CS 301: Lecture Topics

1. Sets. Homeworks are: p. 7: 1, 9, 17, 23, 29, 34, 39, 46; p. 16: 1-10, 13, 15, 19; p.23: 3, 4, 7, 8; p.27: 5-10, 13
   - Notation: enumeration, with ellipses, set-builder predicate
   - \( \mathbb{N} \) is the natural numbers, \( \mathbb{Z} \) is the integers, \( \mathbb{Z}^+ \) is the nonnegative integers, \( \mathbb{R} \) is the reals, \( \mathbb{R}^+ \) is the nonnegative reals, \( \mathbb{Q} \) is the rationals
   - Notation: membership status versus subset status
   - Example: Work with predicates; prove: \( \{ x \in \mathbb{Z} : 4 \mid x \} \subseteq \{ x \in \mathbb{Z} : 2 \mid x \} \).
   - Intervals in \( \mathbb{Z} \) or \( \mathbb{R} \): open, closed, half-open, infinite
   - Empty set. Distinction: \( \{\} = \emptyset \) is different from \( \{\{\}\} = \{\emptyset\} \)
   - Cardinalities (sizes) of sets. \( |A| \) is the cardinality of \( A \), the number of members in \( A \)
   - Subset vs. membership
   - Exercises, p. 7.
   - Def: an ordered pair from sets \( A \) and \( B \) has the form \( (x, y) \) with \( x \in A, y \in B \).
   - Cartesian product of sets \( A \) and \( B \) is \( A \times B = \{(x, y) : x \in A, y \in B\} \).
   - Exercises, p. 10. #3: \( \{ x \in \mathbb{R} : x^2 = 2 \} \times \{ a, c, e \} =? \)
   - \( |A \times B| = |A| \cdot |B| \).
   - Ordered triples, is \( (A \times (B \times C)) = ((A \times B) \times C) = (A \times B \times C) \)?
   - Cartesian powers \( A^n = \underbrace{A \times A \times \cdots \times A}_{n} \) for \( n \in \mathbb{N} \).
   - \( \emptyset \subseteq A \) for any set \( A \).
   - Exercises, p 14. #3 ? List all subsets of \( \{\{\}\} \).
   - #15 ? \( \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - 1 = 0\} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 - x = 0\} \).
   - \( \mathcal{P}(A) \) is the collection of subsets of \( A \). \( |\mathcal{P}(A)| = 2^{|A|} \). Proof?
   - Exercises, p. 16, #20 ? \( |A| = m \Rightarrow |\{X \subseteq \mathcal{P}(A) : |X| \leq 1\}| =? \)
   - Set operations: \( A \cup B, A \cap B, A - B \) (also \( A \setminus B \)), \( \overline{A} = A^c \) (Note domain of discourse)
   - Exercises, p. 18, #3i ? \( A = \{0, 1\}, B = \{1, 2\}, \mathcal{P}(A \times B) =? \)
   - Venn diagrams
   - Exercises, \( \overline{A \cup B} = \overline{A} \cap \overline{B} \)
   - DeMorgan’s Laws: \( \overline{A \cup B} = \overline{A} \cap \overline{B} \) and \( \overline{A \cap B} = \overline{A} \cup \overline{B} \).
   - Commutative Laws: \( A \cup B = B \cup A \) and \( A \cap B = B \cap A \)
   - Expressions involving only \( \cup \) or only \( \cap \) need not have parenthesis. Not so with expressions using both. Venn Diagram for \( A \cap (B \cup C) \)
   - Associative Laws: \( A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C \) and also for \( \cap \), but not for mixed
   - Distributive Laws: \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \) and \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \)
   - Indexed sets: \( \bigcup_{i=1}^{\infty} A_i, \bigcup_{i \in I} A_i \)
   - Well-ordering for natural numbers: If \( X \subset \mathbb{N} \) and \( X \neq \emptyset \), then \( X \) contains a smallest member.
Theorem: Given integers $a$ and $b$ with $b > 0$, there exist integers $q$ and $r$ such that $a = qb + r$, $0 \leq r < b$.
Proof: Let $A = \{a - xb : x \in \mathbb{Z}, a - xb \geq 0\}$, implying $A$ has a smallest member, say $r$. Then, from the definition of $A$,

\begin{align*}
r &= a - qb, \text{ for some } q \in \mathbb{Z} \\
r &\geq 0.
\end{align*}

If $r \geq b$,

\[0 \leq r - b = a - qb - b = a - (q + 1)b \Rightarrow r - b \in A.\]

Since $b > 0$, $r - b < r$. So, $r - b \in A$ is a contradiction of $r$ is the smallest member of $A$.
So $0 \leq r < b$ and $a = qb + r$.

Russell’s paradox: $A = \{X : X \text{ is a set and } X \not\in X\}$. Is $A \in A$?
\begin{align*}
A \in A? \text{ True } \Rightarrow \text{ False, and False } \Rightarrow \text{ True.}
\end{align*}
2. Logic. Homeworks are: p. 35: 2, 3, 4, 5, 7; p. 39: 6, 7, 12; p. 42: 1, 3, 5, 7, 9, 11, 13; p. 44: 1, 3; p. 46: 1, 5, 9, 11; p. 49: 1, 5, 9, 13; p. 51: 1, 5, 7, 9; p. 55: 3, 7, 9; p. 58: 2, 3, 5, 9

• A **statement** is a sentence or mathematical expression that is either definitely true or definitely false.

  Examples:
  - Every even number is divisible by 2. (true)
  - \( \sqrt{2} \in \mathbb{Z} \). (false)
  - Add 2 to both sides of the equation. (not a statement)
  - \( P \): For every \( n \in \mathbb{N} \) with \( n > 1 \), \( 2^n - 1 \) is prime. (false)

• An **open statement** is a sentence containing variables, which may be true or false, depending on the values assigned to the variables.

  Examples:
  - \( Q(x) \): The integer \( x \) is even. (open statement)
  - \( P(x) \): If \( x \in \mathbb{Z} \) is a multiple of 6, then \( x \) is even. (true statement)
  - Every even integer greater than 2 is the sum of two prime numbers. (statement – truth status is unknown). Goldback Conjecture postulated in 1742.

• Logical connectives: and (\( \land \)), or (\( \lor \)), not (\( \neg \)), implication (\( \Rightarrow \)), equivalence (\( \iff \)) or equality (\( = \))

• Truth tables.

\[
\begin{array}{cccccccc}
P & Q & \sim P & \sim Q & P \land Q & P \lor Q & P \Rightarrow Q & \sim P \lor Q & (P \Rightarrow Q) \iff (\sim P \lor Q) \\
T & T & F & F & T & T & T & T & T \\
T & F & F & T & F & T & F & F & T \\
F & T & T & F & T & T & T & T & T \\
F & F & T & T & F & T & T & T & T \\
\end{array}
\]

• Note \( P \lor Q \) means “\( P \) is true or \( Q \) is true or both are true.” That is, \( P \lor Q \) is an **inclusive** “or.”

  The **exclusive** “or” means “either \( P \) is true or \( Q \) is true, but not both.” It is **not** a logical connective. Can implement the exclusive-or with \( (P \lor Q) \land [\sim (P \land Q)] \).

