37181: WEEK 2: PROOFS

37132

$\lim_{x \to a} f(x) = L$

A/Prof Murray Elder, UTS

Wednesday 31 July 2019

$\forall \varepsilon > 0$

$\exists \delta > 0$

$(\qquad)$

PLAN

- proof methods:
  - direct
  - contrapositive
  - contradiction
- rational numbers
- well ordering principle

PROOFS

$p \to q \;\cancel{\Leftrightarrow}\; q \to p$

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

$(p \to q) \wedge (q \to r)$

$\to (p \to r)$

$p \to q$

$\Leftrightarrow$

$\neg q \to \neg p$

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

0 $\quad 1 \quad 2 \quad 3 \ldots$

$-1 \quad -2$

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 $\exists -6$ such that

$$-18 = 3 \cdot (-6)$$

20 divides 100

$\exists\, 5$

DIVIDES

$\neg(\exists s \quad \Leftrightarrow \forall s(\neg \quad)$

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 $\forall s \in \mathbb{Z}$

$14 \neq 3s$

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 for all $s \in \mathbb{Z}$ $14 \neq 3s$.

$\mathbb{Z} = \{ \ldots, -1, 0, 1, 2,$

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 $-18 = 3 \cdot (-6)$

$\frac{14}{3} = 4\frac{2}{3}$

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 $2 \mid n$.

$\mathbb{Z}$

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 $d \in \mathbb{Z}$.

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 $d \in \mathbb{Z}$.

Lemma

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

n is even $\longrightarrow$

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

$$n^2 = (2s)^2 = 2 \cdot 2s^2$$

is also even $\square$

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 $d \in \mathbb{Z}$.

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.

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

Then $n^3 = (2s)^3$

$= 2 \cdot (4s^3)$ so is even $\square$

YOUR TURN

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. $\square$

$n \cdot n = 2s$

$\frac{2s}{n}$

$n^2 = 6$

Lemma

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

Proof.

$\exists s \in \mathbb{Z}$ $\quad n^2 = \cancel{4}s$

$\sqrt{n^2}$, $\sqrt{2}$ $\sqrt{s}$

n

YOUR TURN

$\neg q \to \neg p$

Lemma

$p \to q$

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

Proof.

? direct doesn't work

$\neg(n \text{ even}) \to \neg(n^2 \text{ is even})$

$n \text{ odd} \to n^2 \text{ odd}$

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.

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.

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).

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.

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 $s \in \mathbb{Z}$,

$$n^2 = (\quad)^2$$
$$= 4s^2 + 4s + 1$$
$$= 2(2s^2 + 2s) + 1$$

is odd. $\square$

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. $\square$

Definition

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

$(p \wedge q) \to r$

Lemma

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

n not odd $\to$ $n \leq 2$ or n not prime.

n even $\to$ $n = 2s$.

T $n \leq 2$ or $n > 2$

so $s > 1$.

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.

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: n even $\rightarrow$ $n \leq 2$ or n not prime.

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,

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

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?

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?

$p \rightsquigarrow \varepsilon$

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 $(\neg p \to F) \to p$.

Contradiction.

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

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

N bigger than my list, so not prime.

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?

$\square$

PAUSE

ratio $\frac{a}{b}$

Definition

A number x is called *rational* if $\exists\ a, b \in \mathbb{Z}$, $b \neq 0$ such that $x = \frac{a}{b}$.

$0.33333\ldots = \frac{1}{3}$

RATIONAL NUMBERS

A number x is called *rational* if $\exists\, a, b \in \mathbb{Z}, b \neq 0$ such that $x = \frac{a}{b}$.

For example, $0.3333\ldots$ is rational because it is equal to $\frac{1}{3}$.

A number x is called *rational* if $\exists\, a, b \in \mathbb{Z}, b \neq 0$ such that $x = \frac{a}{b}$.

For example, $0.3333\ldots$ is rational because it is equal to $\frac{1}{3}$.

The set of all rational numbers is denoted by $\mathbb{Q}$. A real number $x \in \mathbb{R}$ is called *irrational* if it is not rational.

