Formula Cookbook
Alexander Wu

Proofs (linalg version)

1 Proofs

Writing proofs is one of the most challenging tasks in discrete mathematics. It requires a different mindset that differs from most problems students have encountered in their mathematical experience so far. While building a solid intuition for writing proofs requires time and experience, there are tricks and guidelines one can keep in mind while learning to master proofs. This note attempts to explicitly point out some of those tricks and guidelines.

This note is not a substitute for learning what proofs are. Make sure to read the note on proofs before attempting this note.

2 Why Are Proofs Hard?

You are probably more or less familiar with questions like this:

Example 1: *What are the solutions to the quadratic equation* $x^2 - 4x + 1 = 0$*?*

Solution: Use the quadratic formula: $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a} = \frac{4 \pm \sqrt{16-4}}{2} = 2 \pm \sqrt{3}$, so $x_1 = 2+\sqrt{3}, x_2 = 2-\sqrt{3}$.

These problems have algorithmic solutions, meaning that there is a clear list of steps to solve it. Sometimes you will need to have some intuition of which technique will be best suited for the problem, but overall you can follow a clear path towards the solution.

Contrast that with a proof problem like this:

Theorem 1. The circle constant π is irrational. That is, there are no two integers p, q such that $\pi = \frac{p}{q}$.

There is no algorithm, often not even guidelines for how to approach a problem like this. The proof of this theorem is out of the scope of this course, but to give you and idea of how immensely difficult it is, this was first proved by Johann Heinrich Lambert in 1761, and the proof begins by proving the following identity:

$$\tan(x) = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \ddots}}}}$$

You can imagine that even after reading this proof, you would still be very confused. How did Lambert even think of writing an infinite fraction like this? How did he discover the right pattern

that is exactly equal to the tangent function? How did he know to even use the tangent function to begin with?

Unfortunately, this is the nature of proofs. The final product often contains no indication of how the proof was discovered, and can seem magical and out of nowhere. Because of this, it is very difficult to learn to do proofs by reading existing proofs. One must also see how proofs can be discovered, and the common techniques used. In addition, experience is an integral part of internalizing the proof mindset. (If you are interested, here is a video explaining Lambert's proof.)

3 A First Example: Linear Independence

To explain the process of finding a proof, we will illustrate a possible thought process here in addition to the final proof.

Theorem 2. The vectors $\begin{bmatrix}1\\2\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}$ are linearly independent.

How can we prove two vectors are linearly independent? To do this, we need to know the definition of linear independence:

Vectors $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$ are linearly independent if and only if $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + ... + c_n\mathbf{v}_n = 0$ is only true for real numbers c_i when all $c_i = 0$.

Therefore, we need to show that $c_1 \begin{bmatrix}1\\2\\0\end{bmatrix} + c_2 \begin{bmatrix}1\\1\\1\end{bmatrix} = 0$ can only be true when $c_1 = c_2 = 0$. Let's look at this equation more closely. It looks like a system of linear equations that we can solve with row reduction. Would solving this equation help?

If we solve this equation for c_1, c_2, we are finding all values such that $c_1 \begin{bmatrix}1\\2\\0\end{bmatrix} + c_2 \begin{bmatrix}1\\1\\1\end{bmatrix} = 0$. We would be happy if the only such values are $c_1 = c_2 = 0$. So, let's solve the equation and hope we get the solution $c_1 = c_2 = 0$.

$$\begin{cases} c_1 + c_2 = 0 \\ c_1 + 2c_2 = 0 \\ c_2 = 0 \end{cases}$$

If we solve this system of equations, the only solution is indeed $c_1 = c_2 = 0$. This means we have proved the theorem.

