Warm-up:
Show "if a^2 is even, then a is even."

HW3 solutions available today

Proof by Contradiction

CSE 311 Autumn 2023
Lecture 13

Trying a direct proof

$\forall a(\texttt{Even}(a^2) \rightarrow \texttt{Even}(a))$ "if a^2 is even, then a is even."

Trying a direct proof

$\forall a(\texttt{Even}(a^2) \rightarrow \texttt{Even}(a))$

Let a be an arbitrary integer and suppose that a^2 is even.

By definition of even, $a^2 = 2k$ for some integer k.

Taking the positive square-root of each side, we get $a = \sqrt{2k}$

....

Therefore a is even.

Taking a square root of a variable is tricky! It's hard to do algebra on.

What should we do?

We're trying to show an implication. How can we transform implications? Could that make it easier?

Maybe a transformation that would "switch the order" so that instead of taking a square root, we're squaring…

Take a contrapositive!

Proving by contrapositive

$\forall a(\texttt{Even}(a^2) \rightarrow \texttt{Even}(a)) \equiv \forall a(\neg\texttt{Even}(a) \rightarrow \neg\texttt{Even}(a^2)) \equiv \forall a(\texttt{Odd}(a) \rightarrow \texttt{Odd}(a^2))$

We argue by contrapositive.

Let a be an arbitrary integer and suppose a is odd.

By definition of odd, $a = 2k + 1$ for some integer k.

Squaring both sides, we get $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$

Rearranging, we get $a^2 = 2(2k^2 + 2k) + 1$. Since k is an integer, $2k^2 + 2k$ is an integer, we thus get that a^2 meets the definition of odd (being 2 times an integer plus one), as required.

Since a was arbitrary, we have that for every odd a, that a^2 is also odd, which is the contrapositive of our original claim.

Proof by contrapositive in general

You might write down the contrapositive for yourself, but it doesn't go in the proof.

Tell your reader you're arguing by contrapositive right at the start! (Otherwise it'll look like you're proving the wrong thing!)

The quantifier(s) don't change! Just the implication inside.

Another Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:

Let a, b, c be arbitrary integers, and suppose $a \nmid (bc)$.

Then there is not an integer z such that $az = bc$

…

So $a \nmid b$ or $a \nmid c$

Another Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:

Let a, b, c be arbitrar c).

Then there is not an

…

so $a \nmid b$ or $a \nmid c$

There has to be a better way!

Another Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

There has to be a better way!

If only there were some equivalent implication…

One where we could negate everything…

Take the contrapositive of the statement:

For all integers, a, b, c: Show if $a|b$ and $a|c$ then $a|(bc)$.

By contrapositive

Claim: For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let a, b, c be arbitrary integers, and suppose $a|b$ and $a|c$.

Therefore $a|bc$

By contrapositive

Claim: For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let a, b, c be arbitrary integers, and suppose $a|b$ and $a|c$.

By definition of divides, $ax = b$ and $ay = c$ for integers x and y.

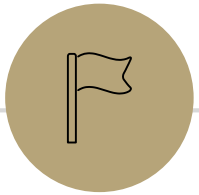
Multiplying the two equations, we get $axay = bc$

Since a, x, y are all integers, xay is an integer. Applying the definition of divides, we have $a|bc$.

Signs you might want to use proof by contrapositive

1. The hypothesis of the implication you're proving has a "not" in it (that you think is making things difficult)
2. The target of the implication you're proving has an "or" or "not" in it.
3. There's a step that is difficult forward, but easy backwards
   e.g., taking a square-root forward, squaring backwards.
4. You get halfway through the proof and you can't "get ahold of" what you're trying to show.
   e.g., you're working with a "not equal" instead of an "equals" or "every thing doesn't have this property" instead of "some thing does have that property"

All of these are reasons you **might** want contrapositive. Sometimes you just have to try and see what happens!



Proof by Contradiction

Proof By Contradiction

Suppose the negation of your claim.

Show that you can derive `False` (i.e. (¬claim) → `F`)

A correct proof shows that the implication is true.

So ¬claim must be `False`.

So claim must be `True`!

Proof By Contradiction Skeleton

Claim: P

Suppose, for the sake of contradiction, $\neg p$

…

q

…

$\neg q$

But q and $\neg q$ is a contradiction! So we must have p.

Proof By Contradiction

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Proof By Contradiction

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

We don't have a fixed target.
That can make this proof harder.

But [] is a contradiction!

