Problema 10. Siguin p, q nombres primers diferents i $r, s \geq 1$ nombres enters.

a) Determineu quants elements del grup $\mathbb{Z}/p\mathbb{Z}$ el generen.

b) Determineu quants elements del grup $\mathbb{Z}/p^r\mathbb{Z}$ el generen.

c) Determineu quants elements del grup $\mathbb{Z}/p^r q^s\mathbb{Z}$ el generen.

Observació 1. Sigui $n \in \mathbb{N}$. Considerem el grup $\mathbb{Z}/n\mathbb{Z}$ amb la suma. Anem a calcular el número d'elements generadors d'aquest grup.

Sabem que $\forall \overline{z} \in \mathbb{Z}/n\mathbb{Z}$, z representant natural mínim de la classe d'equivalència, el número d'elements del subgrup generat per aquest $\overline{z}$ és:

$$\# < \overline{z} >= \frac{mcm(z,n)}{z}.$$

En efecte, $< \overline{z} >= \{\overline{z}, 2\overline{z}, ..., k\overline{z} = \overline{n}\}$, ja que $(k+1)\overline{z} = k\overline{z} + \overline{z} = \overline{n} + \overline{z} = \overline{z}$. Per tant, el número d'elements d'aquest conjunt és un $k \in \mathbb{N}$ tal que $k\overline{z} = \overline{n}$. Aquest k és mínim, és a dir:

$$k = \# < \overline{z} >= \frac{mcm(z,n)}{z}.$$

Ara, per resultats obtinguts a Aritmètica, sabem que

$$mcd(z,n) \cdot mcm(z,n) = zn.$$

Per tant:

$$\# < \overline{z} >= \frac{mcm(z,n)}{z} = \frac{n}{mcd(z,n)}.$$

En definitiva, $\# < \overline{z} >= n$ i, en conseqüència, z és generador de $\mathbb{Z}/n\mathbb{Z}$ si, i només si, $mcd(z,n) = 1$.

Considerem ara un generador $\overline{z}$ de $\mathbb{Z}/n\mathbb{Z}$ (en particular existeix, ja que $\forall n \in \mathbb{N} \setminus \{0\}$ 1 és generador). Sigui $k \in \mathbb{N}$. Aleshores,

$$\# < k\overline{z} >= \frac{n}{mcd(kz,n)} = \frac{n}{mcd(k,n)},$$

ja que $mcd(z,n) = 1$.

Per tant, donat $\overline{z}$ generador de $\mathbb{Z}/n\mathbb{Z}$, els elements generadors d'aquest grup formen el conjunt $\{k\overline{z} \in \mathbb{Z}/n\mathbb{Z} \mid mcd(k,n) = 1\}$ de cardinal $\varphi(n)$, com ja es va veure en Aritmètica.

Així doncs per resoldre l'exercici només cal utilitzar la φ d'Euler de cada n.

Solució. a) Calculem $\varphi(p) = p - 1$.

b) $\varphi(p^r) = p^{r-1}(p-1)$.

c) $\varphi(p^r q^s) = \varphi(p^r)\varphi(q^s)$ ja que p i q són coprimers. $\varphi(p^r)\varphi(q^s) = p^{r-1}(p-1)q^{s-1}(q-1)$.