# WHAT ARE MATHEMATICAL PROOFS AND WHY THEY ARE IMPORTANT?

## INTRODUCTION

Many students seem to have trouble with the notion of a mathematical proof. People that come to a course like Math 216, who certainly know a great deal of mathematics - Calculus, Trigonometry, Geometry and Algebra, all of the sudden come to meet a new kind of mathematics, an abstract mathematics that requires proofs. In this document we will try to explain the importance of proofs in mathematics, and to give a you an idea what are mathematical proofs. This will give you some reference to check if your proofs are correct. We begin by describing the role of proofs in mathematics, then we define the logical language which serves as the basis for proofs and logical deductions. Next we discuss briefly the role of axioms in mathematics. Finally we give several examples of mathematical proofs using various techniques. There is also an excellent document on proofs written by Prof. Jim Hurley (liknked to the course homepage), and I recommend to all of you to read his document as well. You will find there more examples and additional explanations. It is my hope that reading these documents will make your first steps in writing proofs easier.

## 1. The importance of Proofs in mathematics

It is difficult to overestimate the importance of proofs in mathematics. If you have a conjecture, the only way that you can safely be sure that it is true, is by presenting a valid mathematical proof. For example, consider the following well known mathematical theorem:

**Theorem 1** (Euclid)**.** *There are infinitely many prime numbers.*

For those of you who don't remember, a prime number is a positive integer $p > 1$ that cannot be written as a product of two strictly smaller positive integers $a$ and $b$. For example, the number 91 is not prime since it can be written as $91 = 13 \cdot 7$, but 67 is a prime. Although most people have a hunch that there are infinitely many primes, it is not obvious at all. Even today with the powerful computers, all we can do is to verify that there are very large prime numbers, but we still can say nothing about the existence of prime numbers whom size is beyond the ability of the current computers. The only reason that we are one hundred percent sure that the theorem is true, is because a mathematical proof was presented by Euclid some 2300 years ago. We shall give his proof later.

Another importance of a mathematical proof is the insight that it may offer. Being able to write down a valid proof may indicate that you have a thorough understanding of the problem. But there is more than this to it. The efforts to prove a conjecture, may sometimes require a deeper understanding of the theory in question. A mathematician that tries to prove something may gain a great deal of understanding and knowledge, even if his/her efforts to prove that conjecture will end with failure. The following theorem, is due to the giant German Mathematician Karl Friedrich Gauss, and is called the Fundamental Theorem of Algebra.

**Theorem 2** (the Fundamental Theorem of Algebra)**.** *Let $p(x)$ be a non constant polynomial whose coefficients are complex numbers. Then the equation $f(x) = 0$ has a solution in complex numbers.*

In particular this means that equations like $x^6+x^5-3x^2+1 = 0$ have a complex solution, a non trivial fact. The proof that Gauss gave relies heavily on the fact that the complex numbers form a two dimensional plane. In fact, to understand the idea behind the theorem, we need to incorporate knowledge from a seemingly unrelated area of mathematics – Topology. Topology, like usual geometry deals with shapes, but unlike geometry, the shapes are not rigid and may be deforemd (This is a very unproffesional definition). For example, a cube and a ball are topologically equivalent, but both are not equivalent to a donut. The topological fact used by the proof is that if you have two rubber bands lying on a plain, one of them is surrounding a nail stuck in the plane, and the other isn't, then you cannot bring the first rubber band to the situation of the second one without lifting it off the plane or opening it. Using this fact in an ingenious way, where the plane is the plane of complex numbers, gave a proof to the above algebraic. What was demonstrated here is that trying to prove something may lead to a deeper knowledge and to relations to other fields of mathematics. Interestingly, there are additional proofs to the same theorem, each coming from a completely different approach and mathematical knowledge, and it is a challenge to try to understand them all as parts of a bigger picture. The fundamental theorem itself can be used to give a complete explanation why people failed to create a three or more dimensional number system with the $+, -, \cdot, \div$ operations (what we will call a 'Field' later in the course). Understanding the ideas behind the theorem lead to the understanding why the complex numbers are so fundamental in mathematics (this was not recognized by the contemporaries of Gauss).

Part of the difficulties of people in understanding the notion of proofs stem from the fact that people do not have the right picture of what mathematics is. From elementary school through the first years of college we teach people that the goal is to solve an equation or to find a minimum of a function or to find how much wheat we should grow. This is of course something that mathematics can do, but it is not what mathematics is about. Mathematics is about understanding the laws behind numbers, algebra and geometry. It is about finding new and non routine ways to look at these systems and to explain strange phenomena that we may encounter. To make it more interesting, we can even change the laws to create new systems and then study them. An example for such a new system is the notion of a 'Group', that we shall study in this course. Some of these new systems, like groups, shed light on the old ones. Groups have been found to be a necessary utility in understanding questions in number theory, algebra, ,topology, geometry, and modern physics. There is a whole new world of ideas, understanding and discoveries that is invisible to people who only know how to differentiate a function. To enter to this world, it is necessary to use the ideas of abstraction and mathematical proof.

