Introduction to Proof

Written by Andy Tran for the MaPS Correspondence Program

1 Introduction

"Pure mathematics is, in its way, the poetry of logical ideas."

This quote by Albert Einstein highlights one of the most fundamental and beautiful parts of mathematics, that is logic.

In mathematics, we are always looking at **statements** and we are interested in whether these statements are **true** or **false**. Proving that a statement is true means that we do not leave any chance for it to be false. If there is still a chance (whatever tiny it is) that a statement is potentially not true, we can not say that we provide the proof. Thus, it is very important that we understand how we can **rigorously prove** that a statement is true or false, and what techniques we can use to help us achieve this.

In this topic, we will look at the foundations of mathematical logic and a few techniques to prove statements. Hopefully you will gain an insight into the wonderful world of mathematical logic and will gain new tools to prove mathematical statements.

We shall look at a few other important methods of proofs later as their own topics, namely **Mathematical Induction** and the **Pigeonhole Principle**.

2 Definitions

We must begin by defining a few important terms that are used in mathematical proofs.

2.1 Implies

Mathematically notated as "$A \implies B$" which means A **implies** B, this is the most basic way to say that one statement implies that another statement is true. For example, we can say: if n is an odd integer, then $n^2 + 2$ is an odd integer. Or mathematically:

$$n \text{ is odd} \implies n^2 + 2 \text{ is odd}$$

2.2 If and only if

Often abbreviated as "iff" and mathematically denoted as $A \iff B$, this means that $A \implies B$ and $B \implies A$ and so we have a **two-way implication**. For example, we could say that n is an even integer if and only if n^2 is an even integer, that is:

$$n \text{ is even} \iff n^2 \text{ is even}$$

2.3 Converse

This can often be thought of as the "**reverse**" of an implication, that is:

Definition 2.1 *The converse of* $A \implies B$ *is* $B \implies A$.

Note that the converse of a true statement is **not necessarily true**! Consider the following statement:

$$n \text{ is positive} \implies n^2 \text{ is positive}$$

However, the converse of this is certainly not true!

$$n^2 \text{ is positive} \not\implies n \text{ is positive}$$

Notice that if the converse of a statement $A \implies B$ is true, then we have a two-way implication $A \iff B$. If mathematicians can prove that a statement is true, then often a natural question to ask is whether or not its **converse** is true.

2.4 Contrapositive

Definition 2.2 *The contrapositive of an implication* $A \implies B$ *is defined to be*

$$\textit{not } B \implies \textit{not } A$$

The reason why the contrapositive is of so much interest to mathematicians is because an implication is **logically equivalent** to its contrapositive. To see this, consider the following examples.

- "If you eat your vegetables, then you will get dessert." is logically equivalent to "If you do not get dessert, then you did not eat your vegetables".
- "If it is raining, then I will bring my umbrella." is logically equivalent to "If I do not bring my umbrella, then it is not raining".

This will come in very handy when we look at **proof by contrapositive**!

Exercise 2.3 *Consider the true statement "If you are in Sydney, then you are in Australia".*

1. What is the converse of this statement? Is it necessarily true?
2. What is the contrapositive of this statement? Is it necessarily true?

3 Methods of Proof

We can now begin to look at some methods of proof!

3.1 Direct Proof

The most basic type of proof is one where we can use **direct implications** to prove our desired result. For example, consider the following:

Example 3.1 *Prove that the sum of two rational numbers* p *and* q *is also rational.*

Solution: Recall the definition of a rational number to be any number expressible in the form $\frac{m}{n}$ where m and n are integers. Thus, we may write:

$$\begin{aligned} p, q \text{ are rational } &\implies p = \frac{a}{b}, q = \frac{c}{d} \text{ for some integers } a, b, c, d. \\ &\implies p + q = \frac{a}{b} + \frac{c}{d} \\ &\implies p + q = \frac{ad + bc}{bd} \\ &\implies p + q \text{ is expressible in the form } \frac{m}{n} \text{ where } m, n \text{ are integers} \\ &\implies p + q \text{ is rational} \end{aligned}$$

□

We have thus created a **logical chain of implications**, proving that the sum of two rational numbers p and q is also rational.

