CSCI 3313 SPRING 22
LAB 1: MATH REVIEW [DISCRETE 1&2]

Jan. 12th. 2022

SETS AND SET OPERATIONS

- *Set*: intuitively, a collection of non-repeating *objects* $S = \{1, a, \{x, y\}\},\ |S| = 3$
  - $\mathbb{Z}$: set of integers $\mathbb{Z}^+$: set of positive integers $\mathbb{Z}^*$: set of non-negative integers
  - $\mathbb{N}$: set of natural numbers $\mathbb{R}$: set of real numbers $\mathbb{Q}$: set of rational numbers (quotients)
  - $\emptyset$ or $\{\}$: the empty set (not $\{\emptyset\}$, though it makes sense in some other circumstances)
  - U: the universal set, set containing all concerned elements.

- *Set Relations and Operators*
  - Membership Relation: $5 \in \mathbb{Z}$ $5.1 \notin \mathbb{Z}$ $\{1,2\} \in \{\{1\}, \{2\}, \{1,2\}\}$ (set of sets)
  - Subset Relation: $\{1,2\} \subseteq \mathbb{Z}$ $\{1,2\} \subset \{1,2,3\}$
  - Union: $A \cup B$ Intersection: $A \cap B$ Complement: $\bar{A}$
  - De Morgan's Law: $\overline{A \cup B} = \bar{A} \cap \bar{B}$ and $\overline{A \cap B} = \bar{A} \cup \bar{B}$
  - Set Difference, Symmetric Difference, Set XOR, etc.
  - Cartesian Product: if $A = \{1,2,3\}, B = \{x, y\}$, then $A \times B = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}$, set of ordered pairs

ALPHABET AND FORMAL LANGUAGES

One of the Main Topics of this course

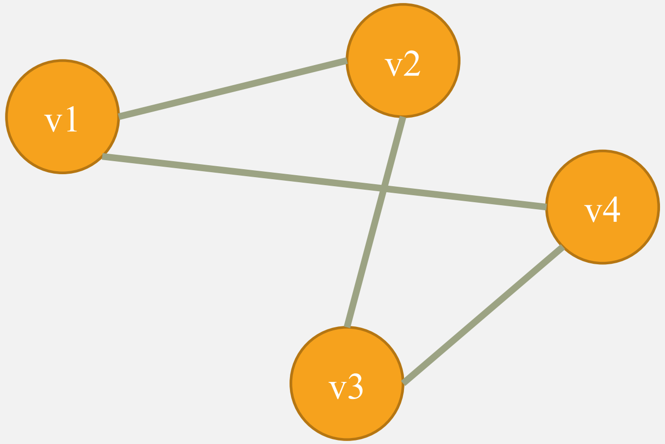
- *Alphabet*: a finite non-empty set of symbols (over which we form strings)
  - e.g., $\Sigma = \{0, 1\}$ the binary symbols (bits) and strings are binary numbers; or $\Sigma = \{a, b, \dots, z\}$ the English alphabet and words written in English alphabet.
- *Words/Strings over an Alphabet*: finite sequences consisted of members in the alphabet; e.g., $w = 1001$, or $s = helloworld$.
- $\Sigma*$ = { *set of all strings over the alphabet*}
- *Language*: set of strings following certain constraints; e.g., $L = \{a^n \mid n \text{ is a multiple of } 3.\}$, or $L = \{a^m b^n \mid m = n, m, n \in \mathbb{Z}^*\}$, or $L = \{\, ww \mid w \in \{0,1\}^* \,\}$.
  - Language L is a subset of $\Sigma*$
- *String Symbols and Operators*
  - Denoted ϵ (epsilon) or λ (lambda), the empty string; NOT to be confused with the EMPTY SET.
  - $|w|$, length of the string w, where $|\epsilon| = 0$.
  - w^R, reverse of the string; e.g., $w = abcd$, then $w^R = dcba$.
  - $s \circ w$, string concatenation; e.g., $s = hello$ and $w = there$, then $s \circ w = hellothere$.
  - Substring: if $w = foundations$ and $v = found$ then v is a substring of w.

