Appendix B

Techniques for Proof Writing

This guide includes some things that I like to keep in mind when I am writing proofs. They will hopefully become second-nature after a while, but it helps to actively think about them when one is first learning to write proofs.

B.1 Basic Proof Writing

There are some books out there that are designed to help you learn to read and write proofs. (A commonly-used one is How to Read and Do Proofs by Daniel Solow. It should be on reserve at Baker-Berry soon, and the library has two additional older copies available.) However, they can be somewhat dry and slow in getting off the ground. For me, the best way to learn to write proofs is to dive in and try to write up proofs of some reasonably simple statements. With this in mind, there are two fundamental aspects of proof writing that need to be mastered.

**Logic:** The first step to writing a proof, and probably the biggest hurdle for most people, is determining the logical steps needed to verify the given statement. In other words, this involves laying down an outline of the argument that you intend to make. There are some things to keep in mind when trying to do this.

- **What am I being asked to prove?** Often this will require you to unravel a definition or two to figure out what you’re really trying to prove.

- **What are the hypotheses?** You’re usually given some assumptions, and then you are asked to deduce something from them. This would usually be written in the form

  “If . . . , then . . . ”

Again, look back at the definitions and decide what the hypotheses are really saying.
• **What theorems might help?** Try to think of definitions and theorems that are related to the given statement. Determine which ones might help you get from the hypotheses to the desired result.

• **Put it all together.** Try to piece together the theorems that you’ve found in a logical way to deduce the result.

**Example B.1.1.** Let’s try to put these ideas into action.

**Prove:** If $a$ and $b$ are relatively prime and $a \mid bc$, then $a \mid c$.

Let’s think about what we need to do here.

• What are we being asked to prove? We want to show that $a \mid c$, which means that we need to show that there is an integer $n$ such that $c = na$.

• What are the hypotheses? There are two: we are told that $a$ and $b$ are relatively prime and that $a \mid bc$. The first means that $\gcd(a, b) = 1$, and the second tells us that there exists $m \in \mathbb{Z}$ such that $bc = ma$.

• What theorems do we have at our disposal? One of the theorems we proved regarding gcds was Bézout’s lemma (or the extended Euclidean algorithm), which said that $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.

• Let’s put it together:

$$\gcd(a, b) = 1 \implies 1 = ax + by \implies acx + bcy = c$$

Now use the other hypothesis:

$$a \mid bc \implies bc = ma \implies bcy = may \implies acx + bcy = acx + may \implies c = a(cx + my) \implies a \mid c$$

In this example we didn’t actually write a proof. We simply outlined the argument, which is the backbone of the proof. Now we need to turn it into something readable. This brings us to the second major aspect of proof writing.
Style: Once you have your argument laid out, the next thing you need to do is to write it up in a nice way. Here are some tips for doing this.

- **Write in proper English.** Use complete sentences, with proper grammar and punctuation. The goal is to make it easy for the reader to understand. If you are unsure of how a particular sentence looks, read it back to yourself and think about how it would sound to the reader.

- **Be clear and precise.** Try to say what you mean in as simply as possible, while still using proper mathematical language. Be careful how you say things, and explain yourself at each step. If there is a step that you have to think about, or that you think may give the reader pause, explain it.

- **Don’t say too much (or too little).** Again, explain yourself thoroughly, but don’t overdo it. Get to the point, and avoid using overly ornate or mellifluous language. At this stage in the game, it’s okay to err on the side of writing too much, but try to not overdo it.

These are all things that will become much easier with practice. Also, reading proofs in the book (or seeing them in class) will give you a better idea of how people tend to talk when they are writing proofs.

**Example B.1.2.** Let’s write up a proper proof of the example.

**Prove:** If \( a \) and \( b \) are relatively prime and \( a \mid bc \), then \( a \mid c \).

**Proof.** Since \( a \) and \( b \) are relatively prime, \( \gcd(a, b) = 1 \), and Bézout’s lemma lets us write

\[
ax + by = 1
\]

for some \( x, y \in \mathbb{Z} \). If we multiply both sides by \( c \), we get

\[
acx + bc y = c.
\]

We are assuming that \( a \mid bc \), so there is an \( m \in \mathbb{Z} \) such that \( bc = ma \). Then

\[
bcy = may,
\]

so

\[
c = acx + bc y = acx + may.
\]

Factoring out \( a \), we get

\[
c = a(cx + my).
\]

But \( cx + my \in \mathbb{Z} \), and this is precisely what it means for \( a \) to divide \( c \).

