Math 220 Fall 2021, Lecture 1: What is a proof?

In this course, we will explore the concept of a proof and you will learn how to tell a proof from a non-proof.

We will not follow any single text; I'll try to mix and match. I'm gravitating towards [LeLeMe], but that won't take us through the entire quarter.

0.1. (De)motivating examples

When you divide an odd integer by 4 with remainder, what can the remainder be? 1 or 3.

Definition 0.1.1. We say that an odd integer is 1**-odd** if its remainder (when divided by 4) is 1.

We say that an odd integer is 3**-odd** if its remainder (when divided by 4) is 3.

Example: The number 13. Is it 1-odd or 3-odd? It is 1-odd, because

$$13 = \underbrace{3}_{\text{the quotient}} \cdot 4 + \underbrace{1}_{\text{the remainder}}.$$

So the 1-odd and the 3-odd integers alternate when you count upwards from 1.

Now, fix a positive integer n, and consider the positive divisors of n. These are the positive integers that you can evenly divide n by (i.e., the positive integers d such that n is an integer multiple of d).

Example: The positive divisors of 6 are $1, 2, 3, 6$.

The positive divisors of 18 are $1, 2, 3, 6, 9, 18$.

[https://sagecell.sagemath.org/]

Now, let's play a game. Fix a positive integer n. Among the positive divisors of n, we count the 1-odd and the 3-odd ones.

For example, for $n = 18$, we find two 1-odd posdivs (= positive divisors), and one 3-odd posdiv.

Some experiments suggest that the # of 1-odd posdivs of n is always $\geq$ (i.e., at least as large as) the # of 3-odd posdivs of n.

(The symbol # means "number".)

Conjecture 1. Let n be a positive integer. Then, n has at least as many 1-odd posdivs as it has 3-odd posdivs.

We can easily check by computer that this is true, e.g., for all $n \in \{1, 2, \ldots, 2000\}$ (this means "for all n ranging from 1 to 2000").

But does this mean it is true for all n ? Could there be exceptions?

Let us study a similar question.

Definition 0.1.2. A **prime number** (or, short, **prime**) is an integer n that is larger than 1 and has the property that its only posdivs are 1 and n itself.

The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

There seem to be infinitely many primes: the further you look, the more you find (although they seem to get sparser as you move up the numbers).

Almost all of the primes are odd. Indeed, the only even prime is 2, because for any even number larger than 2, the divisor 2 would prevent it from being prime.

How many primes are 1-odd? How many are 3-odd?

Conjecture 2. Let n be a positive integer. Then, there are at least as many 3-odd primes up until n as there are 1-odd primes.

This seems equally plausible as Conjecture 1. Experiments work well until you hit $n = 26863$. Then, suddenly, there are more 1-odd primes than there are 3-odd primes!

So we know that Conjecture 2 is **false**. We have **disproved** it using what is called a **counterexample** (an example where it is false). In our case, the counterexample was to choose $n = 26863$. This specific conjecture is known as **Chebyshev's bias**.

What about Conjecture 1? We can check using Sage that it's true for all $n \leq$ 500 000, but does this convince us that it's always true?

We can try to understand why it is true (if it is). In other words, we look for a reason why it should be true.

For an example, take $n = 225$. The posdivs of $225 = 3^2 \cdot 5^2$ are $1, 3, 5, 9, 15, 25, 45, 75, 225$. We can arrange them as a table:

$$\begin{array}{ccc} 1 & 3 & 9 \\ 5 & 15 & 45 \\ 25 & 75 & 225 \end{array} .$$

What is special about this arrangement is that whenever you go 1 step right, you multiply by 3, and whenever you go 1 step down, you multiply by 5.

This kind of reasoning has its limits: How do you know that the posdivs of n always fit into this kind of table? (Actually, they only do if you understand the word "table" liberally: you have to allow multidimensional tables.)