REVIEW: OPERATIONS ON LANGUAGES

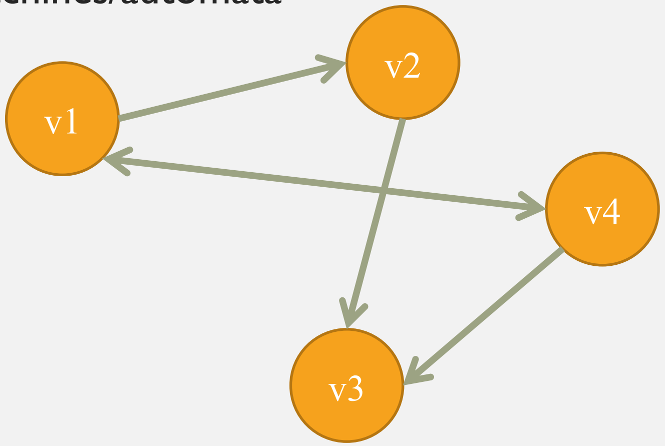
- Set operations (Union, Intersection, etc.)
- Concatenation, Reversal, Star closure
- Question 1: If $L_1 = \{ a^n b^n \mid n \geq 0 \}$ and $L_2 = \{ ab, aa \}$
  - Union: $L_1 \cup L_2 = ?$
  - Intersection: $L_1 \cap L_2 = ?$
  - Difference : $L_2 - L_1 = ?$
- Question 2:
  - Reverse: $L_2^R = ?$
  - Concatenation: $L_1 L_2 = ?$
  - **Star-Closure**: $L_2^* = L_2^0 \cup L_2^1 \cup L_2^2 \cup L_2^3 \cup \ldots$
    - Positive Closure: $L_2^+ = L_2^1 \cup L_2^2 \cup L_2^3 \cup \ldots$

GRAPHS AND TREES

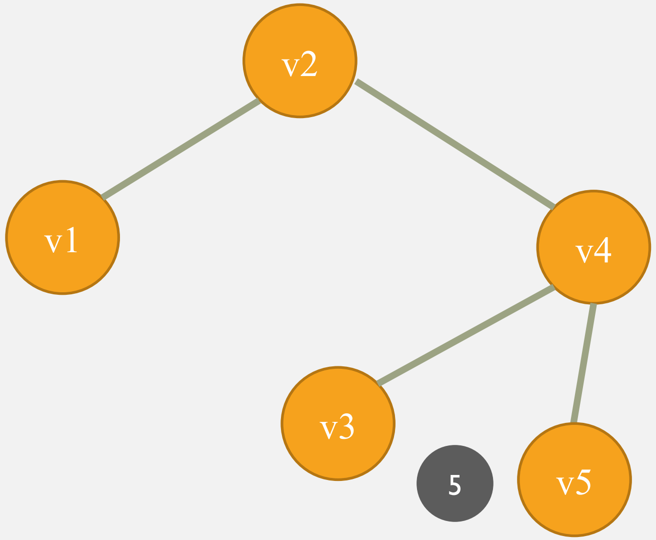
- *Graph*: A graph G is consisted of a Vertex Set $V(G)=\{v_1, v_2,..v_n\}$ and edge set $E(G) \subset \{(x,y) \mid x,y \in V(G)\} = V \times V$
  - Edge Set also defined as $E(G) = \{e_1, e_2, \ldots, e_m\}\, where\ e_i = (x,y), where\ x,y \in V(G)\}$, (as a matrix, or transition function)
  - Undirected:



Directed: of particular relevance in this course, **State Diagrams** to represent machines/automata



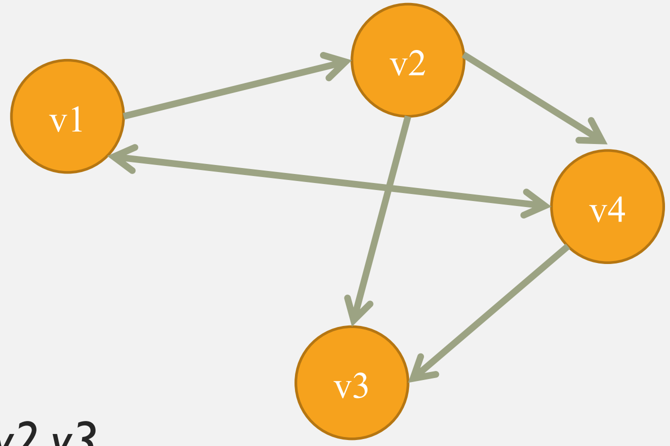
- *Tree*: **Definition T1**: A tree $T = (V, E)$ is a graph that is *acyclic* (has no cycles) and has one *distinct* vertex called the root such that there is exactly one path from root to every vertex.



