Administration
Midterm 1 is not early after all.
We don't think 3 weeks is enough material to merit a midterm.

CS70: Lecture 3. Outline.

1. Proofs
2. Simple
3. Direct
4. by Contrapositive
5. by Cases
6. by Contradiction

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

  " 'anything' $\implies$ true" is **true**

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

  " 'anything' $\implies$ true" is **true**

  so $X \implies (P \vee Q)$ is **true** for all X,

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

  " 'anything' $\implies$ true" is **true**

  so $X \implies (P \vee Q)$ is **true** for all X,

  and in particular, $P \implies (P \vee Q)$ is **true**

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

  " 'anything' $\implies$ true" is **true**

  so $X \implies (P \vee Q)$ is **true** for all X,

  and in particular, $P \implies (P \vee Q)$ is **true**

- P is false.

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

  " 'anything' $\implies$ true" is **true**

  so $X \implies (P \vee Q)$ is **true** for all X,

  and in particular, $P \implies (P \vee Q)$ is **true**
- P is false.

  "**false** $\implies$ 'anything' ", is **true**

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

  " 'anything' $\implies$ true" is **true**

  so $X \implies (P \vee Q)$ is **true** for all X,

  and in particular, $P \implies (P \vee Q)$ is **true**

- P is false.

  "**false** $\implies$ 'anything' ", is **true**

  so "$P \implies$ 'anything' " is **true**.

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

  " 'anything' $\implies$ true" is **true**

  so $X \implies (P \vee Q)$ is **true** for all X,

  and in particular, $P \implies (P \vee Q)$ is **true**
- P is false.

  "**false** $\implies$ 'anything' ", is **true**

  so "$P \implies$ 'anything' " is **true**.

  in particular $P \implies (P \vee Q)$ is **true**.

□

Simple theorem..

Theorem: $P \implies (P \vee Q)$.

Proof:

- P is true.

  $P \vee Q$ is **true**

  " 'anything' $\implies$ true" is **true**

  so $X \implies (P \vee Q)$ is **true** for all X,

  and in particular, $P \implies (P \vee Q)$ is **true**

- P is false.

  "**false** $\implies$ 'anything' ", is **true**

  so "$P \implies$ 'anything' " is **true**.

  in particular $P \implies (P \vee Q)$ is **true**.

$\square$

More detailed but the "same" as truth table proof in some sense.

Proof by truth table.

Theorem: $P \implies (P \vee Q)$.

Proof by truth table.
Theorem: $P \implies (P \vee Q)$.

Proof:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Proof by truth table.

Theorem: $P \implies (P \vee Q)$.

Proof:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Look only at appropriate rows. Where theorem condition is **true.**

Proof by truth table.

Theorem: $P \implies (P \vee Q)$.

Proof:

P	Q	$P \vee Q$
T	T	T
T	F	T
F		T
F		F

Look only at appropriate rows. Where theorem condition is **true.** When P is **true** since we are proving an implication.

An aside from piazza question/answer.
Theorem: $\neg(P \iff Q) \implies (P \implies \neg Q)$.
Proof:

P	Q	$\neg(P \iff Q)$	$P \implies \neg Q$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	F	T

An aside from piazza question/answer.

Theorem: $\neg(P \iff Q) \implies (P \implies \neg Q)$.

Proof:

P	Q	$\neg(P \iff Q)$	$P \implies \neg Q$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	F	T

Look only at appropriate rows. Where theorem condition is **T**.

An aside from piazza question/answer.
Theorem: $\neg(P \iff Q) \implies (P \implies \neg Q)$.
Proof:

P	Q	$\neg(P \iff Q)$	$P \implies \neg Q$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	F	T

Look only at appropriate rows. Where theorem condition is **T**.
When $\neg(P \iff Q)$ is **true** then $P \implies \neg Q$ is **true.**

Existential statement.
How to prove existential statement?

Existential statement.
How to prove existential statement?

Give an example. (Sometimes called "proof by example.")

Existential statement.
How to prove existential statement?

Give an example. (Sometimes called "proof by example.")

Theorem: $\exists x \in N . x = x^2$

Existential statement.
How to prove existential statement?

Give an example. (Sometimes called "proof by example.")