Exercise 3.2 *For an integer x, prove that x is odd if and only if $5x - 1$ is even. (Note: refer to section 4 to see what we need to show for an "if and only if" question)*

Exercise 3.3 *Find all primes p such that $17p + 1$ is a square. (Note: refer to section 4 to see what we need to do for a "find all numbers such that..." question)*

3.2 Proof by Contradiction

Rather than proving that a mathematical statement is true directly, we could instead prove that it is *not false*. We shall look at a famous example below:

Example 3.4 *Prove that there are infinitely many prime numbers.*

Solution: Since we don't have an explicit formula for the prime numbers, it can be quite hard to justify why there must be infinitely many of them. So how about we prove that there **can't** be **finitely** many of them!

For the sake of contradiction, suppose that there are only finitely many primes. This means we can write all the primes out in a list, say $p_1, p_2, p_3, \ldots, p_k$. We now try to find a contradiction, that is we want to show that this list cannot contain all the prime numbers!

To do this, consider the number

$$n = p_1 p_2 p_3 \ldots, p_k + 1.$$

Notice that

$$n - 1 = p_1 p_2 p_3 \ldots p_k$$

is a **multiple** of every prime number. This means that the next integer **can't be a multiple** of any of these primes numbers (since no two consecutive numbers can be divisible by the same prime).

This means that n is **not divisible by any prime numbers**. But every number can be uniquely factorised into primes (this is called the **Fundamental Theorem of Arithmetic**)! This is a contradiction so it is impossible to write all the primes numbers in a finite list, meaning that there are infinitely many primes! □

Exercise 3.5 *Prove that there are infinitely many prime numbers of the form $4k + 3$ where k is an integer.*

Exercise 3.6 *Among a group of 2020 people, prove that there exist two of them who have the same number of friends in that group. Assume that friendship is mutual.*

3.3 Proof by Contrapositive

Recall before that we said that an implication is **logically equivalent** to its **contrapositive**. This means that if we wish to prove that an implication is true, we could instead prove that its contrapositive is true. This has a huge impact on the way we can approach proofs, as in many cases the **contrapositive** of a statement is significantly easier to prove!

Below is an example of this

Example 3.7 *Prove that if a and b are real numbers such that $a + b \geq 10$ then either $a \geq 5$ or $b \geq 5$*

Solution: We can immediately see that it may be a little tricky to find a **direct proof**, so we consider the **contrapositive** of this statement, that is:

$$\text{If } a < 5 \text{ and } b < 5, \text{ then } a + b < 10.$$

Now this question becomes considerably easier!

To structure this proof formally, we would say:

Assume for the sake of contradiction that $a < 5$ and $b < 5$. Thus adding these two inequalities together, we have that

$$a + b < 10$$

which contradicts the initial condition that $a + b \geq 10$. Thus by contradiction, we have that if a and b are real numbers such that $a + b \geq 10$ then either $a \geq 5$ or $b \geq 5$. □

Remark: Notice how we proved that "not B" $\implies$ "not A" and so we concluded $A \implies B$.

Exercise 3.8 *Prove that if x^2 is even for some integer x, then x must be even.*

Exercise 3.9 *Prove that if we try to distribute $kn + 1$ pigeons among k pigeonholes for some integers k and n, then at least one pigeonhole will have at least $n + 1$ pigeons. Assume that pigeons must remain whole.* ***[Note: this is the famous and important Pigeonhole Principle!]***

3.4 Proof by Exhaustion (Cases)

Sometimes we are unable to come up with a single proof that will solve our question, so we can consider **different cases** to solve it part by part.

Example 3.10 *Prove that for any integer n, the number $n^2 + 5n$ is even.*

Solution: This question seems a little difficult to prove directly, or even by contradiction. But it is clear that we could split it into **cases** based on the **parity** (whether a number is odd or even) of n.

Case 1: n is odd
Then we see that n^2 and $5n$ are both odd, so $n^2 + 5n$ must be even.

Case 2: n is even
Then we see that n^2 and $5n$ are both even, so $n^2 + 5n$ must be even.

Thus, we see that in all cases for n, we have that $n^2 + 5n$ is even, so it is even for all integers n. □

Exercise 3.11 *Prove that the square of any integer will leave a remainder of 0 or 1 when divided by 3.*

Exercise 3.12 ***(AIMO 2018 Q10)*** *A pair of positive integers is called* compatible *if one of the numbers equals the sum of all digits in the pair, and the other number equals the product of all digits in the pair. Find all pairs of positive compatible numbers less than 100.*

4 Sufficiency

When we are trying to prove a statement, it is important that we understand what we are **required** to do to have a **complete proof**. Here are a few common types of questions and what we are required to do for a complete proof.