GRAPHS AND TREES

- **Directed Graph**: A graph $G = (V, E)$ consists of a Vertex Set $V(G)$ and an Edge Set $E(G)$ (or simply V and E)
  - Direction is associated with each edge, for example: edge *(v1,v2)* from *v1* to *v2*
    - *Outgoing edge from v1, and incoming edge to v2*

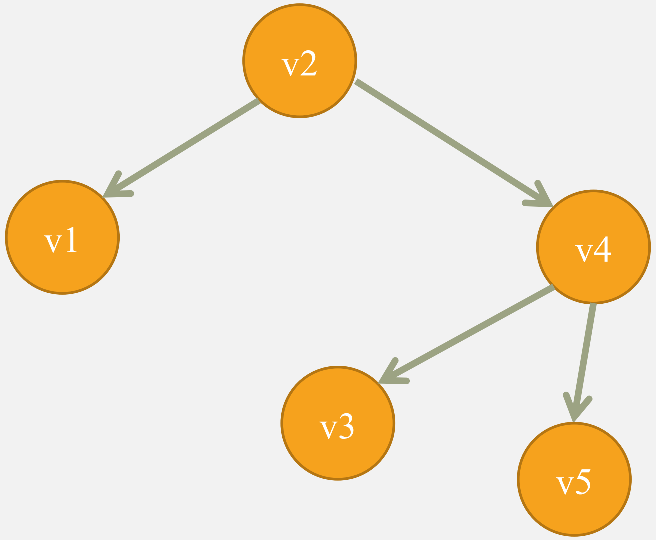
  - A **Path** is a sequence of edges from vi to vj and corresponds to sequence of vertices
  - Path is *simple* if no vertex is repeated (except possibly the last)
  - The **length** of a path is the number of edges in the path
  - A simple path from vertex to itself is called a **cycle**



- Examples:
  - Simple *acyclic path* from *v1* to *v3*: *{(v1,v2), (v2,v3) }* with vertex sequence *v1,v2,v3*
  - Cycle from *v1* to itself: *{(v1,v2), (v2,v4), (v4,v1) }* with vertex sequence *v1,v2,v4,v1*

TREES

- Trees (in our case we consider directed graphs that are trees) are a type of graph
- **Definition T1**: A tree (with directed edges) $T = (V, E)$ is a graph that is *acyclic* (has no cycles) and has one *distinct* vertex called the root such that there is exactly one path from root to every vertex.
  - **Root** has no incoming edges
  - **Leaves** are vertices with no outgoing edges
  - If there is an edge $(v_i\ \ v_j)$ then v_i is parent of v_j and v_j is child of v_i
  - The **level** of a vertex is the length of the path from the root to the vertex
  - The **height** of a tree is the largest level of any vertex in the tree

