Lecture 1: Introduction and Proofs

Finley Holt

February 25, 2025

Notation Reference Table
Below is a quick reference for mathematical symbols used in these notes.

Symbol	Meaning
$\forall$	For all
$\exists$	There exists
$\in$	Element of
$\implies$	Implies
$\iff$	If and only if
$\mathbb{N}$	Set of natural numbers: {0, 1, 2, ...}
$\mathbb{Z}$	Set of integers: {..., -2, -1, 0, 1, 2, ...}

Table 1: List of Notation

1 What is a proof?

A proof is considered across multiple fields as a method for ascertaining the truth.

There are many ways to ascertain truth:

- Observation — we observe an apple falling from a tree and conclude that gravity exists.
- Sampling & counterexamples (showing the opposite rigorously enough that we conclude the opposite is true).
- Judges and juries make decisions on truths.
- The word of God (religion).
- In business, the customer is always right (the customer provides truth).
- In university, a professor can be the source of truth due to their authority (this does not hold in this course as anyone can win an argument in mathematics based on the merit of their argument).
- Inner conviction "There are no bugs in my code".
- "I don't see why not". Pushes burden of proof to the opposite perspective.

A **mathematical proof** is a verification of a **proposition** by a chain of logical deductions from a set of **axioms**.

1.1 Propositions

Definition 1. A **proposition** is a statement that is either *True* or *False*.

Example 1. The following is a simple mathematical proposition:

$$2 + 3 = 5$$

Example 2.

$$\forall n \in \mathbb{N}, \quad n^2 + n + 41 \text{ is prime}$$

Here, $\forall n \in \mathbb{N}$ signifies that the statement following the comma applies to all natural numbers n, and the predicate $n^2 + n + 41$ is prime is being evaluated for each such n.

Let's check if this predicate is true for every natural number n:

n	$n^2 + n + 41$	Prime?
0	41	Yes
1	43	Yes
2	47	Yes
3	53	Yes
⋮	⋮	⋮
20	461	Yes

Table 2: Checking the predicate for n from 0 to 20

This example presents some problems, but we checked 20 examples so it must be true, right? Wrong! For $n = 40$, the equation equals 1681 which equals 41^2. For $n = 41$, the proposition is also false, although 40 is the first breakpoint.

Example 3. Consider the proposition:

$$a^4 + b^4 + c^4 = d^4$$

This proposition states that there are no natural numbers a, b, c, and d such that the equation holds true. This proposition was conjectured to be true by Euler in 1769. It was unsolved for over 2 centuries until it was disproved by Noam Elkies. He came up with $a = 95,800$, $b = 217,519$, $c = 414,560$, and $d = 422,481$. Therefore we can conclude that:

$$\exists\, a, b, c, d \in \mathbb{N} \text{ such that } a^4 + b^4 + c^4 = d^4$$

Example 4.

$$313 \cdot (x^3 + y^3) = z^3 \text{ has no positive integer solutions.}$$

This turns out to be false but the shortest possible counter-example has over 1000 digits.

Why Does this Matter?
This is all very relevant to factoring. Factoring is the way to break crypto systems, most of which are based on number theory and more particularly factoring. If you can find solutions to things like this, you can get an angle and a wedge on factoring. This is why today, RSA uses thousand digit modulases instead of 100 digit modulases like they used to use. If you can break those crypto systems, you can't rule the world but you get close.

Example 5. *The regions in any map can be colored in 4 colors so that adjacent regions have different colors.*

This is known as the 4 Color Theorem, first conjectured by Francis Guthrie in 1853. Over the next century, many false proofs emerged. One of the most convincing was by Alfred Kempe in 1879, which relied on diagrams and was accepted for over a decade. Proofs by picture are often very convincing and very wrong. In creating the pictures, you constrain your thinking to a limit of possibilities that doesn't account for the whole parameter space. It wasn't until 1976 that Kenneth Appel and Wolfgang Haken proved the theorem using a computer to check 1,936 map configurations. This proof was controversial as it was the first major proof to use a computer, but it was later verified by other mathematicians.

Example 6. Every even integer, but 2, is the sum of 2 primes.

$$\text{Ex: } 24 = 11 + 13$$

This is called Golbach's conjecture, made in 1742. This is a very simple proposition and yet, it still remains unproven. It is listed by *The Globe* as one of the great unsolved mysteries.

Example 7.

$$\forall\, n \in \mathbb{Z}, \quad n \geq 2 \implies n^2 \geq 4$$

This statement is true because for any integer n that is greater than or equal to 2, the square of n will always be greater than or equal to 4.

Example of Implication:
Consider the statement: "If pigs fly, then I'm king".

- Let p be "pigs fly" and q be "I'm king".
- The implication $p \implies q$ is true if p is false or q is true.
- In reality, pigs do not fly (p is false). Therefore, the implication $p \implies q$ is true regardless of whether q is true or false.

Example 8.

$$\forall\, n \in \mathbb{Z}, \quad n \geq 2 \iff n^2 \geq 4$$

This statement is false for some values (e.g., if $n = 1$ or $n = 3$, the biconditional does not hold).

p	q	$p \implies q$	$q \implies p$	$(p \iff q)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Table 3: Combined Truth Table for Implications in Both Directions and the Biconditional

1.2 Axioms

Definition 2. An **axiom** is a *proposition* assumed to be *true*. The word axiom comes from Greek, meaning to think worthy.

Making assumptions while doing math is very important. They key in math is to identify your assumptions so that people can see them. The idea is that when you do a proof, anyone that agrees with your axioms must agree with your conclusion.

Example 9. Consider the following axiom: If $A = B$ and $B = C$, then $A = C$. There is no proof of this, but it seems pretty good so we throw it in the bucket of axioms and use it.

Example 10. Euclidean Geometry: Given a line L and a point p not on L, there is exactly one line through p that is parallel to L.

Example 11. Spherical Geometry: Given a line L and a point p not on L, there is no line through p that is parallel to L (on the sphere).

Example 12. Hyperbolic Geometry: Given a line L and a point p not on L, there are infinitely many lines through p that are parallel to L.

Note: The choice of axioms can vary depending on the field of study. In mathematics, different sets of axioms can lead to different geometries, as shown in the examples above. The key is to clearly state your axioms so that others can understand the foundation of your arguments. This flexibility allows for the exploration of various mathematical structures and theories.

Axioms should be:

- **Consistent:** A set of axioms is consistent if no proposition can be proven to be both true and false.
- **Complete:** A set of axioms is complete if it can be used to prove every proposition is either true or false.

In the 1930s, Kurt Gödel proved that there exists no consistent and complete set of axioms for all of mathematics. This is known as the *Incompleteness Theorem*. If you want consistency (which is a must), then there will be true facts that you will not be able to prove.