MATH1902: SOME REMARKS ON PROOFS

The idea behind proofs in mathematics can be explored in entire texts, or at least in big chapters in long textbooks. I will only very briefly discuss some of the methods we use to prove different types of mathematical statements. I won't go through the building blocks of forming arguments and proofs. Words and terms like "syllogism" and "modus ponens" are important, but are also largely just common sense. I'll take it all for granted, and I think we'll be fine.

Proving $\exists$ statements. The symbol $\exists$ means "there exists". I won't usually use it in MATH1902, but it is nice shorthand to use in this small note, and you are free to use it if you like.

For D a set, and $P(x)$ a statement depending on $x \in D$, how do we prove a statement of the form

$$\text{“}\exists x \in D \text{ such that } P(x)\text{”?}$$

This statement is equivalent to "$P(x)$ is true for at least one $x \in D$". So to prove the above statement we need to find one $x \in D$ that makes $P(x)$ is true.

Example 1. Prove that there exists an even integer that can be written two ways as the sum of two (not necessarily distinct) primes.

Proof. We have $10 = 5 + 5$, and $10 = 3 + 7$. Since $3, 5$, and 7 are primes, the result holds. □

Note that the □ symbol on the right signifies the end of the proof.

Example 2. Prove $\exists x \in \mathbb{R}$, such that $x + 5 = 0$.

Proof. Let $x = -5$. Then $x + 5 = (-5) + 5 = 0$. □

Proving $\forall$ statements. The symbol $\forall$ means "for all". I won't usually use it in MATH1902, but it is nice shorthand to use in this small note, and you are free to use it if you like.

For D a set, and $P(x)$ a statement depending on $x \in D$, how do we prove a statement of the form

$$\text{“}\forall x \in D, P(x)\text{”?}$$

This statement is equivalent to "$P(x)$ is true for at all $x \in D$". To prove the above statement we have two options:

(1) Method of Exhaustion, and
(2) Generalised Proof.

We will spend the majority of this note below examining methods to construct a generalised proof. To prove "$P(x)$ is true all $x \in D$" using the method of exhaustion requires checking that $P(x)$ is true for every x in D. This method is useful when D is small, but can be unhelpful when D is large, and impossible to use when D is infinite.

Example 1. Prove that every even number between 2 and 16 can be written as the sum of two prime numbers.

Proof. We have

$$4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ 10 = 3 + 7,\ 12 = 5 + 7, \text{ and } 14 = 7 + 7.$$

□

Not the most elegant or sophisticated proof in the world, but we just check every case, and it certainly does the job!

Example 2. Prove that every even $n \in \mathbb{N}$ can be written as the sum of two prime numbers. (Good luck using the method of exhaustion!)

Proof. This is an exercise![1] □

Disproving $\exists$ statements ctd. To disprove the statement "$\exists x \in D$ such that $P(x)$", we must prove its negation:

$$\sim (\exists x \in D \text{ such that } P(x)) \equiv \forall x \in D, \sim P(x).$$

Here, the $\sim$ symbol stands for negation (so $\sim P$ means "not P"), and $\equiv$ just means "equivalent to". To *disprove* an $\exists$ statement, we must *prove* a $\forall$ statement, and to do this we use the method of exhaustion or a generalised proof.

Example. Disprove the statement "there exists an even prime number that is larger than 5".

Proof. We need to prove that all even primes are less than or equal to 5. But the only even prime is 2, which satisfies $2 \leq 5$. □

Disproving $\forall$ statements. To disprove the statement "$\forall x \in D, P(x)$", we must prove its negation:

$$\sim (\forall x \in D, P(x)) \equiv \exists x \in D \text{ such that } \sim P(x).$$

So to *disprove* a $\forall$ statement, we must *prove* a $\exists$ statement. To do this, it is enough to find one $x \in D$ such that $\sim P(x)$ is true; that is, one $x \in D$ such that $P(x)$ is false. This is called a *counterexample.*

Example 1. Disprove the statement $\forall x \in \mathbb{R}, (x > 0 \text{ or } x < 0)$.