• True statements \((P, Q)\) represents knowledge acquired about a domain of discourse.

• **Conditional** statements \((P \Rightarrow Q)\) represent conditional knowledge.

  Suppose we have proved \( P \Rightarrow Q \) in our domain context. We can be sure that if \( P \) is true, then \( Q \) must be true.

  However, if \( P \) is false, the implication \( P \Rightarrow Q \) gives no information about \( Q \). That is, \( Q \) may be true or false.

  In both cases, the rule is still valid, which is reflected in the judgment \( P \Rightarrow Q \) is true.

  A “proof” of \( P \Rightarrow Q \) essentially shows that the second line of the truth table above **cannot happen** in our domain of discourse.

  Consider “If you pass the final exam, then you will pass the course.”
• $P \Rightarrow Q$ can be stated in various ways.
  – If $P$, then $Q$
  – $Q$, if $P$
  – $Q$, whenever $P$
  – $Q$, provided that $P$
  – Whenever $P$, then also $Q$
  – $P$ is a sufficient condition for $Q$ *
  – For $Q$, it is sufficient that $P$
  – $Q$ is a necessary condition for $P$ *
  – For $P$, it is necessary that $Q$
  – $P$ only if $Q$

• Statements related to $P \Rightarrow Q$:
  – Converse: $Q \Rightarrow P$
  – Contrapositive: $\sim Q \Rightarrow \sim P$ (Equivalent to original statement)
  – Inverse: $\sim P \Rightarrow \sim Q$. (Contrapositive of Converse)

• DeMorgan’s Laws: $\sim (P \lor Q) = (\sim P) \land (\sim Q)$ and $\sim (P \land Q) = (\sim P) \lor (\sim Q)$

• Commutative Laws: $P \lor Q = Q \lor P$ and $P \land Q = Q \land P$

• Distributive Laws: $P \land (Q \lor R) = (P \land Q) \lor (P \land R)$ and $P \lor (Q \land R) = (P \lor Q) \land (P \lor R)$

• Associative Laws: $P \land (Q \land R) = (P \land Q) \land R$, also for $\lor$, but not mixed

• Quantifiers
  – “For all” (universal quantifier): $\forall x, x \in \mathbb{Z} \Rightarrow 2x$ is even
  – $\forall x \in \mathbb{Z}, 2x$ is even
  – $\forall x, 2x$ is even (universe of discourse is $\mathbb{Z}$
  – “There exists” (existential quantifier): $x \in \mathbb{Z}, x$ even $\Rightarrow \exists y \in \mathbb{Z}, x = 2y$
  – $\{x : \exists y, x = 2y\}$ is the set of even integers (universe of discourse is $\mathbb{Z}$

• order of quantifiers matters. Example
  $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x$ is true; Negation: $\exists x, \forall y, y^3 \neq x$
  $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, y^3 = x$ is false; Negation: $\forall y, \exists x, y^3 \neq x$

• Convention: conditional open statements are considered universally quantified. Examples:
  $(4|x \Rightarrow 2|x)$ means $\forall x \in \mathbb{Z}, 4|x \Rightarrow 2|x$
  $f$ differentiable $\Rightarrow f$ continuous means $\forall f : \mathbb{R} \rightarrow \mathbb{R}, f$ differentiable $\Rightarrow f$ continuous

• Translating English into symbolic logic.
  – Goldback Conjecture: Every even integer greater than 2 is the sum of two primes.
    $\forall x \in \mathbb{Z}, x > 2 \Rightarrow \exists y, z \in \mathbb{Z}, y$ is prime, $z$ is prime, $x = y + z$, or with universal quantification convention
    $x \in \mathbb{Z}, x > 2 \Rightarrow \exists y, z \in \mathbb{Z}, y$ is prime, $z$ is prime, $x = y + z$.
  – I don’t eat anything that has a face: $\forall x, F(x) \Rightarrow \sim E(x)$ or simply $F(x) \Rightarrow (\sim E(x))$ with universal quantification convention
• Negation:
  \(- \sim (P \lor Q) = (\sim P) \land (\sim Q); \sim (P \land Q) = (\sim P) \lor (\sim Q)\)
  \(- \sim (P \Rightarrow Q) = \sim ((\sim P) \lor Q) = P \land (\sim Q)\)
  \(- \sim (\forall x, P(x)) = \exists x, \sim P(x); \sim (\exists x, P(x)) = \forall x, \sim P(x)\)
  \(- \sim (\forall x, F(x) \Rightarrow (\sim E(x))) = \exists x, \sim (F(x) \Rightarrow (\sim E(x))) = \exists x, (F(x) \land E(x))\)

  \(- f \text{ approaches limit } L \text{ as } x \text{ approaches } a:\)
  \[\lim_{x \to a} f(x) = L: \forall \epsilon > 0, \exists \delta > 0, 0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon\]
  \[f \text{ does not approach } L \text{ as } x \text{ approaches } a:\)
  \[\sim (\forall \epsilon > 0, \exists \delta > 0, 0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon)\]
  \[\exists \epsilon > 0, \sim (\exists \delta > 0, 0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon)\]
  \[\exists \epsilon > 0, \forall \delta > 0, \sim (0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon)\]
  \[\exists \epsilon > 0, \forall \delta > 0, (0 < |x - a| < \delta) \land (|f(x) - L| \geq \epsilon)\]

• Logical Syllogisms

<table>
<thead>
<tr>
<th>(P \Rightarrow Q)</th>
<th>(P \Rightarrow \sim Q)</th>
<th>(P \lor Q)</th>
<th>(P \land Q)</th>
<th>(P)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(P)</td>
<td>(\sim Q)</td>
<td>(\sim P)</td>
<td>(P \land Q)</td>
<td>(P)</td>
</tr>
<tr>
<td>(Q)</td>
<td></td>
<td>(Q)</td>
<td>(P \lor Q)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(P)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(P \land Q)</td>
<td></td>
</tr>
</tbody>
</table>
3. Counting: Homeworks are p. 66: 3, 7, 9; p. 70: 5, 7; p. 75: 5, 7, 9, 11; p. 78: 3, 5, 7, 9; p. 81: 1, 3, 7, 9

- A list is an ordered sequence of elements — a list is not a set, a list of size 2 is an ordered pair.
- The length of a list is the number of elements in the list. A list of length zero has no elements.
- Example. Suppose the set of elements for constructing lists is the set \( \{a, b, c, d, e, f, g\} \).
  - How many length-4 lists if repetition is allowed? \( 7 \cdot 7 \cdot 7 \cdot 7 = 7^4 = 2401 \)
  - \( \ldots \) if repetitions is not allowed? \( 7 \cdot 6 \cdot 5 \cdot 4 = 840 \)
  - \( \ldots \) no repetition and a mandatory \( e \): no repetition ⇒ exactly one \( e \): 4 choices for \( e \) location, followed by \( 6 \cdot 5 \cdot 4 \) for the rest, giving \( 4 \cdot 6 \cdot 5 \cdot 4 = 480 \).
  - \( \ldots \) repetition is allowed and an \( e \) is mandatory? No \( e \): \( 6^4 = 1296 \Rightarrow 7^4 - 6^4 = (7^2 - 6^2)(7^2 + 6^2) = (13)(85) = 1105 \).