Theorem: $\exists x \in N . x = x^2$

Pf: $0 = 0^2 = 0$

Existential statement.
How to prove existential statement?

Give an example. (Sometimes called "proof by example.")

Theorem: $\exists x \in N. x = x^2$

Pf: $0 = 0^2 = 0$

$\square$

Universal Statement.

$$(\forall x \in N)(P(x))$$

Prove for every instance!!

Universal Statement.

$$(\forall x \in N)(P(x))$$

Prove for every instance!!

Could take a long time...

Universal Statement.

$$(\forall x \in N)(P(x))$$

Prove for every instance!!

Consider an instance $P(x)$, prove it for x without making any assumptions about x.

Universal Quantification Proof: example.

Theorem: For every $n \in N$, $n^3 - n$ is divisible by 3. $(3|n^3 - n\ )$.

Universal Quantification Proof: example.

Theorem: For every $n \in N$, $n^3 - n$ is divisible by 3. $(3|n^3 - n\ )$.

Proof:

$$n^3 - n = (n-1)(n)(n+1)$$

for any n.

Universal Quantification Proof: example.

Theorem: For every $n \in N$, $n^3 - n$ is divisible by 3. $(3|n^3 - n\ )$.

Proof:

$$n^3 - n = (n-1)(n)(n+1)$$

for any n.

One of $(n-1)$,n, $n+1$ is divisible by three.

Universal Quantification Proof: example.

Theorem: For every $n \in N$, $n^3 - n$ is divisible by 3. $(3|n^3 - n\ )$.

Proof:

$$n^3 - n = (n-1)(n)(n+1)$$

for any n.

One of $(n-1)$,n, $n+1$ is divisible by three.

Right hand side is divisible by 3, and so is the left hand side.

□

Universal Quantification Proof: example.

Theorem: For every $n \in N$, $n^3 - n$ is divisible by 3. $(3|n^3 - n\ )$.

Proof:

$$n^3 - n = (n-1)(n)(n+1)$$

for any n.

One of $(n-1)$,n, $n+1$ is divisible by three.

Right hand side is divisible by 3, and so is the left hand side.

□

Did not use anything about n, so proof was valid for any n.

Universal Quantification Proof: example.

Theorem: For every $n \in N$, $n^3 - n$ is divisible by 3. $(3|n^3 - n\ )$.

Proof:

$$n^3 - n = (n-1)(n)(n+1)$$

for any n.

One of $(n-1)$,n, $n+1$ is divisible by three.

Right hand side is divisible by 3, and so is the left hand side.

$\square$

Did not use anything about n, so proof was valid for any n.

Direct Proof: $P \implies Q$. Assume P prove Q.

If and only if..
Theorem: For every n in N, n is even $\iff$ n^2 is even.

If and only if..

Theorem: For every n in N, n is even $\iff$ n^2 is even.

$P =$ 'n^2 is even.'

If and only if..

Theorem: For every n in N, n is even $\iff$ n^2 is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

If and only if..

Theorem: For every n in N, n is even $\iff n^2$ is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

For $P \iff Q$, prove $P \implies Q$ and $Q \implies P$.

If and only if..

Theorem: For every n in N, n is even $\iff n^2$ is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

For $P \iff Q$, prove $P \implies Q$ and $Q \implies P$.

Lemma: For every n in N, n is even $\implies n^2$ is even. $(Q \implies P)$

If and only if..

Theorem: For every n in N, n is even $\iff$ n^2 is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

For $P \iff Q$, prove $P \implies Q$ and $Q \implies P$.

Lemma: For every n in N, n is even $\implies$ n^2 is even. ($Q \implies P$)

n is even $\implies$ $n = 2k$ for some k.

If and only if..

Theorem: For every n in N, n is even $\iff$ n^2 is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

For $P \iff Q$, prove $P \implies Q$ and $Q \implies P$.

Lemma: For every n in N, n is even $\implies$ n^2 is even. $(Q \implies P)$

n is even $\implies n = 2k$ for some k.

$n^2 = (2k)^2$

If and only if..

Theorem: For every n in N, n is even $\iff$ n^2 is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

For $P \iff Q$, prove $P \implies Q$ and $Q \implies P$.

Lemma: For every n in N, n is even $\implies$ n^2 is even. ($Q \implies P$)

n is even $\implies$ $n = 2k$ for some k.