Now that we have a series of logical steps from the given to the conclusion, let's write up the proof:

Proof of Theorem 2. Consider the equation $c_1 \begin{bmatrix}1\\2\\0\end{bmatrix} + c_2 \begin{bmatrix}1\\1\\1\end{bmatrix} = 0$. The solution to this equation gives $c_1 = c_2 = 0$, meaning this is equation is only satisfied in this one case. This is the definition

for linear independence of $\begin{bmatrix}1\\2\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}$, so we have proved the claim. ■

Observe that the final proof is much shorter than the thought process that lead to it. It also doesn't reflect the order in which we would've thought about the problem. No one would see the theorem and first conjure up the equation $c_1\begin{bmatrix}1\\2\\0\end{bmatrix} + c_2\begin{bmatrix}1\\1\\1\end{bmatrix} = 0$ out of thin air; we could only have known this equation is useful by considering first what it means to be linearly independent. However in the proof, we started straight from this equation.

This proof illustrates two useful techniques in coming up with proofs, which are good to keep in mind if you ever feel stuck:

Technique 1. Start from the conclusion. A lot of times it will be very unclear how to get to the conclusion from the assumptions. It can be much easier to start from the conclusion and work your way back. You might have heard you shouldn't assume your conclusion is true. That is correct; instead you start by looking at *what you need to be true in order to prove the conclusion*.

Proofs normally go, "We know A is true, therefore B, therefore C." In this case, we are saying, "We need C to be true, to prove C is it sufficient to prove B, and B is implied by A, which we know to be true." Instead of $A \implies B, B \implies C$, we have $C \impliedby B, B \impliedby A$. Often these statements are joined with "if and only if" like this: $C \iff B, B \iff A$.

When you have obtained the full proof in reverse on scratch paper, you should reverse the order so that it feels more natural, back to $A \implies B, B \implies C$.

Technique 2. Plug in the definition of any concepts or symbols. Often we will deal with new ideas and symbols that you're not familiar with. You can try using their properties that you've learned, but you could also just plug in the definition to convert the problem to a frame of reference you are familiar with.

Sanity check! Where did we use these two techniques in the above thought process?

---

4 Another Example: Invertibility

Theorem 3. A 2×2 matrix $A = \begin{bmatrix}a & b\\c & d\end{bmatrix}$ is invertible if and only if $\det(A) = ad - bc \neq 0$. Moreover, if $\det(A) \neq 0$, then $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix}d & -b\\-c & a\end{bmatrix}$.

How can we prove two statements are in an "if and only if" relationship? Let's try proving implication in both directions.

For proving invertibility implies $\det(A) \neq 0$, let's assume A is invertible. What does that mean? The definition of A being invertible is that there is another 2×2 matrix B such that $AB = BA = I$. So, let's introduce this matrix B.

How can we show some relationship between a, b, c, d? To get some conclusion about the individual entries of A, we must do some operation on those entries instead of talking about everything abstractly. So, let's define the entries of B as well: $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$.

Now we can use the fact that $AB = I$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore:

$$\begin{cases} ae+bg = 1 & (1) \\ af+bh = 0 & (2) \\ ce+dg = 0 & (3) \\ cf+dh = 1 & (4) \end{cases}$$

We want to prove $ad - bc \neq 0$. This doesn't seem very straightforward, so let's try a proof by contradiction. Suppose $ad - bc = 0$.

By looking closely at the equations, we see that (1) and (3) are similar, and (2) and (4) are similar. We don't care about e, f, g, h so we should try to get rid of them. Let's get an expression for e so we can eliminate it from (1) and (3). $e = \frac{1-bg}{a}$, and plugging into (3) we get $c\frac{1-bg}{a} + dg = 0$, or $c - bcg + adg = 0$.

Wait! We have a problem here: you can't divide by a if it's zero. But if we look at the final equation, $c - bcg + adg = 0$, it doesn't divide by a. Wouldn't it be nice if it were still true when $a = 0$? Maybe it is. Let's try plugging in $a = 0$: then we get $bg = 1$ from (1), and the equation $c - bcg + adg = 0$ becomes $c - 1c + 0 = 0$, which is still true. We are allowed to use it either way!