## 2. What are Mathematical Proofs?

2.1. **The rules of the game.** All of you are aware of the fact that in mathematics 'we should follow the rules'. This is indeed the case of writing a mathematical proof. Before we see how proofs work, let us introduce the 'rules of the game'.

Mathematics is composed of statements. The *Law of the excluded middle* says that every statement must be either true of false, never both or none. If it is not true, then it is considered to be false. For example, consider the statement $y = x^2$. In real life's terminology, like with most statements, it is sometimes true and sometimes false. In mathematics it is false since it is not completely true. Take for example $y = 1$ and $x = 2$.

We can make up new statements from old ones. If $P$ and $Q$ are statements, then we have.

| Statement | Notation |
|---|---:|
| $P$ and $Q$ | $P \wedge Q$ (or $P\&Q$) |
| $P$ or $Q$ | $P \vee Q$ |
| If $P$ Then $Q$ (or $P$ implies $Q$) | $P \implies Q$ |
| $P$ if and only if $Q$ (or $P$ and $Q$ are equivalent) | $P \iff Q$ |
| not $P$ | $\neg P$ |

The statement $P \wedge Q$ is true if and only if both $P$ and $Q$ are true. The statement $P \vee Q$ is true if and only if *at least* one of the statements $P$, $Q$ is true. This is what we called the *inclusive or* as opposed to the *exclusive or* that we use in everyday's life. For example, the statement: 'We will have class in the morning or in the afternoon' means in real life that only one of the alternatives will take places (exclusive or). In mathematics however, this includes the possibility that we will have class in the morning as well as in the afternoon (inclusive or). $P \implies Q$ is considered to be false only in the case that $P$ is true and $Q$ is false. Otherwise it is true. This is also in contrast to the plain English. For example, a statement like: 'If it rains now then 2 is a prime number' is mathematically true, despite the fact that there is no relation between the two parts of the statement, and regardless of whether the first part is true or not.
The statement $P \iff Q$ is true if and only if $P$ and $Q$ have the same truth values. We also say that $P$ and $Q$ are equivalent. Finally, $\neg P$ is true if and only if $P$ is false.
Using the above operations we can make more complex statements like

$$((\neg(P \implies Q) \vee (T \wedge P)) \iff (R \implies \neg T).$$

Two additional players in this game are the quantifiers, $\forall$ which means 'for all', and $\exists$ which means 'there exists'. For example, the statement

$$\forall x > 0 \; \exists y (y^2 = x),$$

reads: For all $x > 0$ there exists $y$ such that $y^2 = x$. Let us denote by $\mathbb{Z}^+$ the set of all positive integers. The following statement about

$p \in \mathbb{Z}^+$ says that $p$ is a prime:

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ [p = ab \implies (a = 1) \vee (b = 1)].$$

2.2. **Tautologies and Contradictions.** Logical deductions are based *tautologies.* If we try to give an informal definition, a tautology is a general statement that is true under all possible circumstances. Examples are $P \implies P$, $P \vee \neg P$, *Modus Ponens*: $[P \wedge (P \implies Q)] \implies Q$ or another form of Modus Ponens: $[(P \implies Q) \wedge (Q \implies R)] \implies (P \implies R)$. Notice that the truth of each of these statements is independent of whatever are $P$ and $Q$ and $R$ and whether they are true or false. We can establish a tautology by our understanding of the statement or by constructing a truth table.

A logical deduction is obtained by substituting in a tautology. For example, look at the following deduction:

> All fish are living creatures; All living creatures can move; Therefore all fish can move.

This logical deduction is a substitution in the second form of Modus Ponens where $P$='$x$ is a fish'; $Q$='$x$ is an living creature'; $R$='$x$ can move'.

On the other extreme of logical statements are the *contradictions.* Contradictions are false under all circumstances. In fact every contradiction is the negation of a tautology, and conversely, every tautology is the negation of a contradiction. A typical contradiction is $P \wedge \neg P$. Try to think yourself of some other examples.

2.3. **Axioms.** As it turns out, to prove something requires the knowledge of some previous truths. Logic just supplies the ways that we can deduce a statement from others, but we need some statements to begin with. These initial statements are called axioms. There are two layers of axioms: The axioms of set theory, and the axioms of the mathematical theory in question.

