Review.

Theory: If you drink alcohol you must be at least 18.

Which cards do you turn over?

Drink Alcohol $\implies$ "≥ 18"

"< 18" $\implies$ Don't Drink Alcohol. Contrapositive.

(A) (B) (C) and/or (D)?

Propositional Forms: $\wedge, \vee, \neg$, $P \implies Q \equiv \neg P \vee Q$.

Truth Table. Putting together identities. (E.g., cases, substitution.)

Predicates, $P(x)$, and quantifiers. $\forall x, P(x)$.

DeMorgan's: $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$. $\neg \forall x, P(x) \equiv \exists x, \neg P(x)$.

CS70: Lecture 2. Outline.

Today: Proofs!!!

1. By Example.
2. Direct. (Prove $P \implies Q$.)
3. by Contraposition (Prove $P \implies Q$)
4. by Contradiction (Prove P.)
5. by Cases

If time: discuss induction.

Last time: Existential statement.

How to prove existential statement?

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

Theorem: $(\exists x \in N)(x = x^2)$

Pf: $0 = 0^2 = 0$

$\square$

Often used to disprove claim.

Homework.

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

$a|b$ means "a divides b".

$2|4$? Yes! Since for $q = 2$, $4 = (2)2$.

$7|23$? No! No q where true.

$4|2$? No!

$2|-4$? Yes! Since for $q = 2$, $-4 = (-2)2$.

Formally: for $a, b \in \mathbb{Z}$, $a|b \iff \exists q \in \mathbb{Z}$ where $b = aq$.

$3|15$ since for $q = 5$, $15 = 3(5)$.

A natural number $p > 1$, is **prime** if it is divisible only by 1 and itself.

A number x is even if and only if $2|x$, or $x = 2k$ for $x, k \in \mathbb{Z}$.

A number x is odd if and only if $x = 2k + 1$

Divides.

$a|b$ means

(A) There exists $k \in \mathbb{Z}$, with $a = kb$.

(B) There exists $k \in \mathbb{Z}$, with $b = ka$.

(C) There exists $k \in \mathbb{N}$, with $b = ka$.

(D) There exists $k \in \mathbb{Z}$, with $k = ab$.

(E) a divides b

Incorrect: (C) sufficient not necessary. (A) Wrong way. (D) the product is an integer.

Correct: (B) and (E).

Direct Proof.

Theorem: For any $a, b, c \in Z$, if $a|b$ and $a|c$ then $a|(b-c)$.

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

$b - c = aq - aq' = a(q - q')$ Done?

$(b-c) = a(q-q')$ and $(q-q')$ is an integer so by definition of divides

$a|(b-c)$ □

Works for $\forall a, b, c$?
Argument applies to *every* $a, b, c \in Z$.
Used distributive property and definition of divides.

Direct Proof Form:
Goal: $P \implies Q$
Assume P.
...
Therefore Q.

Another direct proof.

Let D_3 be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of n is divisible by 11, then $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:

$n = 121$ Alt Sum: $1-2+1 = 0$. Divis. by 11. As is 121.

$n = 605$ Alt Sum: $6-0+5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some a, b, c.

Assume: Alt. sum: $a - b + c = 11k$ for some integer k.

Add $99a + 11b$ to both sides.

$$100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)$$

Left hand side is n, $k + 9a + b$ is integer. $\implies 11|n$. $\square$

Direct proof of $P \implies Q$:
Assumed P: $11|a-b+c$. Proved Q: $11|n$.

The Converse

Thm: $\forall n \in D_3, (11 | \text{alt. sum of digits of } n) \implies 11 | n$

Is converse a theorem?

$\forall n \in D_3, (11 | n) \implies (11 | \text{alt. sum of digits of } n)$

Yes? No?

Another Direct Proof.

Theorem: $\forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n)$
Proof: Assume $11|n$.

$$n = 100a + 10b + c = 11k \implies$$
$$99a + 11b + (a - b + c) = 11k \implies$$
$$a - b + c = 11k - 99a - 11b \implies$$
$$a - b + c = 11(k - 9a - b) \implies$$
$$a - b + c = 11\ell \text{ where } \ell = (k - 9a - b) \in Z$$

That is 11|alternating sum of digits. □

Note: similar proof to other. In this case every $\implies$ is $\iff$

Often works with arithmetic properties ...
...not when multiplying by 0.

We have.

Theorem: $\forall n \in N', (11|\text{alt. sum of digits of } n) \iff (11|n)$

Proof by Contraposition

Thm: For $n \in Z^+$ and $d|n$. If n is odd then d is odd.

$n = kd$ and $n = 2k' + 1$ for integers k, k'.

what do we know about d?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

...and prove $\neg P$.

Conclusion: $\neg Q \implies \neg P$ equivalent to $P \implies Q$.

Proof: Assume $\neg Q$: d is even. $d = 2k$.

