Proof Techniques | Instructor: Padraic Bartlett

Lecture 2: Truth and Numbers

Week 1 | *Mathcamp 2012*

When we defined what a proof was in our last lecture, we mentioned that we wanted our proofs to only start by assuming "true" statements, which we said were either previously proven-to-be-true statements or a small handul of **axioms**, mathematical statements which we are assuming to be true. In this lecture, we will describe some of these "true" statements that hold for the integers, rationals, and real numbers, and show how we can use these (relatively few) properties to prove a remarkable range of other results.

We start with the natural numbers, which we define here:

Definition. The **natural numbers**, denoted as $\mathbb{N}$, is the set of the positive whole numbers:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

There are three operations mathematicians typically perform on natural numbers: addition $(+,)$ multiplication $(\cdot,)$ and comparison $(<.)$ These operations satisfy a number of properties, which we list below.

- **Closure**$(+)$: $\forall a, b \in \mathbb{N}$, we have $a + b \in \mathbb{N}$.
- **Identity**$(+)$: $\exists 0 \in \mathbb{N}$ such that $\forall a \in \mathbb{N}$, $0 + a = a$.
- **Commutativity**$(+)$: $\forall a, b \in \mathbb{N}, a + b = b + a$.
- **Associativity**$(+)$: $\forall a, b, c \in \mathbb{N}, (a+b)+c = a + (b + c)$.
- **Closure**$(\cdot)$: $\forall a, b \in \mathbb{N}$, we have $a \cdot b \in \mathbb{N}$.
- **Identity**$(\cdot)$: $\exists 1 \in \mathbb{N}$ such that $\forall a \in \mathbb{N}$, $1 \cdot a = a$.
- **Commutativity**$(\cdot)$: $\forall a, b \in \mathbb{N}, a \cdot b = b \cdot a$.
- **Associativity**$(\cdot)$: $\forall a, b, c \in \mathbb{N}, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Antireflexivity**$(<)$: $\forall a \in \mathbb{N}, a \not< a$.
- **Antisymmetry**$(<)$: $\forall a, b \in \mathbb{N}$, exactly one of $(a < b,\ a = b, b < a)$ holds.
- **Transitivity**$(<)$: $\forall a, b, c \in \mathbb{N}$, if $a < b$ and $b < c$, we have $a < c$.
- **Add. Order**$(<, +)$: $\forall a, b, c \in \mathbb{N}$, if $a < b$, then $a + c < b + c$.

- **Distributivity**$(+, \cdot)$: $\forall a, b, c \in \mathbb{N}, (a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Formally speaking, you can prove that the natural numbers do satisfy all of these properties, if you start with the following very careful definitions:

- Start with the symbol 0, and an operation S, pronounced "successor," that takes in any natural number and returns $S(0)$. In your mind, S should be thought of as the "+1" function.

- Given 0 and this operation S, let $\mathbb{N}$ be all of the things you can create by starting with 0 and repeatedly applying S: i.e. $0, S(0), S(S(0)), S(S(S(0))), \ldots$
- For shorthand, denote the natural number made by n consecutive applications of S as n; then we have $\mathbb{N} = \{0, 1, 2 \ldots\}$.
- Define $a + b$ as simply applying S to a b-many times in a row. Define $a > b$ as the statement that's true if and only if there is no $c \in \mathbb{N}$ such that $a + c = b$. Define $a \cdot b$ as simply adding a to itself b-many times.

We will not prove that these properties listed above follow from these definitions, because it can take a while .

Using the natural numbers, we can easily define the **integers**:

Definition. The **integers**, denoted $\mathbb{Z}$, are all of the positive and negative whole numbers: i.e.

$$\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, 3, \ldots\}.$$

They satisfy all of the properties listed above for the natural numbers, along with the following extra two properties:

- **Inverses**$(+)$: $\forall a \in \mathbb{Z}, \exists$ a unique $(-a) \in \mathbb{Z}$ such that $a + (-a) = 0$.
- **Mult.Order**$(<, \cdot)$: $\forall a, b, c \in \mathbb{Z}$, if $a < b, 0 < c$ then $ac < bc$.

Again, you can rigorously prove that the integers satisfy these properties, starting with some appropriate definitions (listed on Wikipedia/other relevant texts; we won't delve into this too much, but if you're curious it is pretty cool.) Alternately, you can view the integers as what happens if you take $\mathbb{N}$ and then add in all of the symbols you need to satisfy the inverses property we described above.