Doing the same thing for (2) and (4), we get $f = \frac{1-dh}{c}$, and $a\frac{1-dh}{c} + bh = 0$ or $a - adh + bch = 0$. This is again still true if $c = 0$.

We haven't yet used your assumption $ad - bc = 0$. Looking at the two equations we obtained above, we see that $c - bcg + adg = c + g(ad - bc) = c = 0$, and $a - adh + bch = a - h(ad - bc) = a = 0$. a and c are both zero. Could we also get that b and d are zero?

Let's look at what we did. We combined two equations to get $ad - bc$, which we could substitute for zero. Then there will be one more variable left that must be zero. How do we engineer the equations to get that $b = 0$? We need b to be the variable that's leftover.

To do that, we can get an expression for h and substitute it into (2). From (4), $h = \frac{1-cf}{d}$, so $af + b\frac{1-cf}{d} = 0$ or $adf + b - bcf = b + f(ad - bc) = b = 0$. Again this should work even when $d = 0$.

Now we know that a and b are both zero. Does that create a contradiction? Yes! Now (1) can't ever be true. We've proved the first direction!

Before we move on to the second direction, let's see if we can make the "this also works for zero" argument more elegant. Can we prove $a - adh + bch = 0$ without dividing by c? We would like to substitute a complete term like ae or bg, which would avoid dividing. We see that the first term here contains dh, so we can get $dh = 1 - cf$ from (4) and plug that into this equation to get $a - a(1 - cf) + bch = acf + bch = c(af + bh) = 0$ by (2). So, we've proved $a - adh + bch = 0$ more simply.

Note that we did our little proof backwards: because of that, we need to make sure every logical step was joined with "is implied by." To verify that it actually works, we can reverse the order of the steps we took. Start with $af + bh = 0$. This implies $c(af + bh) = acf + bch = a - a + acf + bch = a - a(1 - cf) + bch = a - adh + bch = 0$.

The downside here is that only proved this equation instead of *deriving* it. So, anyone who didn't see our thought process would be convinced the equation is true, but still confused about where it came from. But that's again the nature of proofs: they exist only to convince, and do not explain their own origin.

Now, let's prove the other direction; namely that if $ad - bc \neq 0$, then A has an inverse. In fact, we can prove two things at once here: we can prove that if $ad - bc \neq 0$, then A not only has an inverse, but also has an inverse given by $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. How do we prove this?

Again, remember the definition of an inverse: B is an inverse of A if and only if $AB = BA = I$. Since we have an explicit formula, we can plug it in to verify this. The calculations are left to you as an exercise.

Now, we can organize our logic into a proof:

Proof of Theorem 3. First prove that if A is invertible, then $\det(A) \neq 0$. Assume for contradiction that $\det(A) = ad - bc = 0$. Let the inverse of A be $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$. Then we know $AB = I$, or:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore:

$$\begin{cases} ae + bg = 1 & (1) \\ af + bh = 0 & (2) \\ ce + dg = 0 & (3) \\ cf + dh = 1 & (4) \end{cases}$$

From (2) and (4) respectively, $af + bh = 0$ and $dh = 1 - cf$. This means $c(af + bh) = acf + bch = a - a + acf + bch = a - a(1 - cf) + bcg = a - adh + bch = a - h(ad - bc) = a = 0$. Similarly, $d(af + bh) = adf + bdh = adf + b(1 - cf) = adf + b - bcf = b + f(ad - bc) = b = 0$. This

means $a = b = 0$.

However, if $a = b = 0$, (1) gives $0 = 1$, which is a contradiction. This means $ad - bc \neq 0$, proving the first direction.

