

# Proof by Contrapositive

---

I am unsure how much this discussion warrants a document on its own, but here we are.

We discussed how an implication is logically equivalent to its contrapositive. I want to demonstrate that again, and the fact that you can mix and match proving techniques to your liking, so long as you're making the correct arguments.

## The Problem and the Proof

Let's visit our old friend again.

**Problem 1.** Show that an integer  $n$  is even iff  $n^2$  is even.

**Proof.**  $(\rightarrow)$  Showed earlier.

Let's stop there for a second. When I use the notation  $(\rightarrow)$  or  $(\leftarrow)$ , it is to signify what direction of the bi-implication I'm proving. The direction is literally determined by what statement is written before the *iff*. If instead my problem was **Given an integer  $n$  show that  $n^2$  is even iff  $n$  is even**; I would've used a left arrow instead.

Okay, so now we want to prove the left side implication. That is, for an integer  $n$ , if  $n^2$  is even then  $n$  is even.

Do you see a direct path? Well,  $n^2 = 2m$ . Now what? I cannot extract any info about the nature of  $n$  from this.

So we need an indirect proof. Indeed, a proof by contrapositive.

We want to show that if  $n^2$  is even, then  $n$  is even. The contrapositive of this is that if  $n$  is **not** even, then neither is  $n^2$ .

This is much, *much* simpler to approach. If you take the Fundamental Theorem of Arithmetic for granted, this is a 2 line proof. You don't even need the contrapositive in that case.

What I want to do instead is assume Euclid's Division Lemma.

**Lemma 1.** (Euclid) Given  $a, b > 0$ , there are unique  $q, r$  with  $q \geq 0, 0 \leq r < b$  such that  $a = bq + r$ .

Why do I want to do this? Because I want to talk about a special case of this lemma in another proof technique. Let's continue with our original problem.

$(\leftarrow)$  Suppose we know Euclid's Lemma. Then if  $n$  is not even, *(observe the hesitation in saying  $n$  is odd)*

then  $n$  must be of the form  $2m + 1$ . *(Why do we need the lemma? Recall the definition of an even number.)*

Now consider

$$\begin{aligned}n^2 &= (2m + 1)^2 \\&= 4m^2 + 4m + 1 \\&= 2(2m^2 + 2m) + 1 \\&= 2k + 1 \text{ for } k = 2m^2 + 2m\end{aligned}$$

Hence  $n^2$  is not even. □

This is a proof by contrapositive.

## Conclusion

The main takeaway here is not the proof itself, but rather how an iff proof works and how you can mix and match within the same problems.

Further note the importance of assumptions. If I had assumed the fundamental theorem, I would be done in a matter of two lines – since 2 is prime, the  $2 \mid n^2$  means either  $2 \mid n$  or  $2 \mid n$  (breaking  $n^2$  into  $n$  and  $n$ ). However, under Euclid's Lemma, I had to take the indirect route.

Finally, if it is the case that some bi-implication  $p \iff q$  holds, and even if we are able to prove it, we gain **absolutely no information** about  $p$  or about  $q$ . We only gain that they are either both true or both false, but we do not gain which.

More on this in the next.