$\mathbb{R} \setminus \mathbb{Q}$

A number x is called *rational* if $\exists\, a, b \in \mathbb{Z}, b \neq 0$ such that $x = \frac{a}{b}$.

For example, $0.3333\ldots$ is rational because it is equal to $\frac{1}{3}$.

The set of all rational numbers is denoted by $\mathbb{Q}$. A real number $x \in \mathbb{R}$ is called *irrational* if it is not rational.

Lemma

$\sqrt{2}$ is irrational.

Pf Suppose (for contradiction) $\sqrt{2}$ rat.

$(\neg p \rightarrow \mathbf{F}) \rightarrow p$

Proof.

Suppose (for contradiction) $\sqrt{2}$ is rational. So $\sqrt{2} = \frac{a}{b}$ for a, b integers.

$\exists a, \exists b$ Assume a, b don't have a common factor

$\rightarrow \sqrt{2}\, b = a$

$\not\leftrightarrow 2b^2 = a^2 = 2s\,2s$

$\rightarrow a^2$ is even

$\rightarrow a$ is even

$\rightarrow a = 2s$

$\rightarrow \cancel{2}b^2 = \cancel{2} \cdot 2s^2$

$\rightarrow b^2 = 2s^2$

Proof.

Suppose (for contradiction) $\sqrt{2}$ is rational. So $\sqrt{2} = \frac{a}{b}$ for a, b integers.

Now we make an *extra* assumption. Without loss of generality we can assume $\gcd(a, b) = 1$. (if not, choose a better pair a, b.)

Proof.

Suppose (for contradiction) $\sqrt{2}$ is rational. So $\sqrt{2} = \frac{a}{b}$ for a, b integers.

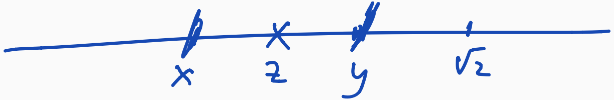
Now we make an *extra* assumption. Without loss of generality we can assume $\gcd(a, b) = 1$. (if not, choose a better pair a, b.)

- square both sides
- multiply both sides by b^2
- then a^2 is even
- so by our Lemma, a is even
- do some more manipulating
- now b^2 is even

$\rightarrow$ b even

$\rightarrow$ contradicts that $\gcd(a,b)=1$.

$\square$



Lemma

Between any two distinct rational numbers you can find another rational number.

Universe is $\mathbb{Q}$

$\forall x \forall y \exists z \, (x < y \rightarrow x < z < y)$

Pf DIRECT.

$\frac{x+y}{2}$

$z = x + \_$

Given $x, y \in \mathbb{Q}$.

$x < y$

Lemma

Between any two distinct rational numbers you can find another rational number.

$$\forall x \in \mathbb{Q}\ \forall y \in \mathbb{Q}[x < y \to \exists z \in \mathbb{Q}(x < z < y)]$$

Lemma

Between any two distinct rational numbers you can find another rational number.

Proof.

(Direct) Let p, q be two rational numbers. Without loss of generality assume $p < q$.

Lemma

Between any two distinct rational numbers you can find another rational number.

Proof.

(Direct) Let p, q be two rational numbers. Without loss of generality assume $p < q$.

Then (by hypothesis) $p = \frac{a}{b}$ and $q = \frac{c}{d}$.

Lemma

Between any two distinct rational numbers you can find another rational number.

Proof.

(Direct) Let p, q be two rational numbers. Without loss of generality assume $p < q$.

Then (by hypothesis) $p = \frac{a}{b}$ and $q = \frac{c}{d}$.

Construct a number in between them:

Lemma

Between any two distinct rational numbers you can find another rational number.

Proof.

(Direct) Let p, q be two rational numbers. Without loss of generality assume $p < q$.

Then (by hypothesis) $p = \frac{a}{b}$ and $q = \frac{c}{d}$.

Construct a number in between them:

$p = \frac{ad}{bd}$ and $q = \frac{cb}{db}$, and we know $ad < cb$ and they are both integers. What if they were just 1 apart?