The second direction, that if $ad - bc \neq 0$ then A^{-1} exists and is given by $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, is left as an exercise. ■

As you may have noticed, this proof again used **Technique 1** and **Technique 2**. We also can see the use of some other techniques:

Technique 3. Make sure you use all of the assumptions given (including ones you make yourself to do a proof by contradiction). It sometimes helps to write them all out. In the middle of a train of thought, it may help to look at the assumptions again and think about which one you haven't leveraged yet.

Technique 4. If you want to prove an equality or inequality, start with one side and manipulate it until you reach the other side. This should be relatively straightforward, but regardless people sometimes forget to try it.

Technique 5. To prove two statements are "if and only if," show that each one implies the other. To prove two values are equal, show that each side is $\leq$ the other. To prove two sets are equal, show that each is a subset of the other.

Sanity check! Where did we use each of these techniques in the above thought process?

---

5 A Final Technique: Greatest Common Divisor

To illustrate one last technique, consider the following theorem:

Theorem 4. Let the greatest common divisor of positive integers x and y ($\gcd(x,y)$) be the maximum integer that divides both x and y. Then any positive common divisor of x and y must divide $\gcd(x,y)$.

Note that the symbol $a \mid b$ means "a divides b." What is the definition of "divides"? It means that for some integer k, $b = ka$. That is, b is a multiple of a.

How can we prove this statement? At first glance there doesn't seem to be any clear direction, so let's look at a few specific numbers.

Let $x = 24, y = 18$. Then the GCD is 6. All positive common divisors of x and y are 1, 2, 3, and 6. These numbers are indeed divisors of 6. But why is this true?

Let's consider what would happen if this weren't true. Let's try to construct an example where the GCD of x and y is 6, but 4 is also a common divisor of x and y. Then x and y must be multiples of both 6 and 4. That means they are both multiples of 12, the least common multiple of 6 and 4. But then 12 would be the actual GCD, not 6!

This seems to suggest an underlying "barrier" that is preventing us from constructing a counterexample. Let's try to use the same argument again, but this time with general variables.

Suppose $\gcd(x,y) = d$. Suppose there is a common divisor c of x and y that does not divide d. This means there exist integers k_1, k_3 such that $x = k_1 c, y = k_3 c$ and integers k_2, k_4 such that $x = k_2 d, y = k_4 d$; but there is no integer k such that $d = kc$. We want to find the least common multiple of c and d.

For example, the least common multiple of 6 and 4 is 12. We can see that $6 \times 4 = 24$, but that goes over; the actual least common multiple is $\frac{24}{2} = 12$. It seems that the last common multiple is the product of the two numbers, divided by their GCD.

With this in mind, let $\gcd(c,d) = e$. Then the least common multiple is $\frac{cd}{e}$. We want to show two things: this divides both x and y, and it is greater than d, thus making it the GCD instead of d. This is just like the example with specific numbers. (Note that we can assume all these numbers are positive.)

To show that it divides x, we know $x = k_1 c = k_2 d$ for integers k_1, k_2. We also know that $c = n_1 e, d = n_2 e$ for coprime integers n_1, n_2 (their GCD is 1). The least common multiple is $\frac{cd}{e} = \frac{n_1 e n_2 e}{e} = n_1 n_2 e$. We want to show that $x = k(n_1 n_2 e)$ for some integer k.

We can try plugging the second set of equations into the first: $x = k_1 n_1 e = k_2 n_2 e$. This means $k_1 n_1 = k_2 n_2$. Since n_1, n_2 can't share factors, k_1 must be divisible by n_2: $k_1 = k n_2$. Finally, this shows $x = k n_2 n_1 e$. In other words, x is a multiple of $n_1 n_2 e$.

Similarly, y is also a multiple of $n_1 n_2 e$. Thus the least common multiple of c, d is a common divisor of x, y.

$n_1 n_2 e = n_1 d$. We want to prove this is greater than d. Since n_1 is positive, we just need to show that it is not 1. Suppose it were 1. Then that would mean $c = n_1 e = e$, and so $d = n_2 e = n_2 c$. Well, c is indeed smaller than d as required... Oh wait, the whole point of c was to not be a divisor of d! So n_1 cannot be 1.