- p. 67, #11: For length-6 lists from \( a, b, c, d, e, f, g, h \) with no repetitions, how many have two consecutive vowels?
  - vowels are \( a, e \); 5 consecutive positions are 1, 2; 2, 3; 3, 4; 4, 5; 5, 6
    - Choose a pair of consecutive positions: 5 choices
    - Choose an ordering of the vowels: 2 choices
    - Fill the remaining 4: \( 6 \cdot 5 \cdot 4 \cdot 3 = 360 \)
    - Total: \( 5 \cdot 2 \cdot 360 = 3600 \).
- Definition of factorial: \( n! = n(n-1)(n-2) \cdots (2)(1) \). Also, \( 0! = 1 \).
  - The number of non-repetitive length-\( n \) lists constructed from a field of \( n \) symbols is \( n! \).
- Example: symbol field \( \{0, 1, 2, 3, 4, 5, 6\} \), list length = 7
  - no repetition: \( 7! = 5040 \)
  - no repetition and first three are odd: \( 3! \cdot 4! = 144 \)
  - repetition allowed and at least one repetition: \( 7^7 - 7! = 823543 - 5040 = 818503 \).
- How many non-repetitive \( k \)-length lists from a field of \( n \) objects?: \( \frac{n(n-1)(n-2) \cdots (n-k+1)}{k} \).

\[
n(n-1) \cdots (n-k+1) = \frac{n!}{(n-k)!}, \text{ for } 0 \leq k \leq n.
\]

A non-repetitive list with \( k \) elements is one of \( k! \) ways of displaying a set with \( k \) elements.
So, in the \( \frac{n!}{(n-k)!} \) lists, the same set appears \( k! \) times.
Consequently, \( \frac{n!}{k!(n-k)!} = \binom{n}{k} \) is the numbers of distinct subsets of size \( k \) from a field of size \( n \).

- \( \binom{n}{k} \) is also called a binomial coefficient. Why?

\[
(x + y)^2 = (x + y)(x + y) = xx + xy + yx + yy = x^2 + 2xy + y^2
\]
\[
(x + y)^4 = \binom{4}{0} x^4 + \binom{4}{1} x^3 y + \binom{4}{2} x^2 y^2 + \binom{4}{3} xy^3 + \binom{4}{4} y^4 = x^4 + 4x^3 y + 6x^2 y^2 + 4xy^3 + y^4.
\]

Binomial Theorem:

\[
(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.
\]

- How many 5-card “hands” are possible with a 52-card deck?

\[
\binom{52}{5} = \frac{52!}{5! \cdot 47!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 26 \cdot 51 \cdot 10 \cdot 49 \cdot 4 = 2,598,960.
\]
• How many “full house” hands? (Three of one rank, two of another)
  Choose two of the thirteen ranks.
  Choose which of the chosen ranks will receive two cards, which fixes three cards for the other rank.
  Choose two of the 4 cards from the 2-card rank.
  Choose three of the 4 cards in the 3-card rank.

\[
\binom{13}{2}\binom{2}{1}\binom{4}{4}\binom{4}{3} = \frac{13 \cdot 12}{2} \cdot 2 \cdot 6 \cdot 4 = 3744.
\]

Chances of a full house: \(\frac{3744}{2598960} = 0.001441\).

• Note \(\binom{n}{k} = \binom{n}{n-k}\). Why?

\[
\binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad \binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}
\]

Also, can pair each subset with its complement. There are \(\binom{n}{k}\) and \(\binom{n}{n-k}\) complements.

• Pascal’s formula for \(0 < k \leq n\),

\[
\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \iff \text{Pascal’s triangle}
\]

• Inclusion-Exclusion. From Venn diagram: \(|A \cup B| = |A| + |B| - |A \cap B|\).

A three-card hand is dealt from a standard 52-card deck. How many different hands are possible for which all 3 cards are red or all three cards are face cards.

Let \(A\) be the set of three-card hands in which all are red; let \(B\) be the set in which all are face. We want \(|A \cup B|\).

\[
|A| = \binom{26}{3}, \quad |B| = \binom{12}{3}, \quad |A \cap B| = \binom{6}{3}, \quad |A \cup B| = \binom{26}{3} + \binom{12}{3} - \binom{6}{3} = \frac{26 
\cdot 25 \cdot 24}{3 \cdot 2 \cdot 1} + \frac{12 \cdot 11 \cdot 10}{3 \cdot 2 \cdot 1} - \frac{6 \cdot 5 \cdot 4}{3 \cdot 2 \cdot 1} = 2600 + 220 - 20 = 2800.
\]

• From Venn diagram: \(|A \cup B \cup C| = \sum_{i=1}^{3} |i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \ldots
\]

\[
\ldots (-1)^{n-1} \sum_{1 \leq i_1 < i_2 < \ldots < i_n} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_n}|
\]

Truncate after a positive term \(\Rightarrow\) over-estimate

Truncate after a negative term \(\Rightarrow\) under-estimate.
• If \( i \neq j \Rightarrow A_i \cap A_j = \emptyset \), then Law of Inclusion-Exclusion simplifies to the **Addition Principle**:

If \( A_1, \ldots, A_n \) are sets with \( i \neq j \Rightarrow A_i \cap A_j = \emptyset \), then

\[
\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i|.
\]

• Example: How many 7-bit binary strings have an odd number of 1’s? 1-count, \( C \), must be 1, 3, 5, or 7. For \( i = 1, 3, 5, 7 \), let \( A_i \) be the number of 7-digit binary strings with \( i \) 1’s. Then \( C = A_1 + A_3 + A_5 + A_7 \)

\[
C = \binom{7}{1} + \binom{7}{3} + \binom{7}{5} + \binom{7}{7} = 7 + \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1} + \frac{7 \cdot 6}{2 \cdot 1} + 1 = 7 + 35 + 21 + 1 = 64.
\]
4. Direct Proof. Homeworks are p. 98: 3, 5, 9, 13, 15, 19, 23, 27

- Definitions: even, odd, divides, multiple, prime, gcd, lcm.
- Direct proof outline for $P \Rightarrow Q$.
- Integer examples: $x$ odd $\Rightarrow x^2$ is odd.
  
  $a \mid b, b \mid c \Rightarrow a \mid c$
  
  $x$ even $\Rightarrow x^2 - 6x + 5$ odd
- $a, b, c \in \mathbb{N} \Rightarrow \text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$
  
  Pf: Let $m = \text{lcm}(ca, cb), n = c \cdot \text{lcm}(a, b)$.
  
  We will show: $m = n$ via $m \leq n$ and $n \leq m$.
  
  $\exists x, y \in \mathbb{N}, \text{lcm}(a, b) = ax = by$
  
  $n = c \cdot \text{lcm}(ca, cb) = cax = cby$ is a multiple of $ca$ and $cb$.
  
  $n$ is a competitor for $\text{lcm}(ca, cb) = m \Rightarrow m \leq n$.
  
  Also, $m = \text{lcm}(ca, cb)$ is a multiple of $ca$ and of $cb$, so $m = cax = cby$ for some $x, y \in \mathbb{N}$.
  