Instead of doing this, our focus for this class is going to be showing how we can use these relatively few properties to prove other statements about these number systems! For example, a property that we didn't list above, but that seems pretty important, is the following:

- **New property**?$(+)$: $\forall a \in \mathbb{Z}, 0 \cdot a = 0$.

Another also-true property, that we also omitted above, is the following:

- **Other new property**?$(+)$: $\forall a \in \mathbb{Z}.(-a) = (-1) \cdot a$.

A question we could ask, given these properties, is the following: should we have listed it above? Or, if we already have the properties we've listed earlier, are these additional properties superfluous: i.e. can we prove that they're true just using the properties we have above, without having to look at the definitions of $\mathbb{Z}$?

As it turns out, we can simply use our earlier properties to prove that these are true! We do this here:

Claim 1.

$$\bullet \textbf{ New property}?(+): \forall a \in \mathbb{Z}, 0 \cdot a = 0.$$

Proof. Take any $a \in \mathbb{N}$. Because of the closure($\cdot$) property, we know that $0 \cdot a$ is also a natural number. Trivially, we know that

$$0 \cdot a = 0 \cdot a.$$

We also know that 0 is an additive identity: therefore, in specific, we know that $0 = 0 + 0$, and therefore that

$$0 \cdot a = (0 + 0) \cdot a.$$

Applying the distributive property then tells us that

$$0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a).$$

Now, we can use the inverse($+$) property to tell us that because $0 \cdot a$ is a natural number, we also know that there is some other natural number $-(0 \cdot a)$ such that $(0 \cdot a) + (-(0 \cdot a)) = 0$. Then, if we add this to both sides of our equality above (which we can do and still get integers because of closure,) we get

$$(0 \cdot a) + (-(0 \cdot a)) = ((0 \cdot a) + (0 \cdot a)) + (-(0 \cdot a)).$$

Applying the inverse property to the left hand side tells us that it's 0; applying the associative property to the right side tells us that

$$0 = ((0 \cdot a) + (0 \cdot a)) + (-(0 \cdot a)) = (0 \cdot a) + ((0 \cdot a) + (-(0 \cdot a))) = (0 \cdot a) + 0 = (0 \cdot a),$$

by applying first the inverse property and then the additive identity property to make the $+0$ go away. Therefore, we've proven that for any $a \in \mathbb{N}$, we have

$$0 = 0 \cdot a.$$

□

We continue to our second proof:

Claim 2.

$$\bullet \textbf{ Other new property}?(+): \forall a \in \mathbb{Z}, (-a) = (-1) \cdot a.$$

Proof. By the multiplicative identity property, we know that $1 \in \mathbb{Z}$; by the additive inverse property, we then also know that $-1 \in \mathbb{Z}$ and that

$$0 = 1 + (-1).$$

Using closure, distributivity, and the multiplicative identity property, we can take any a and multiply it by the left and right hand sides above:

$$0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a).$$

Using our result above, we know that $0 \cdot a = 0$, and therefore that

$$0 = a + (-1) \cdot a).$$

Using the additive inverse property and closure, we know that $-a$ is an integer and that we can add it to the left and right hand sides above:

$$(-a) + 0 = (-a) + (a + (-1) \cdot a)\,.$$

Using the additive identity property at left and associativity/inverses/the additive identity at right gives us

$$(-a) = ((-a) + a) + (-1) \cdot a = 0 + (-1) \cdot a = (-1) \cdot a,$$

whiish is what we claimed. □

These proofs should hopefully persuade you of two things: one, that it's possible to do an awful lot with the properties listed above, and two that it can be really fussy to do so. Throughout most of your Mathcamp courses, we'll generally assume that things like arithmetic work how we think they do, and not bother too much with citing these properties; usually, we'll keep our focus on the stranger/weirder definitions that each class specializes in, rather than these basic arithmetical definitions.

However, it does bear noting that the proofs above is cool in a few ways that aren't immediately obvious, as well. Specifically, we showed that $0 \cdot a = 0$, and that $(-a) = (-1) \cdot a$, using **only** these properties, and not anything special to $\mathbb{Z}$. Therefore, we know that the same result will be true for **anything**[1] that also satisfies these properties! This illustrates another thing that it's always worth paying attention to in your proofs: what facts are you specifically using in a proof? Do you need all of them? Can you extend your proof to covering many other situations, because you only care about a few properties and not the details of the object you're studying? (Keeping this in mind is one of the bigger leaps I made when switching from undergrad to graduate mathematical research.)