This shows that $n_1 n_2 e > d$. But this contradicts d being the GCD of x and y. Therefore, our initial assumption that there is a common divisor c of x and y that does not divide d was wrong.

The process of writing this as a concise proof is left as an exercise. The point was to illustrate our final proof technique:

Technique 6. If you're asked to prove something is always true, try finding a counterexample. Of course, since it's true, you won't find one. But the failed search will help you understand why the statement is always true. Think about what it is that is preventing you from finding a counterexample. That thing is what you need to leverage in your proof.

You can also try relaxing one of your assumptions, so that now you *can* find a counterexample. Ponder how the assumption ensured that your theorem's conclusion holds.

These are by no means the only handy tricks one can use to come up with a proof; some other ones that come to mind are trying to find patterns in examples, trying to do a constructive proof, making a hypothesis and trying to prove it, giving your constructs names and formal definitions, etc. To

see some of these additional patterns at work, read on to our last example.

6 Putting It All Together: An Involved Proof

You are now ready for a more involved proof that uses most of the techniques we have just discussed. Here is a proof you may see in a math textbook, or an exam's solution key:

Theorem 5 (Bézout's identity). *For $x, y \in \mathbb{N}$, if $\gcd(x,y) = d$, then there exist $a, b \in \mathbb{Z}$ such that $ax + by = d$.*

Proof A: Consider the set $S = \{z \mid z = ax + by > 0, a, b \in \mathbb{Z}\}$. Clearly this is a set of positive integers. Let c be the minimum element of this set. We will prove that c divides both x and y, and every common divisor of x, y must divide c.

To prove $c \mid x$ (c divides x), we know that if we divide x by c we obtain some remainder $0 \leq r < d$, or $x = qc + r$ for some $q \in \mathbb{Z}$. Since c is from the set S, $c = ax + by$ for some $a, b \in \mathbb{Z}$. Therefore $x = q(ax + by) + r = qax + qby + r$, or $(1 - qa)x + (-qb)y = r$. Since $1 - qa, -qb$ are integers, r must be either in the set S, or nonpositive. But $0 \leq r < c$, and c is the smallest element in S, so r must be 0. Therefore $c \mid x$.

Similarly, $c \mid y$.

To prove any common divisor of x, y divides c, observe that if $e \mid x$ and $e \mid y$, then $e \mid (ax + by)$ for any $a, b \in \mathbb{Z}$, so we must have $e \mid c$.

Since c is a common divisor of x, y but is a multiple of every common divisor of x, y, it must be the GCD $c = d$. Since $c \in S$, there must exist a, b such that $ax + by = d$. ■

Now, you must be thinking: that kind of makes sense, but how on earth could I have come up with that? Indeed, how would one have thought of defining the set S out of thin air? Why should we consider the minimum element c, or try to prove that any common divisor of x and y divides it?

Now, we will explain how one would've come up with this proof.

7 A First Attempt

For your convenience, we've divided the reasoning into several portions to make it more organized. But when you are actually pondering a proof, your thought process would probably be very messy, without the organization here.

Part 1: Dividing out d

We know d is the GCD of x and y. That means we can separate x and y into $x'd$ and $y'd$ respectively, where x' and y' are coprime. For example if $x = 24, y = 18$, the GCD is 6 so we can write them as $x = 4 \times 6, y = 3 \times 6$.

Why are we doing this? We're not sure yet, but it seems like it might be useful to separate out the common parts of x and y. We want to find a, b where $ax + by = d$, so plugging in our new values our objective becomes $ax'd + by'd = d$, which reduces to finding a, b such that $ax' + by' = 1$. So if we solve this theorem for coprime x', y', we solve it for all general integers x, y!

