MATH 4000/6000 – Homework #1

posted January 14, 2025; due by end of day on January 24, 2025

> You know, for a mathematician, he did not have enough imagination. But he has become a poet and now he is fine. — David Hilbert (1862–1943), talking of an ex-student

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are *required* for those in MATH 6000 and *extra credit* for those in MATH 4000.

Fully explain your answers. In problems #1 and #2 only you must explain which algebraic properties (properties A1–A4, M1–M3, D1 on the handout) you are using at every step of the proof. To facilitate this, you might adopt a "two column" format with each line showing, on the left, a step in the proof and on the right a justification. For example:

$$a \cdot (0+0) = a \cdot 0 + a \cdot 0 \qquad \text{(Distributive law).}$$

Refer to properties by name rather than number (write "Distributive law" and not "D1").

For all other problems, you are expected to do "familiar" algebraic manipulations without citing the algebraic properties on the handout. You may assume all results shown in class, including the following:

$$a \cdot 0 = 0 \qquad \text{and} \qquad 0 \cdot a = 0 \quad \text{for all } a \in \mathbb{Z},$$
$$a \cdot (-1) = -a \qquad \text{and} \qquad (-1) \cdot a = -a \quad \text{for all } a \in \mathbb{Z},$$
$$-(-a) = a \qquad \text{for all } a \in \mathbb{Z}.$$

You may also assume that $a > 0$ is equivalent to $a \in \mathbb{Z}^+$ and that 1 is the least element of $\mathbb{Z}^+$.

0. (UNDERSTANDING CHECKS; DO NOT TURN THIS IN)
   (a) Now that we have proved $a \cdot 0 = 0$ (for all $a \in \mathbb{Z}$), rewrite the proof that $a \cdot (-1) = -a$ (for all $a \in \mathbb{Z}$), making sure to note where you use that $a \cdot 0 = 0$.
   (b) Write out proofs that $0 \cdot a = 0$ and $(-1)a = -a$ that do not use the commutative property of multiplication.
   (c) Recall that when n, k are integers with $0 \le k \le n$, the **binomial coefficient** $\binom{n}{k}$ is defined by $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Check, by expanding and performing algebraic simplifications, that $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ whenever k, n are integers with $0 < k < n+1$.

1. Prove that for all $a, b \in \mathbb{Z}$, we have
   (a) $(-a)b = -(ab)$.
   (b) $(-a)(-b) = ab$.

2. (a) Let $a, b \in \mathbb{Z}$ and suppose that $a < b$. Prove that $a + c < b + c$ for every $c \in \mathbb{Z}$.
   (b) Let $a, b \in \mathbb{Z}$ and suppose that $a < b$. Prove that $ac < bc$ for every $c \in \mathbb{Z}^+$.

   In Problems #1 and #2 (only), quote each time you use one of our fundamental properties (axioms) of $\mathbb{Z}$. For example, if the factorization $bc - ac = (b-a)c$ appears in your solution to 2(b), you must explain from the axioms why this holds. Keep in mind that $u - v$ is shorthand for $u + (-v)$.

3. Let $a, b \in \mathbb{Z}$. Show that $a < b$, $a = b$, or $a > b$, and in fact exactly one of these three holds.

4. Let $a, b \in \mathbb{Z}$.

   (a) Prove that if $a < 0$ and $b < 0$, then $ab > 0$.

   (b) Show that if $a < 0$ and $b > 0$, then $ab < 0$.

   (c) Show that if $ab = 0$, then either $a = 0$ or $b = 0$.

5. Use the Well-Ordering Principle to prove the following version of the Principle of Mathematical Induction.

   Let S be a subset of $\mathbb{Z}^+$. Assume:
   (1) $1 \in S$,
   (2) for all $n \in \mathbb{Z}^+$, if $n \in S$ then also $n + 1 \in S$.
   Then $S = \mathbb{Z}^+$.

   Hint to get you started: If $S \subsetneq \mathbb{Z}^+$, then there is a least positive integer *not* in S.

6. (Laws of exponents) Let $a \in \mathbb{Z}$. Suppose that m, n belong to the set $\mathbb{Z}^+ \cup \{0\}$ of nonnegative integers.

   (a) Prove that $a^m \cdot a^n = a^{m+n}$.

   (b) Prove that $a^{mn} = (a^m)^n$.

   Hint: If $m = 0$ or $n = 0$, this is easy (why?). So you can suppose $m, n \in \mathbb{Z}^+$. Now think of m as fixed and proceed by induction on n.

7. Use the binomial theorem to find formulas for the following sums, as functions of n, where n is assumed to be a natural number.

   (a) $\displaystyle\sum_{k=0}^{n} \binom{n}{k}$.

   (b) $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k}$.

8. Show that if $a, b \in \mathbb{Z}^+$ and $a \mid b$, then $a \leq b$.

9. In this exercise we outline a proof of the following statement, which we will be taking for granted in our proof of the Division Theorem: If $a, b \in \mathbb{Z}$ with $b > 0$, the set

   $$S = \{a - bq : q \in \mathbb{Z} \text{ and } a - bq \geq 0\}$$

   has a least element.

   (a) Prove the claim in the case $0 \in S$.

   (b) Prove the claim in the case $0 \notin S$ and $a > 0$.

   (c) Prove the claim in the case $0 \notin S$ and $a \leq 0$.

   Hint: (a) is easy. To handle (b) and (c), first show that in these cases that S is a nonempty set of natural numbers, so that the well-ordering principle guarantees S has a least element as long as S is nonempty. To prove S is nonempty, show that in case (b), the integer a is an element of S. You will have to work a little harder to prove S is nonempty in case (c).

10. Use the Euclidean algorithm to find $\gcd(314, 159)$ and $\gcd(272, 1479)$. Show the steps, not just the final answer.

6000 problems

11. (*) Prove that there is no subset S of the complex numbers $\mathbb{C}$ satisfying all three of the following properties.

    (1) If $a, b \in S$, then $a + b \in S$.

    (2) If $a, b \in S$, then $a \cdot b \in S$.

    (3) For every $a \in \mathbb{C}$, exactly one of the following holds: (a) $a \in S$, (b) $a = 0$, (c) $-a \in S$.

    You may assume familiar properties of $\mathbb{C}$ for this problem.

12. (*) Prove that the properties of the set $\mathbb{Z}^+$ on the handout uniquely determine $\mathbb{Z}^+$ as a subset of $\mathbb{Z}$.

    Precisely: Assume all of A1–N1, as usual. Furthermore, assume O1 and WOP hold with two subsets P, P' of the integers in place of $\mathbb{Z}^+$. Prove that $P = P'$.