$\square$

FIRST ELEMENT

Defn

natural $\{0, 1, 2, 3, 4,$

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

$\leq$

$\{2, 4, 6, 8, \ldots\}$

$\{1, 2, 16\}$.

p

$p \to q$

$\therefore q$

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Lemma

First elements are unique.

Pf given Any set $S \subseteq \mathbb{N}$

Suppose there are two different first elements a, b $a \neq b$, since a is first $a \leq b$

FIRST ELEMENT

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Lemma

First elements are unique. *(So we can say "the" first element).*

Proof.

FIRST ELEMENT

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Lemma

First elements are unique. *(So we can say "the" first element).*

Proof.

Suppose (for contradiction) there was a set $S \subseteq \mathbb{N}$ and two elements $s, t \in S$ both obeying the definition of first element of S.

FIRST ELEMENT

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Lemma

First elements are unique. *(So we can say "the" first element).*

Proof.

Suppose (for contradiction) there was a set $S \subseteq \mathbb{N}$ and two elements $s, t \in S$ both obeying the definition of first element of S.

Then since $t \in S$ we have $s \leqslant t$ (thinking of t as "an x" in the definition) and since $s \in S$ we have $t \leqslant s$ (thinking of s as an x).

FIRST ELEMENT

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Lemma

First elements are unique. *(So we can say "the" first element).*

Proof.

Suppose (for contradiction) there was a set $S \subseteq \mathbb{N}$ and two elements $s, t \in S$ both obeying the definition of first element of S.

Then since $t \in S$ we have $s \leqslant t$ (thinking of t as "an x" in the definition) and since $s \in S$ we have $t \leqslant s$ (thinking of s as an x).

Then $s = t$ so there was only one. $\square$

The following statement is an *axiom* or fact which does not follow from other facts.

Axiom (Well ordering principle)

Every non-empty subset of $\mathbb{N}$ has a first element.

WELL ORDERING PRINCIPLE

The following statement is an *axiom* or fact which does not follow from other facts.

Axiom (Well ordering principle)

Every non-empty subset of $\mathbb{N}$ has a first element.

Eg: $\{5, 4, 6, 7\}$ has a first element, 4.

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof Define $M = \{n - qd \mid q \in \mathbb{Z}\}$.

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof Define $M = \{n - qd \mid q \in \mathbb{Z}\}$. Then $M \cap \mathbb{N}$ is a subset of $\mathbb{N}$.

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof Define $M = \{n - qd \mid q \in \mathbb{Z}\}$. Then $M \cap \mathbb{N}$ is a subset of $\mathbb{N}$.

It is non-empty because if $n \geqslant 0$ you can take $q = 0$ and if $n < 0$ take $q = 100n$ (which is a negative number, so $-qd$ is a big positive number).

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof Define $M = \{n - qd \mid q \in \mathbb{Z}\}$. Then $M \cap \mathbb{N}$ is a subset of $\mathbb{N}$.

It is non-empty because if $n \geqslant 0$ you can take $q = 0$ and if $n < 0$ take $q = 100n$ (which is a negative number, so $-qd$ is a big positive number).

Therefore by the well ordering principle $M \cap \mathbb{N}$ has a first element, call it r.

Since $r \in M \cap \mathbb{N}$ we have $r \geqslant 0$ and $r = n - qd$ for some $q \in \mathbb{Z}$.

Since $r \in M \cap \mathbb{N}$ we have $r \geqslant 0$ and $r = n - qd$ for some $q \in \mathbb{Z}$.

If $r \geqslant d$ (for contradiction) then $r - d \geqslant 0$ and $r - d = n - (q+1)d$ so belongs to $M \cap \mathbb{N}$, and is smaller than r, contradicting our choice of r as first element. $\square$

NEXT

Workshop then homework sheet to practice these skills (in general, it takes time and lots of practice to fully understand and do proofs).

Next lecture:

- Prove the q, r in the Lemma are unique
- Euclidean algorithm
- Set theory notation