Lecture 3.2: Parity, and proving existential statements

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4190, Discrete Mathematical Structures

Overview

Definition

An integer n is:

- even iff $\exists k \in \mathbb{Z}$ such that $n = 2k$,
- odd iff $\exists k \in \mathbb{Z}$ such that $n = 2k + 1$,
- prime iff $n > 1$ and $\forall a, b \in \mathbb{Z}^+$, if $n = ab$, then $n = a$ or $n = b$.
- composite iff $n > 1$ and $n = ab$ for some integers $1 < a, b < n$.

Examples

Let's think about what would be needed to establish the following statements.

1. (Proving $\exists$). Show that there exists an even integer that can be written as a sum of two prime numbers in two ways.
2. (Disproving $\exists$). Show that there does not exist $a, b, c \in \mathbb{Z}$, and $n > 2$ such that $a^n + b^n = c^n$.
3. (Proving $\forall$). Show that "$2^{2^n} + 1$ *is prime*, $\forall n$".
4. (Disproving $\forall$). Show that the statement "$2^{2^n} + 1$ *is prime*, $\forall n$" is actually false.

In this lecture, we'll focus on parity (even vs. odd), and proving existential statements.

Proving an existential statement

A statement such as

$$\exists x \in U \text{ such that } Q(x)$$

is true iff

$$Q(x) \text{ is true for at least one } x \in U.$$

There are several ways to prove such a statement:

1. Constructively: find or construct such an x.
2. Non-constructively: show that such an x must exist, by an axiom, theorem, or other means.
3. Indirectly: by contrapositive or contradiction.

Examples of constructive proofs

Proposition

There exists an integer that can be written as a sum of two prime numbers in two ways.

Proof

We'll find such an integer. Note that

$$10 = 5 + 5 = 3 + 7.$$

□

Proposition

Let n and m be odd integers. Then $n + m$ is even, i.e., $n + m = 2k$ for some $k \in \mathbb{Z}$.

Proof

We'll construct a way to write $n + m = 2k$.

First, write $n = 2a + 1$ and $m = 2b + 1$ for some $a, b \in \mathbb{Z}$.

Note that $n + m = (2a + 1) + (2b + 1) = 2(a + b) + 2 = 2(a + b + 1)$, hence $n + m$ is even. □

Examples of non-constructive and indirect proofs

Proposition

There exist irrational numbers $x, y \in \mathbb{R}$ such that x^y is rational.

Proof

If $\sqrt{2}^{\sqrt{2}}$ is rational, we're done. (Let $x = y = \sqrt{2}$).

If $\sqrt{2}^{\sqrt{2}}$ is irrational, let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Note that

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = 2.$$

□

Proposition

Prove that if $5n + 2$ is odd, then n is odd.

Proof (by contrapositive)

Suppose that n is even, i.e., $n = 2k$.

Then $5n + 2 = 5(2k) + 2 = 2(5k + 1)$ is even. □

More practice

Proposition

An integer n is even if and only if $n+1$ is odd.

Proof

Disproving existential statements

To disprove an existential statement,

$$\exists x \in U \text{ such that } Q(x),$$

we have to show that

$$\forall x \in U,\ \neg Q(x),$$

i.e., prove a universal statement.

This will be the focus of the next lecture. We've actually done a few of these already.

For example, rephrasing an earlier result:

Proposition

For all odd integers n and m, the sum $n + m$ is even.