Part 2: Trying to find a formula

What should we do now? It would be great if we found an explicit formula for a and b; if there's an explicit formula for them, they certainly exist. But what could we express them in? We already divided out d, so all that's left is x' and y', which doesn't seem like enough to form a formula. Since we're stuck, we can try a few specific numbers to see if we find a pattern.

$x = 3, y = 5 : 3a + 5b = 1$

We find that $a = 2, b = -1$ works. Unfortunately there doesn't seem to be a discernible pattern.

$x = 11, y = 15 : 11a + 15b = 1$

We find $a = -4, b = 3$. There is still no obvious indication how we would obtain these values.

Part 3: Random experimentation

It looks like an explicit formula might not be possible. We'll have to go for a nonconstructive proof: proving a, b exist without actually finding them. How can we do so? We know we must need to use all of the assumptions; right now we haven't yet used that fact that x', y' are coprime. How do we use that?

What's the definition of coprime? It means that the GCD is 1, or equivalently, no integer greater than 1 can divide both x' and y'. That unfortunately isn't a fact that's easy to leverage: it states the absence of something, when we're trying to prove the existence of something.

Nevertheless, we can keep trying stuff until it works. We can turn $ax' + by' = 1$ into $ax' = 1 - by'$. Then we need to find a b such that $1 - by'$ is divisible by x'. We can imagine listing out all of $1 - y'$, $1 - 2y'$, $1 - 3y'$, ... until one is divisible by x'. Our intuition tells us that if x', y' are coprime, eventually there will be a $1 - by'$ that divides x'. But why?

To see why some $1 - by'$ must divide x', we could try to find a counterexample and observe why we fail to find one. If $x' = 5, y' = 3$ then $1 - (1)(3) = -2$, $1 - (2)(3) = -5$, and $1 - (3)(3) = -8$. The second one is a multiple of 5. It seems that 3 and 5 have some inherent property that their multiples will differ by 1 at some point. Unfortunately, we fail to get a hold of some leverage that allows us to continue the proof.

Don't give up yet! To get a better feel for this phenomenon, let's look at an example where x and y are not coprime. Take $4a + 6b$. This sum can be $-4, -2, 0, 2, 4, 6$ etc, but it can never be an odd number because we are only allowed to move in units of 2. But $3a + 5b$ can be all integers because 3 and 5 are coprime.

Part 4: Testing a hunch

This gives us an idea: it seems that the possible values of $ax + by$ will always contain all of the multiples of some value. For example, it can be $1, 2, 3, ...$ or $2, 4, 6, ...$ or $3, 6, 9, ...$ but it can't be $2, 3, 6, 9, ...$ or $1, 3, 5, ...$

Let's try to formalize this and prove it. Let's say the smallest positive value of $ax + by$ for all $a, b \in \mathbb{Z}$ is c. Then all possible values of this expression are kc for some $k \in \mathbb{Z}$. Here we'll just prove that no value can violate this form; it is not needed to prove that every kc is actually obtained.

How do we prove no value can be another form? It's not clear how to prove it directly, so we'll

try contradiction. Suppose $c = a_0x + b_0y$, and there is some violating $e = a_1x + b_1y$. What does it mean to not be of the form kc? Let's say $e = (k+p)c$, where k is an integer and $0 < p < 1$. For example, if $k = 1$ and $p = 0.5$, we have $e = 1.5c$. Why is this not allowed? Well, it seems that if we have c and $1.5c$, we should have $0.5c$ as well to complete the sequence. But $0.5c$ is smaller than c, so it should be the minimum instead!

