Topics in CS: Problem Set 3

Due date: November 23, 2025.

Question 1. (10 points) Compute by hand the multiplicative inverse for

- 7 mod 81
- 13 mod 79

Question 2. (20 points)

1. Write the invertible elements in each of the following sets: $\mathbb{Z}_8$, $\mathbb{Z}_{27}$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{21}$.

   Use your insights as intuition for the following items.
2. Let p be a prime. How many elements in $\mathbb{Z}_{p^3}$ have a multiplicative inverse?
3. Let p and q be distinct primes. How many elements in $\mathbb{Z}_{pq}$ have a multiplicative inverse?

Question 3. (20 points)

1. Let G be a group and let H and K be subgroups of G.
2. Prove or refute the following claim: $H \cap K$ is a subgroup of G.
3. Prove or refute the following claim: $H \cup K$ is a subgroup of G.

Question 4. (25 points)

1. Let $(G, \circ_G)$ and $(H, \circ_H)$ be groups.

   Prove that the set $G \times H = \{(g, h) \mid g \in G, h \in H\}$ is a group with respect to the operation $(g_1, h_1) \circ (g_2, h_2) = (g_1 \circ_G g_2, h_1 \circ_H h_2)$ for every $(g_1, h_1), (g_2, h_2) \in G \times H$.
2. Prove or refute the following claim: $\mathbb{Z}_2 \times \mathbb{Z}_5$ is isomorphic to $\mathbb{Z}_{10}$.
3. Prove or refute the following claim: $\mathbb{Z}_2 \times \mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_{12}$.

Question 5. (25 points)

1. Implement the extended Euclidian algorithm for inputs of arbitrary length.

   Use the algorithm Div you implemented in PS2 for your implementation.
2. Compute the inverse of 1234 modulo 999331.
3. Sample an element in $\mathbb{Z}^*_{999331}$ and compute its multiplicative inverse.

Good luck!