Problema 1. *Demostrar que un grupo abeliano finito no es cíclico si y sólo si contiene algún subgrupo isomorfo a $Z_p \times Z_p$ para algún primo p.*

Solución. Utilizando el teorema de estructura de grupos abelianos finitos existirán números naturales $r, n_1, \ldots, n_r$ tales que

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdot \times \mathbb{Z}/n_r\mathbb{Z} \ ,$$

y además n_i divide a n_{i-1}. Si suponemos que G no es cíclico entonces $r \geq 2$, luego existe al menos n_1 y n_2 que satifacen el teorema de estructura. Como n_2 divide a n_1 existe al menos un factor primo común p. Entonces el subgrupo $H = \langle x, y \rangle$ con

$$x = \left(\frac{n_1}{p} + n_1\mathbb{Z}, 0 + n_2\mathbb{Z}, 0 + n_3\mathbb{Z}, \ldots, 0 + n_r\mathbb{Z} \right)$$

$$y = \left(0 + n_1\mathbb{Z}, \frac{n_2}{p} + n_2\mathbb{Z}, 0 + n_3\mathbb{Z}, \ldots, 0 + n_r\mathbb{Z} \right)$$

es isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Se puede ver que la aplicación

$$\begin{array}{ccc} H = \langle x, y \rangle & \Longrightarrow & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \\ x^m y^n & \longmapsto & (m + p\mathbb{Z}, n + p\mathbb{Z}) \end{array}$$

es isomorfismo. Esta aplicación está bien definida por ser G abeliano. La comprobación de que es isomorfismo se puede ver utilizando el hecho de que el órden de x e y es p.

Ahora demostraremos que si existe un subgrupo ismorfo a $H = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ entonces G no es cíclico. Para ello demostraremos que si G es cíclico entonces todos sus subgrupo son cíclicos:

Sea $G = \langle a \rangle$ cíclico y H un subgrupo de de G. Suponemos que $H \neq \{1\}$, ya que en caso contrario H sería obviamente cíclico y acabaríamos la demostración. Sea k el menor número entero positivo tal que $a^k \in H$, entonces tendríamos que $H = \langle a^k \rangle$, es decir, H es cíclico. En efecto, sea a^n un elemento cualquiera de H. Dividimos n entre k,

$$n = qk + r \ ,$$

con $0 \leq r < k$. Como se verifica que $a^r = a^{n-qk} = a^n(a^k)^{-q}$ pertenece a H y k es el menor entero positivo que tal que $a^k \in H$, tenemos que $r = 0$ y por tanto $n = qk$. Esto nos demuestra que $H \subset \langle a^k \rangle$. Como la inclusión inversa se verifica obviamente, tenemos que $H = \langle a^k \rangle$.

Acabamos de demostrar que si G es cíclico entonces todos sus subgrupos son cíclicos. Para terminar la demostración sólo tenemos que comporbar que $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ no es cíclico. Esto es inmediato al aplicar el teorema de estructura de los grupo abelianos finitos, ya que el grupo $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ está escrito en su forma canónica y entonces no puede existir en número natural n tal que sea isomorfo a $\mathbb{Z}/n\mathbb{Z}$.