Modern mathematics is based on the foundation of set theory and logic. Most mathematical objects, like points, lines, numbers, functions, sequences, groups etc. are really sets. Therefore it is necessary to begin with axioms of set theory. Very fundamental to set theory is the set of positive integers $\mathbb{Z}^+$, which has the natural order relation on it. The *Well ordering principle* is an axiom which says that every nonempty subset of $\mathbb{Z}^+$ has a smallest element. You will find it very difficult to resist to this statement, however, it is considered an axiom without proof. This axiom turns out to be equivalent to the principle of mathematical induction (cf. your textbook p. 4). The axioms of set theory form the basic layer of axioms. It needs to be said that some of the axioms of set theory, like the well ordering principle, are accepted only for being highly intuitive, and have been debated among mathematicians.

On top of this, we have the axioms that define the theory in questions. For example, in geometry we have the axiom which states that *one straight line and only one straight line can pass through two given distinct points.* In modern mathematics there is no point with arguing with such an axiom. If it does not hold, we simply cannot call the objects by the names 'straight line' and 'point'. The axioms serve here as definitions that characterize that mathematical system in question. A mathematical theory is like a chess game and the axioms correspond to the rules of the game. If you don't accept a rule, this is not chess any more. The only kind of debates is to whether the theory is mathematically fruitful or interesting.

2.4. **Proofs.** A proof of a theorem is a finite sequence of claims, each claim being derived logically (i.e. by substituting in some tautology) from the previous claims, as well as theorems whose truth has been already established. The last claim in the sequence is the statement of the theorem, or a statement that clearly implies the theorem. We wish now to give some examples that will illustrate how this works in practice, as well as some techniques of proofs. You can find more examples in the document of Prof. Hurley

**Direct Proofs:** Many theorems are of the form $P \implies Q$, that is, of the form *If ... Then ...* . We begin by assuming $P$ (as well as other established truths) and proceed by using a sequence of Modus Ponenses to derive new statements, the last statement being $Q$. Alternatively we use the second form of Modus Ponens and a sequence of implications to derive $P \implies Q$. Here is an example:

**Theorem 3.** *For any two positive numbers $x$ and $y$,*

$$(*) \quad \sqrt{xy} \le \frac{x+y}{2}.$$

*Proof.* Suppose that $x$ and $y$ are positive numbers. Then $(\sqrt{x}-\sqrt{y})^2 \ge 0$. By algebra this implies that $x+y-2\sqrt{x}\sqrt{y} \ge 0$. Moving $2\sqrt{x}\sqrt{y}$

to the other side we get that $x + y \geq 2\sqrt{xy}$. Dividing both sides by 2 yields the inequality $(*)$ of the theorem as desired. □

Notice that we have used implicitly some general truths from algebra, like $\sqrt{x}\sqrt{y} = \sqrt{xy}$, in conjunction with the statements of the proofs. The use of external knowledge becomes more and more necessary as we go further in developing a theory.

More complex proofs require nested sequences of Modus Ponenses.

**Theorem 4.** *Let $A$ and $B$ be two sets. If $A \cup B = A \cap B$ then $A \subseteq B$.*

*Proof.* Assume that $A \cup B = A \cap B$. We shall prove that $x \in A \implies x \in B$, which by definition is equivalent to the consequence of the theorem. Assume that $x \in A$. Since $A \subseteq A \cup B$, then $x \in A \cup B$. We assumed that $A \cup B = A \cap B$, so $x \in A \cap B$. Finally, $A \cap B \subseteq B$, so consequently, $x \in B$. This concludes the proof □

Notice that we did not end the proof with the consequence of the theorem, but rather with a statement that suffices to imply the theorem by our earlier understanding. Here also we used implicitly some definitions from set theory, like $(x \in D) \wedge (D \subseteq C) \implies (x \in C)$.

Notice that we have made a substential use of the English language. To be absolutely sure that our proofs are valid, we must use the symbolic language and list down all the claims that we used, including the knowledge from algebra or set theory, and to check that the implications really follow from tautologies. This however, will make the proofs cumbersome and more difficult to understand. We choose to resolve this dilemma by using the English language, but in a very limited way, so that the deductions will include only the necessary 'logical' words like 'if','then', 'suppose', 'consequently','or' etc. This, together with some intelligence, makes us quite convinced that our proofs are without flaws, and that if we wish, it would be possible to rewrite the proof in the symbolic structural language.