$n^2 = (2k)^2 = 4k^2$

If and only if..

Theorem: For every n in N, n is even $\iff$ n^2 is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

For $P \iff Q$, prove $P \implies Q$ and $Q \implies P$.

Lemma: For every n in N, n is even $\implies$ n^2 is even. ($Q \implies P$)

n is even $\implies n = 2k$ for some k.

$n^2 = (2k)^2 = 4k^2 = 2 * (2k^2)$

If and only if..

Theorem: For every n in N, n is even $\iff$ n^2 is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

For $P \iff Q$, prove $P \implies Q$ and $Q \implies P$.

Lemma: For every n in N, n is even $\implies$ n^2 is even. ($Q \implies P$)

n is even $\implies$ $n = 2k$ for some k.

$n^2 = (2k)^2 = 4k^2 = 2 * (2k^2) = 2 * l$ for some natural number l.

If and only if..

Theorem: For every n in N, n is even $\iff n^2$ is even.

$P =$ 'n^2 is even.'

$Q =$ 'n is even'

For $P \iff Q$, prove $P \implies Q$ and $Q \implies P$.

Lemma: For every n in N, n is even $\implies n^2$ is even. $(Q \implies P)$

n is even $\implies n = 2k$ for some k.

$n^2 = (2k)^2 = 4k^2 = 2 * (2k^2) = 2 * l$ for some natural number l.

So n^2 is even!!

$\square$

Other direction of implication...

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. ($P \implies Q$)

n^2 is even, $n^2 = 2k$, ...

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. ($P \implies Q$)

n^2 is even, $n^2 = 2k$, ...$\sqrt{2k}$ even?

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' ....

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

Other direction of implication...
Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' ....

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' .... $\neg Q =$ 'n is odd'

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' .... $\neg Q =$ 'n is odd'

Prove $\neg Q \implies \neg P$: n is odd $\implies$ n^2 is odd.

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' .... $\neg Q =$ 'n is odd'

Prove $\neg Q \implies \neg P$: n is odd $\implies$ n^2 is odd.

$n = 2k + 1$

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' .... $\neg Q =$ 'n is odd'

Prove $\neg Q \implies \neg P$: n is odd $\implies$ n^2 is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k + k) + 1.$

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' .... $\neg Q =$ 'n is odd'

Prove $\neg Q \implies \neg P$: n is odd $\implies$ n^2 is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k + k) + 1.$

$n^2 = 2l + 1$ where l is a natural number..

Other direction of implication...
Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' .... $\neg Q =$ 'n is odd'

Prove $\neg Q \implies \neg P$: n is odd $\implies$ n^2 is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k + k) + 1.$

$n^2 = 2l + 1$ where l is a natural number..

... and n^2 is odd!

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' .... $\neg Q =$ 'n is odd'

Prove $\neg Q \implies \neg P$: n is odd $\implies$ n^2 is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k + k) + 1.$

$n^2 = 2l + 1$ where l is a natural number..

... and n^2 is odd!

$\neg Q \implies \neg P$ so $P \implies Q$ and theorem holds. $\square$

Other direction of implication...

Lemma: For every n in N, n^2 is even $\implies$ n is even. $(P \implies Q)$

Proof by contrapositive: $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P =$ 'n^2 is even.' .... $\neg P =$ 'n^2 is odd'

$Q =$ 'n is even' .... $\neg Q =$ 'n is odd'

Prove $\neg Q \implies \neg P$: n is odd $\implies$ n^2 is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k + k) + 1.$

$n^2 = 2l + 1$ where l is a natural number..

... and n^2 is odd!

$\neg Q \implies \neg P$ so $P \implies Q$ and theorem holds. $\square$

Theorem: For every n in N, n is even $\iff$ n^2 is even.

Proof by contradiction:idea

Assume opposite of what we are trying to prove. Show that it leads to an impossible situation. So our assumption must have been false.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both** a **and** b **are even.**

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both** a **and** b **are even.**

Proof: Assume a solution of the form a/b.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both a and b are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

Proof by cases.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both a and b are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd odd - odd +odd = even.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both a and b are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd odd - odd +odd = even. Not possible.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both** a **and** b **are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd odd - odd +odd = even. Not possible.

