What is a Number?

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:

$\downarrow$

(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 <u>group</u> under addition. The element $0 \in \mathbb{Z}$ is called the i<u>dentity</u> el<u>emen</u>t of the group.

<u>Prop</u>: The identity element is unique.

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

① $\forall a \in \mathbb{Z}, \quad a + z_1 = a$
② $\forall a \in \mathbb{Z}, \quad a + z_2 = a$.

Then we conclude that

$$z_1 \overset{②}{=} z_1 + z_2 \overset{①}{=} z_2$$

///

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

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

///

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

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

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

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!

Properties of Order and The Well-Ordering Principle

Last time we discussed the axioms

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

In modern jargon, these 8 axioms tell us that $(\mathbb{Z}, +, \times, 0, 1)$ is a <u>ring</u>

Today we will discuss the order axioms:

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

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

(O3) $0 < 1$.

The notation "$0<1$" means that

"$0 \le 1$ and $0 \ne 1$".

More generally, it is convenient to define the symbols "$<$", "$>$", "$\geq$" to mean

$$(a<b) \Leftrightarrow (a \le b \wedge a \ne b)$$
$$(a>b) \Leftrightarrow (a \not\le b)$$
$$(a \geq b) \Leftrightarrow (a>b \vee a=b).$$

Now I will prove a few basic lemmas about "=" and "≤" that will help you on the homework.

(O4) $a \leq b \wedge c \leq 0 \implies bc \leq ac$.

Proof: Assume that $a \leq b$ and $c \leq 0$. Then we have

$$c + (-c) \leq 0 + (-c) \qquad (O1)$$
$$0 \leq -c \qquad (A3), (A4)$$

and hence (O2) implies

$$a(-c) \leq b(-c)$$
$$-(ab) \leq -(bc) \qquad \text{homework}$$

Finally, add $ab + bc$ to both sides:

$$-(\cancel{ab}) + \cancel{ab} + bc \leq -(\cancel{bc}) + ab + \cancel{bc} \qquad (O1)$$
$$0 + bc \leq ab + 0 \qquad (A4)$$
$$bc \leq ab \qquad (A3)$$

QED.

This allows us to prove an important property of "$=$". I already used this property without proving it and no one complained.

(E) $\forall\, a, b, c \in \mathbb{Z}$ we have

1. $a = b \implies a + c = b + c$.
2. $a = b \implies ac = bc$.

<u>Proof</u>: (1) We have

$$a = b \implies a \leq b \implies a + c \leq b + c \qquad (O1)$$
$$a = b \implies b \leq a \implies b + c \leq a + c. \qquad (O1)$$

Then antisymmetry of "$\leq$" gives $a + c = b + c$.

(2) There are two cases. If $0 \leq c$, then

$$a = b \implies a \leq b \implies ac \leq bc \qquad (O2)$$
$$a = b \implies b \leq a \implies bc \leq ac \qquad (O2)$$

Then antisymmetry gives $ac = bc$.
The case $c \leq 0$ is similar but we use $(O4)$ instead of $(O2)$.

QED.

The following strict versions of (O2), (O4) are true, but they are harder to prove.

$$(O2)' \quad a<b \wedge 0<c \implies ac<bc$$
$$(O4)' \quad a<b \wedge c<0 \implies bc<ac.$$

You will investigate this issue on the HW.

The 11 axioms (A1)–(A4), (M1)–(M3), (D), (O1)–(O3) say that

$$(\mathbb{Z}, \leq, +, \times, 0, 1)$$

is an ordered ring. But this can't be the full definition of $\mathbb{Z}$ because there exist other ordered rings 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 to the least obvious and most important axiom of the integers.

Well-Ordering Axiom.

Let $S \subseteq \mathbb{Z}$ be a set of integers and assume that

- S is not empty ($S \neq \emptyset$)
- S has a lower bound.
  ($\exists b \in \mathbb{Z}, \forall s \in S, b \leq s$).

Then the set S has a least element, i.e.

$$\exists m \in S, \forall s \in S, m \leq s.$$

This axiom is complicated and it will take some time to learn how to use it. Here is a first example.

Theorem: There are no integers between 0 and 1.

Proof: Consider the set of positive integers,

$$S' = \{ n \in \mathbb{Z} : 0 < n \}.$$

This set is non-empty (because $1 \in S'$) and it is bounded below (by 0). Hence by Well-Ordering there exists a smallest positive integer $m \in S'$

I claim that $m = 1$.

Indeed, since $1 \in S'$ and since m is the least element of S' we must have

$$m \leq 1$$

Now assume for contradiction that

$$m < 1.$$

Then multiplying $0 < m$ & $m < 1$ by m gives $0 < m^2$ & $m^2 < m$, which contradicts the minimality of m.

QED.

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>".].

Application of Well-Ordering

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 <u>could</u> take it back to the axioms if we really <u>had</u> to (but we never <u>will</u> 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 <u>don't</u> need it.

The Principle of Induction

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 smallest 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 smallest element of S.

To show this, note that

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

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

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

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: Exercise. ///

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:

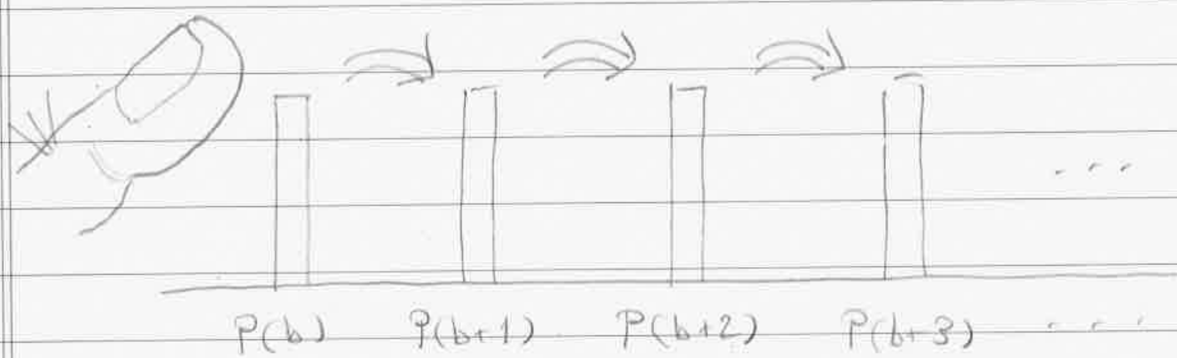
Let $P(n)$ be a statement about the integer $n \in \mathbb{Z}$. If

(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 <u>all</u> 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 lots 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 <u>all</u> $n \geq 0$.

How?

Let's check some small cases:

$$P(0) = \text{"}0 < 1\text{"} = T \quad ✓$$
$$P(1) = \text{"}1 < 2\text{"} = T \quad ✓$$
$$P(2) = \text{"}2 < 4\text{"} = T \quad ✓$$
$$\vdots$$

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 <u>all</u> (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

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

//