WORKSHEET 2: WHAT IS A PROOF?

MATH 2106-D

At first glance, you may think mathematics is about *theorems*, facts about objects like numbers, functions, and patterns. For example, you have seen big theorems in Calculus, like the Fundamental Theorem of Calculus, or the Intermediate Value Theorem. Roughly speaking, this is true. The goal of mathematics is to collect and expand our knowledge of such results. However, as often in life, the journey is just as important as the destination, and a theorem means nothing (and in fact, is *not* a theorem without a proof.

Proofs are the jewels of mathematics, namely, they are what makes mathematics "tick." You may think that some results are "obvious," and therefore don't require a proof. However, proofs are essential for two main reasons. Firstly, "obvious" things may turn out to be false. For example, the assumption in the ancient Greek paradox due to Zeno is that it is "obvious" that the sum of infinitely many positive numbers is infinite (of course, you now know this to be false). As another typical example, if you conjectured, as Euler did in 1769, that there are no positive integers a, b, c, d such that $a^4+b^4+c^4 = d^4$. You might at first make a guess as to whether this is true by taking out a computer and *searching* for an example. However, if you searched in a range requiring $a, b, c, d \leq 400,000$, which is $2.56 * 10^{22}$ choices to look through, you will not find a single counterexample. Hence, you would be forgiven for believing that Euler was right. However, in 1986, Noam Elkies found a counterexample (although his was larger than the smallest counterexample, found later by Roger Frye).

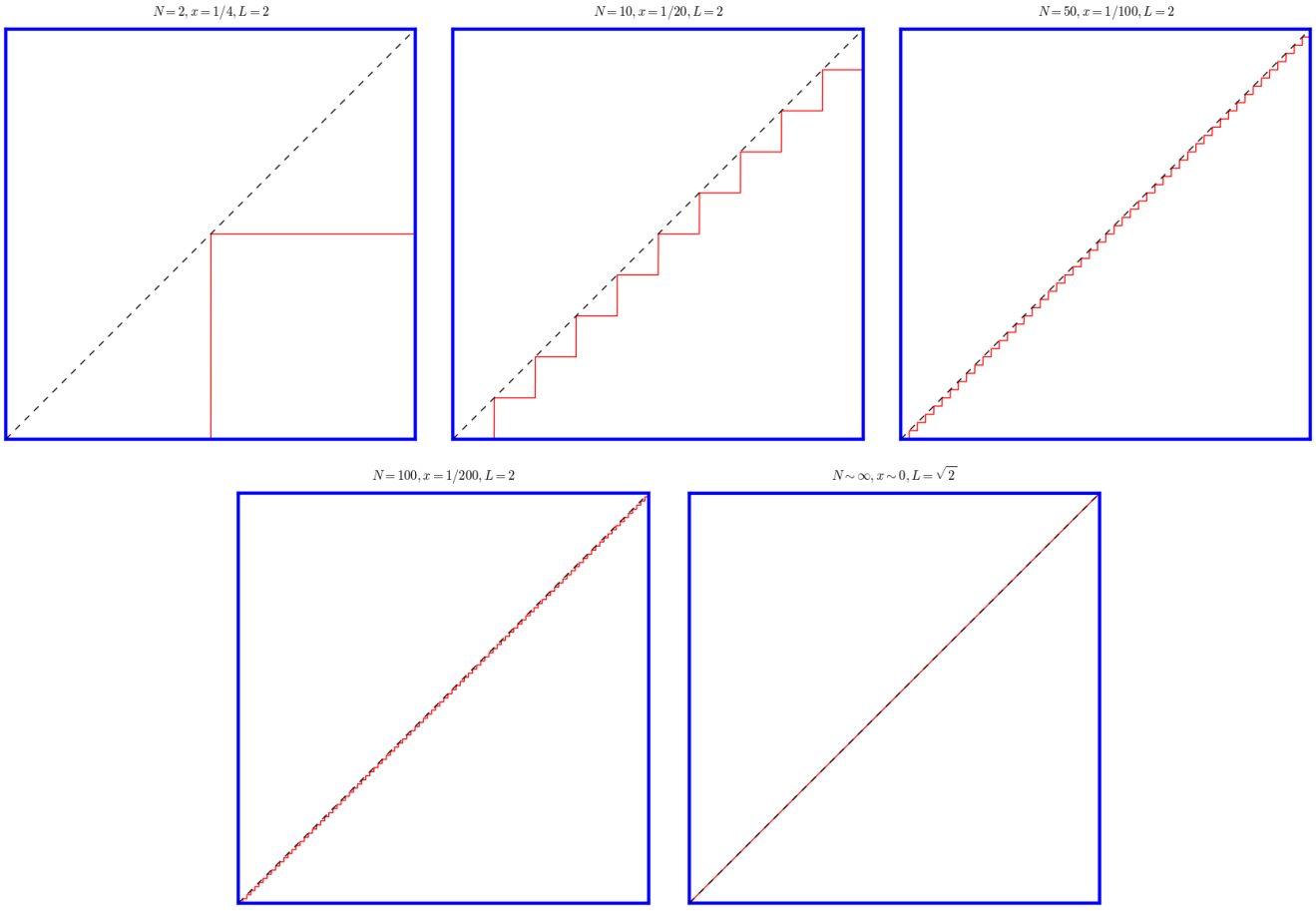
Proofs also give insight into *why* something is true, and lead to new discoveries and to new paths of inquiry. As Sir Michael Atiyah said about the mathematical rock star Gauß, "I think it is said that Gauß had ten different proofs for the law of quadratic reciprocity. Any good theorem should have several proofs, the more the better. For two reasons: usually, different proofs have different strengths and weaknesses, and they generalise in different directions – they are not just repetitions of each other."

