37181 DISCRETE MATHEMATICS

Prof Murray Elder, UTS

Lecture 3: proofs

PLAN

- proof methods:
    - direct
    - contrapositive
    - contradiction

Proofs in mathematics or computer science are based on the argument forms we started to learn last week.

To start with, the main types of proof styles are:

- direct
- contrapositive
- contradiction
- induction

If you do more math or theoretical computer science you will see more styles.

DIVIDES

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\exists s \in \mathbb{Z}$ such that $b = as$.

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\exists s \in \mathbb{Z}$ such that $b = as$.

For example, 3 divides -18 since

DIVIDES

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\exists s \in \mathbb{Z}$ such that $b = as$.

For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\exists s \in \mathbb{Z}$ such that $b = as$.

For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since for all $s \in \mathbb{Z}$ $14 \neq 3s$.

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\exists s \in \mathbb{Z}$ such that $b = as$.

For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since for all $s \in \mathbb{Z}$ $14 \neq 3s$.

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

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* $(p \to r)$ and $(r \to s)$ and $(s \to t)$ and $(t \to q)$).

Recall that an integer n is *even* if

DIRECT

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* ($p \to r$) and ($r \to s$) and ($s \to t$) and ($t \to q$)).

Recall that an integer n is *even* if $2 \mid n$, that is, it can be written as $n = 2d$ for some $d \in \mathbb{Z}$.

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* ($p \to r$) and ($r \to s$) and ($s \to t$) and ($t \to q$)).

Recall that an integer n is *even* if $2 \mid n$, that is, it can be written as $n = 2d$ for some $d \in \mathbb{Z}$.

Lemma

Let $n \in \mathbb{Z}$. If n is even then n^2 is even.

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* $(p \to r)$ and $(r \to s)$ and $(s \to t)$ and $(t \to q)$).

Recall that an integer n is *even* if $2 \mid n$, that is, it can be written as $n = 2d$ for some $d \in \mathbb{Z}$.

Lemma

Let $n \in \mathbb{Z}$. If n is even then n^2 is even.

Proof.

By hypothesis, $n = 2s$ for some $s \in \mathbb{Z}$. Then

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* $(p \to r)$ and $(r \to s)$ and $(s \to t)$ and $(t \to q)$).

Recall that an integer n is *even* if $2 \mid n$, that is, it can be written as $n = 2d$ for some $d \in \mathbb{Z}$.

Lemma

Let $n \in \mathbb{Z}$. If n is even then n^2 is even.

Proof.

By hypothesis, $n = 2s$ for some $s \in \mathbb{Z}$. Then $n^2 = (2s)^2 = 4s^2 = 2(2s^2)$ is even. $\square$

YOUR TURN

Lemma

If $n \in \mathbb{Z}$ is even then n^3 is even.

Proof.

Lemma

If $n \in \mathbb{Z}$ is even then n^3 is even.

Proof.

By hypothesis, $n = 2s$ for some $s \in \mathbb{Z}$. Then $n^3 = (2s)^3 = 2(4s^3)$ is even. $\square$

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

? direct doesn't work $\square$

CONTRAPOSITIVE

Recall that $p \to q$ is logically equivalent to (has the same truth values as) $\neg q \to \neg p$.

Check this with a truth table.

Recall that $p \to q$ is logically equivalent to (has the same truth values as) $\neg q \to \neg p$.

Check this with a truth table.

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Instead of trying to prove this directly, we will prove $\neg$ (n is even) implies $\neg$ (n^2 is even).

Recall that $p \to q$ is logically equivalent to (has the same truth values as) $\neg q \to \neg p$.

Check this with a truth table.

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Instead of trying to prove this directly, we will prove $\neg$ (n is even) implies $\neg$ (n^2 is even).

In other words, if n is odd then n^2 is odd.

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

If n is odd, then $n = 2s + 1$ for some $s \in \mathbb{Z}$,

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

If n is odd, then $n = 2s + 1$ for some $s \in \mathbb{Z}$, so
$n^2 = 4s^2 + 4s + 1 = 2(2s^2 + 2s) + 1$ which is an odd number.

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

If n is odd, then $n = 2s + 1$ for some $s \in \mathbb{Z}$, so
$n^2 = 4s^2 + 4s + 1 = 2(2s^2 + 2s) + 1$ which is an odd number.

Since the statement we have proved (the contrapositive) is logically equivalent to the original statement to be shown, we are done. $\square$

PRIMES

A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

Contrapositive is:

A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

Contrapositive is:

Proof.

A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

Contrapositive is:

Proof.

If n is even then $n = 2s$ so 2 divides n. Then $n \leqslant 2$ or $n > 2$, and if $n > 2$ it it cannot be prime since it has 2 as a divisor. $\square$

A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

Contrapositive is:

Proof.

If n is even then $n = 2s$ so 2 divides n. Then $n \leqslant 2$ or $n > 2$, and if $n > 2$ it it cannot be prime since it has 2 as a divisor. $\square$

Note in my proof, I added a hypothesis $q \vee \neg q$ half way!

PRIMES

If you start to list prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots$$

PRIMES

If you start to list prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots$$

they seem to appear less and less often. So do they run out eventually?

If you start to list prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots$$

they seem to appear less and less often. So do they run out eventually?

Theorem (Euclid)

There are infinitely many different primes.

If you start to list prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots$$

they seem to appear less and less often. So do they run out eventually?

Theorem (Euclid)

There are infinitely many different primes.

This time we have a statement $p =$ "there are infinitely many primes", and we will prove that $\neg p$ implies a contradiction, *i.e.* use $(\neg p \to F) \to p$.

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the distinct primes:

$$p_1,\ p_2,\ \ldots,\ p_n.$$

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the distinct primes:

$$p_1,\ p_2,\ \ldots,\ p_n.$$

Any other number not on this list is not a prime. Okay, now I will challenge that. Consider

$$N = (p_1 p_2 \cdots p_n) + 1$$

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the distinct primes:

$$p_1, \; p_2, \; \ldots, \; p_n.$$

Any other number not on this list is not a prime. Okay, now I will challenge that. Consider

$$N = (p_1 p_2 \cdots p_n) + 1$$

Is N prime or not?

$\square$

NEXT

Next lecture: more proof practice

- rational and irrational numbers
- first element
- well ordering principle