9/28/15

Exam 1 stats:

Total = 24
Average = 18 = 75%
Median = 18
St. Dev. = 4

Very rough grade ranges:

21 − 23 = A
16 − 20 = B
11 − 15 = C

HW3 : TBA.

Today we'll discuss the solutions to Exam 1.

I'll also hand out the formal definition of $\mathbb{Z}$ and we can discuss that too.

9/30/15

Notice: I'm out of town next Mon Oct 5, so class is canceled.

Notice: No class on Fri Oct 9 because of Fall Break.

HW3 will be due after Fall Break on Mon Oct 12.

Today: The definition of $\mathbb{Z}$.

[see handout]

In many ways, Euclid's axioms have been replaced in modern mathematics by the axioms for natural numbers

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

and integers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

We've been using properties of these sets implicitly for a while.

Now I'll show you the formal definition so we can be more confident in our proofs. These axioms will serve you in all of your future math courses.

Definition: Let $\mathbb{Z}$ be a set equipped with four concepts

"$=$", "$\leq$", "$+$", "$\times$".

These concepts satisfy approximately 20 axioms (depending on how you count). Luckily, all of these axioms are "obvious" statements that you are already comfortable with.

We discussed the axioms of "$=$" and "$\leq$" Last time. These are roughly equivalent to Euclid's common notion (but we're being more careful than he was).

Now let's take a look at the axioms of addition:

↓

(A1) $\forall\, a, b \in \mathbb{Z}, \quad a+b = b+a.$

(A2) $\forall\, a, b, c \in \mathbb{Z}, \quad a+(b+c) = (a+b)+c$

(A3) $\exists\, 0 \in \mathbb{Z}, \forall\, a \in \mathbb{Z}, \quad a+0 = a.$

(A4) $\forall\, a \in \mathbb{Z}, \exists\, b \in \mathbb{Z}, \quad a+b = 0$

In modern jargon these axioms say that $\mathbb{Z}$ is a *group* under addition. The element $0 \in \mathbb{Z}$ is called the *identity element* of the group.

Prop: The identity element is unique.

Proof: Suppose we have two elements $z_1, z_2 \in \mathbb{Z}$ satisfying

$\textcircled{1}$ $\forall\, a \in \mathbb{Z}, \quad a + z_1 = a$

$\textcircled{2}$ $\forall\, a \in \mathbb{Z}, \quad a + z_2 = a.$

Then we conclude that

$$z_1 \overset{\textcircled{2}}{=} z_1 + z_2 \overset{\textcircled{1}}{=} z_2 \qquad ///$$

Since the identity element is unique we can give it a special name. We call it "0".

The element b in (A4) is called an additive inverse of a.

<u>Prop</u>: Additive inverses are unique.

<u>Proof</u>: Let $a \in \mathbb{Z}$. Suppose we have two elements $b_1, b_2 \in \mathbb{Z}$ satisfying

① $a + b_1 = 0$

② $a + b_2 = 0$.

Then we conclude that

$$\begin{aligned} b_1 &= b_1 + 0 && \text{(A3)} \\ &= b_1 + (a + b_2) && ② \\ &= (b_1 + a) + b_2 && \text{(A2)} \\ &= (a + b_1) + b_2 && \text{(A1)} \\ &= 0 + b_2 && ① \\ &= b_2 + 0 && \text{(A1)} \\ &= b_2 && \text{(A3)} \end{aligned}$$

///

Since the additive inverse of a is unique we can give it a special name. We will call it "$-a$".

Additive inverses now allow us to define a new operation called subtraction.

Definition: For all $a, b \in \mathbb{Z}$ we define

$$\text{“}a - b\text{''} = a + (-b).$$

Now let's discuss the axioms of multiplication. We will write the product of a & b as ab.

(M1) $\forall a, b \in \mathbb{Z}, \quad ab = ba.$
(M2) $\forall a, b, c \in \mathbb{Z}, \quad a(bc) = (ab)c.$
(M3) $\exists 1 \in \mathbb{Z}, \forall a \in \mathbb{Z}, \quad 1a = a.$

You can check that the element 1 is unique. We call it the multiplicative identity element of $\mathbb{Z}$. [We call 0 the additive identity element.].

Note that there is no axiom (M4) because integers do not necessarily have multiplicative inverses.

Example: Define the integer $2 = 1+1$. There does not exist $q \in \mathbb{Z}$ such that $2q = 1$.

[The proof of this requires the Well-Ordering Axiom, which we haven't discussed yet].

We also require an axiom telling us how addition and multiplication interact.

(D) $\forall a,b,c \in \mathbb{Z}, \quad a(b+c) = ab + ac$.

Q: How does the additive identity 0 interact with multiplication?