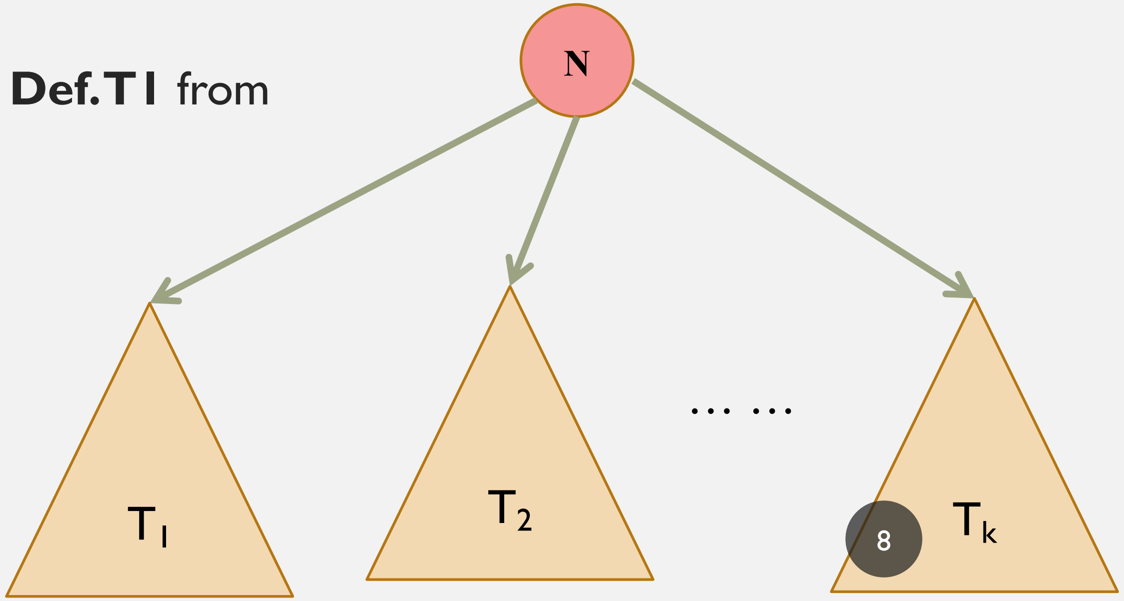


- Root node= v2
- How many Leaves = ?
- What is the height of this tree = ?

TREES- DEFINITION

- **Definition T2**: Trees can be formally defined using recursive (inductive) definition as:
- *Basis*: A single node is a tree, and that node is the root of a tree
- *Recursive step*: If $T_1, T_2, \ldots, T_k$ are trees (each less than n nodes) then we can form a new tree as follows:
  - 1. Begin with a new node N, which is the root of this new tree
  - 2. Add copies of the trees $T_1, T_2, \ldots T_k$
  - 3. Add edges from root node N to roots for each tree $T_1, T_2, \ldots T_K$

- Note: the two definitions T1, T2 are equivalent – i.e., we can prove **Def.T1** from the formal definition given in **Def.T2**.



PROOF METHODS

- What is a proof:
  - A sequence of logical steps, each following from previous steps
  - In logic terms: a propositional formula whose truth can be derived from a sequence of propositions (using the different rules of logical inference)
- Direct
- Induction
- Contradiction
- Contrapositive
- Counter example
- Constructive

PROOF METHOD: DIRECT

- Produce a chain of logically sound deductions that ultimately justifies the expected conclusion.

PROOF METHOD: INDUCTION

- *Outline*
  1. **Base Step**: Verify the base case(s), e.g., $f(1)$ satisfies the conditions for a proposition.
  2. **Induction Hypothesis**: Assume that $f(k)$ satisfies the conditions for some arbitrary intermediate step k.
  3. **Induction Step**: Prove that $f(k+1)$ also satisfies the conditions. *QED*

- *Example*: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{(n+1)n}{2}$ for some $n \in \mathbb{Z}^{+}$.
- *Proof*: Let $f(n)$ be the proposition that $\sum_{i=1}^{n} i = \frac{(n+1)n}{2}$.
  1. **Base Case**:
  2. **Induction Hypothesis**:
  3. **Induction Step**:

Comment: Why does induction work?
Repeated application of *modus ponens*:
P(0) true,
P(0) ⇒ P(1) true;
P(1) ⇒ P(2) true;
…
P(n) ⇒ P(n+1);
…
Therefore P(n).