Case 2: a even, b odd even - even +odd = even.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both a and b are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd odd - odd +odd = even. Not possible.

Case 2: a even, b odd even - even +odd = even. Not possible.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both a and b are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd odd - odd +odd = even. Not possible.

Case 2: a even, b odd even - even +odd = even. Not possible.

Case 3: a odd, b even odd - even +even = even.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both a and b are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd odd - odd +odd = even. Not possible.

Case 2: a even, b odd even - even +odd = even. Not possible.

Case 3: a odd, b even odd - even +even = even. Not possible.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both a and b are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd odd - odd +odd = even. Not possible.

Case 2: a even, b odd even - even +odd = even. Not possible.

Case 3: a odd, b even odd - even +even = even. Not possible.

Case 4: a even, b even even - even +even = even.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, **then both a and b are even.**

Proof: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - a/b + 1 = 0$$

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd odd - odd +odd = even. Not possible.

Case 2: a even, b odd even - even +odd = even. Not possible.

Case 3: a odd, b even odd - even +even = even. Not possible.

Case 4: a even, b even even - even +even = even. Possible.

The fourth case is the only one possible, so the lemma follows.

□

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof:

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof:

Suppose for contradiction.

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof:

Suppose for contradiction.

- There is a solution $x = a/b$ with $a \in Z$ and $b \in N$ and $a, b \neq 0$. ($a = 0$ would be $x = 0$ which is not a solution.)

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof:

Suppose for contradiction.

- There is a solution $x = a/b$ with $a \in Z$ and $b \in N$ and $a, b \neq 0$. ($a = 0$ would be $x = 0$ which is not a solution.)
- May be many, so choose b to be minimal.

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof:

Suppose for contradiction.

- There is a solution $x = a/b$ with $a \in Z$ and $b \in N$ and $a, b \neq 0$. ($a = 0$ would be $x = 0$ which is not a solution.)
- May be many, so choose b to be minimal.
- No common factors for a and b.

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof:

Suppose for contradiction.

- There is a solution $x = a/b$ with $a \in Z$ and $b \in N$ and $a, b \neq 0$. ($a = 0$ would be $x = 0$ which is not a solution.)
- May be many, so choose b to be minimal.
- No common factors for a and b.
- Both a and b cannot be even.

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof:

Suppose for contradiction.

- There is a solution $x = a/b$ with $a \in Z$ and $b \in N$ and $a, b \neq 0$. ($a = 0$ would be $x = 0$ which is not a solution.)
- May be many, so choose b to be minimal.
- No common factors for a and b.
- Both a and b cannot be even.
- Contradicts lemma: "a and b must be even."

Proof by contradiction.
Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof:

Suppose for contradiction.

- There is a solution $x = a/b$ with $a \in Z$ and $b \in N$ and $a, b \neq 0$. ($a = 0$ would be $x = 0$ which is not a solution.)
- May be many, so choose b to be minimal.
- No common factors for a and b.
- Both a and b cannot be even.
- Contradicts lemma: "a and b must be even."

So assumption that there is a rational solution is false and the theorem holds.

Proof by contradiction:form

Theorem: P.

Proof by contradiction:form

Theorem: P.

$$\neg P \implies P_1 \cdots \implies R$$

Proof by contradiction:form

Theorem: P.

$$\neg P \implies P_1 \cdots \implies R$$

$$\neg P \implies P_1 \cdots \implies \neg R$$

Proof by contradiction:form

Theorem: P.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P$ is **false**.

Proof by contradiction:form

Theorem: P.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P$ is **false**.

P is **true**.

$\square$

Recap: $x^5 - x + 1 = 0$ **has no rational solutions.**

Proof by contradiction:form

Theorem: P.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P$ is **false**.

P is **true**.

$\square$

Recap: $x^5 - x + 1 = 0$ **has no rational solutions.**

P – the non existence of rational solution

Proof by contradiction:form

Theorem: P.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P$ is **false**.

P is **true**.

$\square$

Recap: $x^5 - x + 1 = 0$ **has no rational solutions.**

P – the non existence of rational solution

R – a and b are even.

Proof by contradiction:form

Theorem: P.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P$ is **false**.

P is **true**.

$\square$

Recap: $x^5 - x + 1 = 0$ **has no rational solutions.**

P – the non existence of rational solution

R – a and b are even.

