsi $\boxed{X^n - 1 \mid X^m - 1 \iff n \mid m}$ ✓