  Therefore $c \mid m$. Then,
  
  $m/c = ax = by$. That is, $m/c$ is a multiple of both $a$ and $b \Rightarrow m/c \geq \text{lcm}(a, b) \Rightarrow m \geq c \cdot \text{lcm}(a, b) = n$.
  
  $m = n$. ■

- $x, y \in \mathbb{R}^+, x \leq y \Rightarrow \sqrt{x} \leq \sqrt{y}$.
  
  Pf: Note correct for $x = y = 0$. In all other cases, at least one of $x$ or $y$ is strictly positive.
  
  $x \leq y$
  
  $x - y \leq 0$
  
  $(\sqrt{x})^2 - (\sqrt{y})^2 \leq 0$
  
  $(\sqrt{x} + \sqrt{y}) \cdot (\sqrt{x} - \sqrt{y}) \leq 0$
  
  $(\sqrt{x} - \sqrt{y}) \leq 0$
  
  $\sqrt{x} \leq \sqrt{y}$. ■

- $x, y \in \mathbb{R}^+ \Rightarrow 2\sqrt{xy} \leq x + y$.
  
  Pf:
  
  $0 \leq (x - y)^2 = x^2 - 2xy + y^2$
  
  $4xy \leq x^2 + 2xy + y^2 = (x + y)^2$
  
  $2\sqrt{xy} \leq x + y$, by preceding proposition. ■

- $n \in \mathbb{N} \Rightarrow 4|\lbrack 1 + (-1)^n(2n - 1)\rbrack$.
  
  Proof by cases:
  
  Case (1): $n$ is even. That is, $n = 2k$ for some $k$.
  
  $1 + (-1)^n(2n - 1) = 1 + (-1)^{2k}(2(2k) - 1) = 1 + (4k - 1) = 4k$
  
  $4|\lbrack 1 + (-1)^n(2n - 1)\rbrack$
  
  Case (2): $n$ is odd. That is, $n = 2k + 1$ for some $k$.
  
  $1 + (-1)^n(2n - 1) = 1 + (-1)^{2k+1}(2(2k + 1) - 1) = 1 - [2(2k + 1) - 1] = 2 - 2(2k + 1) = -4k$
  
  $4|\lbrack 1 + (-1)^n(2n - 1)\rbrack$. ■
• \( \forall k \in \mathbb{Z}, k \) is a multiple of 4 \( \Rightarrow k = 1 + (-1)^n(2n - 1) \), for some \( n \in \mathbb{N} \).

Proof by cases:

Let \( k = 4a \)

Case (1): \( a = 0 \)

Let \( n = 1 \)

Then \( 1 + (-1)^n(2n - 1) = 1 - (2 \cdot 1 - 1) = 2 - 2 = 0 = 4a = k \).

Case (2): \( a > 0 \)

Let \( n = 2a \in \mathbb{N}. n \) is even.

Then \( 1 + (-1)^n(2n - 1) = 1 + [2(2a) - 1] = 4a = k \).

Case (3): \( a < 0 \)

Let \( n = 1 - 2a \in \mathbb{N}. n \) is odd.

Then \( 1 + (-1)^n(2n - 1) = 1 - [2(1 - 2a) - 1] = 1 - 2(1 - 2a) + 1 = 2 - 2 + 4a = k \)

• If two integers have opposite parity, then their sum is odd.

Pf: Let \( x, y \) be two integers with opposite parity.

Wolog, \( x \) is even and \( y \) is odd.

\( x = 2a, y = 2b + 1 \Rightarrow x + y = 2a + 2b + 1 = 2(a + b) + 1 \Rightarrow x + y \) is odd.
5. Contrapositive proof. Homeworks are p. 108: 3, 7, 11, 13, 17, 19, 23, 27, 31

- \( P \Rightarrow Q \) and \( \sim Q \Rightarrow \sim P \) have the same truth table.
- Sometimes, the contrapositive is much easier. For example,
  
  Proposition: If \( x^2 - 6x + 5 \) is even, then \( x \) is odd.
  
  Proof: Let \( x^2 - 6x + 5 \) be even.
  
  \[
  x^2 - 6x + 5 = 2b, \quad \text{for some integer } b \\
  x^2 - 6x + (5 - 2b) = 0 \\
  x = \frac{6 \pm \sqrt{36 - 4(1)(5 - 2b)}}{2} = \frac{6 \pm \sqrt{16 + 8b}}{2}
  \]

  Is \( x \) rational? Note \( b = 0 \Rightarrow x = (6 \pm 4)/2 = 1, 5 \) (both odd). Other \( b \)? ...

  Try again.
  
  Proof: We prove the contrapositive. Suppose \( x \) is not odd. Then \( x \) is even.
  
  Then \( x = 2b \) for some integer \( b \).
  
  Then \( x^2 - 6x + 5 = (2b)^2 - 6(2b) + 5 = 4b^2 - 12b + 5 = 2(2b^2 - 6b + 2) + 1 \)
  
  So, \( x^2 - 6x + 5 \) is odd.
  
  Therefore \( x^2 - 6x + 5 \) is not even.  

- Working with the contrapositive involves negating statement \( \Rightarrow \) DeMorgan’s Laws.
  
  Proposition: 5 \( \not|x \) \( \not y \Rightarrow (5 \not|x \land 5 \not y) \)
  
  Proof by contrapositive.
  
  Suppose \( \sim (5 \not|x \land 5 \not y) \). That is \( 5|x \lor 5|y \).
  
  Case 1: \( 5|x \). Hedging on a generic \( x \)... Then \( x = 5b \) and \( xy = 5by \Rightarrow 5|xy \)
  
  Case 2: \( 5|y \). Then \( y = 5c \) and \( xy = 5cx \Rightarrow 5|xy \).  

- Definition: For integers \( x, y \), we say \( x \) is congruent to \( y \) mod \( n \) if \( n|(x - y) \). (written \( x \equiv y \mod n \))
  
- Note \( x \equiv y \mod n \) iff \( x \) and \( y \) have the same remainder on division by \( n \).
  
  Proof: Write \( x = q_1n + r_1, \ y = q_2n + r_2 \).
  
  If \( r_1 = r_2 \), then \( x - y = q_1n - q_2n = (q_1 - q_2)n \Rightarrow n|(x - y) \Rightarrow x \equiv y \mod n \).
  
  Conversely, if \( x \equiv y \mod n \), then \( n|(x - y) \Rightarrow (x - y) = qn \Rightarrow q_1n + r_1 - q_2n - r_2 = qn \Rightarrow 
  
  r_1 - r_2 = n(q - q_1 + q_2) \Rightarrow n|(r_1 - r_2) \)
  
  Since \( 0 \leq r_1 < n \) and \( 0 \leq r_2 < n \), we have \( -n < r_1 - r_2 < n \Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2 \).

- Proposition: \( a \equiv b \mod n \Rightarrow a^2 \equiv b^2 \mod n \).
  
  Proof: Suppose \( a \equiv b \mod n \).
  
  Then \( n|(a - b) \Rightarrow a - b = nc \Rightarrow (a + b)(a - b) = (a + b)nc \Rightarrow a^2 - b^2 = nc(a + b) \Rightarrow n|(a^2 - b^2) \).
  
