# MAT 108: Problem Set 2

Solutions

Due 1/24/23 at 11:59 pm on Canvas

**Reminders:**

- Put your name at the top!
- You will receive feedback on PS1 by next Tuesday, 1/24. PS1 revisions are due Friday, 1/27 at 11:59 pm.
- Dr. Zhang will be away all of next week (no instructor office hours). I will be in Germany, where the time is 9 hours ahead of California. You may email me your questions, and I will respond once daily as usual. The TA will still hold his office hours.

**Another reminder** Figuring out how to prove something should feel like doing a puzzle. Writing down and expressing your proof should feel like you're trying to write in a new language. Trust the process!

**How much detail is needed?** In PS2, you no longer need to cite the axioms / propositions from Chapter 1. For example, it's clear to the audience (e.g. your classmates) that $-0 = 0$.

On the other hand, in Chapter 2, we defined the natural numbers $\mathbb{N}$ using a set of axioms that are not very obvious to your peers. You should cite these axioms as you use them.

## Exercise 1

**Prove that $1 \in \mathbb{N}$ via a proof by contradiction. Then, deduce that that if $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$.**

**Remark.** The phrase *deduce that* here is indicating that the second statement follows quite immediately from the first.

SOLUTION.

We want to show that $1 \in \mathbb{N}$. By way of contradiction, assume that 1 is *not* a natural number. Then by Proposition 2.2, we must have $-1 \in \mathbb{N}$ (since $1 \neq 0$).

Now by Axiom 2.1.(ii), since $-1 \in \mathbb{N}$, we must have $(-1) \cdot (-1) = 1 \in \mathbb{N}$. This contradicts our assumption that $1 \notin \mathbb{N}$.

□

## Exercise 2

**Definition.** Let $m, n \in \mathbb{Z}$. If $m - n \in \mathbb{N}$, then we say $n$ *is less than* $m$, and write $n < m$. We also say $m$ *is greater than* $n$, and write $m > n$.

**Prove that there exists no integer $x$ such that $0 < x < 1$.**

SOLUTION.

First, we show by induction that for all $k \in \mathbb{N}$, $k \geq 1$ (i.e. $k = 1$ or $k > 1$).

Let $A = \{k \in \mathbb{Z} : k \geq 1\}$. (Base case) If $k = 1$, then $k \geq 1$, so $1 \in A$. (Induction step) Suppose $n \geq 1$. Since $(n + 1) - n = 1 \in \mathbb{N}$, we have $n + 1 > n > 1$. By transitivity, we have $n + 1 \geq 1$ as well, so $n + 1 \in A$.

By Axiom 2.15, since since $1 \in A$ and we have shown that if $n \in A$ then $n + 1 \in A$, we have $\mathbb{N} \subseteq A$, i.e. for any natural number $k$, $k \geq 1$.

We now show using proof by contradiction that there is no integer $m$ such that $0 < m < 1$. Note that this means $m \neq 0$ and $m \neq 1$.

By way of contradiction, suppose that there is an integer $m$ such that $0 < m < 1$. Then

$$m - 0 = m \in \mathbb{N} \qquad \text{and} \qquad 1 - m \in \mathbb{N}.$$

In the previous paragraph, we showed that, since $m \in \mathbb{N}$, $m \geq 1$. Since $m \neq 0$, we must have $m > 1$, i.e. $m - 1 \in \mathbb{N}$. But we also have $1 - m \in \mathbb{N}$. But this is impossible by Proposition 2.2: since $m \neq 1$, both $m - 1$ and $1 - m = -(m - 1)$ are not 0, so only one of them can be in $\mathbb{N}$.

□

## Exercise 3

Use induction to prove that for any $n \in \mathbb{N}$, the following formula holds:

$$1 + 2 + 3 + \ldots + (n - 1) + n = \frac{n(n+1)}{2}.$$

SOLUTION.

We will induct on $n$. In the base case, $n = 1$, and indeed $1 = \dfrac{1(1+1)}{2}$.

For the induction step, assume that

$$1 + 2 + 3 + \ldots + (n - 1) + n = \frac{n(n+1)}{2}.$$

We want to show that

$$1 + 2 + 3 + \ldots + (n - 1) + n + (n + 1) = \frac{(n+1)(n+2)}{2}.$$

By the induction hypothesis, the left-hand side is equal to

$$\frac{n(n+1)}{2} + (n + 1).$$

Combining fractions and expanding, we have

$$\frac{n(n+1)}{2} + (n + 1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+2)(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

□

## Exercise 4

**Definition.** Let $p \in \mathbb{N}$. If the only $k \in \mathbb{N}$ such that $k \mid p$ are $k = 1$ and $k = p$, then $p$ is *prime*.

**Prove that there are infinitely many prime numbers.**

**Remark.** We haven't rigorously discussed the term *infinite* just yet. We will discuss cardinality in detail in a few weeks. For now, *infinite* means *not finite*.

You should begin by assuming there are finitely many prime numbers, so that you can label them $p_1, p_2, p_3, \ldots, p_n$ for some finite $n \in \mathbb{N}$. Then try to derive a contradiction.

You may use the following Lemma without proof:

**Lemma.** Let $p$ be a prime number, and let $m \in \mathbb{N}$. If $p$ divides $m$, then $p$ does not divide $m + 1$.

(Proving this lemma will be easier once we've developed the language of *modular arithmetic* later on in the course.)

SOLUTION.

By way of contradiction, suppose that there are finitely many primes. Label these $p_1, p_2, \ldots, p_n$, where $n \in \mathbb{N}$. Let $P = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Then for all $i$, $p_i \mid P$.

Now consider the number $P + 1$. Since all $p_i \mid P$, by the lemma we know that none of the $p_i$ divide $P + 1$. This contradicts the fact that every natural number has a prime decomposition.

$\square$