IAP Proofs Workshop 2021 Lectures 2-3

Laura Cui

January 2021

1 Lecture 2

A few logistical reminders: you should all be enrolled on Canvas in order to receive credit for the class. We will also post the materials on the UMA website, but problem sets will be submitted and returned through Canvas. The first problem set is already out, and will be due Friday night. Also, you can sign up for a mentor until the end of the day today! Your mentor can be a resource for this class as well as a guide to taking math classes or exploring related fields at MIT.

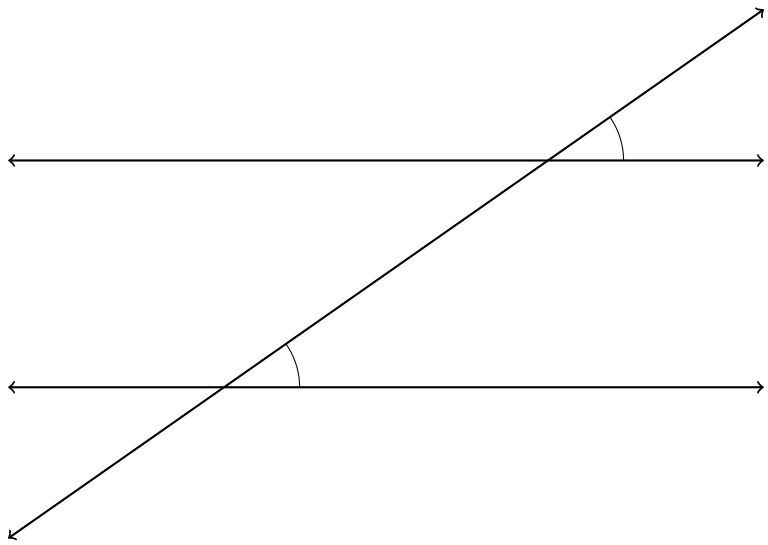
Also, today's lecture will include a lot of "mathematical foundations", which means you'll get a sneak peek at what's going on in the basement. However, just like in the tunnels of MIT, it's alright to be confused! If you like being confused, consider taking a logic class, which will go over these topics in much more depth.

1.1 Introduction to axioms

Last time, we introduced a lot of useful tools for working with mathematical objects. But how do we actually prove anything in math? It turns out that what we need are *axioms*, which are premises that serve as the starting point for all other theorems or facts that we prove.

Definition 1.1
An **axiom** is a proposition which is taken to be true without proof.

Axioms can consist of definitions, or describe "self-evident" properties. As an example, consider the following figure from geometry:



You may recall that if the two lines cut by the transversal are parallel, then the two marked angles must have the same measure. This fact is known as the *parallel postulate*, and is one of the axioms that defines Euclidean geometry, or geometry on a plane. Without it, we couldn't prove that the angles in a triangle sum to 180°—in fact, the sum of angles in a "triangle" on a spherical surface always exceeds 180°!

It's worth noting that we could specify planar geometry in different ways. For example, *Playfair's axiom*, which states that for every line ℓ and a point P not on that line, there is exactly one line through P parallel to ℓ, turns out to be equivalent to the original parallel postulate. However, any "good" set of axioms should be powerful enough to specify which world we live in, flat or spherical.

Keeping track of axioms becomes even more important when we work with more abstract mathematical ideas. If someone comes up to you on the streets and demands to know how many degrees are in his triangle, we can usually assume the triangle can be drawn on a flat plane, but as we'll see later on, these assumptions aren't always obvious.