Continuing our study of different number sets, we can now move to defining the **rational numbers**:

Definition. The **rational numbers**, denoted $\mathbb{Q}$, is the collection of all ratios $\frac{a}{b}$ of integers, where $b \geq 1$ and the greatest common factor of a, b is ± 1. In other words,

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b > 0, \text{ and } \forall c, d, e \in \mathbb{Z} \text{ such that } c \cdot d = a, c \cdot e = b, \text{ we have } c = \pm 1. \right\}$$

The rational numbers satisfy all of the properties listed above for the integers, along with the following new properties:

- **Inverses($\cdot$)** : $\forall a \in \mathbb{Q}, a \neq 0, \exists$ a unique $\frac{1}{a} \in \mathbb{Q}$ such that $a \cdot \frac{1}{a} = 0$.
- **Archimedean($<$)** : $\forall p > 0 \in \mathbb{Q} \exists n \in \mathbb{N}$ such that $0 < \frac{1}{n} < p$.

[1] Things that satisfy the list of properties with respect to $+, \cdot$ (but ignore the $<$ ones) that we listed above are called **rings**; you will see them in many many Mathcamp courses.

Again, you can view the rationals as what happens if you take the integers and add in all of the symbols you'd need to satisfy the multiplicative inverses property[2], along with the resulting things you get by multiplying/adding your new elements together. Note that because the rationals satisfy the same properties as the integers, we get "for free" that $0 \cdot \frac{a}{b} = 0$, for any rational $\frac{a}{b}$.

Finally, we move to the real number system:

Definition. The real numbers, denoted $\mathbb{R}$, have a lot of different definitions. The most common is probably the "infinite decimal sequence" definition, which we give below:

$$\mathbb{R} = \{a_0.a_1a_2a_3a_4\ldots : a_0 \in \mathbb{Z}, a_i \in \{0,\ldots 9\}, i \geq 1\}$$

In the above definition, we regard infinite strings of 9's, like $.999999999\ldots$, to be equivalent to a $+1$ in the next highest decimal place and replacing all of the 9's with 0's: for example, we ask that $.9999999\ldots = 1.000000\ldots$.

The real numbers satisfy all of the properties described above for $\mathbb{Q}$, along with the following remarkably useful property:

- **Completeness($<$)** :For any nonempty collection of elements S contained within $\mathbb{R}$ with an **upper bound,**there is a **least upper bound** $\alpha \in \mathbb{R}$ for that S.

Here, we say that a collection S of real numbers is **bounded above** if and only if there is some **upper bound** $M \in \mathbb{R}$, such that $\forall x \in S, x < M$; similarly, we say that a number α is a **least upper bound** for the set S if

- α is an upper bound for S, and
- Given any other upper bound M of S, either $\alpha = M$ or $\alpha < M$.

An alternate definition for the real numbers is to simply take $\mathbb{Q}$ and throw in all of the numbers required to satisfy our "completeness" property.

It is worth stating that this "completeness" property gives us real numbers that did not exist in $\mathbb{Q}$: i.e. there are rational numbers that are not real numbers! We prove this as follows (in a looser fashion than our earlier proofs, because citing all of the axioms other than our new one would be a pain to read.)

Claim 3. *There is a positive real number α such that $\alpha^2 = 2$.*

Proof. Let S be the collection of all positive numbers x such that x^2 is not greater than 2. We claim that S has an upper bound. There are lots of possible upper bounds for S; one easy choice is 2 (though we could also pick 3, or 25, or really anything else: we just want to find **some** upper bound.) To see that 2 is an upper bound, take any real number x such that $2 < x$. We have that

$$2 < 4 = 2 \cdot 2 < 2 \cdot x < x \cdot x = x^2.$$

[2]Similarly to how we defined **rings** as the kinds of objects that satisfied all of the $+, \cdot$ properties that $(\mathbb{Z}, +, \cdot)$ satisfied, we say that objects that satisfy all of the properties that $\mathbb{Q}$ satisfies (with respect to $+$ and $\cdot$, but not the $<$ ones) are called **fields**. Again, these come up everywhere.

Therefore, we know that x is not in our set S, because $x^2 > 2$. Consequently, any element in S must be such that $x < 2$: therefore, this collection has an upper bound.

We know that S is nonempty, because 1 is in it. Therefore, by completeness, it has a least upper bound: call it α. We claim that $\alpha^2 = 2$. We know that α has to be at least ≥ 1, because $1^2 = 1 < 2$ is in our set S.

To see why $\alpha^2 = 2$, take any real number $M \geq 1$ such that $M^2 \neq 2$.