Proof By Contradiction

If a^2 is even then a is even.

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = s/t$.

Without loss of generality, let s/t be in lowest terms (i.e., with no common factors greater than 1).

Fancy mathematician speak for "I'm choosing more specific values, but it's ok for me to do that."

That's a contradiction! We conclude $\sqrt{2}$ is irrational.

When can I say without loss of generality?

The claim you're trying to prove is fully general still. What you're doing looks like a new assumption but isn't.

Here: we'd just divide p, q by their common factors (i.e., put the fraction in lowest-terms) and continue the proof.

Other common example:

Let x, y be integers; without loss of generality, assume $x \geq y$ (one of them must be bigger, just give the bigger one the name x).

Only use if your reader will immediately agree that you can still prove the claim! If you're worried, tell the reader how to get those values (here, define p, q as the reduced fraction, and continue with p, q as variables).

Proof By Contradiction

If a^2 is even then a is even.

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = s/t$. Without loss of generality, let s/t be in lowest terms (i.e., with no common factors greater than 1).

$$\sqrt{2} = \frac{s}{t}$$

$$2 = \frac{s^2}{t^2}$$

$2t^2 = s^2$ so s^2 is even.

$t^2 = \frac{s^2}{2}$ ⇐ $s = 2k$, $k \in \mathbb{Z}$.

$2t^2 = 4k^2 \Rightarrow t^2 = 2k^2$

s is even

t is even → not lowest terms

That's a contradiction! We conclude $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even then a is even.

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = s/t$. Without loss of generality, let s/t be in lowest terms (i.e., with no common factors greater than 1).

$$\sqrt{2} = \frac{s}{t}$$

$$2 = \frac{s^2}{t^2}$$

$2t^2 = s^2$ so s^2 is even. By the fact above, s is even, i.e. s= $2k$ for some integer k. Squaring both sides $s^2 = 4k^2$

Substituting into our original equation, we have: $2t^2 = 4k^2$, i.e. $t^2 = 2k^2$.

So t^2 is even (by definition of even). Applying the fact above again, t is even.

But if both s and t are even, they have a common factor of 2. But we said the fraction was in lowest terms.

That's a contradiction! We conclude $\sqrt{2}$ is irrational.

Proof By Contradiction

How in the world did we know how to do that?

In real life…lots of attempts that didn't work.

Be very careful with proof by contradiction – without a clear target, you can easily end up in a loop of trying random things and getting nowhere.

What's the difference?

What's the difference between proof by contrapositive and proof by contradiction?

Show $p \to q$	Proof by contradiction	Proof by contrapositive
Starting Point	$\neg(p \to q) \equiv (p \wedge \neg q)$	$\neg q$
Target	Something false	$\neg p$

Show p	Proof by contradiction	Proof by contrapositive
Starting Point	$\neg p$	---
Target	Something false	---

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Suppose for the sake of contradiction, that there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

But [] is a contradiction! So there must be infinitely many primes.

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Suppose for the sake of contradiction, that there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $q = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$

Case 1: q is prime

Case 2: q is composite

But [] is a contradiction! So there must be infinitely many primes.

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Suppose for the sake of contradiction, that there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $q = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$

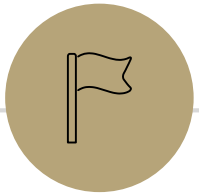
Case 1: q is prime

$q > p_i$ for all i. But every prime was supposed to be on the list $p_1, \ldots, p_k$. A contradiction!

Case 2: q is composite

Some prime on the list (say p_i) divides q. So $q\%p_i = 0$. and $(p_1 p_2 \cdots p_k + 1)\%p_i = 1$. But $q = (p_1 p_2 \cdots p_k + 1)$. That's a contradiction!

In either case we have a contradiction! So there must be infinitely many primes.



Extra Practice

Just the Skeleton

"For all integers x, if x^2 is even, then x is even."

Just the Skeleton

"For all integers x, if x^2 is even, then x is even."

Suppose for the sake of contradiction, there is an integer x, such that x^2 is even and x is odd.

…

[] is a contradiction, so for all integers x, if x^2 is even, then x is even.

Just the Skeleton

"There is not an integer k such that for all integers n, $k \geq n$.

Just the Skeleton

"There is not an integer k such that for all integers n, $k \geq n$.

Suppose, for the sake of contradiction, that there is an integer k such that for all integers n, $k \geq n$.

…

[] is a contradiction! So there is not an integer k such that for all integers n, $k \geq n$.