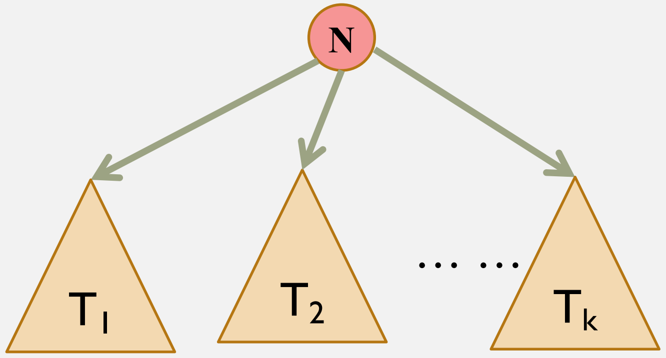
PROOF METHOD: INDUCTION

- *Example*: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{(n+1)n}{2}$ for some $n \in \mathbb{Z}^+$.
- *Proof*: Let $f(n)$ be the proposition that $\sum_{i=1}^{n} i = \frac{(n+1)n}{2}$.
  1. For $n = 1$, the summation on the LHS is 1, and the formula on the RHS gives $\frac{(1+1)\times 1}{2} = 1$. Thus, $f(1)$ is proven to be true.
  2. Assume $f(k)$ is true for some integer $k > 1$; i.e., $\sum_{i=1}^{k} i = \frac{(k+1)k}{2}$.
  3. Now for $f(k+1)$, we observe $\sum_{i=1}^{k+1} i = \frac{(k+1)k}{2} + (k+1) = \frac{k^2+3k+2}{2} = \frac{(k+2)(k+1)}{2}$ which is the RHS when $n = k + 1$. *QED*

- *Pro*: Straightforward (more mechanical).
- *Con*: Need to know (guess?) the answer first. Leads to a lot of computations.

- Usually used for proving *correctness*. Foundation in computer-based proofs – particularly in recursive algorithms.
- *In this course*: Induction proofs on lengths of some strings to show that they **belong to a certain language** and **can be recognized by its associated machine**/automaton.

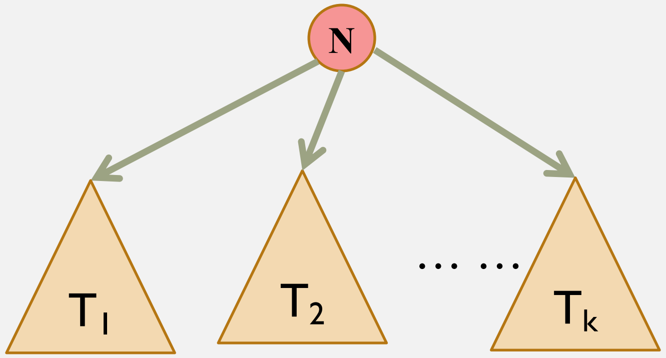
EXERCISE 1: PROOF BY INDUCTION



- Refer to the formal (recursive) definition of trees for this proof.

- **Exercise:** Theorem – Every tree $T = (V, E)$ has one more node than it has edges, i.e., $|V| = |E| + 1$

Instruction:
- Work in breakout groups; members' names.
- Take a screenshot and submit on BB <u>by end of today</u>.
- Everyone will need to submit a copy.


N
T1
T2
… …
Tk

(DIS)PROOF METHOD: CONTRADICTION

- **Proof by Contradiction**
  1. Assume to the contrary of a proposition.
  2. By reaching a contradiction, conclude the initial assumption was incorrect. *QED*

Reductio ad absurdum

- *Example*: For any integer n, if n^2 is odd, then n is odd.

$$\neg(p \Rightarrow q) \;\Leftrightarrow\; \neg(\neg p \vee q) \;\Leftrightarrow\; (p \wedge \neg q)$$

- *Proof:* Assume to the contrary that, given n^2 is odd **and** n is **not** odd.
  - Hence, there exists some integer k such that $n = 2k$.
    - Definition of an even number is n can be expressed as a multiple of 2; odd is 2k+1
  - Then we can derive $n^2 = (2k)(2k) = 2(2k^2)$. *Contradiction*.
  - Therefore, the assumption was incorrect, and the proposition itself is true. *QED*

- *In this course:* Prove by contradiction on **certain properties of a language** to show that the language **CANNOT be recognized (i.e., solved) by the assumed machine model** [via *Pumping Lemma*].

- **Proof by Counter-example**: Disprove using a counter-example.
- *Example*: For any integer n, if n^2 is odd, then n is even. Let $n^2 = 9$, then $n = \pm 3$ which is not even.

PROOF METHOD: CONTRAPOSITIVE

- **Proof by Contrapositive**
- *Rational*: A proposition $A \Rightarrow B$ (if A then B) is logically equivalent to $\neg B \Rightarrow \neg A$ (if not B then not A).

