Math 3140 - Assignment 2

Due September 4, 2026

(1) (a) Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group.
    (b) Show that $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is a group. Give the identity and inverses for every element.

(2) Compute the following multiplicative inverses in $\mathbb{Z}_n$ if possible:
    (a) $[12]^{-1}$ in $\mathbb{Z}_{35}$
    (b) $[14]^{-1}$ in $\mathbb{Z}_{35}$

    Hint: Use the Euclidean Algorithm to compute Bezout's coefficients.

(3) Let $n \geq 2$ and a be integers. Show that $ax \mod n = 1$ has a solution iff $\gcd(a, n) = 1$.

(4) For $n \in \mathbb{N}$, let $\mathbb{Z}_n^*$ denote the set of elements in $\mathbb{Z}_n$ that have a multiplicative inverse. Show that $(\mathbb{Z}_n^*, \cdot)$ is a group.

    Hint: Don't forget to show that $\cdot$ is an operation on $\mathbb{Z}_n^*$, i.e., that the product of invertible elements is invertible again.

(5) Let A, B be subgroups of a group $(G, \cdot)$. Show that $A \cap B$ is a subgroup as well.