Problema 58. Classifiqueu els grups abelians donats pels grups multiplicatius $(\mathbb{Z}/p\mathbb{Z})^*$, on p és un nombre primer ≤ 20.

Observació 1. Sigui $n \in \mathbb{N}$, direm que $g \in Z/n\mathbb{Z}$ és una arrel primitiva mòdul n si l'ordre de g en el grup multiplicatiu $(\mathbb{Z}/n\mathbb{Z})^*$ és $\varphi(n)$; és a dir, g és arrel multiplicativa si, i només si, és generador de $(\mathbb{Z}/n\mathbb{Z})^*$.

Observació 2. Sigui $n \in \mathbb{N} \setminus \{0\}$. $\mathbb{Z}/n\mathbb{Z}$ té arrels primitives si, i només si, $n = 2, 4, p^v$ o $2p^v$, amb p primer natural senar i $v \in \mathbb{N} \setminus \{0\}$.

Solució. Veiem que $\forall p \in \mathbb{N}$ primer, $\mathbb{Z}/p\mathbb{Z}$ té arrels primitives. Si existeix una arrel primitiva vol dir que el grup és cíclic (és generat per aquesta arrel). Queden classificats els grups: $(\mathbb{Z}/p\mathbb{Z})^*$ és cíclic d'ordre $\varphi(p) = p - 1$, $\forall p \leq 20$ primer (de fet, $\forall p$ primer).