Review.

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

Which cards do you turn over?

Drink $\implies "\geq 18"

"< 18" $\implies$ Don’t Drink. Contrapositive.

$\land, \lor, \neg, P \implies Q \equiv \neg P \lor Q.$

Truth Table. Putting together identities. (E.g., cases, substitution.)
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.
Quick Background and Notation.

Integers closed under addition.
\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\(a|b\) means “a divides b”.

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

7|23? No! No \(q\) where true.

4|2? No!

Poll

Formally: \(a|b \iff \exists q \in \mathbb{Z} \text{ where } b = aq\).

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.
Direct Proof.

**Theorem:** For any \(a, b, c \in \mathbb{Z}\), if \(a|b\) and \(a|c\) then \(a|(b - c)\).

**Proof:** Assume \(a|b\) and \(a|c\)

\[b = aq\] and \(c = aq'\) where \(q, q' \in \mathbb{Z}\)

\[b - c = aq - aq' = a(q - q')\] 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 \(a, b, c \in \mathbb{Z}\).

Used distributive property and definition of divides.

Direct Proof Form:

**Goal:** \(P \implies Q\)

**Assume** \(P\).

\[\ldots\]

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 $11 \mid n$.

\[ \forall n \in D_3, (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n \]

Examples:
\begin{align*}
n &= 121 \quad \text{Alt Sum: } 1 - 2 + 1 = 0. \text{ Divis. by 11. As is } 121. \\
n &= 605 \quad \text{Alt Sum: } 6 - 0 + 5 = 11 \text{ Divis. by 11. As is } 605 = 11(55) \\
\end{align*}

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. $\implies 11 \mid n$. \[\square\]

Direct proof of $P \implies Q$:
Assumed $P$: $11 \mid a - b + c$. Proved $Q$: $11 \mid n$. 
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?
Poll
Another Direct Proof.

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

Proof: Assume 11|n.

\[
\begin{align*}
    n &= 100a + 10b + c = 11k \implies \\
    99a + 11b + (a - b + c) &= 11k \implies \\
    a - b + c &= 11k - 99a - 11b \implies \\
    a - b + c &= 11(k - 9a - b) \implies \\
    a - b + c &= 11 \ell \text{ where } \ell = (k - 9a - b) \in \mathbb{Z}
\end{align*}
\]

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 \( n \in \mathbb{Z}^+ \) and \( d \mid n \). If \( n \) is odd then \( d \) is odd.

\[ n = 2k + 1 \] what do we know about \( d \)?

What to do? Is it **even** true?

Hey, that rhymes ... and there is a pun ... colored blue.

Anyway, what to do?

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. \( d = 2k \).

\( d \mid n \) so we have

\[ n = qd = q(2k) = 2(kq) \]

\( n \) is even. \( \neg P \)
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' \( P = 'n^2 \) is even.' .......... \( \neg P = 'n^2 \) is odd' \( Q = 'n \) is even' .......... \( \neg Q = 'n \) is odd' \( P = 'n^2 \) 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 ...
Proof by contradiction:form

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

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

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

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

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

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

or $\neg P \implies False$

Contrapositive of $\neg P \implies False$ is $True \implies P$.

Theorem $P$ is true. And proven. \(\square\)
Theorem: \( \sqrt{2} \) is irrational.

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

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.

\[\square\]
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 \textit{in between} 13 and $q = 30031$ that divides $q$.
- Proof assumed no primes \textit{in between} $p_k$ and $q$. 


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 \( a, b \in \mathbb{Z} \), 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: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

\[
x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2.
\]

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!!!
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.
Don’t assume what you want to prove!
Be really careful!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

$$(x^2 - xy) = x^2 - y^2$$

$$x(x - y) = (x + y)(x - y)$$

$$x = (x + y)$$

$$x = 2x$$

$$1 = 2$$

Dividing by zero is no good.

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 $Q$.

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

By Contradiction:
To Prove: $P$ Assume $\neg P$. Prove $\text{False}$.

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. ...
Poll.

1. The natural numbers.
2. 5 year old Gauss.
3. ..and Induction.
4. Simple Proof.
The natural numbers.

0, 1, 2, 3, ...

..., n, n+1, n+2, n+3, ...

0, 1, 2, 3, ...

..., n, n+1, n+2, n+3, ...
Teacher: Hello class.
Teacher: Please add the numbers from 1 to 100.

Gauss: It's $\frac{(100)(101)}{2}$ or 5050!

Five year old Gauss Theorem: $\forall (n \in \mathbb{N}) : \sum_{i=0}^{n} i = \frac{(n)(n+1)}{2}$.

It is a statement about all natural numbers.

$\forall (n \in \mathbb{N}) : P(n)$.

$P(n)$ is $\sum_{i=0}^{n} i = \frac{(n)(n+1)}{2}$.

Principle of Induction:

- Prove $P(0)$.
- Assume $P(k)$, “Induction Hypothesis”
- Prove $P(k + 1)$. “Induction Step.”
Theorem: For all natural numbers $n$, $0 + 1 + 2 \cdots n = \frac{n(n+1)}{2}$

Base Case: Does $0 = \frac{0(0+1)}{2}$? Yes.

Induction Step: Show $\forall k \geq 0, P(k) \implies P(k+1)$

Induction Hypothesis: $P(k) = 1 + \cdots + k = \frac{k(k+1)}{2}$

$1 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$

$= \frac{k^2 + k + 2(k+1)}{2}$

$= \frac{k^2 + 3k + 2}{2}$

$= \frac{(k+1)(k+2)}{2}$

$P(k+1)!$ By principle of induction...
Note’s visualization: an infinite sequence of dominos.

Prove they all fall down;

- $P(0) =$ “First domino falls”
- $(\forall k) \; P(k) \implies P(k + 1):$ “$k$th domino falls implies that $k + 1$st domino falls”
Climb an infinite ladder?

Your favorite example of forever..or the natural numbers...
Gauss and Induction

Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!  

**Induction Step.** \(P(k) \implies P(k+1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 0 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true  
plus inductive step \(\implies\) true for \(n = 1\) \((P(0) \land (P(0) \implies P(1))) \implies P(1)\)  
plus inductive step \(\implies\) true for \(n = 2\) \((P(1) \land (P(1) \implies P(2))) \implies P(2)\)  

\[
\vdots
\]

true for \(n = k \implies\) true for \(n = k + 1\) \((P(k) \land (P(k) \implies P(k+1))) \implies P(k+1)\)  

\[
\vdots
\]

Predicate, \(P(n)\), **True** for all natural numbers! **Proof by Induction.**
Induction

The canonical way of proving statements of the form

\[(\forall k \in \mathbb{N})(P(k))\]

- For all natural numbers \( n \), \( 1 + 2 \cdots n = \frac{n(n+1)}{2} \).
- For all \( n \in \mathbb{N} \), \( n^3 - n \) is divisible by 3.
- The sum of the first \( n \) odd integers is a perfect square.

The basic form

- Prove \( P(0) \). “Base Case”.

- \( P(k) \implies P(k+1) \)
  - Assume \( P(k) \), “Induction Hypothesis”
  - Prove \( P(k+1) \). “Induction Step.”

\( P(n) \) true for all natural numbers \( n \)!!
Get to use \( P(k) \) to prove \( P(k+1) \)!!!
Next Time.

More induction!
See you on Thursday!