Lemma: Any rational solution implies a and b are even.

Proof by contradiction:form

Theorem: P.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P$ is **false**.

P is **true**.

$\square$

Recap: $x^5 - x + 1 = 0$ **has no rational solutions.**

P – the non existence of rational solution

R – a and b are even.

Lemma: Any rational solution implies a and b are even.

$\neg P \implies \cdots R$

Proof by contradiction:form

Theorem: P.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P$ is **false**.

P is **true**.

□

Recap: $x^5 - x + 1 = 0$ **has no rational solutions.**

P – the non existence of rational solution

R – a and b are even.

Lemma: Any rational solution implies a and b are even.

$\neg P \implies \cdots R$

There is a rational solution where a and b are not both even.

Proof by contradiction:form

Theorem: P.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P$ is **false**.

P is **true**.

$\square$

Recap: $x^5 - x + 1 = 0$ **has no rational solutions.**

P – the non existence of rational solution

R – a and b are even.

Lemma: Any rational solution implies a and b are even.

$\neg P \implies \cdots R$

There is a rational solution where a and b are not both even.

$\neg P \implies \cdots \neg R$

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider

$$q = p_1 \times p_2 \times \cdots p_k + 1$$

.

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider

$$q = p_1 \times p_2 \times \cdots p_k + 1$$

.

- q cannot be one of the primes as it is larger than any p_i.

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider

$$q = p_1 \times p_2 \times \cdots p_k + 1$$

.

- q cannot be one of the primes as it is larger than any p_i.
- q has prime divisor p ("$p > 1$" $=$ R) which is one of p_i.

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider

$$q = p_1 \times p_2 \times \cdots p_k + 1$$

.

- q cannot be one of the primes as it is larger than any p_i.
- q has prime divisor p ("$p > 1$" $=$ R) which is one of p_i.
- p divides both $x = p_1, \ldots, p_k$ and q, and $x - q$ is 1,

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider

$$q = p_1 \times p_2 \times \cdots p_k + 1$$

.

- q cannot be one of the primes as it is larger than any p_i.
- q has prime divisor p ("$p > 1$" $=$ R) which is one of p_i.
- p divides both $x = p_1, \ldots, p_k$ and q, and $x - q$ is 1,
- so $p \leq 1$. (**Contradicts R.**)

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider

$$q = p_1 \times p_2 \times \cdots p_k + 1$$

.

- q cannot be one of the primes as it is larger than any p_i.
- q has prime divisor p ("$p > 1$" $=$ R) which is one of p_i.
- p divides both $x = p_1, \ldots, p_k$ and q, and $x - q$ is 1,
- so $p \leq 1$. (**Contradicts R.**)

The original assumption that "the theorem is false" is false, thus the theorem is true.

Product of first k primes..
Did we prove?

- "The product of the first k primes plus 1 is prime."

Product of first k primes..
Did we prove?

- "The product of the first k primes plus 1 is prime."
- No.

Product of first k primes..
Did we prove?

- "The product of the first k primes plus 1 is prime."
- No.
- The chain of reasoning started with a false statement.

Product of first k primes..
Did we prove?

- "The product of the first k primes plus 1 is prime."
- No.
- The chain of reasoning started with a false statement.

Consider example..

Product of first k primes..
Did we prove?

- "The product of the first k primes plus 1 is prime."
- No.
- The chain of reasoning started with a false statement.

Consider example..

- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 200031 = 59 \times 509$

Product of first k primes..
Did we prove?

- "The product of the first k primes plus 1 is prime."
- No.
- The chain of reasoning started with a false statement.

Consider example..

- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 200031 = 59 \times 509$
- There is a prime *in between* 13 and $q = 200031$ that divides q.

Product of first k primes..

Did we prove?

- "The product of the first k primes plus 1 is prime."
- No.
- The chain of reasoning started with a false statement.

Consider example..

- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 200031 = 59 \times 509$
- There is a prime *in between* 13 and $q = 200031$ that divides q.
- Proof assumed no primes *in between.*

$\square$

Discussion
Proof by contradiction can sometimes be dangerous.

Discussion

Proof by contradiction can sometimes be dangerous.

Derive false statements.

