6.13 La division euclidienne de k par α implique l'existence d'un quotient q et d'un reste r tels que $k = \alpha\, q + r$ avec $0 \leqslant r < \alpha$.

$1 \equiv a^k \equiv a^{\alpha\, q+r} \equiv (a^\alpha)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \mod m$

Puisque $0 \leqslant r < \alpha$ et que α est, par définition, le plus petit entier positif tel que $a^\alpha \equiv 1 \mod m$, il en résulte que $r = 0$.

Dès lors $k = \alpha\, q$, c'est-à-dire que α divise k.