1.2 The natural numbers

Now let's try to write down a list of axioms for the natural numbers. We can start by writing down the natural numbers[1] and thinking about their structure:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ...$$

You're probably familiar with the naturals as "counting numbers".[2] A natural way to think of these numbers is that they start at zero and keep incrementing by one. The most common definition of the natural numbers is known as the *Peano axioms*, and includes the concept of a *successor function* which maps each number to the next one:

[1] In mathematical texts, commas are included before and after ellipses (or, if the list goes on forever, just before)

[2] with the possible exception of zero, depending on who you ask

Definition 1.2 (Peano axioms)
We define the natural numbers as follows:

1. 0 is a natural number.
2. Every natural number n has a successor $S(n)$ which is also a natural number.
3. For any two natural numbers m, n, $S(m) = S(n)$ iff $m = n$.
4. For every natural number n, $S(n) \neq 0$.
5. **(Axiom of induction)** If a property holds for 0, and whenever the property holds for n it also holds for $S(n)$, then the property holds for all natural numbers.

Why are all of these axioms necessary? Recall that in the case of Euclidean geometry, when we removed the parallel postulate, we came up with geometries like spherical surfaces that satisfied the other postulates but didn't look how we wanted. Similarly, we can think of alternative number systems that satisfy some of these five axioms, but don't look quite right.

Example 1.3 (Alternative "number systems")
Here are some examples of "number systems" that don't satisfy all of the Peano axioms:

$$0 \to 1 \to 2 \to 3 \to 4 \circlearrowleft$$

$$0 \to 1 \to 2 \to 3 \to 4 \to \ldots$$
$$\clubsuit \to \diamondsuit \to \heartsuit \to \spadesuit \circlearrowleft$$

$$0 \to 1 \to 2 \to 3 \to 4 \to \ldots$$
$$\star \to \star\star \to \star\star\star \to \ldots$$

The arrows here are to help us visualize the successor of each number, rather than logical implication.

Next class, we'll look at another example of a number system similar to the natural numbers, but which doesn't satisfy all of the axioms!

We'll take a break here to refresh on mathematical symbols and notation. Remember that we should be able to express any mathematical statement in the notation we learned last class. Let's try writing our axioms in a more precise form:

Problem 1.4 (Breakout rooms, 8 minutes)
Translate the Peano axioms into formal mathematical statements using set notation, quantifier logic, and other appropriate logical symbols. (Hint: we can treat "satisfying a property" as equivalent to "belonging to a given set".

Solution

1. $0 \in \mathbb{N}$
2. $\forall n \in \mathbb{N}, S(n) \in \mathbb{N}$
3. $\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, S(m) = S(n) \Leftrightarrow m = n$
4. $\forall n \in \mathbb{N}, S(n) \neq 0$
5. $\forall K, [0 \in K \wedge (n \in K \rightarrow S(n) \in K)] \Rightarrow [\forall n \in \mathbb{N}, n \in K]$

By the way, we've used $\rightarrow$ and $\Rightarrow$ here to both denote implication. In logic, the convention is to use $\rightarrow$ for *formal* implication, such as a conditional phrase in a sentence, and $\Rightarrow$ for *meta-logical* implication, such as when writing down the main conditional in a theorem. However, some authors may choose to exclusively use $\Rightarrow$ for example if they work a lot with functions.

Also, we've written the fifth axiom in terms of sets to be more concrete, but alternatively, we can also use ϕ to represent any property which depends on some argument or number n. We can then rewrite the fifth axiom: $\forall \phi, [\phi(0) \wedge (\phi(n) \rightarrow \phi(S(n)))] \Rightarrow [\forall n \in \mathbb{N}, \phi(n)]$. For those who might be wondering, the fact that sets are completely defined by any predicate or condition on its members has a name as well—the *axiom of extensionality*, or axiom of extension, which is an axiom of set theory.

