Review.

Theorem: 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.
\( \land, \lor, \neg P \implies \neg P \lor Q \).
Truth Table. Putting together identities. (E.g., cases, substitution.)

Direct Proof.

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

**Proof:** Assume \( a \mid b \) and \( a \mid c \)
\( b = aq \) 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 \( a, b, c \)?
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 \( P \). ...
Therefore \( Q \).

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.

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|\( n \).

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

Examples:
\( n = 121 \) All Sum: 1 - 2 + 1 = 0. Divis. by 11. As is 121.
\( n = 605 \) All 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. \( \implies 11 | n \).

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

Quick Background and Notation.

Integers closed under addition.
\( a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \)
\( a \mid b \) means “\( a \) divides \( b \).”
2|4? Yes! Since for \( q = 2, 4 = (2)2 \).
7\|3? No! No \( q \) where true.

4|2? No!

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

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: \( \forall n \in \mathbb{N}, \ (11|n) \implies (11|\text{alt. sum of digits of } n) \)
Proof: Assume 11|n.
\[
\begin{align*}
n &= 100a + 10b + c = 11k \\
99a + 11b + (a + b + c) &= 11k \\
a + b + c &= 11k - 99a - 11b \\
a - b + c &= 11k - 9a - b \\
\end{align*}
\]
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: \( \forall n \in \mathbb{N}, (11|\text{alt. sum of digits of } n) \iff (11|n) \)

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: \( P \).
\[
\begin{align*}
\neg P &\implies P_1 \cdots \implies R \\
\neg P &\implies Q_1 \cdots \implies \neg R \\
\neg P &\implies R \land \neg R = \text{False} \\
\neg P &\implies \text{False} \\
\text{Contrapositive of } \neg P \implies \text{False is True } \iff P. \\
\text{Theorem } P \text{ is true. And proven.}
\end{align*}
\]

Proof by Contraposition

Thm: For \( n \in \mathbb{Z}^+ \) and \( d|n \). If \( n \) is odd then \( d \) is odd.
\[
n = 2k + 1 \text{ what do we know about } d? \\
\text{What to do? Is it even true?} \\
\text{Hey, that rhymes ... and there is a pun ... colored blue.} \\
\text{Anyway, what to do?} \\
\text{Goal: } \text{Prove } P \implies Q. \\
\text{Assume } \neg Q \\
\text{...and prove } \neg P. \\
\text{Conclusion: } \neg Q \iff \neg P \text{ equivalent to } P \implies Q. \\
\text{Proof: Assume } \neg Q: \text{ } d \text{ is even. } d = 2k. \\
\text{ } \text{ } \text{ } \text{ } d|n \text{ so we have} \\
\text{ } \text{ } \text{ } \text{ } n = qd = q(2k) = 2(kq) \\
\text{ } \text{ } \text{ } \text{ } n \text{ is even. } \neg P \\
\]

Contradiction

Theorem: \( \sqrt{2} \) is irrational.
Assume \( \neg P: \sqrt{2} = a/b \text{ for } a, b \in \mathbb{Z} \).
Reduced form: \( a \text{ and } b \text{ have no common factors.} \)
\[
\sqrt{2}b = a \\
2b^2 = a^2 = 4k^2 \\
\]
\( a^2 \) is even \( \iff a \) is even. \\
\( a = 2k \) for some integer \( k \)
\[
b^2 = 2k^2 \\
b^2 \text{ is even } \iff b \text{ is even.} \\
a \text{ and } b \text{ have a common factor. } \text{ Contradiction.}
\]

Another Contraosition...

Lemma: For every \( n \in \mathbb{N}, n^2 \) is even \( \implies n \) is even. \( (P \implies Q) \)
\( n^2 \) is even, \( n^2 = 2k, \ldots \sqrt{2x} \text{ is even?} \)
Proof by contraposition: \( (P \implies Q) \iff (\neg Q \implies \neg P) \)
P = \( \text{"} n^2 \text{ is even.} \ldots \) \( \neg P = \text{\"} n^2 \text{ is odd\"} \)
\( Q = \text{\"} n \text{ is even.} \ldots \) \( \neg Q = \text{\"} n \text{ is odd\"} \)
Prove \( \neg Q \iff \neg P: \text{ } n \text{ is odd } \iff n^2 \text{ is odd.} \\
\text{ } \text{ } \text{ } \text{ } n = 2k + 1 \\
\text{ } \text{ } \text{ } \text{ } r^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1. \\
\text{ } \text{ } \text{ } \text{ } r^2 = 2l + 1 \text{ where } l \text{ is a natural number}. \\
\text{ } \text{ } \text{ } \text{ } ... \text{ and } r^2 \text{ is odd!} \\
\neg Q \iff \neg P \text{ so } P \implies Q \text{ and } \ldots \\
\]

