1) On a $\phi_{p^r m}(X) = \dfrac{\phi_m(X^{p^r})}{\phi_m(X^{p^{r-1}})}$ si p ne divise pas m.

2) Soit p un nombre premier divisant n. On a alors $n = p^r m$ avec p ne divisant pas m et $m \geq 2$. Il suit que $\phi_m(0)$ et $\phi_m(1) \neq 0$ (car 0 et 1 ne sont pas des racines primitives m-ièmes de l'unité si $m \geq 2$).

En remplaçant dans la formule ci-dessus X par 0 ou 1, on voit que $\phi_n(a) = \phi_{p^r m}(a) = 1$ si $a = 0$ ou 1.

Si $m = 1$, alors $n = p^r$ et n n'a qu'un diviseur premier p. On a alors $\phi_{p^r}(0) = 1$

3) On a $n = p_1 p_2 ... p_k$ avec les p_i premiers et deux à deux distincts. On écrit $n = p_k m$ avec $m = p_1 ... p_{k-1}$.

Si $k = 1$, alors $\phi_n(X) = X^{p_1 - 1} + ... + X + 1$. On a donc $\phi_n^{'}(0) = 1$

Si $k \geq 2$, la formule rappelée en 1) implique $\phi_n(X) = \dfrac{\phi_m(X^{p_k})}{\phi_m(X)}$.

En dérivant, on obtient : $\phi_n^{'}(0) = \dfrac{-\phi_m(0)\phi_m^{'}(0)}{\phi_m(0)^2} = -\phi_m^{'}(0)$ car la dérivée de $\phi_m(X^{p_k})$ s'annule en 0. Une récurrence immédiate sur k donne $\phi_n^{'}(0) = (-1)^{k-1}$.

Supposons maintenant que n a un facteur carré d^2. Alors $n = p^r m$ pour un certain premier p (diviseur de d) avec $r \geq 2$ et p ne divise pas m. On dérive de nouveau l'expression donnée en 1) pour obtenir $\phi_n^{'}(0) = 0$.