1.3 Arithmetic

Now that we have our numbers, we can also axiomatically define our familiar arithmetic operations, binary addition and multiplication. We can think of each of these as functions mapping two natural numbers to a natural number, which satisfy certain axioms of their own:

Definition 1.5 (Axioms of addition for natural numbers)
The sum of two numbers $f(a, b) = a + b$ is a function $f : N \times N \rightarrow N$ which satisfies:

1. $a + 0 = a$
2. $a + S(b) = S(a + b)$

Definition 1.6 (Axioms of multiplication for natural numbers)
The product of two numbers $f(a, b) = a \cdot b$ is a function $f : N \times N \to N$ which satisfies:

1. $a \cdot 0 = a$
2. $a \cdot S(b) = a + (a \cdot b)$

We will use the familiar addition and multiplication operators going forward, but it may help to think of operations as functions for some problems! Also, although this might seem like a roundabout way of defining addition (since we already know the successor function is equivalent to adding one), by defining them separately, we avoid some circular arguments later.

Problem 1.7
Show that $S(n) = n + 1$, where $1 = S(0)$.

Solution
From the second axiom of addition, we have for any natural number n, $n+1 = n+S(0) = S(n+0)$, which is equal to $S(n)$ by the first axiom. Thus $S(n) = n + 1$.

1.4 Mathematical induction

Hopefully by looking at some of the examples, we've all convinced ourselves why each of the Peano axioms are necessary. Out of the five axioms, the axiom of induction stands out since it requires us to quantify over sets, not just individual objects or numbers. In other words, while the first four axioms can be expressed in *first-order logic*, the axiom of induction requires *second-order logic*. A fun fact about logic (which you do not need to know how to prove!) is that there are no second order systems of axioms which are both *consistent* (do not admit logical contradictions) and *complete* (every true statement is provable). If you're interested in how to prove these kinds of facts in metalogic, consider taking a logic class!

In the meantime, as we'll see soon, the axiom of induction is also very useful for proving properties of natural numbers (or anything that can be put into a one-to-one correspondence with the natural numbers). This strategy is known as *proof by induction*, and is usually written in terms of three components:

Definition 1.8 (Proof by induction)
A **proof by induction** consists of the three main parts:

1. **Base case:** Show that the property holds for a particular value of $n = a$
2. **Inductive hypothesis:** Assume that the property holds for some value of n
3. **Inductive step:** Assuming the IH, show that the property holds for $n + 1$

Then applying the induction axiom to the property for $n - a$, the property holds for all $n \geq a$.

Example 1.9
Using induction, show that for any natural number n, a set of n elements has 2^n subsets.

Solution
Base case: A set of 0 elements has $1 = 2^0$ subset, the empty set.
Inductive hypothesis: Suppose for some $n \in \mathbb{N}$, a set of n has 2^n subsets.
Inductive step: Consider adding another element to the set. Then all of the subsets of the new set include all of the subsets of the original set, as well as each subset with the $n + 1$-th element appended. Thus we have $2(2^n) = 2^{n+1}$ total subsets. Therefore for all $n \in \mathbb{N}$, a set of n elements has 2^n subsets.

The axiom of induction also admits some important corollaries. Here's one:

Theorem 1.10 (Well-ordering principle)
Every non-empty set of natural numbers contains a least element.

The well-order principle turns out to be *logically equivalent* to the axiom of induction, so much like Playfair's axiom and the parallel postulate, we can use either one in our set of axioms. We won't prove the equivalence in lecture, but it's included as one of the challenge problems on the problem set for this week.

2 Lecture 3

By now those of you who signed up for a mentor should have gotten matched! Check your emails. Also, now that the class roster is more or less finalized, we'll have fixed breakout rooms (but as always, let the course staff know if you have any concerns or questions!). The second problem set will be released today, and is due this Friday at 11:59 PM Eastern.

Today we'll continue to practice with notation and proof by induction, and introduce modular arithmetic as well as rational numbers. It'll be a more concrete day, so you'll also get the chance

to work a bit more in breakout rooms. Also, from here on out, we'll use "natural numbers" and "non-negative integers" interchangeably, and we can assume that most of what we know about natural numbers extends to integers as well.

2.1 Modular arithmetic

Since all of you showed up to class on time, I'm assuming that you're familiar with clocks. Most civilians in the United States use a 12-hour clock, so elapsed time follows arithmetic *modulo* 12; that is, the same numbers will be on my clock 8 hours in the future as were 4 hours in the past.