Here are two more examples of simple proof–writing exercises. We will approach them in the same manner as the previous example.
Example B.1.3. Prove: Let $a, b \in \mathbb{Z}$, and let $m > 0$ be an integer. Then
\[ \text{gcd}(ma, mb) = m \cdot \text{gcd}(a, b). \]

Let’s outline our plan of attack.

- What are we trying to prove? We need to show that $\text{gcd}(ma, mb) = m \cdot \text{gcd}(a, b)$. Our plan will be to show that $\text{gcd}(ma, mb) \leq m \cdot \text{gcd}(a, b)$, and that $m \cdot \text{gcd}(ma, mb) \leq \text{gcd}(ma, mb)$.

- What are the hypotheses? We are simply given that $a, b, m \in \mathbb{Z}$, and that $m > 0$.

- What theorems or definitions might be useful? We know that $d = \text{gcd}(a, b)$ divides $a$ and $b$, so $md$ divides both $ma$ and $mb$. Also, Bézout’s lemma says that there are integers $x$ and $y$ satisfying
\[ ax + by = d, \]
so
\[ mx + mby = md. \]

- Put it all together: $md | ma$ and $md | mb \implies md$ is a (positive) common divisor of $ma, mb \implies md \leq \text{gcd}(ma, mb)$. Also,
\[ mx + mby = md \implies \text{gcd}(ma, mb) | md, \]
so $\text{gcd}(ma, mb) \leq md$. Thus $\text{gcd}(ma, mb) = m \cdot \text{gcd}(a, b)$.

Now we’ll write it up.

Proof. Let $d = \text{gcd}(a, b)$. Since $d$ divides both $a$ and $b$, $md$ divides both $ma$ and $mb$. Since $m > 0$, $md$ is a positive common divisor of $ma$ and $mb$, so it must be smaller than the greatest common divisor. That is, $md \leq \text{gcd}(ma, mb)$. Also, Bézout’s lemma implies that there are integers $x$ and $y$ satisfying
\[ ax + by = d. \]
Multiplying both sides by $m$, we get
\[ mx + mby = md. \]
Since $\text{gcd}(ma, mb)$ divides both $ma$ and $mb$, it divides the left side of this equation. Thus $\text{gcd}(ma, mb)$ divides $md$, so we must have
\[ \text{gcd}(ma, mb) \leq md. \]
Therefore, $md = \text{gcd}(ma, mb)$, or $m \cdot \text{gcd}(a, b) = \text{gcd}(ma, mb)$. 

\[ \square \]
Example B.1.4. Prove: The equation
\[ ax + by = c \]
has integer solutions \( x \) and \( y \) if and only if \( \gcd(a, b) \) divides \( c \).

There are two directions here, so we need to handle them one at a time.

- For the first direction, what are we being asked to prove? We need to show that \( \gcd(a, b) \) divides \( c \).
- What are the hypotheses? We are given that there are integers \( x \) and \( y \) such that \( ax + by = c \).
- What theorems or definitions might be useful? We’ll use the definition of the greatest common divisor, namely that it dives \( a \) and \( b \). If we let \( d = \gcd(a, b) \), we can write
  \[ a = ed \quad \text{and} \quad b = fd \]
  for some integers \( e \) and \( f \).
- Now let’s put it together.
  \[ a = ed \quad \text{and} \quad b = fd \implies c = ax + by = edx + fdy \]
  \[ \implies c = d(ex + fy) \]
  \[ \implies d \text{ divides } c \]
- What do we need to do for the other direction? We assume that \( \gcd(a, b) \) divides \( c \), and we show that \( ax + by = c \) has integer solutions.
- What can we use? First, if \( d = \gcd(a, b) \) divides \( c \), we can write \( c = kd \) for some \( k \in \mathbb{Z} \). Second, we have Bézout’s lemma: there exist \( x_0, y_0 \in \mathbb{Z} \) such that
  \[ ax_0 + by_0 = d. \]
- Now put it together:
  \[ ax_0 + by_0 = d \implies kax_0 + kby_0 = kd = c \]
  \[ \implies a(kx_0) + b(ky_0) = c \]
  so we can take \( x = kx_0 \) and \( y = ky_0 \).