Proof. We need to prove that there exists $x \in \mathbb{R}$ such that $\sim (x > 0 \text{ or } x < 0)$, which means that $x \not> 0$ and $x \not< 0$. Take $x = 0$. Then $x \not> 0$ and $x \not< 0$. □

Example 2. Disprove the statement "$\forall a, b \in \mathbb{R}$, if $a^2 = b^2$, then $a = b$".

Proof. We need to find a, b such that $a^2 = b^2$, but $a \neq b$. Take $a = 2$ and $b = -2$. Then $a^2 = 4 = (-2)^2 = b^2$, but $a \neq b$. □

Method of generalised proof 1 – Direct Proof. There are three main methods of generalised proof. The first is called *direct proof*, and it is one in which we work in a straightforward fashion to the solution.

Example 1. Prove that if $3x - 9 = 15$ then $x = 8$.

Proof. We have

$$3x - 9 = 15 \implies 3x = 24 \implies x = 8.$$

□

Example 2. An integer n is called a perfect square if and only if $n = k^2$ for some integer k. Prove that if $m, n \in \mathbb{Z}$ are perfect squares, then $mn \in \mathbb{Z}$ is a perfect square.

Proof. Let $m, n \in \mathbb{Z}$ be perfect squares. Then $m = j^2$ and $n = k^2$, for some $j, k \in \mathbb{Z}$. Then $mn = j^2k^2 = (jk)^2$, and hence mn is a perfect square. □

The Principle of Mathematical Induction. An example of a direct method of proof worthy of its own little subsection here is the Principle of Mathematical Induction, which says that if $P(n)$ is a statement with domain $n \in \mathbb{N}$, and with

(a) $P(1)$ true; and
(b) $P(k)$ true $\implies P(k+1)$ true for all $k \in \mathbb{N}$,

then $P(n)$ is true for all $n \in \mathbb{N}$.

Example. Prove that $4^n - 1$ is a multiple of 3 for all $n \in \mathbb{N}$.

[1] Actually, let me know if you come up with a proof because this statement is known as the Goldbach Conjecture.

Proof. For $n \in \mathbb{N}$ let $P(n)$ be the statement "$4^n - 1$ is a multiple of 3". We have $4^0 - 1 = 1 - 1 = 0 = 3 \times 0$, and hence $P(0)$ is true. We now assume that $P(k)$ is true, which means that $4^k - 1$ is a multiple of 3. Suppose that $4^k - 1 = 3M$, for some $M \in \mathbb{Z}$. Then we have

$$4^{k+1} - 1 = 4(4^k - 1) + 3 = 4(3M) + 3 = 3(4M + 1),$$

and hence $4^{k+1} - 1$ is a multiple of 3. This means that $P(k + 1)$ is true, and so the Principle of Mathematical Induction says that $P(n)$ is true for all $n \in \mathbb{N}$. □

Method of generalised proof 2 – Proof by Contradiction. We have the following logical equivalence

$$(P \Longrightarrow Q) \equiv (\sim Q \Longrightarrow \sim P).$$

If you haven't seen this before, you should convince yourself of it. This equivalence gives us our *method of proof by contradiction*, which means to prove $P \Longrightarrow Q$, we may prove that $\sim Q \Longrightarrow \sim P$. In other words, we assume the negation of what we are trying to prove, and then use a logical argument to show that we have a contradiction with what we assumed (or a contradiction with some other well-known truth).

Example 1. Try proving the statement

$$\forall n \in \mathbb{N}, \text{ if } n^2 \text{ is even, then } n \text{ is even}$$

using a direct proof, and a proof by contradiction.

Proof. Direct: We have

$$\begin{aligned} n^2 \text{ is even} &\Longrightarrow \exists k \in \mathbb{Z} \text{ with } n^2 = 2k \\ &\Longrightarrow \exists k \in \mathbb{Z} \text{ with } n = \pm\sqrt{2k} \\ &\Longrightarrow \text{? } (n \text{ equals 2 times what?}) \end{aligned}$$

The direct method isn't helping.