There are two possibilities:

1. $1 \leq M^2 < 2$. In this case, consider the number $M + \frac{1}{n}$, for some natural number n. We know that $(M + \frac{1}{n})^2 = M^2 + \frac{2M}{n} + \frac{1}{n^2}$.

   We claim that there is some value of n for which this quantity is less than 2. In other words, we want

   $$2 - M^2 > \frac{2M}{n} + \frac{1}{n^2}.$$

   Because $\frac{1}{n^2} < \frac{1}{n} < \frac{M}{n}$, we know that $\frac{3M}{n} > \frac{2M}{n} + \frac{1}{n^2}$. However, we can easily find a value of n such that

   $$2 - M^2 > \frac{3M}{n}.$$

   Specifically, by dividing both sides by $3M$, we want to find a value of n such that

   $$\frac{2 - M^2}{3M} > \frac{1}{n},$$

   which we can do by using the Archimedean property, because the left-hand-side is positive. Therefore, we've shown that there is some $n \in \mathbb{N}$ such that $(M + \frac{1}{n})^2$ is also < 2.

   Note that this means that M cannot be a least upper bound, as we have found an element in our set S, $M + \frac{1}{n}$, that is greater than it.

2. $M^2 > 2$. In this case, consider the number $M - \frac{1}{n}$, for some natural number n. We know that $(M + \frac{1}{n})^2 = M^2 - \frac{2M}{n} + \frac{1}{n^2}$.

   We claim that there is some value of n for which this quantity is greater than 2. In other words, we want

   $$M^2 - 2 > \frac{2M}{n} - \frac{1}{n^2}.$$

   Because $-\frac{1}{n^2} < 0$, we know that $\frac{2M}{n} > \frac{2M}{n} + \frac{1}{n^2}$. However, we can easily find a value of n such that

   $$M^2 - 2 > \frac{2M}{n}.$$

   Specifically, by dividing both sides by $3M$, we want to find a value of n such that

   $$\frac{M^2 - 2}{2M} > \frac{1}{n},$$

which we can do by using the Archimedean property, because the left hand side is positive. Therefore, we've shown that there is some $n \in \mathbb{N}$ such that $(M - \frac{1}{n})^2$ is also greater than 2.

Note that this means that M cannot be a least upper bound, as we have found an element not in our set S, $M - \frac{1}{n}$, that is smaller than it.

What does this mean for our least upper bound, α? Well, because α is a least upper bound, our above arguments force α^2 to be equal to 2 and positive. So we've shown that there is a positive real number such that its square is 2! We call this the square root of 2, and denote it $\sqrt{2}$. □

Claim 4. *The $\sqrt{2}$ is not a rational number. In other words, there is no pair $a, b \in \mathbb{Z}$, $b > 1$, such that the greatest common factor of a and b is ± 1, such that $\frac{a^2}{b^2} = 2$.*

Proof. First, notice that because $1^2 = 1 < 2$ and $2 < 2^2 = 4$, we have that $\sqrt{2}$ is between 1 and 2. Therefore, the number $\sqrt{2} - 1$ is strictly between 0 and 1.

Take any pair of real numbers a, b, $b \neq 0$, such that $\frac{a}{b} = \sqrt{2}$. Then, we have

$$\begin{aligned}
\frac{a}{b} = \frac{a}{b} \cdot \frac{\sqrt{2}-1}{\sqrt{2}-1} &= \frac{a\left(\sqrt{2}-1\right)}{b\left(\sqrt{2}-1\right)} \\
&= \frac{a\left(\frac{a}{b}-1\right)}{b\left(\frac{a}{b}-1\right)} \\
&= \frac{a\left(\frac{2}{a/b}-1\right)}{a-b} \\
&= \frac{2b-a}{a-b}.
\end{aligned}$$

Therefore, given any fractional representation of the square root of 2 in the form $\frac{a}{b}$, we can always express it instead as a fraction of the form $\frac{2b-a}{a-b}$, which will always have a smaller (but still positive, because $\sqrt{2} > 1$ implies that $a > b$ for any such fraction) denominator.

Can this hold true for fractions? No! In fact, take any fraction of the form $\frac{a}{b}$ where a and b are integers with $b > 0$ and the GCD of a and b equal to 1. If $\frac{a}{b} = \frac{c}{d}$ for some other pair of integers with $d > 0$, we would have to have

$$ad = bc.$$

So, we have that b is a factor of ad; because a and b have no common factors, this in fact means that b is a factor of d, which forces $d > b$.

Therefore, this property does not hold for rational numbers; thus, we know that because the square root of two has this property, it cannot be a rational number. □