  Therefore \( a^2 \equiv b^2 \mod n \).  

- Proposition: \( a, b \in \mathbb{Z}, n \in \mathbb{N}, 12a \neq 12b \mod n \Rightarrow n \not|12 \).
  
  Proof: (Contrapositive) Suppose \( n|12 \Rightarrow 12 = nc \Rightarrow 12(a - b) = nc(a - b) \Rightarrow 12a - 12b = n(ca - cb) \)
  
  \( \Rightarrow 12a \equiv 12b \mod n \).  

- Mathematical Writing...

- Example. Prop: \( \forall a, b \in \mathbb{Z}, a^2 - 4b \neq 2 \).
  Proof. By contradiction. Suppose \( \exists a, b \in \mathbb{Z} \) with \( a^2 - 4b = 2 \).
  Then \( a^2 = 4b + 2 = 2(2b + 1) \Rightarrow a^2 \) is even \( \Rightarrow a \) is even.
  Then \( a = 2c \) for some integer \( c \Rightarrow 2 = a^2 - 4b = (2c)^2 - 4b = 4c^2 - 4b \)
  Divide by 2: \( 1 = 2c^2 - 2b = 2(c^2 - b) \) is even — a contradiction, since 1 is odd.

- Consequences of “proving” \( \sim P \Rightarrow (C \land \sim C) \)
  
  \[
  \begin{array}{|c|c|c|c|c|}
  \hline
  P & C & \sim P & C \land \sim C & (\sim P) \Rightarrow (C \land \sim C) \\
  \hline
  T & T & F & F & T \\
  T & F & F & F & T \\
  F & T & T & F & F \\
  F & F & T & F & F \\
  \hline
  \end{array}
  \]

  That is, \( P \) is equivalent to \( (\sim P) \Rightarrow (C \land \sim C) \).

- General form of proof by contradiction (for statement \( P \))

  \[
  \sim P \\
  \vdash \\
  C \land \sim C \\
  \]

  For \( P = (Q \Rightarrow R) \)
  \[
  \sim (Q \Rightarrow R) \\
  \sim (\sim Q \lor R) \\
  Q \land \sim R \\
  \vdash \\
  C \land \sim C \\
  \]

  For \( P = (Q \Rightarrow R) \)
  \[
  \sim (Q \Rightarrow R) \\
  \sim (\sim Q \lor R) \\
  Q \land \sim R \\
  Q \\
  \sim R \\
  \vdash \\
  \sim Q \\
  Q \land \sim Q \\
  \]

  embedded contrapositive \( \sim R \Rightarrow \sim Q \)

- Prop: \( \sqrt{2} \) is irrational.
  Proof: For purposes of deriving a contradiction, suppose \( \sqrt{2} \) is rational.
  Let \( \sqrt{2} = a/b \), for integers \( a, b \) in lowest terms. That is, \( a, b \) have no common divisor other than 1.
  \( 2 = a^2/b^2 \Rightarrow a^2 = 2b^2 \Rightarrow a^2 \) is even \( \Rightarrow a \) is even \( \Rightarrow a = 2c \) for some integer \( c \)
  \( a/b \) in lowest terms \( \Rightarrow b \) is odd.
  But, \( (2c)^2 = 2b^2 \Rightarrow 4c^2 = 2b^2 \Rightarrow b^2 = 2c^2 \Rightarrow b^2 \) is even \( \Rightarrow b \) is even.
  Therefore \( b \) is both even and odd, a contradiction.

- Prop: There are infinitely many prime numbers.
  Proof: For purposes of deriving a contradiction, suppose there are finitely many prime numbers, say \( 2 = p_1 < p_2 < \ldots < p_n \). Then

  \[
  q = \left( \prod_{j=1}^{n} p_j \right) + 1 > p_n \Rightarrow q \text{ is not prime}
  \]

  \[
  \frac{q}{p_k} = c, \text{ an integer, for some } k \in \{1, 2, \ldots, n\}
  \]

  \[
  \left( \prod_{1 \leq j \leq n, j \neq k} p_j \right) + \frac{1}{p_k} = c
  \]

  \[
  \frac{1}{p_k} = c - \left( \prod_{1 \leq j \leq n, j \neq k} p_j \right),
  \]

  which means \( 1/p_k \) is an integer — a contradiction, since \( p_k \geq 2 \).
Proposition: \( \forall x \in \mathbb{Q}, \exists y, z \not\in \mathbb{Q}, x = y \cdot z. \)

Proof (direct):
Suppose \( r \in \mathbb{Q}, r \neq 0. \)
Then \( r = a/b \) for integers \( a \) and \( b. \)
Write \( r = \sqrt{2} \cdot (r/\sqrt{2}). \)
Since \( \sqrt{2} \) is irrational, we need to prove that \( r/\sqrt{2} \) is also irrational.

Nested proof (contradiction) of \( r/\sqrt{2} \) is irrational:
Suppose \( r/\sqrt{2} \) is rational.
Then, for integers \( c \) and \( d, \)
\[
\frac{r}{\sqrt{2}} = \frac{c}{d}
\Rightarrow \sqrt{2} = \frac{r \cdot d}{c} = \frac{a \cdot d}{bc},
\]
which implies \( \sqrt{2} \) is rational — a contradiction.

End of nested proof
So \( r/\sqrt{2} \) is irrational and \( r = \sqrt{2} \cdot (r/\sqrt{2}), \) the product of two irrational numbers. \( \blacksquare \)
7. Proving Non-conditional statements. Homeworks are p. 127: 3, 9, 15, 21, 27, 33.

- To prove $P \iff Q$, first prove $P \implies Q$ and then $Q \implies P$.
  Use “Conversely” to introduce the second half. Can use different methods in the two proofs.

- To prove a list of equivalent statements, e.g.,
  
  \begin{itemize}
  \item[(a)] The matrix $A$ is invertible
  \item[(b)] The equation $Ax = b$ has a unique solutions for each $b \in \mathbb{R}^n$
  \item[(c)] The equation $Ax = 0$ has only the trivial solution $x = 0$
  \item[(d)] The reduced row echelon form of $A$ is $I_n$
  \item[(e)] $\det(A) \neq 0$
  \item[(f)] The matrix $A$ does not have zero as an eigenvector
  \end{itemize}

Do not need to prove \($\binom{6}{2}\) = 15 equivalences, e.g. \((c) \iff (f)\).

Instead, \((a) \implies (b) \implies (c) \implies (d) \implies (e) \implies (f) \implies (a),\)

or some variation that allows an inference chain from any statement to any other.

- Existence proofs.
  
  Example. Proposition: There exists an even prime number.
  Proof: Consider 2, an even prime number. [Box]

  Example. Proposition: There exists a natural number that can be expressed as the sum of two cubes in two different ways.
  Proof: Consider $1729 = 1^3 + 12^3 = 9^3 + 10^3$.

  Ramanujan number: The smallest natural number that is expressible as the sum of two cubes in two different ways. (Taxi number in Hardy’s visit)

- Existence statement inside a $P \implies Q$ proof.
  