Definition 2.1 (Congruence modulo n)
Given an integer $n > 1$, called a **modulus**, two integers a, b are **congruent** modulo n iff there is an integer k such that $a - b = kn$. We denote this as $a \equiv b \pmod{n}$.

Notice that although we can write $a = kn + b$, b does not need to be the *remainder* when a is divided by n.[3] However, we can define a *modulo* operation such that $a \mod n$ returns the remainder when a is divided by n:

Definition 2.2 (Modulo operation)
Given an integer $n > 1$, for any integer a there is a unique integer r such that $0 \leq r < n$ and there exists an integer k such that $a = kn + r$. Then $a \mod n = r$.

Definition 2.3 (Divisibility)
Given two integers a, b with $a > 0$, a **divides** b if and only if there is an integer n such that $na = b$. We write this as $a \mid b$.

[3] The parentheses signify that the modulus applies to the congruence equation, instead of just b.

Problem 2.4 (Breakout rooms, 6 minutes)
Write down answers to each of the following:

1. $13959344 \mod 4 = ?$
2. Find all values of a such that $5a \equiv 1 \pmod{17}$ and $0 \leq a < 17$.
3. Find a value of a such that $a \equiv -1 \pmod 8$ and $a \equiv 0 \pmod 9$.

Solution

1. 0, notice that since $100 \mod 4 = 0$, we only need to look at the last two digits
2. $a = 7$ is the only value which works
3. The smallest value which works is $a = 63$, though answers may vary

Even though it might seem fairly simple, modular arithmetic is a foundational concept in number theory and a powerful tool for working with integers. Modern cybersecurity relies on modular arithmetic for encryption!

Problem 2.5 (Breakout rooms, 8 minutes)
Prove that for any integer a, $a^2 \equiv 0$ or $1 \pmod 4$.

Solution
Note that all integers are congruent to either $0, 1, 2$, or $3 \pmod 4$. We can therefore consider four separate cases:

0. Consider an integer $a \equiv 0 \pmod 4$. We can write it in the form $4n$, for some integer n. Then $a^2 = 16n^2 = 4(4n^2)$. Since $4n^2$ is also an integer, we have that $a^2 \equiv 0 \pmod 4$.
1. Consider an integer $a \equiv 1 \pmod 4$. We can write it in the form $4n + 1$, for some integer n. Then $a^2 = 16n^2 + 8n + 1 = 4(4n^2 + 2n) + 1$. Since $4n^2 + 2n$ is also an integer, we have that $a^2 \equiv 1 \pmod 4$.
2. Consider an integer $a \equiv 2 \pmod 4$. We can write it in the form $4n + 2$, for some integer n. Then $a^2 = 16n^2 + 16n + 4 = 4(4n^2 + 4n + 1)$. Since $4n^2 + 4n + 1$ is also an integer, we have that $a^2 \equiv 0 \pmod 4$.
3. Consider an integer $a \equiv 3 \pmod 4$. We can write it in the form $4n + 3$, for some integer n. Then $a^2 = 16n^2 + 24n + 9 = 4(4n^2 + 6n + 2) + 1$. Since $4n^2 + 6n + 2$ is also an integer, we have that $a^2 \equiv 1 \pmod 4$.

Since we have covered all the cases, we have that for any integer a, $a^2 \equiv 0$ or $1 \pmod 4$.

On the problem set, you will see a few more examples working with modular arithmetic and related concepts. We will be moving on to other topics in lectures, but we're happy to discuss any of these topics in more detail during office hours or over email/Canvas message.

2.2 The rationals

The natural (no pun intended) extension of integers is the rationals, and you'll see why that is on this week's problem set. Most of you are familiar with rational numbers as everyday fractions, but here's the precise definition:

Definition 2.6 (Rational numbers)
A **rational number** is a number which can be expressed as the ratio of two integers p, q, where $q \neq 0$, and is written as p/q.