Let's try it out: if $c = a_0x + b_0y$ and $e = a_1x + b_1y$, then $e - c = (a_1 - a_0)x + (b_1 - b_0)y$. But we also know $e - c = (k - 1 + p)c$, so $(k - 1 + p)c = c(a_1 - a_0)x + (b_1 - b_0)y$. Hmm, that's not very helpful since $(k - 1 + p)c$ could still be larger than c. Instead, we need to subtract kc. $e - kc = (a_1 - ka_0)x + (b_1 - kb_0)y$ and $e - kc = pc$, so $pc = (a_1 - ka_0)x + (b_1 - kb_0)y$. So this fraction of c can be written as a combination of x and y, but it's smaller than c, contradicting the assumption that c was the smallest. This proves our hypothesis: all possible values of $ax + by$ are a multiple of the smallest value.

Part 5: The final step

Now we know there is some integer c where $c \mid ax' + yx'$ for all a, b. We want to show that $c = 1$, because then we have found there is indeed a, b that makes $ax' + by' = 1$. Could c be any other value? Well, let's look at the equation $ax' + by' = kc$ where a, b, and k vary. Experimenting around, we find that setting $a = 1, b = 0$ we get that $c \mid x'$. Setting $a = 0, b = 1$, we find $c \mid y'$ as well. However, x' and y' are coprime, so c must be 1. And we're done!

If you've read proofs before, you're probably tired of seeing the phrase "we're done." It just means that we've finally connected the last link from the assumptions to the conclusion, forming a complete proof.

However, this messy thought process definitely won't do as a proof. We need to reorganize it to be more clear and concise.

8 Writing Up a Proof

The first draft

Let's see what we did to complete the proof. We divided out d to reduce the problem to proving it in the x, y coprime case. Then after some failed experimentation (but nonetheless useful for intuition), we proved that $ax + by$ is always a multiple of its smallest value. Then we showed that this smallest value c divides both x and y, so it is 1 when x and y are coprime. This proves the coprime case, therefore completing the general case.

With this in mind, let's write our proof's first draft.

Proof B: Consider $x' = \frac{x}{d}$, $y' = \frac{y}{d}$. Define the set $S = \{z \mid z = ax' + by' > 0, a, b \in \mathbb{Z}\}$, and let c be the minimum element of S. We will prove that all elements of S are multiples of c.

Assume that is not the case, that some element $e \in S$ has $e = (k+p)c$ where $k \in \mathbb{Z}$ and $0 < p < 1$. We know for some $a_0, b_0, a_1, b_1 \in \mathbb{Z}$, $c = a_0x' + b_0y', e = a_1x' + b_1y'$. Then $e - kc = (a_1 - ka_0)x' + (b_1 - kb_0)y' = pc < c$. This shows $pc \in S$, but we said c was the smallest element of S, creating a contradiction. Therefore, all elements of S are multiples of c.

We know for any a, b there is some k that satisfies $ax' + by' = kc$. Setting $a = 1, b = 0$ we get $c \mid x'$.

Setting $a = 0, b = 1$ we get $c \mid y'$. Since x', y' are coprime, c must be 1. Therefore, there exist a, b such that $ax' + by' = 1$.

Multiplying this equation by d, we obtain $ax'd + by'd = ax + by = d$. This proves the claim. ■

How did we condense the thought process into this proof? Of course, we threw away all the experimentation that didn't directly lead us to the solution, even if it was helpful for discovering the proof (for example, all the experimentation with explicit values). We also changed the order a bit so that instead of saying "We want A to be true, and we can show that it is sufficient to prove B," we can say "B is true, therefore A is true," which is much more intuitive (for example, we moved the part about dividing d to the end). We threw out the path that lead us to define certain useful constructs and directly defined them without explaining where they came from (for example, we directly jumped to defining the set S).

Hopefully you can now see where some of the elements of the proof above came from (most notably how the set S fell from the sky).

Our first draft is a perfectly fine proof. However, let's just say you want to improve it a bit. You don't like that we had to remove d and operate on x' and y' for the entire proof. It seems like many things we did did not require x' and y' to be coprime. So, let's see if we can rewrite the proof to directly manipulate x and y.

In addition, using a fraction p in an integer proof is weird. Instead, observe that the quantity that is really important is $0 < pc < c$, so let's use $r = pc$ instead.