Contradiction: Assume n^2 even. Now assume that n is not even, which means that n is odd. Let $n = 2k + 1$ for $k \in \mathbb{Z}$. Then we have

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

and since $2k^2 + 2k \in \mathbb{Z}$, this means n^2 is odd. But this contradicts our assumption that n^2 is even. So we cannot have n odd, and hence it must be even. □

Example 2. Use a proof by contradiction to prove that if $y \in \mathbb{R}$ is irrational, then $y + 7 \in \mathbb{R}$ is also irrational.

Proof. Let y be irrational. Assume that $y + 7$ is not irrational, which means $y + 1$ is rational. Let $y + 7 = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ and $b \neq 0$. Then

$$y = \frac{a}{b} - 7 = \frac{a - 7b}{b} \in \mathbb{Q}.$$

But this contradicts that y is irrational, and hence $y + 7$ must be irrational. □

Method of generalised proof 3 – Proof by Cases. How would we go about proving the statement

$$\text{"If } x \neq 0 \text{ or } y \neq 0, \text{ then } x^2 + y^2 > 0\text{"?}$$

We would need to split it into cases, right? Such problems are proved by the proof by cases method. This method is used whenever you wish to prove a statement of the form

$$(P \text{ or } Q) \Longrightarrow R.$$

The only problem with this method of proof is that it is not always obvious when this method is required.

Example 1. Prove that if $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$.

Proof. First suppose that $x \neq 0$. Then $x^2 > 0$, and since $y^2 \geq 0$, we have $x^2 + y^2 > 0$.

Now suppose that $y \neq 0$. Then $y^2 > 0$, and since $x^2 \geq 0$, we have $x^2 + y^2 > 0$. □

Example 2. Prove that $\forall m \in \mathbb{N}$, $m^2 + m + 1$ is odd.

Proof. First suppose that m is even. Let $m = 2k$ for $k \in \mathbb{Z}$. Then

$$m^2 + m + 1 = (2k)^2 + (2k) + 1 = 4k^2 + 2k + 1 = 2(2k^2 + k) + 1,$$

and since $2k^2 + k \in \mathbb{Z}$, we know that $m^2 + m + 1$ is odd.

Now suppose that m is odd. Let $m = 2j + 1$ for $j \in \mathbb{Z}$. Then

$$m^2 + m + 1 = (2j + 1)^2 + (2j + 1) + 1 = 4j^2 + 6j + 3 = 2(2j^2 + 3j + 1) + 1,$$

and since $2j^2 + 3j + 1 \in \mathbb{Z}$, we know that $m^2 + m + 1$ is odd. So $m^2 + m + 1$ for all $m \in \mathbb{N}$. □

A final word on writing mathematics We write mathematics using full sentences and correct grammar (as correct as we can be!). This means that proofs should typically contain a mixture of English and mathematical symbols and calculations, rather than being overly wordy, or just made up of mathematical symbols. Here are three proofs of a very simple problem:

Claim. The sum of an even integer and an odd integer is an odd integer.

Proof 1. An integer is even if it is two times another integer, and an integer is odd if it is two times another integer plus one. Therefore the sum of an even and odd integer is two times the sum of the two other integers plus one, and this has the form of two times an integer plus one, which means it is odd. □

Proof 2.

$$\begin{aligned} n &= 2i, m = 2j + 1 \\ m + n &= 2i + 2j + 1 \\ m + n &= 2(i + j) + 1 \end{aligned}$$

□

Proof 3. Suppose m is an even integer, and n is an odd integer. This means there are integers i and j such that $m = 2i$, and $n = 2j + 1$. Then we have

$$m + n = 2i + 2j + 1 = 2(i + j) + 1.$$

Since the sum of two integers is again an integer, we know that $i + j$ is an integer, and so the sum $m + n$ has the form $2k + 1$ for some integer k. Hence $m + n$ is odd. □

Hopefully we agree that Proof 3 is the clearest and nicest proof to read! :)