# Lecture 3.3: Proving universal 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 prime factorization and proving universal statements.

# Proving a universal statement

Examples of universal statements have the form

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

or

$$\forall x \in U \text{ if } P(x), \text{ then } Q(x).$$

There are several ways to prove such a statement:

(i) Exhaustion: if $|U| < \infty$, verify that it holds for all $x \in U$.
(ii) Direct proof: let $x \in U$ be arbitrary, and show that $P(x)$ implies $Q(x)$.
(iii) Indirect proof (contrapositive): assume $\neg Q(x)$ and show $\neg P(x)$.
(iv) Indirect proof (contradiction): assume $\neg Q(x)$ for some $x \in U$, and find a contradiction.

## Examples

1. $\forall n = 0, 1, \ldots, 40$: $n^2 - n + 41$ is prime.
2. $\forall n \in \mathbb{Z}$: $n$ is odd implies that $n^2$ is odd.
3. $\forall r, s \in \mathbb{R}$: if $r \in \mathbb{Q}$ and $s \notin \mathbb{Q}$, then $r + s \notin \mathbb{Q}$.
4. $\forall$ primes $p$, there is a larger prime $q > p$.

To disprove a universal statement, it suffices to find one counterexample.

# Proving universal statements

## Examples

1. $\forall n = 0, 1, \dots, 40$: $n^2 - n + 41$ is prime.
2. $\forall n \in \mathbb{Z}$: $n$ is odd implies that $n^2$ is odd.
3. $\forall r, s \in \mathbb{R}$: if $r \in \mathbb{Q}$ and $s \notin \mathbb{Q}$, then $r + s \notin \mathbb{Q}$.
4. $\forall$ primes $p$, there is a larger prime $q > p$.

# Disproving universal statements

## Definition

The $n^{\text{th}}$ Fermat number is $F_n := 2^{2^n} + 1$.

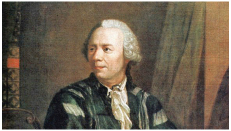
The first few are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, $F_5 = 4294967297$.

## Conjecture (Pierre Fermat, 1650)

$F_n$ is prime for all $n$.

In 1732, Leonhard Euler disproved Fermat's conjecture by demonstrating

$F_5 = 2^{2^5}+1 = 2^{32}+1 = 4294967297 = 641 \cdot 6700417$ .



So far, every $F_n$ is known to be composite for $5 \leq n \leq 32$. In 2014, a computer showed that $193 \times 2^{3329782} + 1$ is a prime factor of

$$F_{3329780} = 2^{2^{3329780}} + 1 > 10^{10^{10^6}} .$$

It is not known if any other Fermat primes exist!

# Some conjectures

## Conjecture

The number $n^2 - n + 41$ is prime, for all integers $n \geq 0$.

## Counterexample

This is true for $n = 0, 1, \ldots, 40$, but $41^2 - 41 + 41 = 41^2$ is not prime.

## Conjecture (Leonhard Euler, $18^{\text{th}}$ century)

There are no integer solutions to $a^4 + b^4 + c^4 = d^4$.

## Counterexample (1987)

$95800^4 + 217519^4 + 414560^4 = 422481^4$.

## Goldbach Conjecture ($18^{\text{th}}$ century)

Every even integer greater than 2 is the sum of two prime numbers.

## Current state of knowledge

True for (at least) $n = 4, 6, \ldots, 4 \times 10^{18}$.