Modus Tollens

- *Example*: For any integer n, if n^2 is even, then n is even.
- *Proof*: To prove the stated proposition is to prove the proposition that "If n is not even, then n^2 is not even."
  - Hence, there exists some integer k such that $n = 2k + 1$ is not even, i.e., odd.
  - Then it is obvious that $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2k' + 1$ is odd, i.e., not even. *QED*

EXERCISE 2: PROOF BY CONTRADICTION

- **Definition C1**: An integer at least 2, is a prime number if it is not divisible by any integer other than itself and 1.
- Assumption (this is actually **Theorem C2 – Integer Factorization**): Every positive integer can be expressed as a unique product of prime numbers (including powers of primes). [Fundamental Theorem of Arithmetic]
  - 864 = 32 * 27 = (2*2*2*2*2) * (3*3*3) = $2^5 * 3^3$

- **Exercise:** Prove that there are an infinitely many prime numbers.

PROOF METHOD: CONSTRUCTION

- *Rational*: Construct mathematical object(s) based on the constraints and prove/disprove the argument.

- *Example*: Is there a set R containing all other sets (without any other constraints, or *unrestricted comprehension*)?
- *Proof* [*Russell's Paradox*]:
  - *Construction*: Let R be the set of sets that are not members of themselves, i.e., $R = \{x \mid x \notin x\}$.
  - Such construction is equivalent to saying $R \in R \Leftrightarrow R \notin R$.
  - In other words: in the forward direction, if R is a member of R, then by the definition of the construction, R is not a member of R in the first place; contradiction. Or conversely, if R is not a member of R, i.e., not a member of itself, then R must have been included in R by the construction; contradiction.
  - Therefore, there's no such R exists.

- *In this course*: a <u>similar</u> constructive proof is applied to prove the **Halting Problem is not Turing-Decidable**.
- Different from the universal set U, which usually has some restrictions, e.g., $U = \Sigma^* = \{0,1\}^*$ or $U = a^*b^*$.

ADDITIONAL EXAMPLES

PROOF METHOD: INDUCTION

- **Exercise 3:** Prove that $1^2 + 2^2 + \cdots + n^2 = \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ for some $n \in \mathbb{Z}^+$.
- *Proof*: Let $f(n)$ be the proposition that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

1. **Base Case**: For $n = 1$, the summation on the LHS is 1, and the formula on the RHS gives $\frac{1\times(1+1)(2+1)}{6} = 1$. Thus, $f(1)$ is true.
2. **Induction Hypothesis**: Assume $f(k)$ is true for some integer $k > 1$; i.e., $\sum_{i=1}^{k} i = \frac{k(k+1)(2k+1)}{6}$.
3. **Induction Step**: Now for $f(k+1)$, we observe … …

QED

MODULAR ARITHMETIC

- *Modular Arithmetic*
  - A positive integer n equals to b modulo a, for positive integers a, b is equivalent to saying $n = ka + b$ for some positive integer k; i.e., b is the remainder of n divided by a.
  - A positive integer n is congruent to another positive integer m modulo a, or $n \equiv m \ (mod\ a)$, if they have the same remainder when divided by a; an alternative but equivalent way to say is that $m - n$ divides a (assuming $\mathrm{m} \geq n$ with out loss of generality).

  - $13 \equiv 3\ (mod\ 5) \Leftrightarrow 2{\times}5 + 3 = 13$; equivalently, $(13 - 3) = 10$ divides 5.
  - $x \equiv 3\ (mod\ 5)$, then $x \in \{3, 8, 13{,}18, \dots\}$ if we focus on the positive side of the number line.

  - *Parity*: An integer n is even <u>if and only if</u> ($\Leftrightarrow$) $n \equiv 0\ (mod\ 2)$; and n is odd *iff* $n \equiv 1 (mod\ 2)$.
    - From above it follows that an even integer can be written as *n*= *2k* and an odd integer is *(2k+1) for some integer k*

(DIS)PROOF METHOD: CONTRADICTION

- **Exercise 4**: Prove $\sqrt{2}$ is irrational. *What we do:* Assume to the contrary that $\sqrt{2}$ is rational; then it can be written in the form of a/b for two integers that has no common divisors.
  - Definition: a rational number a/b where a,b have no common divisors
- *Proof:* Assume to the contrary that $\sqrt{2}$ is a rational number, i.e., $\sqrt{2}$ = p/q

- **Exercise 5**: For any integer n, if $n \equiv 2\ (mod\ 4)$, then $n \not\equiv 3\ (mod\ 6)$.
- *Proof:* Assume to the contrary that, given $n \equiv 2\ (mod\ 4)$, it is also true that $n \equiv 3\ (mod\ 6)$.