The second draft

Proof C: Define the set $S = \{z \mid z = ax + by > 0, a, b \in \mathbb{Z}\}$, and let c be the minimum element of S. We will prove that all elements of S are multiples of c.

Assume that is not the case, that some element $e \in S$ has $e = kc + r$ where $k \in \mathbb{Z}$ and $0 < r < c$. We know for some $a_0, b_0, a_1, b_1 \in \mathbb{Z}$, $c = a_0x + b_0y, e = a_1x + b_1y$. Then $e - kc = (a_1 - ka_0)x + (b_1 - kb_0)y = r < c$. This shows $r \in S$, but we said c was the smallest element of S, creating a contradiction. Therefore, all elements of S are multiples of c.

We know for any a, b there is some k that satisfies $ax + by = kc$. Setting $a = 1, b = 0$ we get $c \mid x$. Setting $a = 0, b = 1$ we get $c \mid y$. This shows that c is a common divisor of x and y.

Suppose f is another common divisor of x and y. Then f must divide $a_0x + b_0y = c$, which means $c = d$ must be the GCD of x and y. Therefore there exist a, b such that $ax + by = d$. ■

Sanity check! Which proof techniques did we use in the above thought process? Where and how?

This is now looking suspiciously similar to the proof given at the beginning. You might have your personal preference, but proof A is arguably better structured, even if it's a little longer. You can probably see how massaging proof C a little more, taking some alternate paths, could give us proof A.

Note that all the massaging we did was only possible because we had ample time, and wanted an elegant proof. If you're attempting a proof on an exam, you might need to settle for a slightly

messier version. However, I encourage you to try to massage your proofs a little more whenever you have the time.

Congratulations on finishing a very involved proof! Though mastering proofs will likely still take a lot of practice, hopefully you are now better equipped to tackle challenging problems with a proof-writing mindset.

9 Summary: Proof Techniques

Hopefully you now understand the art of writing proofs a little better. Unlike algorithmic calculations, discovering a proof requires a lot of trial and error, and the final product contains only traces of the pains it took it write it. This is also why simply understanding a proof in the solutions is not enough to claim you've mastered it; you need to think about how you could've come up with it on your own, etc.

Let's summarize the main proof techniques discussed.

1. Start from the conclusion and work backwards on scratch paper.
2. Plug in the definition of any symbols or operators.
3. Make sure you use all of the assumptions given.
4. If you want to prove an equality or inequality, start with one side and manipulate it until you reach the other side.
5. To prove two values are equal, show that each side is $\leq$ the other. To prove two statements are "if and only if," show that each one implies the other. To prove two sets are equal, show that each is a subset of the other.
6. Try to find a counterexample. Think about why it is hard to find one. You can also relax one of the assumptions and see if you can now find a counterexample.

Sanity check! Are there any other proof techniques you've noticed?

---

10 Exercises

1. Write up the proof of **Theorem 4**. *Bonus*: Can you massage the proof to make it more concise/organized?
2. Prove the stronger version of **Theorem 4**. That is, for $x, y \in \mathbb{Z}$, d is the greatest common divisor of x and y if and only if every common divisor of x and y divides d (and $d > 0$).
3. Prove that for any $a, b \in \mathbb{R}$ and a function $f : \mathbb{R} \to \mathbb{R}$,
   $\int_a^b f(x)dx = \int_a^b f(a+b-x)dx$

4. There n students, and each student points to one other student. Give a ball to one of the students. When handed the ball, a student passes the ball to the student they are pointing to. Prove that the ball must eventually be passed in a cycle forever; that is, student s_1 passes to s_2, s_2 to s_3, etc, until s_k passes to s_1.

5. *Bonus*: watch this video about an unexpectedly hard proof problem on the International Mathematical Olympiad. *Extra bonus*: write up a proof for this problem. (This video was one of the inspirations of this note.)