  Proposition: $\forall a, b \in \mathbb{N}, \exists m, n \in \mathbb{Z}, \gcd(a, b) = am + bn$.
  Proof: Suppose $a, b \in \mathbb{N}$.
  
  Let $A = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$ and let $d$ be the smallest number in $A$. (Note $A$ is bounded from below.)
  
  $d \in A \implies d = am + bn$, for some $m, n \in \mathbb{Z}$.
  
  At this point we have the existence of a candidate $d$. There remains to show that $d = \gcd(a, b)$.
  
  Write $a = qd + r$ with $0 \leq r < d$.
  
  Embedded proof by contradiction: Suppose $r > 0$
  
  $r = a - qd = a - q(am + bn) = a(1 - qm) + b(-qn) \implies r \in A$
  
  Then $r < d$ contradicts the fact that $d$ is the smallest number in $A$.
  
  So, $r = 0 \implies a = qd \implies d|a$.
  
  Similarly, $d|b$.
  
  Now, $d|a$ and $d|b$ implies $d$ is a competitor for $\gcd(a, b)$. Hence $d \leq \gcd(a, b)$.
  
  Since $\gcd(a, b)$ divides both $a$ and $b$, we conclude $a = x \cdot \gcd(a, b)$ and $b = y \cdot \gcd(a, b)$ for some integers $x, y$. Then,
  
  $0 < d = am + bn = x \cdot \gcd(a, b) + y \cdot \gcd(a, b) = \gcd(a, b) \cdot (xm + yn),$
  
  so $d$ is a positive multiple of $\gcd(a, b) \implies d \geq \gcd(a, b)d$.
  
  Therefore $d = am + bn = \gcd(a, b)$. [Box]

- Constructive vs non-constructive proofs.
  
  Example. $\exists x, y \not\in \mathbb{Q}, x^y \in \mathbb{Q}$.
Proof (non-constructive):
Let \( x = (\sqrt{2})^{\sqrt{2}}, y = \sqrt{2} \).
If \( x \notin \mathbb{Q} \), then
\[
x^y = \left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} \cdot \sqrt{2}} = (\sqrt{2})^2 = 2 \in \mathbb{Q},
\]
which gives \( x, y \notin \mathbb{Q} \) for which \( x^y \in \mathbb{Q} \).
On the other hand, if \( x \in \mathbb{Q} \), then \( y^y = (\sqrt{2})^{\sqrt{2}} = x \in \mathbb{Q} \).
In either case, we have an irrational number to an irrational power producing a rational result. □

Second proof (constructive):
Let \( x = \sqrt{2}, y = \log_2 9 \).
\[
x^y = \left(\sqrt{2}\right)^{\log_2 9} = \left(\sqrt{2}\right)^{\log_2 3^2} = (\sqrt{2})^{2 \log_2 3} = \left(\left(\sqrt{2}\right)^2\right)^{\log_2 3} = 2^{\log_2 3} = 3.
\]
We know that \( \sqrt{2} \) is irrational, so it remains to show that \( \log_2 9 \) is irrational.
Embedded proof by contradiction.
Suppose \( \log_2 9 \) is rational. Then \( \log_2 9 = a/b \) for integers \( a, b \).
\[
2^{a/b} = 9
\]
\[
(2^{a/b})^b = 9^b
\]
\[
2^a = (3^2)^b = 3^{2b}
\]
But \( 2^a \) is even and \( 3^{2b} \) is odd — a contradiction.
We conclude that \( x^y \) is rational and that \( x, y \) are irrational. □

- To prove: \( A \subseteq B \) — direct, contrapositive.
- To prove: \( A = B \).
- Perfect numbers: \( n \) is perfect if \( n \) is the sum of its divisors, excluding itself. \( 6 = 1 + 2 + 3 \) implies \( 6 \) is perfect.
  28, 496, 8128 are perfect.
- If \( S = \sum_{k=0}^{n} r^k \) for \( r \neq 0 \), then \( S = (r^{n+1} - 1)/(r - 1) \).
- Let \( P \) be the set of perfect numbers. Let \( A = \{2^{n-1}(2^n - 1) : n \in \mathcal{N}, \text{ and } 2^n - 1 \text{ is prime}\} \).

Proposition: \( A \subseteq P \)
Proof: Suppose \( p \in A \). Then, \( p = 2^{n-1}(2^n - 1) \) for some \( n \in \mathcal{N} \) for which \( 2^n - 1 \) is prime.
Since \( 2^n - 1 \) is prime, any divisor of \( p \) is either \( 2^k \), for some \( 0 \leq k \leq n - 1 \)
- or -
\( 2^k(2^n - 1) \), for some \( 0 \leq k \leq n - 1 \).

Can arrange divisors of \( p \) as follows:

\[
\begin{array}{ll}
2^0 & 2^0(2^n - 1) \\
2^1 & 2^1(2^n - 1) \\
2^2 & 2^2(2^n - 1) \\
\vdots & \vdots \\
2^{n-2} & 2^{n-2}(2^n - 1) \\
2^{n-1} & 2^{n-1}(2^n - 1) = p \\
\end{array}
\]

We obtain \( S \), the sum of the divisors, excluding the last, \( 2^{n-1}(2^n - 1) = p \):

\[
S = \sum_{k=0}^{n-1} 2^k + \sum_{k=0}^{n-2} 2^k(2^n - 1) = \frac{2^n - 1}{2 - 1} + (2^n - 1) \sum_{k=0}^{n-2} 2^k \\
= (2^n - 1) + (2^n - 1) \cdot \frac{2^{n-1} - 1}{2 - 1} = (2^n - 1) + (2^n - 1)(2^{n-1} - 1) \\
= (2^n - 1)[1 + (2^{n-1} - 1)] = 2^{n-1}(2^n - 1) = p
\]

Therefore \( p \in P \). We conclude \( A \subseteq P \). □

Is \( A = P \)? not known. Do know that \( A \) contains all of the even perfect numbers.
So, are there any odd perfect numbers? .....

- To disprove \( P \), simply prove \( \sim P \).
  For example, to disprove \( \forall x, P(x) \), prove \( \exists x, \sim P(x) \). That is, provide a counter-example — a spoiler.

- If \( P \) is \( \forall x, Q(x) \Rightarrow R(x) \), a counter-example is an \( x \) such that \( Q(x) \land \sim R(x) \).

- Disprove: \( \forall n \in \mathbb{Z}, n^2 - n + 11 \) is prime.
  Note conjecture is true for \(-3 \leq n \leq 10\). But, consider \( n = 11 : (11)^2 - 11 + 11 = 11 \cdot 11 \), which is not prime.

- If \( P \) is \( \exists x, P(x) \), we disprove \( P \) by proving \( \forall x, \sim P(x) \).