Proofs can be easy, proofs can be hard (requiring tens of thousands of pages by around 100 authors in the case of the classification of finite simple groups ...), and moreover, proofs can be illuminating, or just tedious checking of mundane things.

(1) To know what is a proof, we first have to know what *isn't* a proof. Consider the following "proof" that the length of the diagonal of a unit square is 2, even though we know by the Pythagorean theorem that it is $\sqrt{2}$.

Let N be a positive integer. Consider the following path from the lower left corner of the square to the upper right corner. First go right a distance of $1/N$ units, then go up the same distance, then right, etc., until you reach the opposite corner (see the pictures below for several N). Then notice that there are always $2N$ segments of this path, each of length $1/N$, so the overall length of this path is always 2 (intuitively, if you drive between two points along streets arranged in a sqare grid pattern, the distance you must travel to get between the points is always the same no matter how narrow the blocks are). As the pictures below indicate, this path, for large N, is indistinguishable from the diagonal of the

square for very large N, and so the limit of the paths as $N \to \infty$ seems to be the diagonal itself. Thus, the diagonal should have the same length, that is, 2.



Explain why this argument is wrong, and why this is *not* a valid proof.

(2) Consider the *triangular numbers*, given by $T_n = 1 + 2 + \ldots + n = \sum_{j=1}^{n} j$. Show that $T_n = n(n+1)/2$ in the following way. First write out the numbers $1 + \ldots + n$ on the page. Now write the sum of the same numbers on a line below this sum, but write them *backwards*. Notice something about the columns of this array of numbers, and use this to deduce the final formula.

(3) Show that for every $m \in \mathbb{Z}$, $3|(m^3 - m)$. Do this by considering the three cases: $x = 3n$ for some integer n, $x = 3n + 1$ for some integer n, $x = 3n + 2$ for some integer n (why does this suffice?). Do you think that $4|(m^4 - m)$ divides for all integers m? What about the claim that $5|(m^5 - m)$?

(***) Can you discover a similar formula for $\sum_{j=1}^{n} j^2$? Can you *prove* it?