Exercício 1 (Capítulo 6, exercício 23)**.** Mostre que $n = \sum_{d|n} \phi(d)$, para todo $n \in \mathbb{N} = \{1, 2, \cdots\}$.

Solução:

Seja G um grupo cíclico de ordem n gerado por g. Sabemos que dado d um divisor de n, existe $g^k \in G$ tal que $|g^k| = d$. Assim, podemos escrever

$$G = \bigcup_{d|n} \{\text{elementos de ordem } d\},$$

onde a união é disjunta. Logo $n = |G| = \sum_{d|n} \#\{\text{elementos de ordem } d\}$. Lembre-se de que

$$\begin{aligned} \phi : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \#\{m \leq n \mid \text{mdc}(m, n) = 1\} \end{aligned}$$

Assim, dado $d \mid n$, vamos mostrar que $\#\{\text{elementos de ordem } d\} = \phi(d)$. Note que o único elemento de ordem 1 em G é a identidade, logo $\phi(1) = 1 = \#\{\text{elementos de ordem } 1\}$. Seja $d \neq 1$ um divisor de G, isto é, $n = d\ell$. Sabemos que g^k, com $1 \leq k \leq n$, tem ordem d, se e somente se, $\frac{n}{\text{mdc}(k,n)} = d$, ou seja, se e somente se $\text{mdc}(k, n) = \frac{n}{d} = \ell$. Isso equivale a $\text{mdc}(\frac{k}{\ell}, \frac{n}{\ell}) = 1$. Como $\frac{n}{\ell} = d$ e denotando $K = \frac{k}{\ell}$. Dessa forma, g^k em G tem ordem d, se e somente se $\text{mdc}(K, d) = 1$, onde $1 \leq K \leq d$, já que $1 \leq k \leq n$. Portanto, a quantidade de elementos em G que têm ordem d é a quantidade de k tais que $|g^k| = d$, o que equivale a quantidade de K tais que $\text{mdc}(K, d) = 1$. Isso significa que $\#\{\text{elementos de ordem } d\} = \phi(d)$. ⊠