Now we’ll try to write it up nicely.
Proof. Suppose first that there are integers $x, y \in \mathbb{Z}$ such that $ax + by = c$. Let $d = \gcd(a, b)$. Since $d$ divides both $a$ and $b$, there are integers $e, f \in \mathbb{Z}$ such that $a = ed$ and $b = fd$. Then

$$ax + by = edx + fdy = d(ex + fy).$$

But $ax + by = c$, so

$$c = d(ex + fy),$$

and $d$ divides $c$.

Conversely, suppose that $d$ divides $c$. Then there is an integer $k$ satisfying $c = kd$. By Bézout’s lemma, there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$ax_0 + by_0 = d.$$

Thus

$$k(ax_0 + by_0) = kd,$$

or

$$a(kx_0) + b(ky_0) = c.$$

If we set $x = kx_0$ and $y = ky_0$, then $ax + by = c$, so we are done.

As a final note on style, people usually use a symbol to indicate the end of a proof. The most common is a simple square, which can be open or filled: □ or ■. (The default in \LaTeX is an open square.) Some people will also use an open or closed diamond, or double or triple hatch marks (// or ///). Older proofs sometimes end with Q.E.D, which is an abbreviation of the Latin “quod erat demonstrandum,” or “which was to be demonstrated.”

### B.2 Proof by Contradiction

The proofs we’ve written so far are direct proofs: we started with the hypotheses and we made a chain of logical deductions to eventually prove the given statement. This is generally the most desirable way to prove something, but it may not always work. Even if it does work, it may not be the best way. To this end, there is another proof technique called proof by contradiction.

Proof by contradiction, or in Latin, reduction ad absurdum, is an alternative to writing a direct proof. Instead of assuming the hypotheses and directly proving the result, you assume the hypotheses and you assume that the result is not true. You then try to make logical deductions until you arrive at a contradiction, which is a sort of logical conundrum. This contradiction should then lead you to conclude that there is a faulty assumption somewhere, and the only possibility is the assumption that the result is false. In summary:
Proof by Contradiction: Suppose that you are asked to prove a statement of the form

“If $A$, then $B$.”

To prove this by contradiction:

1. Assume $(A)$ and $(\neg B)$.

2. Investigate the logical implications of these assumptions. (Use any theorems, definitions, etc. that you know.)

3. Arrive at a contradiction.

4. Conclude that $B$ must be true after all.

There is one thing that should be noted before we continue. A proof by contradiction is not generally considered to be an aesthetically pleasing proof, and the technique should always be used as a last resort. That is, you should always try first to prove something directly, and then attempt a contradiction proof if a direct proof is too difficult. However, contradiction is sometimes the only way, and sometimes it may even give a nicer proof than those that can be obtained directly.

The following example is the oldest known proof by contradiction. There are actually many other known proofs of this statement, but the contradiction proof is still well-known due to its simplicity.

**Example B.2.1.** Prove that there are infinitely many prime numbers.

*Proof.* Suppose not—that is, let’s assume that there are only finitely many prime numbers, say

$$p_1, p_2, \ldots, p_n.$$ 

Consider the integer

$$N = p_1 p_2 \ldots p_n + 1.$$ 

Observe that none of the primes $p_1, \ldots, p_n$ divide $N$. Since we are assuming that these are all the prime numbers, $N$ has no prime divisors. But every integer can be written as a product of primes, so we have arrived at a contradiction. Therefore, our assumption that there are only finitely many primes must be faulty. We can thus conclude that there must be infinitely many primes.

Here is another example. The details are a little more straightforward, and you simply need to “follow your nose” after making the necessary assumptions.

**Example B.2.2.** Suppose that $a \in \mathbb{Z}$. Prove that if $a^2$ is even, then $a$ is also even.
Proof. Assume that $a^2$ is even, but that $a$ is odd. Then

$$a = 2n + 1$$

for some $n \in \mathbb{Z}$. If we compute $a^2$, we get

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

which is odd. But we are assuming that $a^2$ is even, so we have arrived at a contradiction. Therefore, our assumption that $a$ is odd must be invalid, and we can conclude that $a$ must be even.

