A Careful Pf of:

If G is a finite cyclic group and $d \mid |G|$ then $\exists$ exactly $\varphi(d)$ elements of order d in G

Pf/ Let a be a generator G; we want k s.t $\operatorname{ord}(a^k) = d$. $\therefore$

$$d = \frac{|G|}{\gcd(|G|, k)}$$

which is equivalent to

$$(\dagger) \quad \gcd\left(d, \frac{kd}{|G|}\right) = 1$$

Consider the function

$$\{k \mid \operatorname{ord}(a^k) = d\} \longrightarrow \{x \in [d] \mid \gcd(x,d) = 1\}$$

$$k \longrightarrow x = \frac{kd}{|G|}$$

First let's prove that $\frac{kd}{|G|}$ lies in $[d]$.

We know that $\frac{kd}{|G|}$ is an integer if $\operatorname{ord}(a^k) = d$ from the derivation of $(\dagger)$. Since $k \leq |G|$ $\frac{kd}{|G|} \leq d$. The derivation of $(\dagger)$ also guarantees that $\gcd(x,d) = 1$. The function is clearly 1-1.

Next we prove ontoness. Consider x s.t $\gcd(x,d) = 1$ and the equation

$$\frac{kd}{|G|} = x$$

Thus $$k = \frac{|G| x}{d}$$

is an integer and since the derivation of (+) is an iff derivation, it follows that

$$d = \frac{|G|}{\gcd(|G|, k)} = \operatorname{ord}(a^k)$$

$\therefore$ the function is onto.

Of course

$$|\{k \mid \operatorname{ord}(a^k) = d\}| = |\{x \in [d] \mid g(x, d) = 1\}|$$
$$= \varphi(d)$$