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

If a odd then a^2 is odd

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

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

⋮

a is even

Proof by Contradiction

CSE 311 Winter 2022
Lecture 15

If a^2 is even then a is even

Proof:

We argue by contrapositive.

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

a^2 is odd.

If a^2 is even then a is even

Proof:

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.

$a^2 = (2k+1)^2 = 4k^2 + 4k + 1$.

Factoring, $a^2 = 2(2k^2 + 2k) + 1$.

Since k was an integer, $2k^2 + 2k$ is an integer.

So a^2 is odd by definition.

Announcements

We're posting the handouts and solutions for this week's section later today.

- We think you could use another example or two of properly formatted induction proofs.
- They're primarily "study for the midterm" materials…no harm having those early.

You should still go to section this week through, your TAs are more useful than the written solutions.

I'll post the slides for Friday (induction practice day) late tonight as well.

Stamp Collection, Done Wrong

Define $P(n)$ I can make n cents of stamps with just 4 and 5 cent stamps.

We prove $P(n)$ is true for all $n \geq 12$ by induction on n.

Base Case:

12 cents can be made with three 4 cent stamps.
Inductive Hypothesis Suppose $P(k)$, $k \geq 12$.

Inductive Step:

We want to make $k + 1$ cents of stamps. By IH we can make k cents exactly with stamps. Replace one of the 4 cent stamps with a 5 cent stamp.

$P(n)$ holds for all n by the principle of induction.

Stamp Collection, Done Wrong

What if the starting point doesn't have any 4 cent stamps?

Like, say, 15 cents = 5+5+5.

Proof By Contradiction

Proof By Contradiction

Goal P

Start: $\neg P$

Suppose the negation of your claim.

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

Start → Ending

If your proof is right, the implication is true.

So ¬claim must be `False`.

So claim must be `True`!

T → claim

True

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.

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

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 $\sqrt{2} = s/t$

Let $p = \frac{s}{\gcd(s,t)}$, $q = \frac{t}{\gcd(s,t)}$ By the fundamental theorem of arithmetic, we have divided out all common factors of s, t and so p, q have no more common prime factors. Therefore the $\gcd(p, q) = 1$.

$\sqrt{2} = \frac{p}{q}$

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 $\sqrt{2} = s/t$

Let $p = \frac{s}{\gcd(s,t)}, q = \frac{t}{\gcd(s,t)}$ By the fundamental theorem of arithmetic, we have divided out all common factors of s, t and so p, q have no more common prime factors. Therefore the $\gcd(p, q) = 1$.

$\sqrt{2} = \frac{p}{q}$

$2 = \frac{p^2}{q^2}$

$2q^2 = p^2$ so p^2 is even.

$2q^2 = p^2 \rightarrow p$ is even

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 $\sqrt{2} = s/t$

Let $p = \frac{s}{\gcd(s,t)}, q = \frac{t}{\gcd(s,t)}$ By the fundamental theorem of arithmetic, we have divided out all common factors of s, t and so p, q have no more common prime factors. Therefore the $\gcd(p, q) = 1$.

$\sqrt{2} = \frac{p}{q}$

$p = 2k \quad k \in \mathbb{Z}$

$2 = \frac{p^2}{q^2}$

$p^2 = 4k^2$

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

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

$2q^2 = 4k^2$

So q^2 is even. Applying the fact above again, q is even.

$q^2 = 2k^2$

But if both p and q are even, $\gcd(p, q) \geq 2$. But we said $\gcd(p, q) = 1$

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?

$p \rightarrow q$

Show $p \rightarrow q$	Proof by contradiction	Proof by contrapositive
Starting Point	$\neg(p \rightarrow q) \equiv (p \wedge \neg q)$	$\neg q$
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:

"There are no prime #'s past a certain point"

"there are a limited # of 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 $p_1, p_2, \dots, p_k$.

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 $q = \boxed{p_1 \cdot p_2 \cdot \cdots \cdot p_k} + 1$

$p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_k + 1$

Case 1: q is prime

$q > p_i \; \forall i$

Case 2: q is composite

some p_i $\quad q \,\%\, p_i = 0$

$p_1 \cdots p_k$ $\quad q \,\%\, p_i = 1$

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.