

# What is a proof?

A good proof should have:

- A clear statement of what is to be proved (labeled as Theorem, Lemma, Proposition, or Corollary).
- The word “Proof” to indicate where the proof starts.
- A clear indication of flow.
- A clear justification for each step.
- A clear indication of the conclusion.
- The abbreviation “QED” (“Quod Erat Demonstrandum” or “that which was to be proved”) or equivalent to indicate the end of the proof.

# Summary of Proof Methods

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Exhaustive Proof
- Proof by cases

# Statement of Theorems

The following are equivalent:

- The sum of two positive integers is positive.
- If  $m, n$  are positive integers then their sum  $m + n$  is a positive integer.
- For all positive integers  $m, n$  their sum  $m + n$  is a positive integer.
- $(\forall m, n \in \mathbb{Z}) [((m > 0) \wedge (n > 0)) \rightarrow ((m + n) > 0)]$

# Number Definitions

## Definition

An integer  $n$  is *even* if  $n = 2k$  for some integer  $k$ , and is *odd* if  $n = 2k + 1$  for some integer  $k$ .

## Definition

A number  $q$  is *rational* if there exist integers  $a, b$  with  $b \neq 0$  such that  $q = a/b$ .

## Definition

A real number that is not rational is *irrational*.

# Closure

- $\mathbb{Z}$  is closed under addition.  
If  $a, b \in \mathbb{Z}$  then  $a + b \in \mathbb{Z}$ .
- $\mathbb{Q}^{\neq 0}$  is closed under division.  
If  $q, r \in \mathbb{Q}^{\neq 0}$  then  $\frac{q}{r} \in \mathbb{Q}^{\neq 0}$ .
- $\mathbb{Z}^{\neq 0}$  is *not* closed under division.  
 $\frac{3}{5} \notin \mathbb{Z}^{\neq 0}$ .

# Direct Proofs

- The square of an even number is even.
- The product of two odd numbers is odd.
- The sum of two rational numbers is rational.

Do in class.

# Proof by Contraposition

- If  $3n + 2$  is odd, where  $n$  is an integer, then  $n$  is odd.
- If  $n^2$  is even, where  $n$  is an integer, then  $n$  is even.
- If  $n = ab$ , where  $a$  and  $b$  are positive integers, then  $a \leq \sqrt{n}$  or  $b \leq \sqrt{n}$ .      What is the domain for  $n$ ?

Do in class.

# Proof by Contradiction

- At least four of any 22 days must fall on the same day of the week.
- $\sqrt{2}$  is irrational.

Do in class.



# Proofs of Equivalence

- If  $n$  is an integer, then  $n$  is odd if and only if  $n^2$  is odd.
- The following statements about the integer  $n$  are equivalent:
  - ▶  $n$  is even.
  - ▶  $n - 1$  is odd.
  - ▶  $n^2$  is even.

Do in class.

# Exhaustive Proofs

- For all positive integers  $n$  with  $n \leq 4$ ,  $(n + 1)^3 \geq 3^n$ .
- There are no integer solutions to the equation  $x^2 + 3y^2 = 8$ .

Do in class.

# Interesting vs Boring: Round I

- Every number  $\leq 100$  can be written as the sum of nine cubes. Can be proven by exhaustion. **boring proof of boring statement.**
- Every number can be written as the sum of nine cubes. Can be proven by **very interesting mathematics**
- Is nine optimal? Yes: 23 requires nine cubes.

**Do in Class**

# Interesting vs Boring: Round II

- Every number can be written as the sum of nine cubes. Nine is optimal since 23 requires nine.
- If every number except 23 can be written as the sum of eight cubes that seems **more interesting**.

**What is the Right Question to Ask?**

# Proofs by Cases

- For every integer  $n$ ,  $n^2 \geq n$ .
- If  $n$  is odd then  $n^2 = 8m + 1$  for some integer  $m$ .

Do in class.

# Existence Proofs

There exists a positive integer that is the sum of two cubes of positive integers in two different ways.

$$\begin{aligned} &(\exists p, q, r, s, n \in \mathbb{Z}^+) \\ &[(p \neq q) \wedge (p \neq r) \wedge (p \neq s) \\ &\wedge (q \neq r) \wedge (q \neq s) \wedge (r \neq s) \\ &\wedge (n = p^3 + q^3) \wedge (n = r^3 + s^3)] \end{aligned}$$

**Tell Story**

# Existence Proofs

$$(\exists x, y \in \mathbb{R} - \mathbb{Q})[x^y \in \mathbb{Q}]$$

Do in class.