**Proofs by Negation:** This is another strategy of proving a theorem $P \implies Q$. We begin by assuming that $P$ is true and $Q$ is false i.e. we assume $P \wedge \neg Q$. The proof proceeds until we derive contradiction $F$. This completes the proof, since something must be wrong and the only questionable thing was our assumption $P \wedge \neg Q$. Thus if $P$ is true, $Q$ must be true too. Technically, we have based our proof scheme on the tautology:

$$[(P \wedge \neg Q) \implies F] \implies [P \implies Q],$$

where $F$ is a contradiction. Here is an example:

**Theorem 5.** *There are infinitely many prime numbers*

Notice that we can view the theorem as an If-Then theorem by claiming that if $S$ is the set of prime numbers then $S$ is an infinite set.

*Proof.* Suppose, by negation, that the set $S$ of prime numbers is finite. Then we can write it as the set $\{p_1, p_2, \dots p_n\}$ where $p_1, p_2, \dots, p_n$ are distinct numbers. The product $N = p_1 p_2 \cdots p_n$ is clearly a multiple of each of the numbers $p_1, p_2, \dots, p_n$. Therefore, the number $N + 1$ is not a multiple of neither $p_1, p_2, \dots, p_n$. On the other hand, by the fundamental theorem of arithmetic (see textbook p. 6), $N + 1$ is a product of prime numbers so it is a multiple of at least one prime number. This is a contradiction because $N + 1$ is not a multiple of $p_1, p_2, \dots, p_n$ which are *all* the prime numbers. The proof is complete. □

**Mathematical Induction** Suppose that we have a sequence of claims $P(1), P(2), \dots$ and we wish to prove them all at once. This amounts to the claim $\forall n P(n)$ (i.e. For all $n$, $P(n)$ is true). Rather then proving this directly, we can use the principle of mathematical induction:

$$P(1) \wedge \forall n[P(n) \implies P(n+1)] \quad \implies \quad \forall n P(n).$$

In words, this means as follows:
*Suppose that we have proved the following two statements:*

(1) [The induction basis] $P(1)$ *is true, and*
(2) [The induction step] *For all* $n$*, if* $P(n)$ *is true, then* $P(n+1)$ *is true*

*Then for all* $n$*,* $P(n)$ *is true.*

The induction principle makes sense because upon establishing the statements $P(1)$, $P(1) \implies P(2)$, $P(2) \implies P(3)$, etc., we can use a sequence of Modus Ponenses to establish $P(2), P(3)$ and so on.

As we mentioned above, the principle of mathematical induction may be seen as a consequence of the well ordering principal. It turns out that the converse is also true, namely, that the well ordering principal can be proved from mathematical induction. In some mathematical literature the induction principle is taken to be an axiom rather than the equivalent well ordering principle.

We shall now give an example. Suppose that we want to show that for every $n \in \mathbb{Z}^+$, the number $17^n - 10^n$ is divisible by 7. We will prove this by induction. Let $P(n)$ be the claim that $17^n - 10^n$ is divisible by

7. First, if $n = 1$, then $17^1 - 10^1 = 7$ so $P(1)$ is true. Secondly, assume that $P(n)$ is true. We shall now prove that this implies that $P(n+1)$ is true. We compute:

$$17^{n+1} - 10^{n+1} = 17 \cdot 17^n - 10 \cdot 10^n = (7+10) \cdot 17^n - 10 \cdot 10^n = \\ = 7 \cdot 17^n + 10 \cdot 17^n - 10 \cdot 10^n = 7 \cdot 17^n + 10 \cdot (17^n - 10^n).$$

Now, $7 \cdot 17^n$ is clearly divisible by 7. By the induction hypothesis, $17^n - 10^n$ and so $10 \cdot (17^n - 10^n)$ is divisible by 7. By the computation above we have shown that $17^{n+1} - 10^{n+1}$ is divisible by 7. By the induction principle we are done.

There is a slightly different version of induction, where the induction step (2) is replaced with
(2)' *If $P(k)$ is true for all $k \leq n$, then $P(n+1)$ is true*
In some situations like the following one, the latter version applies rather than the usual version. Suppose that we play the following game. You are given a pile of $N$ matches. You break the pile into two smaller piles of $m$ and $n$ matches. Then you form the product $2mn$ and remember it. Next, you take one of the piles and break it into two smaller piles (if possible), say of $m'$ and $n'$ matches. You form the product $2m'n'$ and add it to the $2mn$ that you had before, so now you have $2mn + 2m'n'$. You proceed again by breaking one of the piles into two and adding the resulting product. The process is finished when you finally have $N$ piles of one match in each. By convention, if $N = 1$ then you don't do anything and the result is 0. Try to take a pile of five matches and play this game several times, each time breaking to piles in a different way. What do you see? In fact the following theorem is true:

**Theorem 6.** *If you start from a pile of $N$ matches, no matter how you break it, the sum of the computed products will always be $N^2 - N$.*

*Proof.* We will use the second version of induction on $N$. First, if $N = 1$ then the resulting sum is $0 = N^2 - N$. If $N = 2$ then there is only one way to break it, namely to $m = 1$ and $n = 1$ so that we end up with $2mn = 2 = N^2 - N$. Assume that $N \geq 2$ and the theorem is true for all $k \leq N$. To prove the theorem for $N + 1$, we begin with a pile of $N + 1$ matches and break it into two plies of $m$ and $n$ matches, so that $N + 1 = m + n$. By the induction hypothesis, breaking up the $m$ pile will contribute to the sum $m^2 - m$, and similarly the second pile will contribute $n^2 - n$, no matter how we continue to break them. Therefore the total sum is $2mn + (n^2 - n) + (m^2 - m)$. A little algebra shows that this equals to $(m+n)^2 - (m+n) = (N+1)^2 - (N+1)$ as desired. □

**The Pigeon Hole Principle:** is a frequently used principle in finite mathematics and is often used in proofs of existence. To illustrate the principle (and explain its name), suppose that you have $n$ pigeon holes, but more than $n$ pigeons. If you are to put all your pigeons in the holes, then the pigeon hole principle says that in at least one pigeon hole you will have to put more than one pigeon. To state this in a more mathematical language, recall that if $A$ is a finite set, then the *order of* $A$, which is denoted by $|A|$, is the number of elements in $A$. The pigeon hole principle will say that if $A$ and $B$ are finite sets with $|A| > |B|$ and $f : A \to B$ is a function, then $f$ is not one to one, i.e. there exist $x, y \in A$, $x \neq y$, such that $f(x) = f(y)$.

Here is an example. Suppose that you take the numbers $1, 2, \ldots, 10$ and rearrange them as you like. As you know there are $10! = 3,628,800$ different rearrangements. After you have rearranged, you look for the longest partial sequence, which is rearranged by ascending or descending order. For example, if you have rearranged the numbers to have $4, 3, 6, 5, 9, 10, 1, 7, 2, 8$ you notice that the partial sequence $4, 3, 5, 7, 8$ is in ascending order. If you look hard enough you will not find a longer ascending/descending partial sequence. Your goal is to rearrange the numbers in the 'most effective way' so that the longest ascending/descending partial sequence is the shortest possible. How well can you do? The following theorem gives the answer:

**Theorem 7.** *In any rearrangement of the numbers* $1, 2, \ldots, 10$*, there is always a partial sequence of four numbers which is ordered in an ascending or descending order.*

*Proof.* We will prove this existence theorem using the pigeon hole principle. Pick up any rearrangement and let the rearranged numbers be $x_1, \ldots, x_{10}$. To each index $1 \leq i \leq 10$, let $a(i)$ be the length of the longest ascending partial sequence that ends with $x_i$, and let $d(i)$ be the length of the longest descending partial sequence that begins with $x_i$.

We claim that if for two indices $i$ and $j$, $a(i) = a(j)$ and $d(i) = d(j)$, then necessarily $i = j$. Indeed suppose by negation that $i \neq j$. Then of course $x_i \neq x_j$ and there are two cases: (i) $x_i < x_j$, in which we could append $x_j$ to the longest ascending sequence ending in $x_i$ and thus get yet a longer ascending sequence ending in $x_j$ which shows that

$a(j) > a(i)$. In case (ii), $x_i > x_j$ and a similar argument shows that now $d(i) > d(j)$. In either cases there is a contradiction to our assumption that $a(i) = a(j)$ and $d(i) = d(j)$.

Suppose by negation that in our rearrangement the longest ascending/descending partial sequence consists of less than 4 numbers. Then clearly for each $i$, $a(i)$ and $d(i)$ can only have the values of 1 or 2 or 3. Then we have a function

$$f : \{1, \dots, 10\} \to \{(1,1), (1,2), (1,3), \dots, (3,2), (3,3)\},$$

given by $f(i) = (a(i), d(i))$. Now $f$ is a function from a set of 10 elements to a set of 9 elements. By the pigeon hole principle, $f$ is not one to one, and there exist indices $i \neq j$ such the pairs $(a(i), d(i)) = f(i) = f(j) = (a(j), d(j))$. As explained above this is impossible. □

**Exercise.** *Try to find a rearrangement of the numbers* $1, \dots, 10$*, such that the longest ascending/descending partial sequence is of length* $4$*.*