Today: Induction
Reading: Chap. 5.1, 5.2
Next week: Induction, Induction, Induction (Chap. 5)
Positive Integers: (1,2,3,4,5,...)

- $a_1 = 1$
- $a_{n+1} = a_n + 1$

Odd Positive Integers: (1,3,5,7,...)

- $b_1 = 1$
- $b_{n+1} = b_n + 2$

Fibonacci numbers: (1,1,2,3,5,8,13,...)

- $f_1 = 1$, $f_2 = 1$
- $f_{n+2} = f_n + f_{n+1}$
Natural Numbers

Natural numbers (Positive Integers): \((1,2,3,4,5,\ldots)\)

- \(a_1 = 1\)
- \(a_{n+1} = a_n + 1\)

Defining the set of natural numbers \(\mathbb{N}\):

- \(1 \in \mathbb{N}\)
- If \(n \in \mathbb{N}\) then \(n + 1 \in \mathbb{N}\)
- These two rules define all elements of \(\mathbb{N}\)

Defining a function \(f : \mathbb{N} \rightarrow X\)

- \(f(1) = 1\)
- \(f(n + 1) = f(n) + (2n - 1)\)
Odd (positive) numbers

- 1 is odd
- If $n$ is odd, then $n + 2$ is also odd
- All odd numbers can be obtained this way
Inductively defined sets

Odd (positive) numbers

- 1 is odd
- If \( n \) is odd, then \( n + 2 \) is also odd
- All odd numbers can be obtained this way

All train stations that can be reached by train starting from San Diego (Santa Fe)

- San Diego can be (trivially) reached
- If station \( X \) can be reached, and there is a train from \( X \) to \( Y \), then \( Y \) can be reached
We want to prove that a property $P(n)$ is true for all natural numbers $n \in \mathbb{N}$.

Proof by induction:

- Base case: Show that $P(1)$ is true
- Inductive Step: Show that for every $n$, if $P(n)$ is true the $P(n + 1)$ is true
- Conclusion: $P(n)$ is true for every natural number $n$

Let $S$ be the set of all $n$ such that $P(n)$ is true.

Base case: $1 \in S$

Inductive step: if $n \in S$ then $(n + 1) \in S$

Since these rules define all possible elements of $\mathbb{N}$, it must be $S = \mathbb{N}$. 
We want to prove that a property $P(n)$ is true for all natural numbers $n \in \mathbb{N}$.

Proof by induction:

- Base case: Show that $P(1)$ is true
- Inductive Step: Show that for every $n$, if $P(n)$ is true the $P(n+1)$ is true
- Conclusion: $P(n)$ is true for every natural number $n$

Let $S$ be the set of all $n$ such that $P(n)$ is true.

- Base case: $1 \in S$
- Inductive step: if $n \in S$ then $(n+1) \in S$

Since these rules define all possible elements of $\mathbb{N}$, it must be $S = \mathbb{N}$.
Assume

- $P(1)$
- $\forall n. P(n) \rightarrow P(n + 1)$

Then we have,

- $P(1)$
A more intuitive explanation

Assume

- $P(1)$
- $\forall n. P(n) \rightarrow P(n + 1)$

Then we have,

- $P(1)$
- $P(2)$ because $P(1) \rightarrow P(2)$
A more intuitive explanation

Assume

- \( P(1) \)
- \( \forall n. P(n) \rightarrow P(n + 1) \)

Then we have,

- \( P(1) \)
- \( P(2) \) because \( P(1) \rightarrow P(2) \)
- \( P(3) \) because \( P(2) \rightarrow P(3) \)
A more intuitive explanation

Assume

- $P(1)$
- $\forall n. P(n) \rightarrow P(n + 1)$

Then we have,

- $P(1)$
- $P(2)$ because $P(1) \rightarrow P(2)$
- $P(3)$ because $P(2) \rightarrow P(3)$
- $P(4)$ because $P(3) \rightarrow P(4)$
A more intuitive explanation

Assume

- $P(1)$
- $\forall n. P(n) \rightarrow P(n + 1)$

Then we have,

- $P(1)$
- $P(2)$ because $P(1) \rightarrow P(2)$
- $P(3)$ because $P(2) \rightarrow P(3)$
- $P(4)$ because $P(3) \rightarrow P(4)$
- $P(5)$ because $P(4) \rightarrow P(5)$
A more intuitive explanation

Assume

- \( P(1) \)
- \( \forall n. P(n) \rightarrow P(n + 1) \)

Then we have,

- \( P(1) \)
- \( P(2) \) because \( P(1) \rightarrow P(2) \)
- \( P(3) \) because \( P(2) \rightarrow P(3) \)
- \( P(4) \) because \( P(3) \rightarrow P(4) \)
- \( P(5) \) because \( P(4) \rightarrow P(5) \)
- \( \ldots \)
Example 1

The sum of the first $n$ odd natural numbers is a square.