$d|n$ so we have

$n = qd = q(2k) = 2(kq)$

n is even. $\neg P$ $\square$

Another Contraposition...

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?

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

$P =$ '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.

$n = 2k + 1$

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

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

... and n^2 is odd!

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

Proof by contradiction:form

Theorem: $\sqrt{2}$ is irrational.

Must show: For every $a, b \in Z$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

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

$\neg P \implies Q_1 \cdots \implies \neg R$

$\neg P \implies R \wedge \neg R \equiv$ False

or $\neg P \implies$ *False*

Contrapositive of $\neg P \implies$ *False* is *True* $\implies P$.
Theorem P is true. And proven. $\square$

Contradiction

Theorem: $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in Z$.

Reduced form: a and b have no common factors.

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

$$2b^2 = a^2 = 4k^2$$

a^2 is even $\implies$ a is even.

$a = 2k$ for some integer k

$$b^2 = 2k^2$$

b^2 is even $\implies$ b is even.
a and b have a common factor. Contradiction.

□

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

$$q = (p_1 \times p_2 \times \cdots p_k) + 1.$$

- 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 $x = p_1 \cdot p_2 \cdots p_k$ and q, and divides $q - x$,
- $\implies p|(q-x) \implies p \leq (q-x) = 1$.
- so $p \leq 1$. (**Contradicts** R**.**)

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

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..

- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$
- There is a prime *in between* 13 and $q = 30031$ that divides q.
- Proof assumed no primes *in between* p_k and q.

Poll: Odds and evens.

x is even, y is odd.

Even numbers are divisible by 2.

Which are even?

(A) x^3
(B) y^3
(C) $x+5x$
(D) xy
(E) xy^5
(F) $x+y$

A, D, E all contain a factor of 2.

$x = 2k$, and $x^3 = 8k = 2(4k)$ and is even.

y^3. Odd?

$y = (2k+1)$. $y^3 = 8k^3 + 24k^2 + 24k + 1 = 2(4k^3 + 12k^2 + 12k) + 1$.

Odd times an odd? Odd.

Any power of an odd number? Odd.
 Idea: $(2k+1)^n$ has terms
 (a) with the last term being 1

Proof by cases.

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

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.*

Reduced form $\frac{a}{b}$: a and b can't both be even! + Lemma
$\implies$ no rational solution. □

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

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

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 cases.

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

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

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ 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, we have irrational x and y with a rational x^y (i.e., 2).

One of the cases is true so theorem holds. □

Question: Which case holds? Don't know!!!

Poll: proof review.

Which of the following are (certainly) true?

(A) $\sqrt{2}$ is irrational.

(B) $\sqrt{2}^{\sqrt{2}}$ is rational.

(C) $\sqrt{2}^{\sqrt{2}}$ is rational or it isn't.

(D) $(2^{\sqrt{2}})^{\sqrt{2}}$ is rational.

(A),(C),(D)

(B) I don't know.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$.

Start with $12 = 12$.

Divide one side by 3 and the other by 4 to get
$4 = 3$.

By commutativity theorem holds. $\square$

Don't assume what you want to prove!

Be really careful!

Theorem: $1 = 2$

Proof: For $x = y$, we have

$$
\begin{aligned}
(x^2 - xy) &= x^2 - y^2 \\
x(x-y) &= (x+y)(x-y) \\
x &= (x+y) \\
x &= 2x \\
1 &= 2
\end{aligned}
$$

□

Poll: What is the problem?

(A) Assumed what you were proving.

(B) No problem. Its fine.

(C) $x - y$ is zero.

(D) Can't multiply by zero in a proof.

Dividing by zero is no good. Multiplying by zero is wierdly cool!

Also: Multiplying inequalities by a negative.

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

Summary: Note 2.

Direct Proof:

To Prove: $P \implies Q$. Assume P. Prove Q.

$a|b$ and $a|c \implies a|(b-c)$.

By Contraposition:

To Prove: $P \implies Q$ Assume $\neg Q$. Prove $\neg P$.

n^2 is odd $\implies$ n is odd. $\equiv$ n is even $\implies$ n^2 is even.

By Contradiction:

To Prove: P Assume $\neg P$. Prove False .

$\sqrt{2}$ is rational.

$\sqrt{2} = \frac{a}{b}$ with no common factors....

By Cases: informal.

Universal: show that statement holds in all cases.

Existence: used cases where one is true.

Either $\sqrt{2}$ and $\sqrt{2}$ worked.

or $\sqrt{2}$ and $\sqrt{2}^{\sqrt{2}}$ worked.

Careful when proving!

Don't assume the theorem. Divide by zero.Watch converse. ...

CS70: Note 3. Induction!

Poll. What's the biggest number?

(A) 100

(B) 101

(C) n+1

(D) infinity.

(E) This is about the "recursive leap of faith."