MAT 4233 — Problem Set 1

Due Tuesday 8 September 2026, at the start of the Q&A session.

This set covers the five meetings of 20 August through 3 September: the arithmetic of the integers (Childs Ch. 3), congruence and the ring $\mathbb{Z}_n$ (Childs Ch. 5–6), binary operations and isomorphic binary structures (Li–Zhao §1.1–1.2), plane isometries and the finite symmetry groups of the plane (Rosebrock Ch. 1, Beardon §3.1–3.4, and the complex-geometry handout), and the group axioms together with their first consequences (Li–Zhao §1.3).

Maximum six pages. Each problem is scored on *completeness* alone, not on correctness: **2** for a nominally complete solution, **1** for a clearly partial one, **0** for nothing submitted or for filler with no substance. Any submission containing non-human-readable content, stray characters, or unproofread AI output scores 0 for that item.

Sources. AI assistance, solution keys, collaboration and the internet are all permitted, without restriction. Include one line naming what you used. Note that at the Q&A session we name the problem you are to explain; you do not choose, so be ready on all six.

Notation. We write $\mathbb{Z}_n$ for the integers modulo n, and $[a]$ for the class of a in $\mathbb{Z}_n$. C_n denotes the cyclic group of order n, and D_n the group of all symmetries of a regular n-gon, so that $|D_n| = 2n$ (some authors write D_{2n} for this same group; we shall not).

Problem 1 (The extended Euclidean algorithm —Bézout's identity)

1. Run the extended Euclidean algorithm on 2024 and 748 to compute $d = \gcd(2024, 748)$. By backwards substitution find integers x, y with $2024x + 748y = d$ (Bézout identity).

2. Prove that for integers a, b not both zero,

$$\gcd(a, b) = 1 \quad \text{if and only if} \quad ax + by = 1 \qquad \text{for some } x, y \in \mathbb{Z}.$$

3. Using part 2, prove *Euclid's lemma*: if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Problem 2 (congruences and $\mathbb{Z}_n$)

1. Solve the congruences:

   a. $15x \equiv 9 \pmod{21}$.
   b. $12x \equiv 14 \pmod{21}$.

2. Prove that $[a]$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$.

3. Suppose instead that $\gcd(a, n) = d > 1$. Prove that $[a]$ is a *zero divisor* in $\mathbb{Z}_n$: there exists $[b] \neq [0]$ in $\mathbb{Z}_n$ such that $[a][b] = [0]$. (Apart from $[0]$, all elements of $\mathbb{Z}_n$ are invertible or zero divisors —never not both.)

Problem 3 (abstract properties of a given operation)

On the set $\mathbb{Z}$ of integers, define the operation

$$a * b := a + b - ab.$$

1. Is the operation $*$ associative? Commutative? Show that it admits a neutral ("identity") element.
2. Find all invertible elements of $\mathbb{Z}$ (with respect to $*$). Is $\mathbb{Z}$ a group with operation $*$?
3. Let $\varphi\colon \mathbb{Z} \to \mathbb{Z}$ be the function $x \mapsto \varphi(x) := 1 - x$. Show that φ is an isomorphism from $(\mathbb{Z}, *)$ to $(\mathbb{Z}, \cdot)$, where $\cdot$ is the ordinary operation of multiplication of integers.
4. Use part 3 to redo parts 1 and 2 more quickly.

Problem 4 (disproving isomorphisms)

1. Prove that the binary structures $(\mathbb{Q}, +)$ and $(\mathbb{Q}^{>0}, \cdot)$ are *not* isomorphic, where $\mathbb{Q}^{>0}$ denotes the set of strictly positive rationals. (*Hint:* There are many structural / abstract properties that one possesses, but not the other.)
2. Generalize your findings to extract the method from 1 as a theorem of the form: *"If $(A, \cdot)$ and $(B, *)$ are sets each with a binary operation, and if [...], then A and B are not isomorphic."* Prove your theorem.

Problem 5 (similitudes of the plane as complex maps)

Recall from the complex-geometry handout that every similarity transformation of the plane, viewed as a map $\mathbb{C} \to \mathbb{C}$, has exactly one of the two forms $f^{+}_{a,b}(z) := az + b$ (if orientation-preserving) or $f^{-}_{a,b}(z) := a\bar{z} + b$ (if reversing) where $a, b \in \mathbb{C}$, and $a \neq 0$. The set of all such (resp., of orientation-preserving, orientation-reversing) similarities is denoted S_2 (resp., S_2^+, S_2^-).

1. By explicit computation(s), show that $\langle \mathrm{S}_2, \circ \rangle$ is a group, where $\circ$ is the operation of composition of functions.
2. Is S_2^+ a subgroup of S_2? Is S_2^-?
3. Show that the properties "orientation-preserving" and "orientation-reversing" of similarities (under *composition*) behave in a formally identical way to the properties "even" and "odd" of integers under *addition*. (Lurking beneath this observation lie the notions of *homomorphic image* and *quotient group*.)
4. For every natural $n \geq 2$, show that S_2^+ has cyclic subgroup isomorphic to C_n. Find an additional n elements in S_2^- to obtain a $2n$-element subgroup of S_2 isomorphic to D_n.