Claim: $\sum_{i=1}^{n} (2i - 1) = n^2$
Example 1

The sum of the first $n$ odd natural numbers is a square.

**Claim:** $\sum_{i=1}^{n}(2i - 1) = n^2$

**Proof:** by induction on $n$

- Base case: if $n = 1$, then $\sum_{i=1}^{1}(2i - 1) = 2 - 1 = 1 = 1^2$
- Inductive step: For any $n$,
  - assume $\sum_{i=1}^{n}(2i - 1) = n^2$.
  - We need to prove $\sum_{i=1}^{n+1}(2i - 1) = (n + 1)^2$
Example 2

Claim: \( \sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} = \frac{1}{2} n^2 + \frac{1}{2} n \)

Base Case:

Inductive Step:
Claim: $\sum_{i=1}^{n} i^2 = 1 + 4 + 9 + \ldots + n^2 = ???$

Try to solve. Can you?

(A) Yes; (B) No; (C) Yes, but I am not sure
Example 3

Claim: $\sum_{i=1}^{n} i^2 = 1 + 4 + 9 + \ldots + n^2 = ???$

Try to solve. Can you?

(A) Yes; (B) No; (C) Yes, but I am not sure

Idea:

- $\sum_{i=1}^{n} i^2 = an^3 + bn^2 + cn + d$ for some constants $a, b, c, d$. 

Daniele Micciancio  
CSE20: Discrete Mathematics
Example 3

Claim: \[ \sum_{i=1}^{n} i^2 = 1 + 4 + 9 + \ldots + n^2 = ??? \]

Try to solve. Can you?

(A) Yes; (B) No; (C) Yes, but I am not sure

Idea:

- \[ \sum_{i=1}^{n} i^2 = an^3 + bn^2 + cn + d \] for some constants \( a, b, c, d \).
- \( n = 0 : 0a + 0b + 0c + d = 0 \)
- \( n = 1 : a + b + c + d = 1 \)
- \( n = 2 : 8a + 4b + 2c + d = 1 + 4 = 5 \)
- \( n = 3 : 27a + 9b + 4c + d = 1 + 4 + 9 = 14 \)

My solution:

\( a = \frac{1}{3}, b = \frac{1}{2}, c = \frac{1}{6}, d = 0 \). Is it correct?
Claim:  \( \sum_{i=1}^{n} i^2 = 1 + 4 + 9 + \ldots + n^2 = ??? \)

Try to solve. Can you?

(A) Yes; (B) No; (C) Yes, but I am not sure

Idea:

\[
\sum_{i=1}^{n} i^2 = an^3 + bn^2 + cn + d \text{ for some constants } a, b, c, d.
\]

\[
\begin{align*}
n = 0 & : 0a + 0b + 0c + d = 0 \\
n = 1 & : a + b + c + d = 1 \\
n = 2 & : 8a + 4b + 2c + d = 1 + 4 = 5 \\
n = 3 & : 27a + 9b + 4c + d = 1 + 4 + 9 = 14
\end{align*}
\]

Can you find \( a, b, c, d \)?

(A) Yes; (B) No; (C) Yes, but I am not sure my answer is correct
Example 3

Claim: \[ \sum_{i=1}^{n} i^2 = 1 + 4 + 9 + \ldots + n^2 = ??? \]

Try to solve. Can you?

(A) Yes; (B) No; (C) Yes, but I am not sure

Idea:

- \[ \sum_{i=1}^{n} i^2 = an^3 + bn^2 + cn + d \] for some constants \( a, b, c, d \).
- \( n = 0 : 0a + 0b + 0c + d = 0 \)
- \( n = 1 : a + b + c + d = 1 \)
- \( n = 2 : 8a + 4b + 2c + d = 1 + 4 = 5 \)
- \( n = 3 : 27a + 9b + 4c + d = 1 + 4 + 9 = 14 \)

Can you find \( a, b, c, d \)?

(A) Yes; (B) No; (C) Yes, but I am not sure my answer is correct

My solution: \( a = 1/3, b = 1/2, c = 1/6, d = 0 \). Is it correct?
\[ \forall n \geq 0. \sum_{i=1}^{n} i^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} = \frac{2n^3 + 3n^2 + n}{6} \]

**Base case:**

**Inductive Step:**

- Assume \( \sum_{i=1}^{n} i^2 = \frac{2n^3 + 3n^2 + n}{6} \)

- Want to prove: \( \sum_{i=1}^{n+1} i^2 = \frac{2(n+1)^3 + 3(n+1)^2 + (n+1)}{6} \)
Claim: For all $n \geq ?$, $2^n < n!$

Question: What is the smallest $n$ such that $2^n < n!$

(A) $n=1$; (B) $n=3$; (C) $n=4$; (D) $n=5$;
Claim: For all $n \geq 5$, $2^n < n!$

Question: What is the smallest $n$ such that $2^n < n!$?