A: $\forall a \in \mathbb{Z}, \quad 0a = 0$

To prove this we will use a Lemma.

☆ Cancellation Lemma:

For all $a,b,c \in \mathbb{Z}$ we have

$$(a+b = a+c) \Rightarrow (b = c).$$

Proof:
$$\begin{aligned} b &= b+0 && \text{(A3)} \\ &= b+(a+(-a)) && \text{(A4)} \\ &= (b+a)+(-a) && \text{(A2)} \\ &= (c+a)+(-a) && \text{assumption} \\ &= c+(a+(-a)) && \text{(A2)} \\ &= c+0 && \text{(A4)} \\ &= c. && \text{(A3)} \end{aligned}$$
///

[we use (A1) so often that it gets too tedious to mention it.]

Prop: $\forall a \in \mathbb{Z}$, $0a = 0$.

Proof: Let $a \in \mathbb{Z}$. Then we have

$$\begin{aligned} 0+0 &= 0 && \text{(A3)} \\ (0+0)a &= 0a && \\ 0a+0a &= 0a && \text{(D)} \\ \cancel{0a}+0a &= \cancel{0a}+0 && \text{(A3)} \\ 0a &= 0 && \text{cancellation} \end{aligned}$$

///

Q: Why don't we take $0a = 0$ as an axiom?

A: Because we don't need to!

On HW3 you will investigate how subtraction interacts with multiplication.

You will show that $\forall a, b \in \mathbb{Z}$ we have

- $-(-a) = a$
- $(-a)b = a(-b) = -(ab)$
- $(-a)(-b) = ab$.

Have you ever wondered why

negative × negative = positive ?

The reason is because it follows logically from the obvious properties of addition and multiplication.

We have no choice!

10/2/15

No class next Monday
No class next Friday.
Wednesday, yes.
I'll post HW3 later today and it will be due on Mon Oct 12.

We are discussing the definition of $\mathbb{Z}$.

Last time we discussed the axioms of addition and multiplication

$$(A1)-(A4),\ (M1)-(M3),\ (D)$$

In modern jargon, these 8 axioms tell us that $\mathbb{Z}$ is a (commutative) ring. [This terminology was introduced by David Hilbert in 1897. I have no idea why.]

Next we will discuss the axioms of order, but first some terminology.

Recall that we defined "$\leq$" to satisfy the rules

- $\forall a \in \mathbb{Z},\ a \leq a$
- $\forall a, b \in \mathbb{Z},\ (a \leq b \wedge b \leq a) \Rightarrow (a = b)$
- $\forall a, b, c \in \mathbb{Z},\ (a \leq b \wedge b \leq c) \Rightarrow (a \leq c)$.

It is also convenient to define the symbols "$\geq$", "$<$", "$>$" by

$$(a < b) \Longleftrightarrow (a \leq b \wedge a \neq b)$$
$$(a > b) \Longleftrightarrow (a \not\leq b)$$
$$(a \geq b) \Longleftrightarrow (a > b \vee a = b).$$

Here are the axioms of order:

(O1) $\forall a, b, c \in \mathbb{Z},\ (a \leq b) \Rightarrow (a + c \leq b + c)$

(O2) $\forall a, b, c \in \mathbb{Z},\ (a \leq b \wedge 0 \leq c) \Rightarrow (ac \leq bc)$

(O3) $0 < 1$.

These are the modern version of Euclid's "common notions". In particular, (O3) is the modern version of

"The whole is greater than the part".

[Actually, we implicitly used (O1) last time but I didn't mention it.

↓

We used it when we said that

$$(b=c) \Rightarrow (a+b=a+c).$$

It would be fairly tedious to actually prove this so let's stop worring about it. From now on you can use obvious facts like this without proof (unless I tell you not to).]

These first 11 axioms tell us that $\mathbb{Z}$ is an *ordered ring*.

But this *can*'t be the full definition of $\mathbb{Z}$ because there are other ordered rings in the world, such as

$$\mathbb{Q} \quad \& \quad \mathbb{R}.$$

Q: What is special about $\mathbb{Z}$ that distinguishes it among all the ordered rings?

This leads us to the least obvious and the most important axiom

Define the natural numbers

$$\mathbb{N} := \{ a \in \mathbb{Z} : 1 \leq a \} = \{ 1, 2, 3, \cdots \}.$$

☆ Well-Ordering Axiom :

Every non-empty subset of $\mathbb{N}$ has a smallest element.

