Problems 3

1. We denote by $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$.
   (a) If $\bar{a}\bar{b} = \bar{0}$ and $\gcd(a, n) = 1$, show that $\bar{b} = \bar{0}$.
   (b) Show that $\bar{a}$ is invertible in $\mathbb{Z}_n$ if and only if $\bar{a}\bar{b} = \bar{0}$ implies $\bar{b} = \bar{0}$.

2. Let $G = \{g_1, g_2, \cdots, g_r\}$ be an abelian group and consider the element $a = g_1 g_2 \cdots g_r \in G$. Show that $a^2 = 1_G$.

3. Apply the previous question to $G = \mathbb{Z}_p^*$ to prove Wilsons Theorem : for p prime,

$$(p-1)! \equiv -1 \bmod p.$$

4. Show that

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

   is a subgroup of $\mathrm{GL}(\mathbb{Z})$ isomorphic to $\{1, -1, i, -i\}$.

5. Show that the circle group $\mathbb{C}^0 = \{z \in \mathbb{C}, |z| = 1\}$ is not isomorphic to $\mathbb{R}^*$.