5.11 1) (a) Si a est un multiple de p, alors p divise a et p^k : $1 < p \leqslant \mathrm{pgcd}(a, p^k)$, si bien que a et p^k ne sont pas premiers entre eux.

(b) Supposons que a et p^k ne soient pas premiers entre eux.
Posons $d = \mathrm{pgcd}(a, p^k) > 1$.

Il existe un entier q tel que $a = d\,q$.

D'après l'exercice 4.11, tout diviseur de p^k est de la forme p^β avec $0 \leqslant \beta \leqslant k$. Donc, $d = p^\beta$ avec $1 \leqslant \beta \leqslant k$.

On conclut que $a = d\,q = p^\beta\,q$ est un multiple de p.

2) Déterminer le nombre d'éléments de l'ensemble

$$\{a \in \mathbb{Z} : 1 \leqslant a \leqslant p^k \text{ et } \mathrm{pgcd}(a, p^k) \neq 1\}$$

revient à compter le nombre de multiples de p compris entre 1 et p^k.
Il s'agit des entiers suivants : $1 \cdot p\,, 2 \cdot p\,, 3 \cdot p\,, \ldots\,, p^{k-1} \cdot p$.
Il y en a par conséquent p^{k-1}.

3) $\varphi(p^k)$ est le nombre d'éléments de l'ensemble

$$\{a \in \mathbb{Z} : 1 \leqslant a \leqslant p^k \text{ et } \mathrm{pgcd}(a, p^k) = 1\}$$

Attendu que l'ensemble $\{a \in \mathbb{Z} : 1 \leqslant a \leqslant p^k\}$ contient p^k éléments et que l'ensemble $\{a \in \mathbb{Z} : 1 \leqslant a \leqslant p^k \text{ et } \mathrm{pgcd}(a, p^k) \neq 1\}$ contient p^{k-1} éléments, on conclut que

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \tfrac{1}{p}\right)$$