- Disprove: \( \exists x \in \mathbb{R}, x^4 < x < x^2 \).
  Need to show \( \forall x \in \mathbb{R}, x^4 < x < x^2 \) is false.
  Proceed by contradiction. Suppose \( x^4 < x < x^2 \) is true for some \( x \in \mathbb{R} \).
  Then \( x \neq 0 \), and \( x > x^4 > 0 \). So, \( x \) is positive.
  Dividing by \( x \) gives \( x^3 < 1 < x \) which implies \( x^3 - 1 < 0 < x - 1 \). Continue via algebra:
  \[
  \begin{align*}
  x^3 - 1 &< 0 < x - 1 \\
  (x - 1)(x^2 + x + 1) &< 0 < x - 1 \\
  x^2 + x + 1 &< 0 < 1, \text{ a contradiction, since } x \text{ positive means } x^2 + x + 1 > 0. 
  \end{align*}
  \]
10. Mathematical Induction: Homeworks are p. 167: 3, 7, 11, 19, 24, 27

- For statements $\forall n \in S, P(n)$, where $S$ is an ordered set bounded from below (and therefore containing a smallest element, say $m$).
- Simple induction: (1) Basis step: Prove $P(m)$ by any of the methods discussed previously. (2) Prove $\forall n > m, P(n-1) \Rightarrow P(n)$, or $\forall n \geq m, P(n) \Rightarrow P(n+1)$.
- Prop: $\forall n \in \mathbb{N}, 1 + 3 + 5 + \ldots + (2n - 1) = n^2$.

Proof: (1) Basis. Let $n = 1$ and observe the sum continues through $(2n - 1) = 2(1) - 1 = 1$. So, the sum contains one summand, namely 1.

The sum is 1, and so is $n^2$.

(2) Induction. Suppose proposition for $n = k$: $1 + 3 + 5 + \ldots + (2k - 1) = k^2$.

For $k + 1$, sum is $1 + 3 + 5 + \ldots + (2k - 1) + [2(k + 1) - 1] = k^2 + 2(k + 1) + 1 = k^2 + 2k + 1 = (k + 1)^2$. ■

- If $n$ is a non-negative integer, then $5 | (n^5 - n)$.

Proof: Basis: if $n = 0$, then $n^5 - n = 0$ and therefore $5 | (n^5 - n)$.

Induction: Assume for $k \geq 0$, $5 | (k^5 - k)$. Need to show that $5 | ((k + 1)^5 - (k + 1))$.

$$(k + 1)^5 - (k + 1) = k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 = (k^5 - k) + 5(k^4 + 2k^3 + 2k^2 + k) = 5x + 5(k^4 + 2k^3 + 2k^2 + k),$$

for some integer $x$.

So, $5 | ((k + 1)^5 - (k + 1))$. ■

- Mathematical induction is deductive reasoning — as opposed to inductive reasoning.

- Suppose $a_1, a_2, \ldots, a_n$ are $n \geq 2$ integers, and suppose prime $p$ divides $\prod_{j=1}^n a_j$. Then $p | a_i$ for some $i \in \{1, 2, \ldots, n\}$. That is, if a prime divides a product, then the prime divides at least one of its factors.

Basis: $n = 2$, in which case $p | a_1a_2$.

Case (1): $p | a_1$, and we are finished.

Case (2): $p \nmid a_1$. In this case gcd($p, a_1$) = 1 (since $1, p$ are the only competitors, and $p$ doesn’t work).

Then $1 = \gcd(p, a_1) = xp + ya_1$ for some integers $x, y$. (Result from Chapter 7)

$$1 = xp + ya_1$$

$$a_2 = xpa_2 + ya_1a_2 = p \left( xa_2 + y \frac{a_1a_2}{p} \right)$$

As we are assuming that $p | a_1a_2$, we conclude that $p | a_2$.

Induction: Suppose $k \geq 2$ and $p | \prod_{j=1}^k a_j \Rightarrow p | a_j$ for some $1 \leq j \leq k$.

Then $\prod_{j=1}^{k+1} a_j = \left( \prod_{j=1}^k a_j \right) \cdot a_{k+1}$.

So $p | \prod_{j=1}^k a_j \Rightarrow p | \left( \prod_{j=1}^k a_j \right) \cdot a_{k+1}$, which implies $p | \prod_{j=1}^k a_j$ or $p | a_{k+1}$.

If $p | a_{k+1}$, we are finished.

Otherwise, $p | \prod_{j=1}^k a_j$, and the induction hypothesis forces $p | a_j$ for some $1 \leq j \leq k$. ■

- Strong (complete) induction: To prove $\forall n \in S, P(n)$, (1) prove $P(n)$ for $n = 1, 2, \ldots, k$, then (2) for $n \geq k$, prove $P(1) \wedge P(2) \wedge \ldots \wedge P(n) \Rightarrow P(n + 1)$.

Prop: $\forall n \in \mathbb{N}, 12 | (n^4 - n^2)$.

Try simple induction. Basis: If $n = 1$, then $n^4 - n^2 = 0$ and $12 | 0$.

Induction: assume for $k \geq 1$ and try to prove for $k + 1$.

For $n = (k + 1)$,

$$n^4 - n^2 = (k + 1)^4 - (k + 1)^2 = k^4 + 4k^3 + 6k^2 + 4k + 1 - k^2 - 2k - 1 = (k^4 - k^2) + 4k^3 + 6k^2 + 2k$$

$$= 12x + 4k^3 + 6k^2 + 2k \ldots$$

18
Can’t factor out a 12.
Try strong induction.
First prove cases $n = 1, 2, 3, 4, 5, 6$:

$$
\begin{align*}
  n = 1 & \implies n^4 - n^2 = 1^4 - 1 = 0, 12\mid 0 \\
  n = 2 & \implies n^4 - n^2 = 16 - 4 = 12, 12\mid 12 \\
  n = 3 & \implies n^4 - n^2 = 81 - 9 = 72 = 6 \cdot 12 \\
  n = 4 & \implies n^4 - n^2 = 256 - 16 = 240 = 20 \cdot 12 \\
  n = 5 & \implies n^4 - n^2 = 625 - 25 = 600 = 50 \cdot 12 \\
  n = 6 & \implies n^4 - n^2 = 1296 - 36 = 1260 = 105 \cdot 12
\end{align*}
$$

Now, for $k \geq 6$, show $12|n^4 - n^2$ for $n = 1, 2, \ldots, k$ implies $12|[(k + 1)^4 - (k + 1)^2]$

$$
(k + 1)^4 - (k + 1)^2 = [(k - 5) + 6]^4 - [(k - 5) + 6]^2 \\
= (k - 5)^4 + 4(k - 5)^3 \cdot 6 + 6(k - 5)^2 \cdot 6^2 + 4(k - 5) \cdot 6^3 + 6^4 \\
- (k - 5)^2 - 2(k - 5) \cdot 6 - 6^2 \\
= (k - 5)^4 - (k - 5)^2 + 24(k - 5)^3 + 216(k - 5)^2 + 852(k - 5) + (6^4 - 6^2) \\
= 12x + 12 \cdot 2(k - 5)^3 + 12 \cdot 18(k - 5)^2 + 12 \cdot 71(k - 5) + 12y,
$$

where $(k - 5)^4 - (k - 5)^2 = 12x$ and $(6^4 - 6^2) = 12y$ by the induction hypothesis. ♦

- **Definitions:** graph, cycle, tree (unique path between any two vertices $\Leftrightarrow$ no cycles)
- **Proposition:** For all $n \in \mathcal{N}$, if a tree has $n$ vertices, then it has $n - 1$ edges.