Problem 2.7 (Breakout rooms, 3 minutes)
Write the definition of the rationals in set-builder notation.

Solution
$\mathbb{Q} = \{p/q \mid p \in \mathbb{Z} \wedge q \in \mathbb{Z} \wedge q \neq 0\}$. We can also write $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z} \wedge q \in \mathbb{Z} \backslash \{0\}\}$.

In case you're curious why we use $\mathbb{Q}$ and $\mathbb{Z}$ for the rationals and integers, Q stands for quotient, and Z stands for *zahlen*, which is German for "number" or "integer".

One useful property of rational numbers is that they can always be expressed in "simplest form", also known as the *canonical form*.

Definition 2.8
For any two positive integers a, b, the **greatest common divisor** of a and b is the largest positive integer n such that $n \mid a$ and $n \mid b$.

Theorem 2.9 (Canonical form)
Any rational number can be written as the ratio of two unique integers p, q such that $q > 0$ and the greatest common divisor of $|p|$ and q is 1. (In other words, for any integer $n > 1$, n does not divide both $|p|$ and q.)

Problem 2.10 (Breakout rooms, 5 minutes)
Translate Theorem 2.9 into quantifier logic.

Solution
$\forall x \in \mathbb{Q}, \exists\, p \in \mathbb{Z} \wedge \exists\, q \in \mathbb{N}[q > 0 \wedge \forall n \in \mathbb{Z}(n > 1 \Rightarrow \neg(n \mid |p| \wedge n \mid q))]$

Notice that the greatest common divisor of two numbers is always well defined, since for any integer there must be a finite non-empty set of integers which divide it. The smallest element of this set is always 1, and the largest is itself. The intersection of two such sets therefore must also have a largest element. We will skip showing that the canonical form is unique, but the proof is very similar to another one that we'll see in the last part of class!

2.3 Beyond rationals: a sneak peak

As nice as fractions are, many numbers can't be expressed as the ratio of two integers. In fact, it turns out that almost all of the real numbers are *irrational*! We'll talk more about what the size of infinite sets means in a later lecture.

Another neat historical fact: the discovery of irrational numbers is usually attributed to one of Pythagoras' students, who is said to have drowned himself after the discovery out of denial. Hopefully proving it for yourself brings all of you joy rather than existential dread!

Theorem 2.11
$\sqrt{2}$ is irrational.

Proof
Suppose for the sake of contradiction that $\sqrt{2}$ is rational. Then from Theorem 2.9 that it can be written in the form $\sqrt{2} = p/q$ for two integers p, q, where $q > 0$ and the greatest common divisor of $|p|$ and q is 1. Squaring both sides, we have $2 = p^2/q^2 \implies p^2 = 2q^2$, so $2|p^2$. However, this means that p must be even, so there exists an integer a such that $p = 2a \implies p^2 = 4a^2 \implies 4a^2 = 2q^2 \implies q^2 = 2a^2$. But by the same logic, q must then also be divisible by 2, so 2 is a common divisor of p and q, which is a contradiction. Thus $\sqrt{2}$ cannot be rational.

This is one of the classic examples of a *proof by contradiction*, where we assume the opposite of what we're trying to prove, then show that it leads to a logical contradiction!

There are many surprising properties of irrational numbers. Here's one of them:

Theorem 2.12
There exist irrational numbers x, y such that x^y is rational.

Proof
Suppose for the sake of contradiction that the theorem is false, that is, for any two irrational numbers x, y, x^y is also irrational. Then since $\sqrt{2}$ is irrational, so is $\sqrt{2}^{\sqrt{2}}$. It must follow that $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$ is also irrational. However, $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$, which is rational, giving us a contradiction. Thus the theorem must be true.

There are a couple of other ways to prove this theorem. The one we've given here is an example of a *non-constructive proof*, which means that we've shown the theorem is true without saying anything directly about the value of $\sqrt{2}^{\sqrt{2}}$.