To be formal : If $S \subseteq \mathbb{N}$ with $S \neq \emptyset$ [$\emptyset$ is the "empty set"] then there exists $m \in S$ such that for all $a \in S$ we have

$$m \leq a.$$

In symbols : Let $\wp(\mathbb{N})_{\neq \emptyset}$ be the set of nonempty subsets of $\mathbb{N}$. Then

"$\forall S \in \wp(\mathbb{N})_{\neq \emptyset}, \exists m \in S, \forall a \in S, m \leq a$." //

↓

This axiom is logically much more complicated than the others and it took a long time to realize its importance. [It was first stated by Giuseppe Peano in 1889 in an equivalent form called the "principle of <u>induction</u>".].

For convenience, we often use the following equivalent form:

☆ Well-Ordering Axiom.

- Any nonempty subset of $\mathbb{Z}$ that is bounded below has a least element.
- Any nonempty subset of $\mathbb{Z}$ that is bounded above has a greatest element.

///

Here's our first application.

Theorem: Let $\alpha \in \mathbb{R}$ and $\alpha \notin \mathbb{Z}$. Then there exists an integer $m \in \mathbb{Z}$ such that

$$m-1 < \alpha < m .$$

Proof: Define the set

$$S := \{ n \in \mathbb{Z} : \alpha < n \} \subseteq \mathbb{Z}.$$

Since this set is non-empty and bounded below, it has a least element; call it $m \in S$. By definition we have

$$\alpha < m.$$

Now consider $m-1 \in \mathbb{Z}$. Since $m-1 < m$ and since m is the least element of S we conclude that $m-1 \notin S$, i.e.,

$$\alpha \not< m-1.$$

In other words, $m-1 \leq \alpha$. Finally, since $\alpha \notin \mathbb{Z}$ and $m-1 \in \mathbb{Z}$ we know that $m-1 \neq \alpha$, hence

$$m-1 < \alpha. \qquad ///$$

[You will use this on HW3 to prove that for all $d \in \mathbb{Z}$ we have

$$\sqrt{d} \notin \mathbb{Z} \Rightarrow \sqrt{d} \notin \mathbb{Q}.$$]

From this point on (unless otherwise stated) we will use the axioms of $\mathbb{R}$ rather informally. Instead of taking every proof all the way back to the axioms, we will take it to the point where we are confident that we could take it back to the axioms if we really had to (but we never will really have to).

This is how formalism is usually treated in mathematics. It's like insurance; it's there if we need it, and we hope we don't need it.

10/7/15

No class Friday (Fall Break)
HW3 due Monday.

Last time we finished discussing the definition of $\mathbb{Z}$, including the most important and least-obvious axiom.

☆ Well-Ordering Axiom:

- Any non-empty subset of $\mathbb{Z}$ that is bounded below has a least element.
- Any non-empty subset of $\mathbb{Z}$ that is bounded above has a greatest element.

Here's a joke application.

Theorem: There are no uninteresting natural numbers.

Proof: Suppose for contradiction that there exists an uninteresting natural number and let $S \subseteq \mathbb{N}$ be the set of these.

Since $S \neq \emptyset$ (by assumption) and since S is bounded below (by 0), Well-ordering implies that S has a *smallest* element, say $m \in S$.

But then m is "the smallest uninteresting natural number", which is *interesting*. This contradicts the fact that $m \in S$.

///

Remark: By contrast, there are *plenty* of uninteresting real numbers because $\mathbb{R}$ does not satisfy Well-Ordering.

Here's a more serious application. Our original proof of $\sqrt{2}$ had some gaps because we never proved the following two statements:

- Every fraction can be written in lowest terms.
- Every integer is of the form $2k$ or $2k+1$, for some $k \in \mathbb{Z}$, but not both.

Now I'll give a fully rigorous proof using Well-Ordering.

Theorem: $\sqrt{2} \notin \mathbb{Q}$.

Proof: Suppose for contradiction that $\sqrt{2} \in \mathbb{Q}$, so we can write $\sqrt{2} = a/b$ for some $a, b \in \mathbb{Z}$ with $b \geq 1$.

Now define the set

$$S = \{ n \in \mathbb{N} : n \cdot \sqrt{2} \in \mathbb{Z} \} \subseteq \mathbb{N}.$$

Note that $S \neq \emptyset$ because $b \geq 1$ and $b\sqrt{2} = a \in \mathbb{Z}$ imply that $b \in S$. So by Well-Ordering there exists a sm<u>allest</u> element $m \in S$.

Now we will try to find a contradiction. Since $\sqrt{2} \notin \mathbb{Z}$, we proved last time that there exists an integer $c \in \mathbb{Z}$ such that

$$c < \sqrt{2} < c+1$$
$$0 < \sqrt{2} - c < 1.$$

Multiply everything by m to get

$$0 < m(\sqrt{2} - c) < m .$$

If we can show that $m(\sqrt{2} - c) \in S$ then this will be a contradiction because m is the <u>smallest</u> element of S.