Discussion

Proof by contradiction can sometimes be dangerous.

Derive false statements.

Perhaps from a **false step** in the middle instead of from the original **false assumption**.

Discussion

Proof by contradiction can sometimes be dangerous.

Derive false statements.

Perhaps from a **false step** in the middle instead of from the original **false assumption**.

In a direct proof, nonsense is a warning sign.

Discussion
Proof by contradiction can sometimes be dangerous.

Derive false statements.

Perhaps from a **false step** in the middle instead of from the original **false assumption**.

In a direct proof, nonsense is a warning sign.

In a contradiction proof, it is the nature of the beast.

Why use contradiction?
Could we do a direct proof for primes?

Why use contradiction?
Could we do a direct proof for primes?

One way: make a formula to generate another prime from finite set of primes.

Why use contradiction?
Could we do a direct proof for primes?

One way: make a formula to generate another prime from finite set of primes.

(E.g., product of first k primes plus 1?)

Why use contradiction?
Could we do a direct proof for primes?

One way: make a formula to generate another prime from finite set of primes.

(E.g., product of first k primes plus 1?)

Euclid proved that there were infinitely many primes (see above) but did not provide a formula.

Why use contradiction?
Could we do a direct proof for primes?

One way: make a formula to generate another prime from finite set of primes.

(E.g., product of first k primes plus 1?)

Euclid proved that there were infinitely many primes (see above) but did not provide a formula.

Lazy guy?

Why use contradiction?
Could we do a direct proof for primes?

One way: make a formula to generate another prime from finite set of primes.

(E.g., product of first k primes plus 1?)

Euclid proved that there were infinitely many primes (see above) but did not provide a formula.

Lazy guy?

Two millennia later, we still don't know a formula to generate yet "another" prime.

Stopped here in class: 8/31/2011.
Some of it was due to various good questions. If you weren't in class, come next time!
We may cover the next couple of slides in class. That remains to be seen.
Cheers, Satish Rao

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational.

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
-

$$x^y =$$

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
- $$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$$

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
-

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}*\sqrt{2}}$$

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
- $$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}*\sqrt{2}} = \sqrt{2}^2 = 2.$$

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
-

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}*\sqrt{2}} = \sqrt{2}^2 = 2.$$

Thus, in this case, we have irrational x and y with a rational x^y (i.e., 2).

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: x^y is rational. Done!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
-
$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}*\sqrt{2}} = \sqrt{2}^{2} = 2.$$

Thus, in this case, we have irrational x and y with a rational x^y (i.e., 2).

One of the cases is true so theorem holds.

Be careful.
Theorem: $3 = 4$

Be careful.
Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 and you get $4 = 3$. $\square$

Be careful.
Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 and you get $4 = 3$. $\square$

You can't assume what you want to prove.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 and you get $4 = 3$. $\square$

You can't assume what you want to prove.

Theorem: $3 = 4$

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 and you get $4 = 3$. $\square$

You can't assume what you want to prove.

Theorem: $3 = 4$

Proof:

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 and you get $4 = 3$. $\square$

You can't assume what you want to prove.

Theorem: $3 = 4$

Proof:

If $a = b$, then $ax = bx$.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 and you get $4 = 3$. □

You can't assume what you want to prove.

Theorem: $3 = 4$

Proof:

If $a = b$, then $ax = bx$.

So, for $x = 0$, $3x = 4x$, which implies $3 = 4$.

□

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 and you get $4 = 3$. $\square$

You can't assume what you want to prove.

Theorem: $3 = 4$

Proof:

If $a = b$, then $ax = bx$.

So, for $x = 0$, $3x = 4x$, which implies $3 = 4$.

$\square$

$P \implies Q$ does not mean $Q \implies P$.

Be careful.
Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 and you get $4 = 3$. $\square$

You can't assume what you want to prove.

Theorem: $3 = 4$

Proof:

If $a = b$, then $ax = bx$.

So, for $x = 0$, $3x = 4x$, which implies $3 = 4$.

$\square$

$P \implies Q$ does not mean $Q \implies P$.

See notes...

Extra slides

Definitions..

Axiom A proposition that we assume is true without proof
EX: Peano axioms for natural numbers

Theorem A proposition that we can prove to be true.

Conjecture A proposition that we think is true but don't know how to prove.