Chapter 3: Proofs

Some Rules:

- You may assume and use basic properties of numbers (so long as they are correct).
- You may use any result proved in class or in the homework.
- Break down your argument into steps, each of which is clearly justified.
- When in doubt, err on the side of giving more details rather than less. (Very often, when people are lazy about giving full details, they fail to realize that there is actually a logical error or gap in their argument.)

This is one of the reasons that writing proofs is important!

- It is best to avoid overusing logical symbols (like "$\Rightarrow$"), though sometimes they can be helpful.

In the next few lectures we will consider various examples of proof methods.

Direct Proofs:

- When we prove "$P \Rightarrow Q$" is true by a direct chain of reasoning:

$$\text{"} P \Rightarrow P' \Rightarrow P'' \Rightarrow \cdots \Rightarrow Q \text{"}$$

Examples:

Proposition: For positive real numbers a, b,

$$a < b \Rightarrow a^2 < b^2.$$

When we write this it means we are claiming the proposition is true.

Proof:

Let a and b be positive real numbers.

Suppose $a < b$.

Then, since $a > 0$, $a^2 < ba$.

Similarly, since $b > 0$, $ba < b^2$.

Thus $a^2 < ba < b^2$, as required.

Since a and b were arbitrary, the result follows for all positive real numbers a and b $\square$

We fix the free variables involved in the predicates $a<b$ and $a^2<b^2$ so that these predicates become propositions.

To prove an implication we always assume the hypothesis is true and then prove the conclusion is true.

Proposition: For real numbers a, b,

$$a < b \implies 4ab < (a+b)^2.$$

Scratchwork:

Given real numbers a, b,

$$\begin{aligned} 4ab < (a+b)^2 &\iff 4ab < a^2 + 2ab + b^2 \\ &\iff 0 < a^2 - 2ab + b^2 \\ &\iff 0 < (a-b)^2 \\ &\iff a \neq b. \end{aligned}$$

→ **Proof:**

Given real numbers a, b,

$$\begin{aligned} a < b &\implies a \neq b \\ &\implies 0 < (a-b)^2 \\ &\implies 0 < a^2 - 2ab + b^2 \\ &\implies 4ab < a^2 + 2ab + b^2 \\ &\implies 4ab < (a+b)^2 \end{aligned}$$

as required. $\square$

Divisibility of Integers

Definition: Let a and b be integers. We say that *a divides b* if there is an integer q such that $aq = b$.

Note: If $a \neq 0$ then $aq = b \implies q = \frac{b}{a}$.

Notation: "$a \mid b$" means "a divides b".

Definition: An integer a is said to be *even* if $2 \mid a$, otherwise it is said to be *odd*.

We can list the even integers

$$\ldots, -4, -2, 0, 2, 4, 6, \ldots$$

so the odd integers are

$$\ldots, -3, -1, 1, 3, 5, \ldots$$

and we have:

Basic Fact: An integer a is odd if and only if $a+1$ is even.

Proposition: The square of an even integer is even. That is, for integers a,

$$2 \mid a \Rightarrow 2 \mid a^2.$$

Proof:

Let a be an even integer.

Then $a = 2q$ for some integer q.

So $a^2 = 4q^2 = 2(2q^2)$.

Now $2q^2$ is an integer, so $2 \mid a^2$. $\square$

Now let's consider a different method of proof:

Proof by Cases.

Proof by Cases (Example):

Proposition: For integers a, b, if $a+b$ is even then a and b are both odd or both even.

Proof: Let a, b be integers. Suppose $a+b$ is even. The integer a must be either even or odd, so we divide into cases.

Case 1 (a even): If a is even then $a = 2m$ for some integer m. Since $a+b$ is even, $a+b = 2n$ for some integer n. So

$$b = (a+b) - a = 2n - 2m = 2(n-m).$$

Since $n-m$ is an integer, b is even.

Case 2 (a odd): If a is odd then $a = 2m+1$ for some integer m. Since $a+b = 2n$ for some integer n we have

$$\begin{aligned} b &= (a+b) - a = 2n - 2m - 1 \\ &= 2(n-m) - 1 = 2(n-m-1) + 1. \end{aligned}$$

Since $n-m-1$ is an integer, b is odd. $\square$