Here’s one for you to try on your own if you want more practice. It is a commonly-studied proof by contradiction, so you can probably find the proof written down in any number of places.

**Exercise B.1.** Prove that $\sqrt{2}$ is an irrational number.

### B.3 Mathematical Induction

There is another proof technique, called the Principle of Mathematical Induction, which is used in special situations. One generally employs it to prove a statement that depends on an integer $n$. For example, you might be asked to prove that some formula, written in terms of $n$, holds for all $n \in \mathbb{Z}$. If you are lucky, you might be able to prove it directly. However, it’s possible to envision, at least in principle, a systematic way of writing down such a proof. You could prove the result for $n = 1$, and then use this fact to induce the result for $n = 2$. You could then prove it for $n = 3$, then $n = 4$, and so on, proving each case by using the previous one. Obviously we can’t actually write a proof this way—it would require a lot of work, and we’d have to prove an infinite number of cases. Fortunately, mathematical induction gives us the ability to do all of this in one fell swoop.

**Principle of Mathematical Induction:** Suppose that you are asked to prove that a statement $P(n)$, depending on $n \in \mathbb{Z}^+$, is true for all $n$. To prove this via induction, there are two steps:

- **Base case:** Prove that $P(1)$ is true.

- **Inductive step:** Assume that $P(n - 1)$ is true, and use this to prove that $P(n)$ is true.
Example B.3.1. Prove that for all $n \in \mathbb{Z}^+$,

$$1 + 2 + \cdots + n = \frac{1}{2} n(n + 1).$$

Proof. We need to check first that the formula holds for $n = 1$. The left side is simply 1, and the right side is

$$\frac{1}{2} \cdot 1 \cdot (1 + 1) = \frac{1}{2} \cdot 1 \cdot 2 = 1,$$

so the formula holds for $n = 1$.

Now we need to handle the inductive step. Assume that the formula holds for $n - 1$, i.e., that

$$1 + 2 + \cdots + (n - 1) = \frac{1}{2} (n - 1)(n).$$

Then

$$1 + 2 + \cdots + n = 1 + 2 + \cdots + (n - 1) + n$$

$$= \frac{1}{2} (n - 1)n + n$$

$$= \left( \frac{1}{2} (n - 1) + 1 \right) n$$

$$= \left( \frac{1}{2} (n - 1 + 2) \right) n$$

$$= \frac{1}{2} n(n + 1).$$

Now try the following example, which actually relates to abstract algebra.

Example B.3.2. If $G$ is an abelian group and $a, b \in G$, prove that

$$(ab)^n = a^n b^n$$

for all $n \in \mathbb{Z}^+$.

Proof. For $n = 1$, we simply have

$$(ab)^1 = ab = a^1 b^1,$$
so the base case holds. Now assume that \((ab)^{n-1} = a^{n-1}b^{n-1}\). Then
\[
(ab)^n = (ab)^{n-1}(ab) = a^{n-1}b^{n-1}ab
\]
by assumption. Since \(G\) is abelian,
\[
a^{n-1}b^{n-1}ab = a^{n-1}a^{n-1}b = a^n b^n.
\]
Therefore, the result holds by induction. \(\square\)

If you want to read more about mathematical induction, or if you want to try
other problems, the latter half of Section 0 in Saracino is devoted to induction.
There are more examples, and there are several exercises that would allow you to
practice proofs by induction.

### B.4 Proof by Contrapositive

So far we’ve practiced some different techniques for writing proofs. We started with
direct proofs, and then we moved on to proofs by contradiction and mathematical
induction. The method of contradiction is an example of an **indirect proof**: one
tries to skirt around the problem and find a clever argument that produces a logical
contradiction. This is not the only way to perform an indirect proof—there is
another technique called **proof by contrapositive**.

Suppose that we are asked to prove a **conditional statement**, or a statement
of the form

“If \(A\), then \(B\).”