4.1 Do all numbers in a set satisfy a certain property?

Consider the following statement:

> *"Every even integer greater than 2 can be expressed as the sum of two primes."*

Do you think this statement is **true** or **false**? What would you have to do to prove that it is true? What would you have to do to prove that it is false?

Remark: This statement is known as **Goldbach's Conjecture** and is one of the oldest open (unsolved) problems in mathematics.

In general, if we are interested in whether all the elements of a set S, (in the example above: S = every even integer greater than 2) **satisfy a certain property** (being expressible as the sum of two primes) we have the option of:

- Proving it is true by finding **a general proof** that must be true for each element in S.
- Proving it is false by finding **a counterexample**.

You can see that the first option seems much more difficult than the second option. Thus if we want to show that a statement is **always** true, we will often need to use some clever tricks and techniques, some of which we have learnt in this topic.

Exercise 4.1 *Can every positive integer be expressed as the sum of different numbers of the form 2^n where n is a non-negative integer? If so, is this representation unique?*

4.2 Do any numbers in a set satisfy a certain property?

Consider another statement:

> *"A perfect number is a positive integer that is equal to the sum of its positive divisors excluding itself. Are there any odd perfect numbers?"*

Do you think there are any odd perfect numbers? What would you need to do to prove that an odd perfect number **exists**? What would you need to do to prove that there are **no** odd perfect numbers?

Remark: This statement is also an open problem in mathematics.

Similar to before, if we are interested in whether **there exists** an element of a set S (eg. the set of perfect numbers), with a certain property (eg. being odd), we can either:

- Find **an example** of an element in S with that property.
- Find **a general proof** that every element in S does not satisfy the property.

Again, you can see that the second option seems considerably harder than the first one, and so requires a clever argument.

Exercise 4.2 *Can you find any four distinct numbers p, q, r, s such that $pq + rs = ps + qr$?*

4.3 Find all numbers in a set that satisfy a certain property.

Now consider this statement:

> *"Find all pairs of positive consecutive integers such that they are non-trivial integer powers, that is they are expressible in the form a^b where $a > 1$ and $b > 1$."*

Can you find any pairs of consecutive non-trivial integer powers? What would you need to do to show that you have found **all** of them?

Remark: It turns out that the only such pair is $(8, 9)$ as $8 = 2^3$ and $9 = 3^2$. This is known as Mihailescu's Theorem which was proven in 2002. It was known as Catalan's Conjecture for more than a hundred years before it was proven.

To solve this sort of question where we want to find **all numbers** in a set S that satisfy a given property, we need to complete two tasks:

- Find the group of numbers in S and show that **they satisfy the property**.
- Show that every other group of numbers in S **does not satisfy the property**.

In the example above, the set S was the set of pairs of consecutive positive integers and the property was "being a pair of non-trivial integer powers".

Exercise 4.3 *Find all non-negative integers x such that $x^2 + x + 1$ is a perfect square.*

4.4 Find the largest/smallest number in a set that satisfies a certain property.

Suppose we ask the following question:

> *"Find the smallest number that can be expressed as the sum of two positive cubes in two different ways."*

Can you find any numbers that can be written as the sum of two positive cubes in two different ways? How can we rigorously show that we have found the **smallest** number that satisfies this property?

Remark: It turns out that the smallest number is 1729 as $1729 = 1^3 + 12^3 = 9^3 + 10^3$. 1729 is also called the Hardy-Ramanujan number based off an anecdote between the 20th century mathematicians Godfrey Hardy and Srinivasa Ramanujan.

To solve this sort of question where we want to find the **smallest** number in a set S that satisfies a given property, we need to complete two tasks:

- Find the number n in S and show that **it satisfies the property**.

- Show that every other number less than n **does not satisfy the property**.

In the example above, the set S was the set of positive integers and the property was "being the sum of two positive cubes in two different ways". This idea also applies to finding the **largest** number in a set satisfying a given condition.

Exercise 4.4 *Find the largest integer that can't be expressed in the form $4a + 7b$ where a and b are non-negative integers.*