CSCA67 Worksheet – Indirect Proofs

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

1 Proof by Contradiction

Claim. $\sqrt{2}$ is irrational.

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

We know how to say that $\sqrt{2}$ is rational:

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

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

A.

Proof continued...

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. Suppose that the set is *not* infinite.

Proof continued...

Summary:

Proof by Contradiction.
Claim: P
Assume $\neg P$.
Derive a *false* statement.
Conclude the assumption was wrong. Therefore P.

2 Proof by Contrapositive

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

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

We can write this formally as

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

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

Write the contrapositive of our claim:

Proof by Contrapositive.

Claim. Let $n \in \mathbb{N}$, if $2^n - 1$ is prime then n is prime.

Proof.

Contrapositive:

Let's complete the proof:

Summary:

PROOF BY CONTRAPOSITIVE.

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

Let $x \in D$ be arbitrary.

Assume $\neg q(x)$.

$\vdots$

Derive $\neg p(x)$, so $\neg q(x) \to \neg p(x)$.

By the contrapositive, $p(x) \to q(x)$.

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

Extra practice: On your own time, prove each of the following:

- $\forall x \in \mathbb{Z}, (x^2 - 6x + 5)$ is even $\rightarrow x$ is odd.
- $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, (y^3 + yx^2 \leq x^3 + xy^2) \rightarrow y \leq x$.
- $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \forall n \in \mathbb{N}, (a \equiv_n b) \rightarrow (a^2 \equiv_n b^2)$.

3 Proof by Cases - aka Proof by Exhaustion

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

Proof.

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