We know that we can try to prove it directly, which is always the more enlightening
and preferred method. If a direct proof fails (or is too hard), we can try a contra-
diction proof, where we assume \(\neg B\) and \(A\), and we arrive at some sort of fallacy.
It’s also possible to try a proof by contrapositive, which rests on the fact that a
statement of the form

“If \(A\), then \(B\).” \((A \implies B)\)

is logically equivalent to

“If \(\neg B\), then \(\neg A\).” \((\neg B \implies \neg A)\)

The second statement is called the **contrapositive** of the first. Instead of proving
that \(A\) implies \(B\), you prove directly that \(\neg B\) implies \(\neg A\).

**Proof by contrapositive:** To prove a statement of the form

“If \(A\), then \(B\),” do the following:

1. Form the contrapositive. In particular, negate \(A\) and \(B\).
2. Prove directly that \(\neg B\) implies \(\neg A\).
There is one small caveat here. Since proof by contrapositive involves negating certain logical statements, one has to be careful. If the statements are at all complicated, negation can be quite delicate. However, sometimes the given proposition already contains certain negative statements, and contrapositive is the natural choice.

**Example B.4.1.** Prove by contrapositive: Let \( a, b, n \in \mathbb{Z} \). If \( n \nmid ab \), then \( n \nmid a \) and \( n \nmid b \).

**Proof.** We need to find the contrapositive of the given statement. First we need to negate “\( n \nmid a \) and \( n \nmid b \).” This is an example of a case where one has to be careful, the negation is

\[
\text{“} n \mid a \text{ or } n \mid b \text{.”}
\]

The “and” becomes an “or” because of DeMorgan’s law. The initial hypothesis is easy to negate: \( n \mid ab \). Therefore, we are trying to prove

\[
\text{“If } n \mid a \text{ or } n \mid b, \text{ then } n \mid ab.\text{”}
\]

Suppose that \( n \) divides \( a \). Then \( a = nc \) for some \( c \in \mathbb{Z} \), and

\[
ab = ncb = n(cb),
\]

so \( n \mid ab \). Similarly, if \( n \mid b \), then \( b = nd \) for some \( d \in \mathbb{Z} \), and

\[
ab = nd = n(ad),
\]

so \( n \mid ab \). Therefore, we have proven the result by contraposition. \( \square \)

Here’s another example. In this one, a direct proof would be awkward (and quite difficult), so contrapositive is the way to go.

**Example B.4.2.** Prove by contrapositive: Let \( x \in \mathbb{Z} \). If \( x^2 - 6x + 5 \) is even, then \( x \) is odd.

**Proof.** Suppose that \( x \) is even. Then we want to show that \( x^2 - 6x + 5 \) is odd. Write \( x = 2a \) for some \( a \in \mathbb{Z} \), and plug in:

\[
x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5
\]

\[
= 4a^2 - 12a + 5
\]

\[
= 2(2a^2 - 6a + 2) + 1.
\]

Thus \( x^2 - 6x + 5 \) is odd. \( \square \)
B.5 Tips and Tricks for Proofs

The four proof techniques that we’ve talked about are really the only ones that people ever use. However, there are some general tips regarding the types of statements that you may be asked to prove. You’ve probably seen many of these via example in these notes, but we’ll list them here anyway.

**If and only if:** Sometimes you are asked to prove something of the form “A if and only if B” or “A is equivalent to B.” The usual way to do this is to prove two things: first, prove that “A implies B,” and then prove that “B implies A.” Use any of the possible techniques to prove these two implications.

**Uniqueness:** You are often asked to prove that some object satisfying a given property is unique. We’ve seen before that the standard trick is to assume that there is another object satisfying the property, and then show that it actually equals the original one.

**Existence:** This sort of proof often goes hand in hand with uniqueness. You are given some specified property, and then asked to show that an object exists which has that property. There are often two ways to do this. One can offer up a **constructive** proof, in which the object is explicitly constructed. A nonconstructive proof is the exact opposite—it shows that the object exists, but it gives no indication as to what the object looks like.

**Existence and Uniqueness:** As stated before, existence and uniqueness go hand in hand. Sometimes you will be asked to prove that an object satisfying some property exists and is unique. This can be done in either order. Sometimes it is easy to prove that the object exists, and then to show that it is unique. However, the existence proof may seem daunting, and it is often helpful to prove uniqueness first. The uniqueness proof may give some hints as to what the object must look like.