**Proof:** (Strong Induction) Let $V$ and $E$ be the sets of vertices and edges respectively.

**Basis:** if $n = 1$, then $|V| = 1$ and $|E| = 0 = n - 1$.

**Induction:** Suppose the proposition is true for $n = 1, 2, \ldots, k$.

Now consider a tree of size $k + 1$.

Choose any edge and remove it, producing two trees with vertex counts $V_1 = n_1$ and $V_2 = n_2$, respectively. Of course $n = n_1 + n_2$, since no vertices are lost.

Let $E_1$ and $E_2$ be the edge sets in these two trees. Since both $n_1, n_2 \leq n$, the induction hypothesis gives

$$
\begin{align*}
  |E_1| & = n_1 - 1 \\
  |E_2| & = n_2 - 1 \\
  |E| & = |E_1| + |E_2| + 1, \text{ where the 1 accounts for the removed edge} \\
  |E| & = (n_1 - 1) + (n_2 - 1) + 1 = n_1 + n_2 - 1 = n - 1 = |V| - 1. \,
\end{align*}
$$

- **Note essential use of strong induction in the above example.**
- **Proof be smallest counter-example is a mixture of induction and contradiction.**
- **Proposition:** If $n \in \mathcal{N}$, then $4|(5^n - 1)$.

**Proof:** (by smallest counter-example)

For $n = 1$, we have $5n - 1 = 5^1 - 1 = 4$, so $4|(5^n - 1)$.

For purposes of deriving a contradiction, suppose that $\forall n \in \mathcal{N}, 4|(5^n - 1)$ is false.

Then $\exists n \in \mathcal{N}, 4 \nmid (5^n - 1)$.

Consequently, since $\mathcal{N}$ is bounded from below, there exists a smallest $n$, say $n = k$ for which $4 \nmid (5^k - 1)$. $k \neq 1$, since we have proved $4|(5^1 - 1)$. 
So, \( k > 1, \) and \( k - 1 \in \mathcal{N} \) exhibits \( 4| (5^{k-1} - 1) \). Then, for some integer \( a \),

\[
5^{k-1} - 1 = 4a \\
5(5^{k-1} - 1) = 20a \\
5^k - 5 = 20a \\
5^k - 1 = 20a + 4 = 4(5a + 1).
\]

So \( 4|(5^k - 1), \) a contradiction.

- Fundamental theorem of arithmetic: Any integer \( n > 1 \) has a unique prime factorization. That is, if \( n = \prod_{i=1}^{j} p_i = \prod_{i=1}^{k} q_i \) are two prime factorizations of \( n \), then \( j = k \) and the primes \( p_1, \ldots, p_j \) and \( q_1, \ldots, q_k \) are the same primes, differing only in order of presentation.

Proof: First existence, then uniqueness.

Existence via strong induction on the set \( \{2, 3, 4, \ldots\} \).

Basis: For \( n = 2 \), we have a prime factorization, namely 2, of length 1.

Induction: For \( n > 2 \), we assume \( n \) has a prime factorization, and we then consider \( n + 1 \).

Case (a): \( n + 1 \) is prime \( \Rightarrow n \) is its own prime factorization.

Case (b) \( n + 1 \) is composite. That is, \( n + 1 = ab \), with \( 1 < a, b < n + 1 \).

By the induction hypothesis, \( a = p_1p_2\cdots p_j \) and \( b = q_1q_2\cdots q_k \) for primes \( p_i, q_i \).

Then \( n + 1 = ab = p_1p_2\cdots pjq_1q_2\cdots q_k \), a prime factorization. This completes the existence part of the proof.

Uniqueness by smallest counter-example.

For \( n = 2 \), the factorization is unique.

Now, for purposes of deriving a contradiction, let \( n > 2 \) be the smallest counter-example to admit two different prime factorizations:

\( n = \prod_{i=1}^{j} p_i = \prod_{i=1}^{k} q_i \)

Then, \( p_1|n \Rightarrow p_1|q_1q_2\cdots q_k \).

Earlier in this chapter, we show for prime \( r \), if \( r|a_1a_2\cdot a_i \) then \( r|a_i \), for one of the \( a_i \).

So, \( p_1|q_1q_2\cdots q_k \Rightarrow p_1|q_i \) for some \( 1 \leq i \leq k \Rightarrow p_1 = q_i \) (since both are primes).

Divide \( n = p_1p_2\cdots p_j = q_1q_2\cdots q_k \) by \( p_1 = q_i \) gives \( p_2p_3\cdots p_j = q_1q_2\cdots q_i-1q_{i+1}\cdots q_k \), two factorizations of \( n/p_1 \) of size \( j - 1 \) and \( k - 1 \)

Since \( n/p_1 < n \), the induction hypothesis states that the prime set \( p_2, p_3\cdots p_j \) and the prime set \( q_1, q_2, \ldots q_{i-1}q_{i+1}\cdots q_k \) are the same set.

Adding \( p_1 = q_i \) into the sets gives \( p_1p_2\cdots p_j \) and \( q_1q_2, \ldots, q_k \) are the same sets of primes. ■

- Fibonacci sequence: \( 1, 1, 2, 3, 5, 8, 13, 21, \ldots \)

\[
F_1 = 1 \\
F_2 = 1 \\
F_n = F_{n-2} + F_{n-1}, \text{ for } n > 2.
\]

- Proposition: \( F_{n+1}^2 - F_n F_{n+2} - F_n^2 = (-1)^n \).

Proof (Induction).

Base case: \( n = 1 \Rightarrow F_{n+1}^2 - F_n F_{n+2} - F_n^2 = F_2^2 - F_2 F_1 - F_1^2 = 1^2 - 1 \cdot 1 - 1^2 = -1 = (-1)^n \)

Induction: Let \( E_k = F_{k+1}^2 - F_k F_{k+1} - F_k^2 = (-1)^k. \) Then

\[
E_{k+1} = F_{k+2}^2 - F_{k+2} F_{k+1} - F_{k+1}^2 = (F_{k+1} + F_k)^2 - (F_{k+1} + F_k)F_{k+1} - F_{k+1}^2 \\
= F_{k+1}^2 + 2F_{k+1}F_k + F_k^2 - F_{k+1} F_{k+1} - F_k F_{k+1} - F_{k+1}^2 = -F_{k+1} + F_{k+1} F_k + F_k \\
= -[F_{k+1}^2 - F_{k+1} F_k - F_k^2] = (-1)^k = E_k = (-1)^{k+1}. ■
\]
• Have $F_{k+1}^2 - F_{k+1}F_k - F_k^2 = (-1)^k$. Divide by $F_k^2$,
\[
\left(\frac{F_{k+1}}{F_k}\right)^2 - \frac{F_{k+1}}{F_k} - 1 = \frac{(-1)^k}{F_k^2} \to 0, \text{ as } k \to \infty.
\]

So, $F_{k+1}/F_k$ nearly satisfies $x^2 - x - 1 = 0$ for large $k$. Solution is
\[
x = \frac{1 \pm \sqrt{1 + 4}}{2} = \frac{1 \pm \sqrt{5}}{2} = 1.618, -0.618.
\]

The negative root is clearly inappropriate, so $F_{k+1} \approx 1.618 \cdot F_k$ for large $k$. That is, almost a geometric sequence...