This Week

• Finish last week’s proof

For all integers $a$, $b$ and $n$ with $n \geq 1$, $a \equiv_n b$ iff $n$ divides $a - b$.

• Indirect Proofs

→ Proof by Contrapositive
→ Proof by Contradiction
1 Indirect Proofs

There are two main indirect proof methods. Proof by contrapositive and proof by contradiction.

1.1 Proof by Contrapositive

If we need to prove an implication such as \( \forall x \in D, p(x) \rightarrow q(x) \) then we have the option of proving \( \forall x \in D, \neg q(x) \rightarrow \neg p(x) \).

Let’s practice writing the contrapositive (and the negation for when we write proofs by contradiction):

For each of the following statements, write in predicate logic as an implication, then the contrapositive and then the negation. Assume that the universe is \( \mathbb{Z}^+ \).

1. Divisibility by 21 is a sufficient condition for divisibility by 7.

2. \( m \) divides \( p \) is a necessary condition for \( m \) to divide \( n \) and \( n \) to divide \( p \).

3. There are some integers whose squares are odd. Use \( q(n) : n^2 \text{ is odd} \) and \( p(n) : n \text{ is odd} \).

4. The square of any odd integer is odd.
Now let’s write a proof by *contrapositive*:

**Claim.** Suppose $x$ and $y$ are positive real numbers such that the geometric mean does not equal the arithmetic mean, *i.e.* $\sqrt{xy} \neq \frac{x+y}{2}$, then $x \neq y$.

We can write this formally as

$$\forall x \in \mathbb{R}^+, \forall y \in \mathbb{R}^+, \sqrt{xy} \neq \frac{x+y}{2} \rightarrow x \neq y$$

Notice that proving this directly is hard...so let’s try the *contrapositive*.

Write the contrapositive of our claim:

**Proof by Contrapositive.**
Summary:

**Proof by Contrapositive.**

Claim: \( \forall x \in D, p(x) \rightarrow q(x) \)

Let \( x \in D \) be arbitrary.

Assume \( \neg q(x) \).

\[ \vdash \]

Derive \( \neg p(x) \), so \( \neg q(x) \rightarrow \neg p(x) \).

By the contrapositive, \( p(x) \rightarrow q(x) \).

Conclude \( \forall x \in D, p(x) \rightarrow q(x) \).

---

1.2 **Proof by Contrapositive Practice**

**Claim.** \( \forall x \in \mathbb{Z}, (x^2 - 6x + 5) \) is even \( \rightarrow \) \( x \) is odd.

**Proof.**

**Claim.** \( \forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \forall n \in \mathbb{N}, (a^2 \not\equiv_n b^2) \rightarrow (a \not\equiv_n b) \).

Why is this hard to prove directly?

**Proof.**
Claim. \( \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, (y^3 + yx^2 \leq x^3 + xy^2) \rightarrow y \leq x. \)

Proof.

**CHALLENGE.** Let \( n \in \mathbb{N}, \) if \( 2^n - 1 \) is prime then \( n \) is prime.

**Proof.** State the *contrapositive:*

Let’s complete the proof:
2 Proof by Contradiction

For our next examples we need a basic definition and a theorem.

Definition.

A prime number is a number that can only be divided evenly by 1 or itself.

Fundamental Theorem of Arithmetic.

Any integer greater than 1 is either a prime number, or can be written as a unique product of prime numbers (ignoring the order).

2.1 Proof by Contradiction

Claim. \(\sqrt{2}\) is irrational.

Proof. What does irrational mean? How can we express this in mathematical notation?

Q. How do we symbolically write that \(\sqrt{2}\) is rational?

A.

Then to say irrational, we simply put a not in front:

Q. How can we show that for all pairs of integers \(p, q, \sqrt{2} \neq \frac{p}{q}\)? This is very hard. Solution?

A.

Proof. We want to show that \(\sqrt{2}\) is irrational.

We will use proof by contradiction.

Suppose that \(\sqrt{2}\) is rational. Then,
Q. How many prime factors does $p^2$ have? $q^2$?

A.

Q. How many prime factors does $2p^2$ have?

A.

Therefore...

And we can conclude that our original assumption that $\sqrt{2}$ is rational must be incorrect and $\sqrt{2}$ is irrational.

Another proof...

Theorem.

There are an infinite number of primes.

Proof.

Q. How can we prove this directly? How can we show a set is infinite?

A. Not easy in this case.
We will prove that there are an infinite number of primes using *proof by contradiction*.

**Summary:**

**Proof by Contradiction.**

Claim: \( P \)

Assume \( \neg P \).

Derive a *false* statement.

Conclude the assumption was wrong. Therefore \( P \).

**Q.** Suppose our claim \( P \) above is of the form \( \forall x \in X, a(x) \rightarrow b(x) \). What is \( \neg P \)?

**A.**
2.2 Proof by Contradiction Practice

Prove the following claims using proof by contradiction.

Claim: \( \forall n \in \mathbb{Z}, n^2 \text{ is even } \rightarrow n \text{ is even} \).

Proof.

First restate the claim by taking the negation.

Now prove the claim.

Claim: The difference of any rational number and any irrational number is irrational.

Proof.

First restate the claim by taking the negation.

Now prove the claim.

Claim: \( \sqrt{5} \text{ is irrational.} \)

Proof.

First restate the claim by taking the negation.

Now prove the claim.

3 Proof by Cases - aka Proof by Exhaustion

Claim. Prove that if \( n \in \mathbb{Z} \), then \( 3n^2 + n + 14 \) is even.

Proof.

Two cases:

Case 1: \( n \) is even.

Case 2: \( n \) is odd.
Proof by Cases.

Claim: \( \forall x \in D, p(x) \rightarrow q(x) \)

Split the domain \( D \) into disjoint sets \( S_1, S_2, \ldots, S_k \) such that their union equals \( D \).

For each set \( S_i \) show that \( \forall x \in S_i, p(x) \rightarrow q(x) \).

Since \( \bigcup_i S_i = D \), conclude that \( \forall x \in D, p(x) \rightarrow q(x) \).

More Practice - All proof techniques.

Claim. Prove for every prime number \( p > 3 \), \( p = 6n + 1 \) or \( p = 6n + 5 \). First write the statement using quantifiers and logic and then prove it’s correctness.

Claim. \( \forall a \in \mathbb{Z}, a \equiv_6 3 \rightarrow a \not\equiv_3 2 \)

Prove the statement.