4.2. Proof Writing Tips

1) It should be clear to the reader what is being proven.

In literature the most common way of doing this is to state the theorem followed by it's proof. For example,

> Theorem: ____________________________
> *Proof.* ____________________________ □

2) Clearly mark the beginning and end of the proof.

Typically we indicate the start of a proof with the word "Proof" and the end of the proof with □ which stands for quod erat demonstrandum (QED).

3) Proofs should be self-contained.

All variables should be introduced in the proof or theorem statement. The reader should be able to just read the theorem and proof in order to understand it. If you need to reference previous results, they should be cited. For example "by Lemma 1, ...".

4) Proofs should be grammatically correct.

We write proofs in English. Make sure you are following the rules of English.

5) The reader should be informed about the status of the proof.

In order for the reader to follow your argument, they need to know the things you are assuming and your goals. This is often done with phrases such as "Assume that __________" and "We claim that __________".

6) Justify each assertion made.

Every non-trivial assertion needs to have a reason presented to the reader. For example, compare

> There is an integer k such that $n = 2k$

v.s.

> Because n is even, there is an integer k such that $n = 2k$.

The second sentence is easier for the reader to follow.

7) Use words of phrases to connect the logic between sentences.

The reader should be able to follow the logic behind your argument. Commonly used words and phrases include "since", "because", "thus", "therefore", "hence", "then", "notice that", etc.

8) Show equations and inequalities on separate lines centered so that they are easy to read.

In the argument below, we put the crucial equations on a separate line making them stand up.

> Let m and n be integers. Then there are integers k and j such that $m = 2k$ and $n = 2j$. Notice that
>
> $$\begin{aligned} m + n &= 2k + 2j \\ &= 2(k + j). \end{aligned}$$
>
> Therefore, $m + n$ is even.

4.2.1 Common Mistakes

1) Argument from example(s).

Consider the argument

> Because $2^2 > 2$ and $3^2 > 3$, it follows that $x^2 > x$.

While examples may be convincing and are a good way of testing your conjecture, they are not proofs and may be misleading. For example, the conclusion we stating here is false when $0 \leq x \leq 1$.

2) Using the same symbol for different things.

Each object should have their own symbol. In the argument

> Let m and n be odd. By definition $m = 2k + 1$ and $n = 2k + 1$.

we are using k as a placeholder for two different integers. This can be confusing to the reader. In this particular example the reader may be under the assumption that $m = n$.

3) Jumping to conclusion.

The proof below is jumping to the conclusion by missing a crucial step:

> Let $m = 2r$ and $n = 2s$. Then $m + n = 2r + 2s$ implying that $m + n$ is even.

4) Assuming the result.

Make sure your argument is not circular! For example the argument below for the product of odd integers is odd is circular:

> Let m and n be odd. Since the product of odd integers is odd, mn is odd.

Your proof cannot assume the result is true. You may assume the result is false if doing a proof by contradiction.

5) Use of any instead of some.

The word "any" has a different implication than "some". For example in

> Suppose m is an odd integer. By definition of odd, $m = 2k + 1$ for *any* integer k.

the word "any" is implying that k can be anything we want as long as it is an integer. The correct word here would be "some" since there is only one correct integer k.

6) Use of if instead of because.

Example:

> Suppose p is prime. If p is prime, then p cannot be written as the product of primes.

Here the phrase "if p is prime" is redundant as we have already assumed that p is prime. While it does it make your proof incorrect, it is confusing to the reader.

7) Overuse of symbols.

While it is perfectly fine to use symbols in your proof, an overuse of symbols can make it hard to read. For example, consider the proof below that the sum of even integer is even.

> $\exists k, j \in \mathbb{Z}$ such that $n = 2k$, $m = 2j$.
> $n + m = 2k + 2j = 2(k + j)$.
> $(k + j) \in \mathbb{Z}$.
> $\therefore n + m$ is even.

4.2.2 Example Proofs

Theorem 4.2.1. *The difference of an odd integer and an even integer is odd.*

Proof. Let m be an odd integer and n an even integer. Then by definition there are integers k and j such that $m = 2k + 1$ and $n = 2j$. Notice that

$$\begin{aligned} m - n &= 2k + 1 - 2j \\ &= 2(k - j) + 1. \end{aligned}$$

Let $t = k - j$. Then $t \in \mathbb{Z}$ and $m + n = 2t + 1$. Therefore, by definition, $m - n$ is odd. □

Theorem 4.2.2. *There is not a positive integer n such that $n^2 + 3n + 2$ is prime.*

Proof. It suffices to show that for all positive integers n, $n^2 + 3n + 2$ is not prime. Suppose n is a positive integer. By factoring we get that

$$n^2 + 3n + 2 = (n + 2)(n + 1).$$

Since $n+2$ and $n+1$ are integers and $n+1 > 1$, $n+2 > 2$, it follows that n^2+3n+2 is not prime as it is the product of two integers. □

Definition 4.2.3. An integer n is a **perfect square** if $n = k^2$ for some integer k.

Theorem 4.2.4. *For every integer n, $4(n^2+n+1)-3n^2$ is a perfect square.*

Proof. Let $n \in \mathbb{Z}$. Notice that

$$\begin{aligned} 4(n^2+n+1)-3n^2 &= 4n^2+4n+4-3n^2 \\ &= n^2+4n+4 \\ &= (n+2)^2. \end{aligned}$$

Let $t = n+2$. Then $4(n^2+n+1)-3n^2 = t^2$. Since $t \in \mathbb{Z}$ it follows that $4(n^2+n+1)-3n^2$ is a perfect square. $\square$

Theorem 4.2.5. *If n is an even integer, then $(-1)^n = 1$.*

Proof. Recall that $(-1)(-1) = 1$. Let n be even. Then there is an integer k such that $n = 2k$. Notice that

$$\begin{aligned} (-1)^n &= (-1)^{2k} \\ &= ((-1)^2)^k \\ &= 1^k \\ &= 1. \end{aligned}$$

Therefore, $(-1)^n = 1$. $\square$

Remark 4.2.5.1. In the proof for theorem 4.2.5, we assumed that the product of two negatives is positive. This can be proven using the distributive law:

$$\begin{aligned} (-x)(-y) &= (-x)(-y) + \overbrace{x(-y+y)}^{=0} \\ &= (-x)(-y) + x(-y) + xy \\ &= (-x+x)(-y) + xy \\ &= xy. \end{aligned}$$