To show this, note that

$$m(\sqrt{2} - c) = \underset{\substack{\rotatebox{90}{$\in$} \\ \mathbb{Z}}}{m\sqrt{2}} - \underset{\substack{\rotatebox{90}{$\in$} \\ \mathbb{Z}}}{mc} \in \mathbb{Z}$$

and then $0 < m(\sqrt{2}-c) \implies m(\sqrt{2}-c) \in \mathbb{N}$.
Finally, note that

$$m(\sqrt{2} - c)\sqrt{2} = \underset{\substack{\rotatebox{90}{$\in$} \\ \mathbb{Z}}}{2m} - \underset{\substack{\rotatebox{90}{$\in$} \\ \mathbb{Z}}}{cm\sqrt{2}} \in \mathbb{Z} .$$

We conclude that $m(\sqrt{2} - c) \in S$, as desired.

///

The nice thing about this proof is that it easily generalizes to prove the following.

Theorem: For all $a \in \mathbb{Z}$ we have

$$\sqrt{a} \notin \mathbb{Z} \implies \sqrt{a} \notin \mathbb{Q}.$$

Proof: HW3 Problem 3. ///

Discussion: We have already seen two equivalent statements of the Well-Ordering Axiom. There are many more. Maybe the most famous version is called the "Principle of Induction".

☆ Principle of Induction:

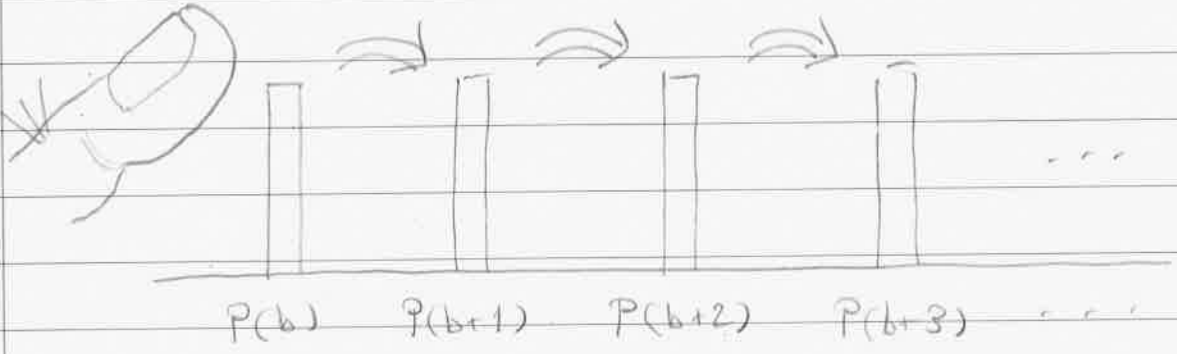
Let $P(n)$ be a statement about the integer $n \in \mathbb{Z}$. IF

① $P(b) = T$ for some $b \in \mathbb{Z}$, and
② $\forall n \in \mathbb{Z}_{\geq b}$, $P(n) \implies P(n+1)$,

then we conclude that $P(n) = T$ for all integers $n \geq b$. ///

[I don't expect you to be able to absorb this the first time you see it. In my experience it takes students quite a while to absorb what this is saying. Don't worry; you will have <u>lots</u> of practice. I just wanted to put it out there today so your sub-conscious can start thinking about it.]

I think of induction as follows. We want to knock down a line of dominoes:



Step ① is your finger and step ② is gravity. These two contributions are very different and both of them are necessary if you want to knock down <u>all</u> of the dominoes.

Example: Let $n \in \mathbb{Z}$ and consider the statement $P(n) =$ "$n < 2^n$". We would like to prove that $P(n) = T$ for all $n \geq 0$.

How?

Let's check some small cases:

$P(0) =$ "$0 < 1$" $= T$ ✓

$P(1) =$ "$1 < 2$" $= T$ ✓

$P(2) =$ "$2 < 4$" $= T$ ✓

$\vdots$

I could have my computer check many more cases, but eventually the computer and I will both be dead.

In order to prove that $P(n) = T$ for all (infinitely many) $n \geq 0$ we need some kind of abstract principle. This is exactly what induction does for us.

Here's the argument:

↓

Let n be some fixed but arbitrary integer greater than 1, and assume for induction that $n < 2^n$. In this case we have

$$n+1 < n+n < 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

We have shown that for all $n \geq 2$ we have

$$P(n) \Longrightarrow P(n+1).$$

///

Since we already checked that $P(2) =$ " $2 < 4$ " $= T$, the Principle of Induction now tells us we are allowed to say that

$$P(n) = T \quad \forall \; n \geq 2.$$

Since we also checked that $P(0) = P(1) = T$, we can say that

$$P(n) = T \quad \forall \; n \geq 0.$$

///