Proof by contradiction: example

Theorem: There are infinitely many primes.
Proof:
\[ \begin{align*}
&\text{Assume finitely many primes: } p_1, \ldots, p_k. \\
&\text{Consider number } q = (p_1 \times p_2 \times \cdots p_k) + 1. \\
&\text{ } \text{ } \text{ } \text{ } q \text{ cannot be one of the primes as it is larger than any } p_i. \\
&\text{ } \text{ } \text{ } \text{ } q \text{ has prime divisor } p (\text{"} p > 1 = R \text{"} ) \text{ which is one of } p_i. \\
&\text{ } \text{ } \text{ } \text{ } p \text{ divides both } x = p_1 \cdot p_2 \cdots p_k \text{ and } q, \text{ and divides } q - x, \\
&\implies p | q - x \iff p \leq q - x = 1. \\
&\text{ } \text{ } \text{ } \text{ } \text{so } p \leq 1. \text{ (Contrads } R \text{).} \\
\text{The original assumption that \"the theorem is false\" is false,} \\
\text{thus the theorem is proven.}
\]
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 $p_n$ and $q$.

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.
Don’t assume what you want to prove!

Be really careful!

Theorem: $1 = 2$
Proof: For $x = y$, we have

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

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 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.

Careful when proving!
Don’t assume the theorem. Divide by zero. Watch converse.
CS70: Note 3. Induction!

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, ...

A formula.

Teacher: Hello class.
Teacher: Please add the numbers from 1 to 100.
Gauss: It's 100 \times 101 \over 2 \text{ 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.”

Gauss induction proof.

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

\[ 1 + \cdots + k + (k + 1) = \frac{k(k+1)+1}{2} + (k + 1) \]
\[ = \frac{k(k+1) + 2(k+1)}{2} \]
\[ = \frac{k^2 + 3k + 2}{2} \]
\[ = \frac{(k+1)(k+2)}{2} \]

P(k + 1)! By principle of induction...

Notes visualization

Note's visualization: an infinite sequence of dominos.

Prove they all fall down:

▶ P(0) = “First domino falls”
▶ \( \forall k \, P(k) \implies P(k+1) \): “kth domino falls implies that k + 1st domino falls”

Climb an infinite ladder?

P(0)
P(1)
P(2)
P(3)
P(n)
P(n + 1)
P(n + 2)
P(n + 3)

\( \forall k \, P(k) \implies P(k+1) \)
\( P(0) \implies P(1) \implies P(2) \implies P(3) \ldots \)
\( \forall n \in \mathbb{N} \) P(n)

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

Child Gauss: (∀n ∈N)(∑n
i=1 i = n(n+1)
2 ) Proof?

Idea: assume predicate P(n) for n = k. P(k) is ∑k
i=1 i = k(k+1)
2 .

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

∑k+1
i=1 i = (∑k
i=1 i) + (k + 1) = k(k+1)
2 + k + 1 = k+1(k+2)
2 .

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

Induction Step. P(k) ⇒ 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 ∑0
i=1 i = 0 = 0(0+1)
2 . Base Case.

Statement is true for n = 0 P(0) is true
plus inductive step ⇒ true for n = 1 (P(0)+P(1) ⇒ P(1) ⇒ P(2))
... true for n = k ⇒ true for n = k + 1 (P(k)+P(1) ⇒ P(k+1) ⇒ P(k+2))

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

Induction

The canonical way of proving statements of the form
(∀k ∈N)(P(k))

▶ For all natural numbers n, 1 + 2 + ··· + n = n(n+1)
2 .
▶ For all n ∈N, n3 −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) ⇒ 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!