(A) $n=1$; (B) $n=3$; (C) $n=4$; (D) $n=5$;

- Base case: $n = 4$
- Inductive Step:
Claim: For any sets $A_1, \ldots, A_n$ ($n \geq 2$), $(\bigcup_{k=1}^{n} A_k)^c = \bigcap_{k=1}^{n} A_k^c$

- Base case:
- Inductive Step:
**Pie Fight:** A number of people stand in a yard at mutually distinct distances. At the same time, each person throws a pie at their nearest neighbor.

**Claim:** If the number of people is odd, then there is at least one survivor.
Pie Fight: A number of people stand in a yard at mutually distinct distances. At the same time, each person throws a pie at their nearest neighbor.

Claim: If the number of people is odd, then there is at least one survivor.

Proof: By induction on $n = 2k + 1$

- Base case: $n = 1$. Trivial.
- Inductive Step: Assume $n \geq 3$, and claim is true for $n - 2$ people.
- Let $A, B$ be the people closest to each other, and $S$ the rest.
- Necessarily, $A, B$ throw pies at each other.
- What can you say about $S$?
**Strong Induction**

- **Induction:**

  \[
  P(1) \land (\forall n \geq 1. P(n) \rightarrow P(n + 1))
  \]

  \[
  \forall n \geq 1. P(n)
  \]

- **Strong Induction:**

  \[
  Q(1) \land (\forall n \geq 1. [Q(1) \land \cdots \land Q(n)] \rightarrow Q(n + 1))
  \]

  \[
  \forall n \geq 1. Q(n)
  \]

**Theorem:** Induction and Strong Induction are equivalent.
Induction:
\[(P(1) \land (\forall n \geq 1.P(n) \rightarrow P(n+1))) \implies (\forall n \geq 1.P(n))\]

Well Ordering Principle:
“Every nonempty set of positive integers has a smallest element”

**Theorem:** Induction and the Well Ordering Principle are equivalent
Theorem: Every positive integer can be written as a product of primes.
**Theorem:** For every integer \( a \) and positive integer \( d \geq 1 \), there exist (unique) integers \( q, r \) such that \( a = qd + r \) and \( 0 \leq r < q \)

Base case:

(A) \( a = 0 \); (B) \( a = 1 \); (C) \( d = 0 \); (D) \( d = 1 \);
Theorem: For every integer \( a \) and positive integer \( d \geq 1 \), there exist (unique) integers \( q, r \) such that \( a = qd + r \) and \( 0 \leq r < q \)

Base case:

(A) \( a = 0 \); (B) \( a = 1 \); (C) \( d = 0 \); (D) \( d = 1 \);

Proof by induction on \( a \).

- Base case:
- Inductive Step:
**Theorem:** For every integer $a$ and positive integer $d \geq 1$, there exist (unique) integers $q, r$ such that $a =qd + r$ and $0 \leq r < q$

Base case:

(A) $a = 0$; (B) $a = 1$; (C) $d = 0$; (D) $d = 1$;

Proof by induction on $a$.

- Base case:
- Inductive Step:

Did we prove the theorem?

(A) Yes; (B) No; (C) Yes, but only for $a \geq 0$
```python
def divRem1(a, d):  # a, d: integers, a>=0, d>0
    if (a < d):
        (q, r) = (0, a)
        return (q, r)
    else:
        (q, r) = divRem1(a - d, d)
        return (q + 1, r)
```

Daniele Micciancio  
CSE20: Discrete Mathematics
def divRem1(a, d):  # a, d: integers, a>=0, d>0
    if (a < d):
        (q, r) = (0, a)
        return (q, r)
    else:
        (q, r) = divRem1(a - d, d)
        return (q + 1, r)

def divRem(a, d):  # a, d: integers, d>0
    if (a >= 0):
        return (divRem1(a, d))
    else:
        (q, r) = divRem(a + d, d)
        return (q - 1, r)
divRem1 :: (Integer, Integer) -> (Integer, Integer)
divRem1 (a, d) =
    if (a < d) then (0, a)
    else let (q, r) = divRem1 (a - d, d)
            in (q + 1, r)

divRem :: (Integer, Integer) -> (Integer, Integer)
divRem (a, d) =
    if (a >= 0) then divRem (a, d)
    else let (q, r) = divRem (a + d, d)
            in (q - 1, r)
Other inductively defined sets

Binary strings (BS):
- "" is a BS (empty string)
- If $w$ is a BS, then $s_0$ is a BS
- If $w$ is a BS, then $s_1$ is a BS

Palindromes:
- "" is a Palindrome
- "x" is a Palindrome (for any symbol "x")
- If $W$ is a Palindrome, then $xWx$ is a palindrome (for any symbol "x")

Well parenthesized expressions (WPE)
- [] is a WPE
- if $w$ is a WPE, then [$w$] is a WPE
- if $u,w$ are WPE, then $uw$ is a WPE